SMART CITY SECURITY ISSUES: THE MAIN ATTACKS AND COUNTERMEASURES

Ouidad Saber, Tomader Mazri

National School of Applied Sciences, University Ibn Tofail, Kenitra, Morocco – (ouidad.saber, tomader.mazri) @uit.ac.ma

KEY WORDS: Smart City, Services, Applications, Security Attacks, Icts, Security Solutions

ABSTRACT:

A smart city is an urban area based on a variety of services that uses information and communication technologies (ICTs) to improve operational efficiency and citizen's quality of life. It also leans towards meeting the economic, social, environmental, and cultural needs of dwellers. Technologies can add many benefits to smart city to facilitate communication and efficiently manage assets, resources, and services. However, technologies bring new security issues that need to be addressed to ensure data confidentiality, integrity, and availability. This paper provides an overview of the smart city concept by highlighting its main applications and services, presenting some susceptible attacks that can touch the security of applications, and some good practices to ensure the smart city security.

1. INTRODUCTION

Smart city was popularized in early 2010 to describe how recent technological advancements and data can enable more efficiently city management. Smart cities are defined as collaboratively built, resilient, and inclusive cities that use various types of technologies and data to achieve a better quality of life for all of their residents (Toli & Murtagh, 2020). Hence, a smart city is a city that privileges information and communication technologies (ICTs) to promote better interaction with its citizens and to guarantee its inhabitants an improved quality of life and environment despite the growing development of the city.

In (Giffinger & Gudrun, 2010), six axes are defined to measure whether a Smart City is well-performing. These dimensions are Smart economy, Smart people, Smart governance, Smart mobility, Smart environment, and Smart living, each including various factors and indicators (Figure 1).

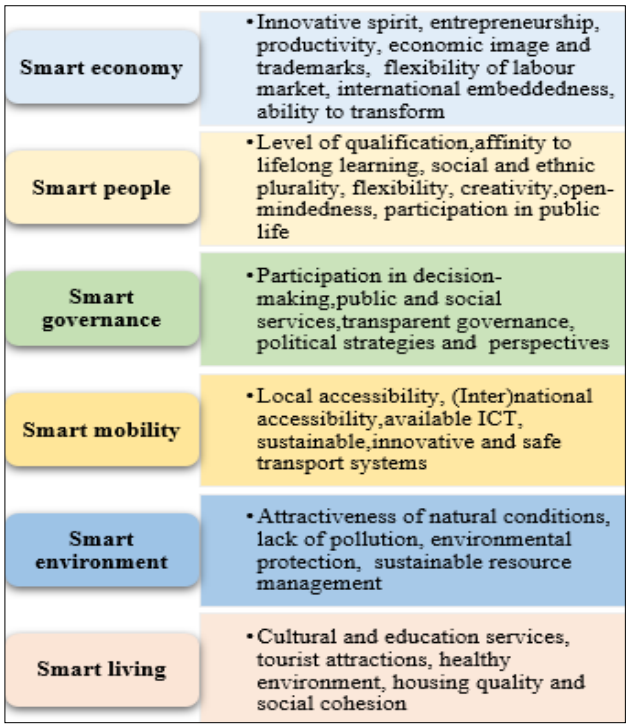

Figure 1. Smart city dimensions

The first dimension is smart economy that is based on innovation and entrepreneurship, high-productivity, labour market flexibility, openness to international and inter-regional cooperation and capacity for change. In other words, an economy based on natural resources utilisation is replaced by a new economic model in which the driver of development is innovation and modern ICTs.

The second dimension is smart people. This axe includes various aspects such as lifelong learning by the continuous improvements in the competence and qualifications of citizens, social and ethnic plurality, open-mindedness, flexibility, creativity, and participation in public life.

The third dimension is smart governance. It is an intelligent public management in which public participation in decision-making and transparency of actions, as well as the quality and availability of public services and improvement in government services are given top priority through the use of intelligent technologies.

The fourth dimension is smart mobility. This axe refers to the city's national and international accessibility, as well as the use of information and communication technologies (ICTs) that can make traffic flows more efficient and transportation systems more sustainable, innovative and safe within and outside the city.

The fifth dimension is smart environment. It aims to adapt the smart city with climate change. For this reason, it employs a variety of technologies to improve public awareness of environmental conditions and services such as electricity, water, and gas. The objective of smart environment is to change people's habits, reduce waste, and improve resource's efficiency. Thus, smart environment consists of four factors: attractivity of natural conditions, no pollution, environmental protection, and sustainable resource management.

The sixth dimension is smart living which comprises an efficient system of high-quality urban public space where education facilities should be provided by establishing world-class colleges and universities. It should also have tourist attractions, as well as world-class hospitals with all the latest technology-enabled devices and equipment to allow a healthy lifestyle for every resident. Also, citizens should have access to high-quality housing, as well as social cohesion (Manville, C. et al., 2014).

Smart cities bring a new concept and model, which applies the new generation of information technologies, such as Internet of Things, cloud computing, big data, wireless technologies, etc. to facilitate the planning, construction, management, and smart services of cities (Toh et al., 2020). In addition to these technologies, smart city uses numerous devices (tablets, laptops, phones, etc.), connected sensors, and objects. Hence, the integration of all these technologies and devices can make the smart city face several cyberattacks.

The objective of this paper is to present an overview of the smart city applications, the main cyberattacks concerning information and communication security, and some solutions to deal with these cyberattacks. The content of the paper is organized as follows: In Section 2 we present the main applications and services of the smart city. Section 3, describes some smart city attacks. Solutions to address attacks in Section 4. Conclusion and future work are discussed in Section 5.

2. SMART CITY APPLICATIONS

Smart city applications are based on the six main dimensions mentioned above. These applications cover fields, for instance, transportation (intelligent road networks, connected cars and public transport), public utilities (smart electricity, water and waste), education, health, buildings, surveillance, payment, voting, etc. In this section, we will present some potential applications of the smart city.

2.1 Smart Payment

Smart payment is a system that improves and facilitates payment services. For example, digital wallet is a smart payment method that allows one party to make electronic transactions with another party by bartering digital currency units for goods and services. This can include online purchasing or in-store purchasing (using technologies that connect smartphones to the physical world such as NFC (Near Field Communication), QR codes, etc.). Digital wallet helps in various transactions such as making payments (electricity, water, fees etc), shopping online, booking train and flight seats and many more (Tiwari et al., 2019).

A growing number of companies (Pavilion Hotels & Resorts, Microsoft, Tesla, etc.) are embracing cryptocurrencies, allowing customers to use them as an official method of payment for their goods and services (Walsh, 2021). Hence, cryptocurrency is one of the developments of the blockchain that is often used as a decentralized digital currency. Cryptocurrency means a virtual currency that has no physical form, it has many types such as Bitcoin, Ethereum, Litecoin, Monero, and many other type (Amsyar et al., 2020).

2.2 Smart Voting

To replace the traditional voting system, in (Lakshmanan et al., 2018), a smart voting system through Facial Recognition was proposed where there are three levels of verification used for the voters. The first level is the verification of unique id number (UID), the second level is the verification of election id number (EID), and the third level is face recognition or face matching.

Voting through Blockchain is discussed in (Jafar et al., 2021) where the blockchain technology can be used to pass votes between two parties, the electorate is one party and the candidate who earns the vote is the other, without having a controlling central authority body. Blockchains generate cryptographically secure voting records. Votes are recorded accurately, permanently, securely, and transparently. No one can modify or manipulate them.

In (Peter et al., 2018), a smart voting system based on finger print was proposed. If the fingerprint enrolled by the voter matches the one in the database, the voter can register to vote. If the fingerprint does not match, the system blocks the process.

2.3 Smart Transportation

Congestion and parking are two of the most serious issues that large cities face. For this reason, the smart city has given birth to several smart mobility services. For example:

Smart transportation which represent a powerful tool to improve access to information regarding traffic flow, to detect abnormal road traffic , to accurately determine the operation of vehicles and infrastructure, and to efficiently provide the traffic information for drivers using ubiquitous connectivity, remote sensors, intelligent processing, big data analysis, etc (Ge et al., 2017).

Smart parking is a method of using information and communication technologies to assist drivers in finding more efficiently satisfying parking spaces. Smart parking would enable the following; sense vehicle occupancy in real-time, guide residents and visitors to available parking, help traffic in the city flow more freely, etc.(Lin, 2015).

Smart roads will take over many advances such as, roads that automatically weigh cars/trucks, charge vehicles, roads with smart traffic signs, roads with V2X and VANETS, roads with smart street lights, roads with smart traffic violation detection, etc.(Toh et al., 2020).

2.4 Smart Healthcare

Smart healthcare is a healthcare system that leverages wearable devices, the internet of things, and mobile internet to dynamically access information, connect people, materials, and institutions in the healthcare industry. Smart healthcare intelligently controls and responds to medical ecosystem demands. IoT and related technologies can be used for real-time monitoring and alerts generation, telemedicine which refers to providing healthcare to people remotely, home and elderly healthcare that can be deployed at homes for continuous monitoring of patients, etc. (Tian et al., 2019).

2.5 Smart Buildings

Smart buildings use ICTs to provide automated building operations and control, connect building systems together to optimize operations and whole-building performance, and allow occupants to interact with the building by providing visibility into its operations and actionable information. Smart buildings may also interface with the power grid, which is an increasingly significant characteristic for utility demand response implementation. There are many systems in smart building such as Heating, Ventilating, and Air Conditioning Systems(HVAC), lighting control systems, access control systems, etc.(King, 2017).

2.6 Smart Learning Environments

Smart learning environments are supported by technologies to allow learners to access digital resources, interact with learning systems from anywhere and at any time, provide the necessary

learning guidance, supportive tools, and learning suggestions in the right place, at the right time, and in the right form. There are many different types of technologies used to promote and enhance learning which include both hardware and software. Hardware includes tangible objects such as interactive whiteboard, smart table, e-bag, etc. Software includes all kinds of learning systems and tools, online resources, virtual reality, etc.(Zhu et al., 2016).

2.7 Smart Grid

According to the National Institute of Standard and Technology (NIST) smart grid is "A modernized grid that enables bidirectional flows of energy and uses two-way communication and control capabilities that will lead to an array of new functionalities and applications"(Melvin, 2014).

A smart grid is an electric system that integrates information, two-way, cyber-secure communication technologies, and computational intelligence across electricity generation, transmission, distribution, and consumption to create a system that is clean, safe, secure, reliable, efficient, and sustainable. The key features of smart grid are: optimized, distributed generation, self-healing, interactive, secure, environment friendly, etc.(Anderson et al., 2018).

2.8 Smart Surveillance Systems

Smart surveillance system is a system that has intelligent capability to assess surveillance data automatically and take appropriate actions such as generating alarm or warning. It is interdisciplinary topic that involves electronic (sensing device), computer vision and pattern recognition, artificial intelligence, etc. It is used in various environments, such as public transport area, governmental building, remote military surveillance, etc.(Ibrahim, 2016).

2.9 Smart Water Management

A smart water system can contribute to more sustainable water services, leakage reduction and detection, water conservation and monitoring, operational optimization, financial loss reduction, and improved customer experience. Some of the main smart water management tools are data acquisition and integration (e.g. sensor, smart pipes, smart meters),data dissemination (e.g. WiFi, Internet), management and control (e.g. supervisory control and data acquisition (SCADA)) (Ramos et al., 2020).

2.10 Smart Waste Management

Smart waste management is all the activities and actions required to manage waste from its inception to its final disposal. This encompasses waste collection, transportation, treatment and disposal, as well as monitoring and regulation. Smart waste management relies on smart sensor-based dustbins that will judge the level of waste in dustbins and send a message directly to the municipal corporation which will use the smart transportation systems to choose the shortest path. It can sense all types of waste material, whether solid or liquid (Mahajan et al., 2017).

3. SMART CITY SUSCEPTIBLE ATTACKS

Cyberattacks seek to alter, disrupt, deceive, degrade, or destroy smart city systems and networks, as well as information and/or programs resident in or transiting these systems or networks. Generally, there are three specific forms of cyberattacks against smart city systems (Figure 2): **availability** attacks that aim to close a system down or deny service use, **confidentiality** attacks that seek to extract information and monitor activity, and **integrity** attacks that pursue to enter a system to alter information and settings without being noticed by the legitimate operator/ owner (Levy-Bencheton et al., 2015).

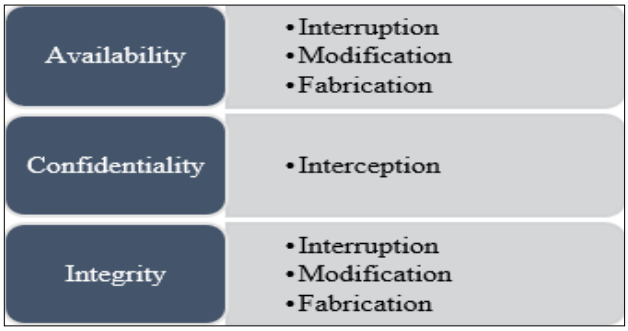

Figure 2. Goals of security attacks

There are many smart cities cyberattacks, for example:

DoS & DDoS: For denial-of-service (DoS), a malicious node sends a stream of messages to the target node and thereby isolate it from the network. For distributed dos (DDoS), the stream of messages is sent at the same time by a number of malicious nodes.

Wormhole: An intruder catches the data packets and replays them to another malicious node by using a wormhole link (a tunnel) (Kalinin et al., 2021).

Man-in-the-middle (MitM): An attacker eavesdrops and possibly modifies the communication between two nodes who think they have a direct communication.

Social engineering: An intruder physically interacts and manipulates users of the smart city systems.

Jamming: This attack can disturb the wireless communication, it causes Denial of Service attack (Deogirikar & Vidhate, 2017),

Malware: It is a malicious software that can gain illegal access to the system. It can also use internal weaknesses of the system to steal, change, and ruin physical system components and related information (Al-Turjman et al., 2019). Categories of malware include ransomware, worms, trojans, viruses, rootkits, botnets and spyware (Mayol et al., 2016).

False information: An attacker transmits erroneous messages on the network.

Message modification: An intruder transmits altered messages on the network.

Eavesdropping: An attacker implants eavesdropping tools in specific network for spying on communication channels, capturing the network traffic behaviour and getting the network map.

Masquerading: An intruder tries to steal information by pretending to be a legal device or entity (Al-Turjman et al., 2019).

Sleep Deprivation: It keeps the nodes awake which will result in a more power consumption, and will cause the nodes to shut down**.**

Sybil attack: An adversary creates multiple identities of itself to transmit messages to different nodes on the network (Andrea et al., 2015).

Replay attack: An attacker is able to intercept the network packets, he could retransmit the intercepted data as if they sent by a legitimate user.

Malicious node injection: An adversary could insert a malicious object among legitimate ones in the network.

Malicious code injection: An attacker could insert a malicious code into a smart city object.

Object tampering: Such IoT objects are vulnerable to hardware attacks like the alteration of operating system or firmware, the circuit modification, the extraction of cryptography keys etc. (Akram et al., 2018).

Theft: It is possible by stealing intangible stuff such as sensitive data, information, software and cryptographic key, etc. and by stealing tangible physical objects such as hand held devices and technological equipment (Levy-Bencheton et al., 2015).

In this section, we will present some attacks that harm the functionality of smart city applications.

3.1 Smart Transportation Attacks

Man in the middle: Malicious attackers can eavesdrop on vehicular communication and implant false information or distort messages between them.

Masquerading: By using false identities, a vehicle can actively mask its own identity in order to appear as another vehicle. This method is frequently used in conjunction with other types of attacks.

False Information: A vehicle can send false information and data through the network which can affect the behaviour of other vehicles and lead to illusion attacks (when an attacker broadcast warning messages that do not correspond to the current situation, it produces an illusion to the vehicles in their neighbourhood).

Wormhole: To tunnel packets from one place to broadcast them in another, the attacker should have control of at least two nodes of the vehicular network that are distinct from one to another and have a very high-speed connection between the two nodes (Al-Turjman & Lemayian, 2020).

Message modification: Smart transportation devices such as traffic signals, toll tag readers and cameras are extremely vulnerable to message modification attack that is defined as any intentional modification, insertion, or deletion of data by authorized or unauthorized users, including employees that compromises the data.

Theft: Smart transportation is susceptible to theft of cryptographic keys to decentralized ticketing systems that can cause serious financial and reputational damage, theft of employees' mobile devices which can contain smart transportation data and information, theft of credentials or other sensitive information.

DDoS : Smart transportation infrastructure is the most prevalent target of DDoS assaults (Levy-Bencheton et al., 2015). By using malicious nodes to create a large number of bogus identities, an attacker can disrupt the vehicular network, jam signals, or even cause a collision.(Al-Turjman & Lemayian, 2020). For instance, the train delays and travel service interruptions that took place in Sweden occurred because of a series of DDoS attacks targeting their transportation systems (Reo, 2017).

Malicious code Injection: After getting access to the vehicle networks and ECUs (electronic control units), an attacker may introduce damaging codes into the ECUs. Viruses, Trojan horses and spyware may infiltrate a vehicle through this approach too.(Thing & Wu, 2016).

Sybil attack: An attacker uses a large number of pseudonymous to persuade vehicles to take different paths, informs vehicles about the jam by claiming there are more than a hundred vehicles ahead, etc.(Deeksha et al., 2017).

3.2 Smart Healthcare Attacks

Object tampering: A tampered medical equipment don't only threaten patient safety (e.g., if a pacemaker is disabled or the settings of an insulin pump are altered), but also patient privacy and hospital operations in general.

DoS: The Boston Children's Hospital (BCH) was the victim of a denial-of-service attack, with three major consequences: inability to electronically route prescriptions to pharmacies, inability to access remotely hosted electronic health records, and downtime e-mail for departments where e-mail is critical processes.

Social engineering: An attacker may get access to smart healthcare ICT assets including networked medical devices, identification components, and client devices through social engineering. With access to ICT assets, information can be easily misused, and social engineering would be impossible without the involvement of hospital staff.

Ransomware: It is a form of malware that restricts access to a system and demands the user to pay a ransom to remove the restriction. The Klinikum Arnsberg and the Lukas Hospital in Neuss were both attacked by file encrypting ransomware. The ransomware was able to enter the system at the Klinikum Arnsberg thanks to an e-mail attachment.

Theft of equipment: In the United Kingdom, the North West London Hospitals NHS Trust wrote off more than £220,000 in stolen medical equipment over a one-year period in 2010-2011.A few years later an unencrypted laptop containing the personal information of 8 million patients was stolen from a storeroom at the NHS North Central London (Mayol et al., 2016).

Replay attack: An unauthorized user get access to the smart healthcare system, the intruder captures the network traffic and send the message to the receiver acting as the original sender (Rughoobur & Nagowah, 2017).

Sybil attack: It is one of the most prevalent attacks in which a malicious node uses morphing identities to generate sybil nodes. It threatens the security and privacy of the smart healthcare system. Sybil nodes can get an authorized node identity and then misbehave, for example, by receiving, sending, or editing patient's information (Vaishnavi & Sethukarasi, 2021).

3.3 Smart Buildings Attacks

Masquerading: An attacker gains remote access to the smart building's network infrastructure with the purpose of obtaining

secret data. This attack is commonly used in conjunction with other attacks such as the replay attack.

Eavesdropping: An attacker can monitor data flow in and out of the smart building network. The communication could contain sensitive information that the building's users don't want to be exposed to unauthorized individuals.

Replay attack: A copy of a legitimate service request sent from a device in the smart building network can be captured and stored by an attacker. Then, he replied it to get the service that the smart building user is allowed to use.

DoS: An attacker can send an unlimited number of messages to overburden the services of the smart building network. As a result, legitimate users are unable to access the smart building network's services.(Ul Rehman & Manickam, 2016).

DDoS: In 2016, DDoS attack took down the central heating system during winter in Finland and caused both material damage and a need to relocate residents elsewhere. In 2014, the DDoS attack against the Target Store in USA led to unauthorized access to more than 100000 devices revealing customers data including 53 million emails and credit card information.

Ransomware: In 2017, a ransomware attack was on a fully booked hotel in Austrian Alps where people were locked out of their rooms until a ransom was paid (Hachem et al., 2020).

3.4 Smart Learning Environment Attacks

Authentication: attacker will attempt to masquerades as a legitimate user when accomplishing this attack on the smart learning environment. There are various ways to masquerades as a legal user. One of the simplest ways is to steal credential or password from legitimate users.

Session Eavesdropping: An attacker will monitor the traffic sent and received between the smart learning environment users. The attacker will not change the traffic content, but he will monitor the traffic flow between users and the smart learning environment.

Replay: An attacker will intercept a communication channel between the smart learning environment users and record down the encrypted message that will then allow him to masquerade as a legitimate user.

Man-in-the-Middle: An attacker will act as the middle man and intercept messages sent between users and servers in the smart learning environment. Both smart learning environment users and servers might not know that their communication session has been compromised by a third party when this attack is conducted.

Integrity Attacks : Attackers can modify or destroy the information or data stored in the smart learning systems without any permission or authorization in order to achieve their desired goals (Chung et al., 2014).

3.5 Smart Grid Attacks

DoS: Smart grid is vulnerable to DoS attacks because it relies IP, such attacks can prevent message packets from being sent over the network or block the access to meter measurements.

Jamming: A malicious node may send wireless signals in the same frequency band utilized by the smart grid network

Replay: An attacker may send false messages or may retransmit same message multiple times. These erroneous messages have a negative impact that can engage or overload the receiver unnecessarily resulting in malfunctioning or slow down the entire smart grid communication

Malware: It can be used by an intruder to bring down smart meters or other critical resources. Malware can also alter or delete sensitive data from smart grids systems. (Yadav et al., 2016)..

Eavesdropping: This attack can compromise the confidentiality of the metering reports by an adversarial party (Carlos Lopez et al., 2015).

Object tampering: It is frequently the first step in a more sophisticated attack. A compromised IED (intelligent electric device) such as a circuit breaker might intentionally break a circuit and cause a power outage (Li et al., 2012).

3.6 Smart Surveillance Attacks

Malware: In USA, on March, 2021, the ransomware attack affected 150,000 security cameras at banks, jails, schools, and carmaker Tesla.

DDoS: In French web host OVH, on September, 2016, it was the largest DDoS attack ever recorded at over 600 Gbps in size targeting IoT devices, including routers, IP cameras and digital video recorders.

Man-in-the-middle: This attack could allow the attacker to secretly relay and possibly modify the communications between two devices (cameras, sensors, etc.).

Steganography: It is a technique for making use of the unused or less important information bits of the user content (images, videos). For example, malicious payloads can be embedded into a set of PNG files that can be then compiled into a legitimate application. (Vennam et al., 2021).

DoS: If a camera or DVR (digital video recorder) has been compromised, the attacker can cause a camera to stop transmitting video content, erase historic content, prevent access to the DVR, etc. which affect the availability of service, data, and resources.(Kalbo et al., 2020).

3.7 Smart Water Attacks

Dos: This attack can make the system inaccessible by preventing sensors to send data, the controllers from receiving data and issuing commands, or the actuators from receiving commands and executing actions. DoS attacks can be carried out in a variety of ways, including jamming wireless channels, flooding wired channels with additional traffic, or overloading SCADA system with additional request.

Malicious code injection: This attack may exist when an attacker can gain access to the network, then he insert physically a malicious code into a smart water system

Eavesdropping: An attacker can collect information about the signals sent to the smart water system actuators (Taormina et al., 2017).

Object tampering: This attack is possible when an attacker is physically near to a smart water system device and can replace part of the hardware to manipulate the data or to get the

information inside the device (e.g., data, cryptographic key, communications channels, etc.).

Malicious node injection: An intruder can inject a virtual node in the network which, in turn, enable him to gain access to the network and control the flow of data in the smart water system (Mahmoud & Wu, 2020).

3.8 Smart Waste Attacks

Object tampering: An adversary can harm the smart sensor-based dustbin by physically changing it entirely or partly. The adversary can also electronically interrogate the nodes to gain access and alter sensitive information of the smart waste system.

Man-in-the-Middle: It allows the attacker to interfere between two sensors of the smart waste system to access restricted data and violate the privacy of the two nodes by monitoring, eavesdropping, and controlling the communication between them (Andrea et al., 2015).

Sybil Attack: A malicious node in the smart waste system can take the identities of multiple nodes and acts as them which lead to false information being accepted by reception nodes.

Sleep Deprivation Attack: In the smart waste system, sensor nodes are powered by replaceable batteries, the attacker use more power that results in shutting down the dustbin sensor nodes which can, for instance, produce bad smell, locked dustbin, etc (Deogirikar & Vidhate, 2017).

4. GOOD PRACTICES TO ADDRESS ATTACKS

The main security mechanisms for making smart city networks and data secure should be applied by using cryptographic algorithms which are the backbone of security and privacy protection for the smart city applications. They avoid the access of unauthorized parties during the data storing, processing and sharing. In 2016, (Mahmood et al., 2016) developed a lightweight authentication mechanism for an IoT scenario that can protect end-to-end users communications from distributed DoS attacks.

Additionally, providing security and privacy of data circulating in the smart city network through the use of blockchain which is a distributed ledger system that offers a decentralized, trusted, secured approach to information and transaction sharing among stakeholders instantly with no intermediaries of centralized authority (Cui et al., 2018).

Furthermore, establishing a virtual private network that extends a private network across a public network and allows benefiting from the functionality, security and management policies of the private network.

Moreover, deploying network intrusion detection that inspect all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack.

Also, implementing an information security policy is also an efficient security measurement to define the elements to protect, the procedures to follow, the organization of security, etc. A common example is ISO 270001.

Additionally, using access control that limits unauthorized access and provides evidences in case of tampering. There are two main types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and computer equipment in the smart city environment. Logical access control limits connections to computer networks, system files and data in the smart city network.

Furthermore, other very important elements that needs to be adopted and applied on smart city services are: regular auditing that allows an inspection or examination of infrastructure (digital or physical) in order to measure or improve its appropriateness, safety, efficiency, or other characteristics. Creation of activity logs that offer evidence and analysis capacity in case of an incident. They provide a good indicator of what happened and how an attack was materialized effectively. And maintenance of backups that ensures the integrity of data recovery in the case of corruption or loss (Levy-Bencheton et al., 2015).

5. CONCLUSION AND FUTURE WORK

This paper presents a general overview of the smart city environment and its applications. In addition, several smart city security attacks that can affect confidentiality, integrity, and availability have been investigated, as well as some countermeasures to deal with these cyberattacks.

Smart City's cyber security is affected by the emergent integration of technologies and the intensive communication which lead to unbounded attack surface. Hence, smart city security will always remain a very complicated challenge. The main weakness is that it has no centralized infrastructure, which poses a security challenge against cyberattacks. It is difficult to control the attackers. For this reason, we need to make for each smart city application a detailed security study by specifying the attack scenarios and their impacts, as well as implementing solutions for each attack. In the future work, we will achieve a part of this goal by performing a security study for smart transportation systems.

REFERENCES

Akram, H., Konstantas, D., & Mahyoub, M. (2018). A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model. *International Journal of Advanced Computer Science and Applications*, *9*(3). https://doi.org/10.14569/IJACSA.2018.090349

Al-Turjman, F., & Lemayian, J. P. (2020). Intelligence, security, and vehicular sensor networks in internet of things (IoT)-enabled smart-cities : An overview. *Computers & Electrical Engineering*, *87*, 106776. https://doi.org/10.1016/j.compeleceng.2020.106776

Al-Turjman, F., Zahmatkesh, H., & Shahroze, R. (2019). An overview of security and privacy in smart cities' IoT communications. *Transactions on Emerging Telecommunications Technologies*, *n/a*(n/a), e3677. https://doi.org/10.1002/ett.3677

Amsyar, I., Christopher, E., Dithi, A., Khan, A. N., & Maulana, S. (2020). The Challenge of Cryptocurrency in the Era of the Digital Revolution : A Review of Systematic Literature. *Aptisi Transactions on Technopreneurship (ATT)*, *2*(2), 153-159. https://doi.org/10.34306/att.v2i2.96

Anderson, R., Ghafurian, R., & Gharavi, H. (2018). *Smart Grid The Future of the Electric Energy System*.

Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015). Internet of Things : Security vulnerabilities and challenges. *2015 IEEE Symposium on Computers and Communication (ISCC)*, 180-187. https://doi.org/10.1109/ISCC.2015.7405513

Carlos Lopez, Arman Sargolzaei, Hugo Santana, & Carlos Huerta. (2015). Smart Grid Cyber Security : An Overview of Threats and Countermeasures. *Journal of Energy and Power Engineering*, *9*(7). https://doi.org/10.17265/1934-8975/2015.07.005

Chung, S. K., Yee, O. C., Singh, M. M., & Hassan, R. (2014). SQL injections attack and session hijacking on e-learning systems. *2014 International Conference on Computer, Communications, and Control Technology (I4CT)*, 338-342. https://doi.org/10.1109/I4CT.2014.6914201

Cui, L., Xie, G., Qu, Y., Gao, L., & Yang, Y. (2018). Security and Privacy in Smart Cities : Challenges and Opportunities. *IEEE Access*, *6*, 46134-46145. https://doi.org/10.1109/ACCESS.2018.2853985

Deeksha, Kumar, A., & Bansal, M. (2017). A review on VANET security attacks and their countermeasure. *2017 4th International Conference on Signal Processing, Computing and Control (ISPCC)*, 580-585. https://doi.org/10.1109/ISPCC.2017.8269745

Deogirikar, J., & Vidhate, A. (2017). Security attacks in IoT : A survey. *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 32-37. https://doi.org/10.1109/I-SMAC.2017.8058363

Ge, Y., Liu, X., Tang, L., & West, D. M. (2017). *Smart transportation in China and the United States*. 20.

Giffinger, R., & Gudrun, H. (2010). Smart cities ranking : An effective instrument for the positioning of the cities? *ACE: Architecture, City and Environment*, *4*(12), 7-26. https://doi.org/10.5821/ace.v4i12.2483

Hachem, J. E., Chiprianov, V., Babar, M. A., Khalil, T. A., & Aniorte, P. (2020). Modeling, analyzing and predicting security cascading attacks in smart buildings systems-of-systems. *Journal of Systems and Software*, *162*, 110484. https://doi.org/10.1016/j.jss.2019.110484

Ibrahim, S. W. (2016). A comprehensive review on intelligent surveillance systems. *Communications in Science and Technology*, *1*(1). https://doi.org/10.21924/cst.1.1.2016.7

Jafar, U., Aziz, M. J. A., & Shukur, Z. (2021). Blockchain for Electronic Voting System—Review and Open Research Challenges. *Sensors*, *21*(17), 5874. https://doi.org/10.3390/s21175874

Kalbo, N., Mirsky, Y., Shabtai, A., & Elovici, Y. (2020). The Security of IP-Based Video Surveillance Systems. *Sensors*, *20*(17), 4806. https://doi.org/10.3390/s20174806

Kalinin, M., Krundyshev, V., & Zegzhda, P. (2021). Cybersecurity Risk Assessment in Smart City Infrastructures. *Machines*, *9*(4), 78. https://doi.org/10.3390/machines9040078

King, J. (2017). Smart Buildings : Using Smart Technology to Save Energy in Existing Buildings. *SMART BUILDINGS*, 55.

Lakshmanan, V., Ramasamy, V., & Angelinblessy, J. (2018). *Smart Voting System Support through Face Recognition*.

Levy-Bencheton, C., Darra, E., Bachlechner, D., Friedewald, M., Mitchener-Nissen, T., Lagazio, M., & Kung, A. (2015). *Cyber Security for Smart Cities—An Architecture Model for Public Transport.pdf*. https://doi.org/10.2824/846575

Li, X., Liang, X., Lu, R., Shen, X., Lin, X., & Zhu, H. (2012). Securing smart grid : Cyber attacks, countermeasures, and challenges. *IEEE Communications Magazine*, *50*(8), 38-45. https://doi.org/10.1109/MCOM.2012.6257525

Lin, T. S. (2015). *Smart parking : Network, infrastructure and urban service* [These de doctorat, Lyon, INSA]. https://www.theses.fr/2015ISAL0138

Mahajan, Prof. S. A., Kokane, A., Shewale, A., Shinde, M., & Ingale, S. (2017). Smart Waste Management System using IoT. *International Journal of Advanced Engineering Research and Science*, *4*(4), 93-95. https://doi.org/10.22161/ijaers.4.4.12

Mahmood, Z., Ning, H., & Ghafoor, A. (2016). Lightweight Two-Level Session Key Management for End User Authentication in Internet of Things. *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 323-327. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.78

Mahmoud, H., & Wu, W. (2020, février 10). Cyber-Physical System Security Open Challenges in Smart Water Networks. *Zenodo*. 17th International Computing & Control for the Water Industry Conference, Exeter UK. https://doi.org/10.5281/zenodo.3661113

Manville, C., Cochrane, G., Cave, J., Millard, J., Pederson, J.K., Thaarup, R.K., Liebe, A., Wissner, M., Massink, R.A., & Kotterink, B. (2014). *Mapping smart cities in the EU*. European Parliament ; Directorate General for Internal Policies. Policy Department Economic and Scientific policy A. http://resolver.tudelft.nl/uuid:1fac0e18-8dd3-406d-86fe-ce1e6a22e90c

Mayol, J., Manzoni, A., Calcavecchia, F., iliev, Y., Kabisch, B., Lovis, C., Morgenstern, M., Gomes, R., Gerald, G., Glynos, D., Antonatos, S., Fletcher, G., & Jespersen, P. (2016). *Smart Hospitals Security and Resilience for Smart Health Service and Infrastructures NOVEMBER 2016 Smart Hospitals About ENISA*. https://doi.org/10.2824/28801

Melvin, H. (2014). The role of ICT in evolving SmartGrids. *The 10th International Conference on Digital Technologies 2014*, 235-237. https://doi.org/10.1109/DT.2014.6868720

Peter, M. V., Priya, V., Petchammal, H., & Muthukumaran, D. N. (2018). *Finger Print Based Smart Voting System*. *2*(2), 6.

Ramos, H. M., McNabola, A., López-Jiménez, P. A., & Pérez-Sánchez, M. (2020). Smart Water Management towards Future Water Sustainable Networks. *Water*, *12*(1), 58. https://doi.org/10.3390/w12010058

Reo, J. (2017, octobre 19). DDoS Attacks on Sweden's Transit System Signal a Significant Threat. *Corero*.

https://corero.com/ddos-attacks-on-swedens-transit-system-signal-a-significant-threat/

Rughoobur, P., & Nagowah, L. (2017). A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare. *2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS)*, 811-817. https://doi.org/10.1109/ICTUS.2017.8286118

Taormina, R., Galelli, S., Tippenhauer, N. O., Salomons, E., & Ostfeld, A. (2017). Characterizing Cyber-Physical Attacks on Water Distribution Systems. *Journal of Water Resources Planning and Management*, *143*(5), 04017009. https://doi.org/10.1061/(ASCE)WR.1943-5452.0000749

Thing, V. L. L., & Wu, J. (2016). Autonomous Vehicle Security : A Taxonomy of Attacks and Defences. *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 164-170. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.52

Tian, S., Yang, W., Grange, J. M. L., Wang, P., Huang, W., & Ye, Z. (2019). Smart healthcare : Making medical care more intelligent. *Global Health Journal*, *3*(3), 62-65. https://doi.org/10.1016/j.glohj.2019.07.001

Tiwari, P., Garg, V., & Singhal, A. (2019). A study of Consumer adoption of Digital Wallet special Reference to NCR. *2019 9th International Conference on Cloud Computing, Data Science Engineering (Confluence)*, 664-669. https://doi.org/10.1109/CONFLUENCE.2019.8776939

Toh, C. K., Sanguesa, J. A., Cano, J. C., & Martinez, F. J. (2020). Advances in smart roads for future smart cities. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *476*(2233), 20190439. https://doi.org/10.1098/rspa.2019.0439

Toli, A. M., & Murtagh, N. (2020). The Concept of Sustainability in Smart City Definitions. *Frontiers in Built Environment*, *6*. https://doi.org/10.3389/fbuil.2020.00077

Ul Rehman, S., & Manickam, S. (2016). A Study of Smart Home Environment and its Security Threats. *International Journal of Reliability, Quality and Safety Engineering*, *23*(03), 1640005. https://doi.org/10.1142/S0218539316400052

Vaishnavi, S., & Sethukarasi, T. (2021). SybilWatch : A novel approach to detect Sybil attack in IoT based smart health care. *Journal of Ambient Intelligence and Humanized Computing*, *12*(6), 6199-6213. https://doi.org/10.1007/s12652-020-02189-3

Vennam, P., T. C., P., B. M., T., Kim, Y.-G., & B. N., P. K. (2021). Attacks and Preventive Measures on Video Surveillance Systems : A Review. *Applied Sciences*, *11*(12), 5571. https://doi.org/10.3390/app11125571

Walsh, D. (2021, août 29). *The major companies that accept Bitcoin and other cryptos as payment*. Euronews. https://www.euronews.com/next/2021/08/29/paying-with-cryptocurrencies-these-are-the-major-companies-that-accept-cryptos-as-payment

Yadav, S. A., Kumar, S. R., Sharma, S., & Singh, A. (2016). A review of possibilities and solutions of cyber attacks in smart grids. *2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH)*, 60-63. https://doi.org/10.1109/ICICCS.2016.7542359

Zhu, Z.-T., Yu, M.-H., & Riezebos, P. (2016). A research framework of smart education. *Smart Learning Environments*, *3*(1), 4. https://doi.org/10.1186/s40561-016-0026-2