Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

Architecture Of Security And Data Protection In Smart Cities

Dr. Md. Amir Khusru Akhtar[1] , Mr. Amit Kumar Upadhyay[2]

[1]Associate Professor & HOD Computing And Information Technology Usha Martin University, Ranchi, Jharkhand

[2]Assistant Professor, Computer Science, Mangalayatan University, Beswan, Uttar Pradesh

ABSTRACT

Governments throughout the globe are progressively making large investments in the creation of smart cities. Over time, rather than via a single choice, cities have progressed from digital to green to linked to sustainable to eco-friendly to eco-friendly and so on. In today's technological revolution, we're seeing the rise of GPU-based multi-core computers, 5G connection, cloud computing, and artificial intelligence. Several of these new technologies have contributed to the development of smart cities. There are many new technologies that have emerged in the present period such as 5G wireless connection and quick GPU multi-core-based servers, big data, cloud computing, artificial intelligence, and data analytics. There are a number of new technologies that have aided in the creation of smart cities and their implementation. In this article, we lay out a framework for smart city security and explain exactly what we meant by it.

KEYWORDS: Security, Data Protection, Smart Cities, Architecture

INTRODUCTION

66 percent of the world's population is expected to live in cities by 2050, with more than 54 percent presently residing in cities. Cities' long-term survival is being jeopardised by a broad variety of technological, social, economic, and organisational difficulties brought on by the fast growth of the population and increasing urbanisation. As a result, most governments are looking to implement "smart" principles to maximise the use and exploitation of both physical and intangible assets.

The term "smart city" refers to the intelligent and coordinated use of all available technology and resources to create connected, livable, and sustainable metropolitan

areas. Digital technologies can be used to optimise the generation, monitoring and consumption of various types and sources of energy and resources, as well as smart buildings, which can independently control and manage lighting and temperature systems, security, as well as energy consumption. Smart mobility, on the other hand, enables intelligent mobility by utilising in-vehicle technology.

LITERATURE REVIEW

SAID DAOUDAGH (2021) There has been an increase in the creation of smart city services that exchange a large amount of (personal) data as a result of the proliferation of mobile devices. If they are not properly managed, they might pose a severe security and privacy risk. Developing an architecture for smart cities that is able to include a distributed identity management system that ensures privacy while employing attribute-based credentials is our primary aim in this effort (p-ABC).

DIPAK S. GADE (2021) Comprehensive research into the topic's literature as well as consultations with field scientists, subject matter experts, and industry professionals are all part of the data collection process. The most recent breakthroughs in Smart City technology have been documented in a thorough study. Smart City services are employing a wide range of cutting-edge tools and technology to tackle their real-world problems, according to a review of the available literature and interviews with relevant stakeholders and an analysis of their own datasets.

MEHDI SOOKHAK (2021) Modern breakthroughs in information and communication technology have spawned a new paradigm for cities to better serve their residents by dynamically optimizing the use of available resources. Smart cities employ a variety of components, including ubiquitous sensors, heterogeneous networks, huge databases, and powerful data centres, to acquire, transport, store, and intelligently interpret real-time information. Better decision-making, reduced energy consumption, enhanced transportation, improved healthcare, and greater education are just a few of the benefits that smart cities may provide to their residents.

CHALEE VORAKULPIPAT (2021) Integration of ICT and innovation to manage complicated data storage and transmission in a smart city is a distinct feature of this type of urban environment. Most of the technology used in smart cities is cutting-edge and may not be available elsewhere. Aside from that, today's smart cities are being utilized as test beds or showcases for new technology, the security and privacy of which are as of yet undetermined. Because of this, critical information based on certain technologies is vulnerable to a variety of attacks. A smart city's security and privacy are intertwined.

CHENMA (2021) Cities all over the world are adopting new technology and transforming into "smart cities.". Citizens' quality of life is enhanced by new technologies. The employment of any technology, however, presents additional concerns and challenges. With smart cities, the actions of one person or group can put the entire community at risk. Cyber-security issues (such as information leakage and

harmful cyber-attacks) affect the behavior of smart cities because of their reliance on information and communication technologies.

UNDERSTANDING SMART CITIES

Human vs. City Analogy

There are certain similarities between people and cities. Living and working in cities is what makes them what they are. The vitality of a city is directly linked to its businesses and residents. The brain, senses, and physical body combine to form the human being. Reasoning and decision-making take place in the brain, which is also where information is processed and stored. Gathering information from the world around us is made possible by our senses (eye, ear, nose, skin). Last but not least, the human body does all the various tasks required to keep us alive. Similarly, a smart city might be seen as having a similar structure to a human being.

System Architecture

There are four basic components to building a smart city from an ICT perspective: sensors (edges), platforms (data and AI), and apps,

$$\text{SMART CITY} = [\text{sensors}] + [\text{edge}] + [\text{platform}] + [\text{applications}]$$

The Internet of Things (IoT) is projected to play a significant role in a city's entire smart city platform (the Internet of Things). "Inputs" to the smart city system will include devices such as cameras, temperature sensors, microphones, and water meters. Sensors connect with the physical world through a variety of wired or wireless (such as Bluetooth, NB-IoT, etc.) networks in order to gather data. As a general term, gateways are known as collecting points. It is typical for sensors to convey data over wireless networks using the MQTT or CoAP messaging protocols. The messages are often tiny in size and light in weight so that the sensors can communicate this data more efficiently. The REST API is the standard means via which cloud-based smart city apps can communicate with the gateway.

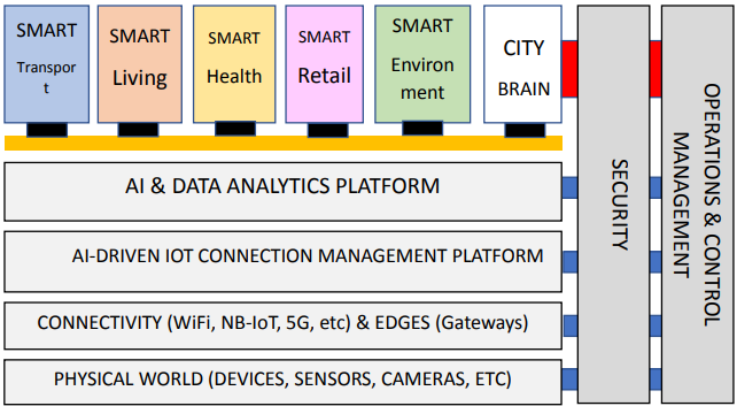

Figure 1: "A proposed Smart City System Architecture, where security and city Management cut across all layers."

Figure 1 depicts the system architecture of a smart city, which includes four horizontal and two vertical levels, as well as the applications that reside on top of each. Data-AI, IoT management, and connection are the other three tiers of the IoT stack, which are all horizontal in nature. Sensors and other devices (cameras, sensors) are the first layer of a smart city system that provides inputs The connectivity layer connects sensors to collecting locations (gateways). Connectivity management for the Internet of Things (IoT) resides at the edge of the network, where it collects sensor data provided across various channels and protocols. Last but not least, the data-AI layer helps smart city applications by processing and analysing data.

Data and insights will be used in various ways by different smart city apps at the upper layer, and events will be triggered appropriately. Analyzing and predicting the correct output can be done using artificial intelligence technologies. A data and processing layer is included in every smart city application. Because of the several administrations involved and the inherent bottleneck that occurs when anything goes wrong, it is almost hard to create a single data and AI platform layer that can be utilised for all of the potential smart city applications.

Architecture's vertical levels cover security, operations, and control management. These apps are considered silos since they have no need to communicate with other smart city applications that have been designed for commercial or residential properties such as a private home estate. The development and implementation of public smart city applications will demand the utilisation of government resources:

a. Management of operations and quality assurance

b. Connectivity and interoperability of software applications

c. a full range of safety measures

It is possible for the government to centrally control the many smart city subsystems, such as transportation, the environment, public security, and so on, through the IOC (intelligent operations centre). Various government smart city applications will be able to connect and interact with each other thanks to this architecture. In the case of a crime happening at a road junction, for example, the police will need to deploy smart transportation, smart intersection, and smart light post apps. This gadget should be able to control adjacent or on-site cameras as well. These applications need to be able to communicate and exchange data with one another in order for the government-hosted smart city applications to be successful.

End-to-end security must be embedded into all tiers of the smart city platform to maintain integrity, prevent intrusions, and malicious assaults on the smart city system. Because of this, all horizontal layers of security must be protected. Devices must be

safeguarded in order to avoid tampering. Sensor data must be encrypted before it can be delivered via a secure cable or wireless channel. Both locally and remotely, accessing devices should be restricted to those who have been granted permission to do so. Data should be stored securely using distributed storage. Data should only be accessible to legitimate apps and individuals. Each smart city application's data may be seen as an independent entity in a private or public cloud. You may choose to make them public or private, depending on your choices. Data management regulations are in existence in a number of countries, and authorities have control over the data and its abuse depending on where the data are held. We'll explore smart city security in further depth in the next section.

"SECURITY FOR SMART CITIES"

How to view the security problem?

Smart city security is just one facet of a much wider problem. Development of specialised smart city applications, such as intelligent transportation and health and environment and intelligent living, are known as "silos" in the industry. A more relevant question is: What factors underlie the regulation and availability of these smart city applications, as well as their efficient use?

What is there to secure?

In order to create smart city security solutions, it is necessary to consider the following factors: (a) what needs to be protected; (b) the attackers' intended outcomes; and (c) the sorts of attacks. We must examine the assets of a smart city if we are to know what needs to be safeguarded. This includes its people, its resources, and the services it provides. The term "resources" is what I'm referring to:

(a) Money, commodities (such as gold), and other financial assets (stocks, etc),

(b) Communications, the Internet, data centers, workplaces, residences, and other types of infrastructure are all examples of

(c) All of the things we need to live a normal life: water and electricity, food and medicine, etc.

Securing Water Supply

Water is a life-sustaining necessity for humans, thus protecting it is a top issue. For both human use and business purposes, a city's existence is dependent on the availability of water (in restaurants, etc). Attacks on water supply locations and water transportation have the potential to impair water supplies. By shutting off power pumps and cutting water lines, the attackers themselves may carry out such assaults. In many cases, on-site assaults are deterred by the presence of security guards and monitoring cameras.

Securing Energy

The bulk of smart city apps are now powered by electricity. If there is no electricity, many smart city services and companies will be rendered inoperable. A reliable energy supply and distribution system is thus essential for smart cities. The process of generating energy may be stopped if the site is damaged physically or if the electricity-generating process is stopped. In the case of a power outage, a backup power source must be in place to guarantee that the site's power production is not disturbed. However, when it comes to power delivery, transmission lines, transformers, and switches, as well as power plants, are all included. By disrupting the power supply, an attack on one of these components can disable all of the smart city apps. Terrorists are reportedly eyeing power plants as prospective targets for attacks, hoping to cause widespread blackouts and spark riots across the country. A thorough plan and structure are required to ensure the safety of the city's electrical supply.

Securing Connectivity

In order to link sensors, cameras, data centers, and other components of smart city infrastructure, we need connection. As a result, in addition to electricity, communication is a vital lifeline for smart cities. Both wired and wireless network infrastructures are capable of enabling connectivity. The Internet of Things (IoT) can be said to be secure with this method (IoT). Hardware, data, and communications linkages all need to be protected in the IoT world. There is a lot of overlap between hardware security (tamper-proof), access and authentication controls. A combination of encryption and lightweight, secure end-to-end transport protocols safeguards data and connections. Fixed broadband and cell phone networks employ existing telecom networks that have been hijacked a few times. Smart cities, on the other hand, are expected to have higher levels of security than conventional ones, which necessitates raising the bar for security in smart cities.

Wi-Fi Security:

Wireless networks must be secured in order to do so. Access to the link must be restricted via a secure media access control (MAC) protocol. As a result of the Wi-Fi Alliance's development of WPA (Wi-Fi Protected Access), the initial Wi-Fi security standard, more advanced data encryption and user authentication capabilities were added to Wi-Fi.

Bluetooth Security:

Security modes 1, 2, 3, and 4 are available for Bluetooth-enabled devices. It is up to the device maker to decide which option to include. Most Bluetooth users may establish "trusted devices" that can transfer data without the user's awareness. Bluetooth users. Whether or whether other devices may connect to a user's gadgets is entirely up to the individual user. Both service-level and device-level security must work together to make Bluetooth devices secure. In order to ensure the privacy of personal information,

authorization and identification processes limit Bluetooth service usage to registered users and require users to make informed choices when opening files or allowing data transfers. These security measures must be activated on the user's phone or other devices in order to prevent unauthorised access. Setting the Bluetooth settings to "non-discoverable" will prevent any Bluetooth devices from being discovered.

LORAWAN Security:

Lora WAN's security architecture is based on standard algorithms and end-to-end security. Lora WAN security features include mutual authentication, integrity protection, and secrecy. As part of the network join process, a Lora WAN end device and the Lora WAN network establish mutual authentication. As a result, only authentic and authorized devices will be able to access authentic and legitimate networks. Origin authentication, integrity protection, and replay protection are all included in Lora WAN MAC and application messaging encryption. As a result of this protection and mutual authentication, eavesdroppers will not be able to decipher network communication, and it will not be possible for rogue actors to replay it. Aside from the end-to-end encryption of application payloads, Lora WAN security adds additional security measures. Integrity and encryption are both protected by CMAC2 and CTR3, respectively, using the AES cryptographic primitive. App Key and EUI-64-based Dev EUI are unique to each Lora WAN device, which are used to authenticate it during the device authentication procedure.

SIG Fox Security:

SIG Fox is a fantastic pick in terms of price and power. Radio communication between base stations and the SIG Fox Cloud is protected via virtual private networks and signature-based authentications (VPN). Users access the SIG Fox Cloud over encrypted HTTPS connections. SIG Fox devices cannot be accessed over the Internet unless they pass via the SIG Fox core network, and data is protected both while in transit and while being stored on SIG Fox devices. Message authentication and replay attack avoidance are key components of data-in-motion security. In order to verify the sender's identity, a message token and an authentication key are utilised. For hardware security, SIG Fox base stations and the core network rely on TPM (Trusted Platform Module, also known as ISO/IEC 11889).

CONCLUSION

Smart cities are popping up all over the globe, but implementing them has proven difficult for both corporations and governments. An all-encompassing security structure and protocols must be in place for a smart city in order to protect its citizens. Water, electricity, data, connection, the city's brain, and crucial municipal services are just a few of the things that make up a city. This article emphasises the need of security for a smart city and presents a list of probable assaults, as well as highlighting areas to protect and safeguard (police, fire, banking, healthcare, and transit) (police, fire, banks,

healthcare, and transport). New and urgent smart city security issues need a systemic strategy that encompasses devices, applications, service providers, and customers.

REFERENCE

1. Said Daoudagh (2021),"Data Protection by Design in the Context of Smart Cities: A Consent and Access Control Proposal," 2021, 21, 7154. https://doi.org/10.3390/s21217154

2. dipak s. gade (2021)," Disruptive Technologies for Efficient and Sustainable Smart Cities," International Journal of Management, Technology, and Social Sciences (IJMTS), ISSN: 2581-6012, Vol. 6, No. 2, August 2021

3. Mehdi Sookhak (2021)," Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges," IEEE communications surveys & tutorials, vol. 21, no. 2, second quarter 2019

4. Chalee Vorakulpipat (2021)," Security and Privacy in Smart Cities," Volume 2021 |Article ID 9830547

5. H. Chourabi, T. Nam, S. Walker, J. R. Gil-Garcia, S. Mellouli, K. Nahon, T. a. Pardo, and H. J. Scholl, ―Understanding Smart Cities: An Integrative Framework,‖ 2012 45th Hawaii Int. Conf. Syst. Sci., pp. 2289–2297, Jan. 2012.

6. Alawadhi, Suha, et al. "Building understanding of smart city initiatives." Electronic Government. Springer Berlin Heidelberg, 2012. 40-53.

7. Bakıcı, Tuba, Esteve Almirall, and Jonathan Wareham. "A smart city initiative: the case of Barcelona." Journal of the Knowledge Economy 4.2 (2013): 135-148.

8. Sanchez, Luis, et al. "Smart Santander: IoT experimentation over a smart city testbed." Computer Networks 61 (2014): 217-238.

9. Kitchin, Rob. "The real-time city? Big data and smart urbanism." GeoJournal79.1 (2014): 1-14.

10. Shelton, Taylor, Matthew Zook, and Alan Wiig. "The ‗actually existing smart city'." Cambridge Journal of Regions, Economy and Society 8.1 (2015): 13-25.