SECURITY AND PRIVACY CHALLENGES IN SMART CITIES

CSC 4980 & 6980: Topics in Computer Science - Security in IOT

Kausthub Kodamagulla, Kamidi Shruthi Reddy, Nagasai Anjani Kumar Thadishetty

kkodamagulla1@student.gsu.edu, skamidi1@student.gsu.edu, nthadishetty1@student.gsu.edu

Date: December 5th, 2022

Abstract: The evolution of smart cities is taking place on a global scale. These are brought about by developments in information technology, which while they open up new economic and social possibilities also put our security and privacy expectations in jeopardy. With the help of technology like smartphones, people are already connected. Smart city administrators, designers, integrators, and organizations face major political, technical, and socioeconomic hurdles as a result of the interconnected and complex nature of these new entities. New applications and services for enhancing inhabitants' daily lives in the areas of decision-making, energy use, transportation, healthcare, and education are possible in smart cities. Although smart cities may denote great advancement in technological evolution , security and privacy concerns need to be carefully considered. This paper aims to make a survey of various security issues in smart cities, and it also provides a thematic taxonomy of security and privacy concerns in smart cities in order to emphasize the security requirements for developing a secure smart city.

Contents:

INTRODUCTION

From the past 15 years, term “Smart City” has caught everyone’s curiosity that led to digital transformation in urban sector, health management system, administration, construction, security sector thereby, resulting in a sustainable-secure living environment through embedding information and communication technologies such as Internet of Things (IOT), Cloud Computing, Big Data Processing, Machine Learning, AR/VR, Geographic Information Systems, etc. An increased rate in urbanization across the globe led to investing and setting up large number of smart city infrastructures integrated with various devices that aids the people in smart transportation, smart governance, smart health systems, etc. A recent report by United Nations Population Fund quoting that, the number of rural people worldwide is declining but the world can expect up-to 1.5 billion urbanized areas by 2035 and can exceed 3 billion by 2050 resulting huge urban land consumption, excess burden on health care systems, energy, living conditions. Majority of nations aim to address the effects of urbanization by developing information-cutting edge technological tool-based infrastructure i.e., smart city that optimizes urban-spatial organization, resources, increases efficiency and safety. Building a smart city involves four sections; perception layer, communication layer, support layer, application layer. Perception layer involves sensor technology for a physical object, radio frequency identification (RFID) technology, other data collection and monitoring technologies. Communication layer summarizes the information collected from smart home, intelligent systems, internet, etc. Support layer integrates the summarized information from different sources and sets a base for a specified application in smart city. Application layer provides direct applications to citizens of smart city based on summarized data and determines the measures for an optimized performance. In the four-tier system of smart city, perception or sensor layer is consider most prominent because all the physical objects with multiple sensors are embedded with advance automation technologies such as machine learning, computer vision, artificial intelligence that provides feedback to the users.

In a smart city, all IOT enabled physical devices connected over a network communicate with each other, exchange information upon pre-specified protocols and result in sharp monitoring, tracking, identification, etc. Thereby, making the people’s life productive and hassle-free. As there is an increase in building large number of smart city architectures, there also exists many privacy and security issues due to vulnerabilities existing in architecture of smart city. These include cyber-attacks, un-authorized access to personal devices, intended data leakages, sybil attacks, denial of service (DoS). There are no such security measures that can detect system loopholes, data leakages in an IOT system and wireless sensor networks (WSN) aren't capable of finding all kinds of attacks. A neural network based online network intrusion detection system (NIDS) named "Kitsune" is proposed by various research scholars that detects normal and network attacks in a local network. The drawback of implementing this neural network based architecture is that, physical IOT devices aren't capable of storing vast amount of data and training them on neural network. It is proved that, a novel wireless technology "Long Range (Lo Ra) Communication through wireless communication protocols" based IOT system tends to provide more security in a smart city [referred paper number]. Many privacy safe-guarding methods such as data encryption, bio-metric verification, anonymous authentication have been introduced in IOT environment. Unfortunately, these doesn't furnish satisfactory results. The foremost reason is, multiple sensors embedded in an IOT device are of low computational power. Thereby, only simple encryption and verification techniques can be implemented which paves a way for attackers to easily bypass the existing safe-guard mechanisms. To tackle privacy issues such as encryption threats in an IOT system, many researchers preferred deep learning-based intrusion detection systems. In an IOT system, huge amount of data is collected from multiple IOT devices and gets stored in a centralized servers which may face vulnerabilities such as sensitive data breach, multiple authentications or management. In order to reduce the overall data management cost, enabling a secure data communication and exchange across the devices, providing security against attacks such as stealing personal data, un-authorized access over the system; an integration of IOT system with block chain technology is implemented.

The contribution of this study is summarized as follows:

- We present the knowledge on the IOT based architecture, components, characteristics of a smart city and need of smart city that enhances the well-being of citizens while ensuring a balanced economic growth.
- Various security requirements of smart environment are discussed.
- We discuss and asses various protection mechanisms involving technologies such as cryptography, block chain technology, machine learning, data mining, deep learning.

IOT BASED ARCHTECTURE OF SMART CITY

The architecture can be divided into 4 components, which is depicted in Fig.1.

1. **Perception Layer:** This low-level layer in IOT-Based architecture is also termed as sensing layer or recognition layer. The perception layer is mainly focus on data collection from real-world IOT devices such as heterogenous devices, actuators, sensors such as RFID, 2D-Barcodes and transmitting the data to the network layer for further analysis. Collected data may be about environmental conditions, location, etc.
2. **Network Layer:** This is also called transmission layer, the core layer in the IoT architecture that depends on basic networks such as the Internet, Wireless Sensor Networks and communications networks. The responsibility of this layer is to transmit the data collected by the perception layer and to connect smart things, network devices and servers.
3. **Support Layer:** This layer works very close with the application layer and helps in data processing before it gets stored in a data centre or cloud. Support layer provides assistance for the requirements of applications through computing techniques such as cloud computing, Deep Learning, Machine Learning.
4. **Application Layer:** This layer is responsible for providing industry/user specific applications based on depth analysis of processed data. This layer defines all the applications deployed in an IOT device. It acts as an interface between IOT devices, network and IOT applications such as smart cities, smart homes, etc. It provides multiple services to the applications based on data collected in perception layer.

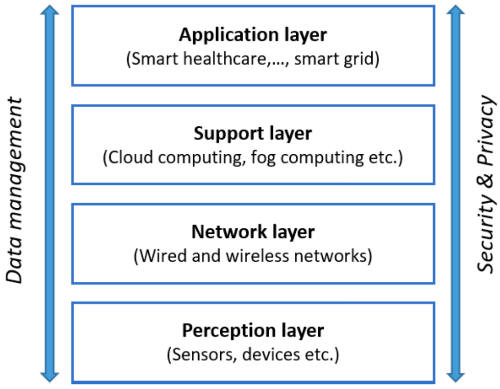

Fig.1. IOT Architecture of Smart City

A smart city is demonstrated by several building blocks as depicted in Fig.2.

1. **Smart Governance:** The moto of smart governance system is to serve citizens through data interconnectivity, institutions, proceedings. Apart from this, smart governance enables citizens to get involved in public decisions and city planning that can improve the efficiency and simultaneously maintaining data transparency among the public. For example, e-governance system for SSN allows individuals to schedule their appointment online rather than waiting in a queue for their turn to come-up.
2. **Smart energy:** This includes Energy Generation Systems, Energy Distribution and Storage Systems, and Smart Energy Management Systems. This system controls and manage the energy consumption of every community or house-hold.
3. **Smart Transportation:** This involves intelligent transport systems that serve the public by enhancing safety, speed and reliability. This system helps the citizens to plan their travel in an economic and faster way.
4. **Smart Healthcare:** This helps in better prediction of patient's health based on their electronic records, remote monitoring of patient's vitals and provide insights for effective treatment.
5. **Smart Security:** This involves emergency handling, alarms, cyber security analysis, personal safety of citizens, etc.
6. **Smart Utilities:** This system helps to reduce overconsumption of resources such as water, gas, electricity that aids to economic growth and contribute to environmental protection. Smart meters are widely applied in smart grids to monitor the distributed energy resources, smart water meters and smart light sensors are used to manage the resources and mitigate the energy loss.

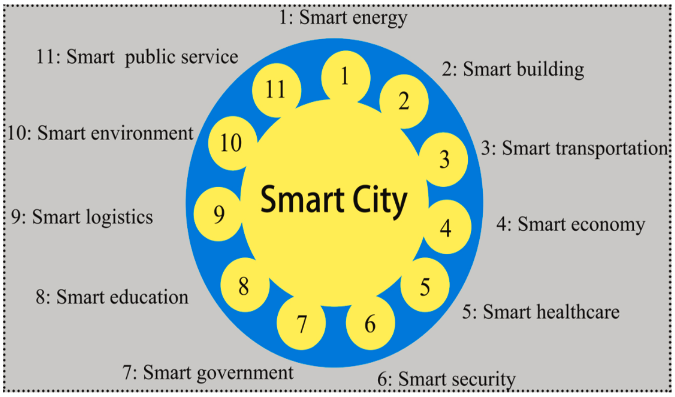

Fig.2. Building blocks of Smart City

CHARACTERISTICS OF SMART CITY

1. **Heterogeneity:** All the devices in an IOT system are heterogenous i.e., independent to each other, distributed, used by multiple users. Additionally, it covers a wide range of IoT nodes, communication protocols, technologies, mobility, platforms, and a variety of hardware functions.
2. **Resource Constraint:** Most of IOT enabled devices are constrain to storage, processing speed, memory, network interfaces. Energy efficient but low-cost and processing power devices are embedded in smart cities.
3. **Mobility:** This refers to various technologies like wireless communication, continuous real- time monitoring of the traffic, emergency alarm system, various sensor enabled devices are spread across the city.
4. **Connectivity and Scalability:** Connectivity allows all the devices in a smart city to be interconnected over a network and communicate. Scalability is another important aspect for smart cities. Since, there an increase in smart city communities, a smart city can't operate without scalable mechanisms.
5. **User Involvement:** The main purpose of setting up smart cities is to improve citizens life through edge-cutting technologies. Full involvement of residents in using theses cutting edge technologies tend to improve their quality and gain more insights in terms of protection mechanisms.

SECURITY REQUIREMENTS OF SMART CITY

The remainder of this part mostly focuses on identifying the requirements linked to safeguarding smart cities in light of the features of IoT devices, the complex environment of smart cities, and the security and privacy risks stated earlier.

1. **Authentication and Confidentiality:** The fundamental prerequisite for each layer of a smart system is authentication, which is required to establish identities and guarantee that only authorized users can access services throughout a heterogeneous system. Particularly, IoT devices installed in smart cities can verify the network, other nodes, and management station communications. Furthermore, it is critical to create cutting-edge technology to ensure real-time and accurate authentication because the amount of authentication data is expanding explosively in smart cities.

Confidentiality serves as a safeguard against active attacks and unauthorized disclosure of information. Attackers are considered to be able to access devices or listen in on communications in IoT-based applications. Therefore, encryption-based technologies are frequently used to create dependable communication and storage systems in order to safeguard the secrecy of information transmitted between nodes. It is noteworthy that the design of identification and authentication systems is challenging due to transparency and dependability.

2. **Availability and Integrity:** Generally speaking, availability means that tools and services must be reachable when required. According to our issue, intelligent systems or apps should be able to continue operating effectively even when under attack. A smart system must also be able to recognize any abnormal conditions and be able to halt additional system damage because these devices are vulnerable to attacks. Resilience is defined as a system's capacity to withstand multiple defects and failures brought on by attacks and major disasters. To counteract attacks that are becoming more sophisticated, defence mechanisms should be strong and able to learn adaptively. The security of IoT devices as well as the data transferred between them, and the cloud must be guaranteed. Data can readily be tampered with during the transmission process in a smart application because it involves the interchange of data across numerous devices. Although some techniques, including firewalls and protocols, can control data traffic in IoT communications, they cannot ensure the integrity at endpoints due to the majority of IoT devices' limited computational capability.
3. **Light Weight Intrusion Detection and Prediction:** A smart system may only be considered secure if it has the capacity to monitor its operational circumstances and to promptly identify any anomalous events, according to the vulnerabilities of the devices and networks used in a smart city. Three common approaches to using the traditional intrusion detection system (IDS) are misuse detection, anomaly detection, and specification-based detection. However, the straightforward adaptation of a global IDS solution is unrealistic and inflexible in the heterogeneous and complex smart city ecosystem. Furthermore, resource-constrained sensors and devices require the development of lightweight intrusion detection techniques. Predicting risks and being aware of them beforehand is preferable to discovering them after an attack and trying to recover. To achieve security status awareness and automatically foresee various attacks on smart apps, it is crucial to design intelligent IPS systems.
4. **Privacy Protection:** Since privacy protection and security are intertwined, all of the

previously listed requirements may have an impact. This subsection is necessary to cover some security requirements that were left out of earlier subsections. Sensitive data leakage, whether intentional or unintentional, is the main cause of privacy breaches in smart city scenarios. This is in addition to some common harms, such as packet interception in communication, malware in mobile devices and applications, hacking on servers, and permission falsification. A thorough study from 2017 found that four types of data—observable data, repurposed data, published data, and leaked data which contain significant amounts of sensitive user data and can be utilized to violate privacy. Application of appropriate and efficient countermeasures, such as encryption techniques, anonymity mechanisms, and even cutting-edge strategies like differential privacy, is necessary to prevent usage by unauthorized parties. Even when a system is safe and not compromised by criminals, the privacy of citizens can occasionally be violated. The potent data mining techniques are one possible mechanism for this to happen. Some service providers and third parties can readily find the personal information of consumers using data mining methods, as shown by the example given by. So it is necessary to use privacy-preserving data mining (PPDM) strategies.

SECURITY AND PRIVACY ISSUES IN SMART CITIES:

1. **Botnet Activities in IOT Based Smart City:** IoT systems are under attack from freshly discovered IoT botnets. The "Mirai" botnet serves as a good illustration because it has the ability to infect many heterogeneous IoT devices, disseminate infection to them, and then launch a DDoS attack on target servers. IoT devices sometimes have weak or no security when compared to computers and smartphones.
2. **Driverless Car Threats in Smart Cities:** In order to decrease traffic accidents and create a cleaner, more intelligent society, high-tech corporations have invested billions of dollars in the development of autonomous vehicles (AVs). However, this fast-expanding use has been viewed as a significant security risk since, if an AV is compromised, both life safety and data privacy are at risk. In particular, hackers can take advantage of security flaws to launch remote assaults that affect the steering, brakes, and engine. Furthermore, there may be serious privacy concerns due to the vast amounts of personal information that a self-driving car's computer system collects.
3. **Smart City Risks Posed by AI:** In numerous smart applications, such as the automatic control of trade systems, home appliances, and pacemakers, AI systems play essential

roles. However, there are security issues associated with AI's expanding use. For instance, service providers and device manufacturers can utilize data mining technology to harvest sensitive information and analyse personal data in excess of what is necessary to achieve the core goals of the connected services. Additionally, hackers that are knowledgeable about AI are becoming more sophisticated. Hackers may be able to use specific strategies to decrease the training effects and reduce the dependability of the algorithms.

SECURITY AND PRIVACY PROTECTION TECHNOLOGIES:

1. **Cryptography**: Cryptography aids in prevention of un-authorized access of disturbed parties in the cycle of data revealing, storing, processing and storing. Light weight encryption and decryption algorithms are embedded into IOT devices since, these devices are of low computational power. Lighter encryption algorithms for IOT devices involving end-to-end users' communication protection from DDoS (Denial of Services) attacks, public key encryption are implemented. Homomorphic Encryption Techniques are used in electricity consumption aggregation in smart grids, solving cloud security issues and embedded into health monitoring systems
2. **Blockchain:** This allows the IOT enabled devices to operate in a distributed manner. So, various frameworks involving blockchain technologies are implemented that guarantee the security of system and increase the reliability, efficiency. Various security issues in automatic transportation systems are tacked by blockchain technology. Blockchain is implemented in cloud to scale up the IOT networks by combining with software defining networking and fog computing.
3. **Biometrics:** This is used mainly for authentication in smart cities which involves recognizing behavioural and biological characteristics of person by automatically collecting human data such as fingerprints, voice, faces, signatures. In order to protect the personal stored data of users, key negotiation and mutual authentication protocol involving biometrics is introduced that not only mitigates security attacks but also keeps the communication secure.
4. **Machine Learning and Data Mining:** Various machine learning algorithm embedded devices are commonly used in a smart city. Wireless sensor networks (WSN) are adopted with various ML algorithms in-order to maintain a secure data sensing and prevent intrusions in WSN. Various feature selection and model selection methods are

used in detecting various wi-fi attacks in a smart city. Data Mining is used in in finding new regulations and legitimate information form vast amounts of data collected by multiple sensors and devices in smart city. Various privacy preserving data mining technologies have been implemetd in-order to protect user's sensitive information.

5. **Deep Learning:** Deep Belief Networks (DBN) and Deep Neural Networks (DNN) were utilized to build a novel method for detecting and classifying dangerous malicious URL's that tend to corrupt the IOT device. Various Convolutional Neural Network (CNN) and Recurrent Neural Network (RNN) based intrusion detection systems, cyber-attack detection systems are implemented in smart cities.

FUTURE SCOPE:

The concept of "smart cities" describes how future, digitally connected cities should function. The profitability and appeal of smart cities depend on their capacity to secure quality of life improvements. This article outlined three problems with privacy and security in smart cities. How can personal privacy be maintained in a smart city that makes use of data mining and rapid data sharing with numerous stakeholders? How will this problem be solved? Data integration expands the digital surface of a smart city, increasing the potential for security breaches. What happens to the information gathered by a smart city?

What purposes might data collection be utilized for? How will data mining methods and AI technologies in a smart city impact the physical security of the city? The risk profile of the smart city is mapped, there are tiered security models, cryptographic techniques are used, data is transparent, and emergency contingency plans are used, in that order, as solutions to the many issues. In the end, security and privacy issues can only be solved most successfully by taking a comprehensive approach to both. Because the smart city is made up of so many interconnected devices, security and privacy solutions must focus on a system of protection rather than just a collection of individual defences. In order to build smart cities, it will be essential to use layered security strategies and open privacy standards. The number of accessible services and applications in the smart city is growing. The usage of ICT services and applications may not be taught to all citizens, nevertheless. Therefore, the possibility for study is to develop efficient means of instructing urban citizens in the usage and comprehension of new ideas.

CONCLUSION

There are numerous security and privacy risks as a result of the increased use of smart applications. The creation of more sophisticated protection frameworks and models is crucial and in great demand in both the academic and industrial worlds. More than half of the world's population now resides in urban areas. The idealized smart city has come to pass, despite the fact that there are still disparities in how we view them (for instance, there is still a cyber danger). For smart city operations to run smoothly, managing cyber security is crucial. Even though various new methods using emerging technologies have been developed in recent years, there is still a long way to go in ensuring that various security challenges of smart city applications are being satisfied.

REFERENCES:

1. Rath, Abinash & Kannapiran, E. & Almahirah, Mohammad & Bora, Ashim Chowdhury, Shanjida. (2022). “Artificial Intelligence Empowered Internet of Things for Smart City Management” 10.1007/978-3-031-07012-9_18.
2. Cui, Lei & xie, gang & Qu, Youyang & Gao, Longxiang & yang, yunyun. (2018) “Security and Privacy in Smart Cities: Challenges and Opportunities” IEEE Access. PP. 1-1. 10.1109/ACCESS.2018.2853985.
3. Chen, Dongliang & Wawrzynski, Pawel & Lv, Zhihan. (2020) “Cyber Security in Smart Cities: A Review of Deep Learning-based Applications and Case Studies. Sustainable Cities and Society” 66. 102655. 10.1016/j.scs.2020.102655.
4. Javed, Abdul Rehman & Zikria, Yousaf & Rehman, Saif & Shahzad, Faisal & Jalil, Zunera. (2021) “Future Smart Cities: Requirements, Emerging Technologies, Applications, Challenges, and Future Aspects”.
5. Braun, Trevor & Fung, Benjamin & Iqbal, Farkhund & Shah, Babar. (2018) “Security and Privacy Challenges in Smart Cities. Sustainable Cities and Society”. 39. 10.1016/j.scs.2018.02.039.
6. T. Singh, A. Solanki, S. K. Sharma, A. Nayyar and A. Paul, "A Decade Review on Smart Cities: Paradigms, Challenges and Opportunities," in IEEE Access, vol. 10, pp. 68319-68364, 2022, doi: 10.1109/ACCESS.2022.3184710.