A STUDY OF SMART CAMPUS ENVIRONMENT AND ITS SECURITY ATTACKS

Ghizlane Ikrissi, Tomader Mazri

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

KEY WORDS: Smart Campus, Internet of Things, RFID, Security Attacks, Smart Environment, Ubiquitous Computing, Smart Learning

ABSTRACT:

The smart campus is a sustainable and well-connected environment that aims to improve experience, efficiency and education. It uses a variety of interconnected components, smart applications and networked technologies to facilitate communication, make more efficient use of resources, improve performance, security and quality of campus services. However, as with many other smart environments, the smart campus is vulnerable to many security issues and threats that make it face many security-related challenges that limit its development. In our paper, we intend to provide an overview of smart campuses by highlighting the main applications and technologies used in this environment, presenting several vulnerabilities and susceptible attacks that affect data and information security in the smart campus. Moreover, we discuss the major challenges of smart campus and we conclude by overviewing some current security solutions to deal with campus security issues.

1. INTRODUCTION

Ubiquitous computing (ubicomp) summarizes the idea that computers can appear in multiple forms at anytime and anywhere. Ubicomp is also the idea of a physical word with many sensors, actuators, and other computational elements that can be found even within objects of our daily life and connected through a continuous network, so from this idea, the Smart Environment is developed (Friess et al., 2017). The term smart environment indicates the ability to autonomously obtain and apply knowledge in the surroundings (Ahmed et al., 2016). There certainly are many examples and applications of smart environment, such as smart home, smart cities, smart health, smart campus and more. In this paper, we will focus on the smart campus environment.

Smart campus refers to the devices, applications and technologies needed to create new experiences, improve efficiency and provide advanced applications and services to campus users who are students, staff, visitors and people performing multiple tasks in campus buildings (Muhamad et al., 2017). In general, developing a smart campus means successfully achieving certain objectives, such as providing very high-quality and intelligent services, improving environmental sustainability, reducing operational costs, making communication and education generally easier and better. So, the smart campus is not only about deploying smart platforms to effectively perform campus-related services but it is a broad concept that includes many electronic and physical objects that communicate and interact with each other.

Smart Campus is a smart city subset (Nathan et al., 2018). It is seen as a small city in certain aspects such as the number of functions, users, activities, and connections (Muhamad et al., 2017). It is similar to a smart city in the way it is organized, which revolves around six smart areas (Fernández-Caramés, Fraga-Lamas, 2019): smart governance, smart people, smart mobility, smart environment, smart living, smart economy. (Figure1)

Smart campus services provided may be similar to those provided by a smart city but adapted to campus needs (e.g. resource efficiency, energy/grid monitoring, mobility/transport services, user behaviour monitoring etc). Nevertheless, there are several differences with smart cities regarding the architectures and the technologies that can be applied to smart campuses. The campus size is smaller than the smart city size because actually, we can find many urban campuses in the city. Also, the number of devices required to be deployed is fewer than those needed in the smart city, which can reduce deployment costs (Fernández-Caramés, Fraga-Lamas, 2019).

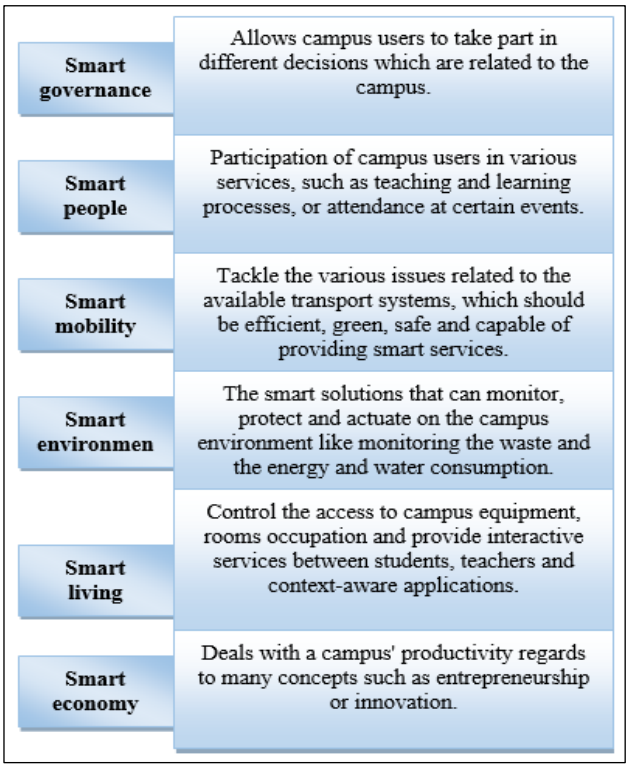

Figure 1. Smart Campus Areas

Many technologies are used in the smart campus development process, such as cloud computing, embedded computing, artificial intelligence, biometrics, IoT technologies that are widely used on smart campuses, and other smart applications. It also uses numerous devices (tablets, laptops, phones, etc.) and connected sensors and objects which are generally designed to perform simple tasks, and their components are relatively limited.

So, the integration of all these technologies and devices make smart campus face several vulnerabilities.

All these vulnerabilities can be exploited by an attacker to allow him to access and manipulate the system in order to perform unauthorized actions and many attacks that affect the confidentiality, integrity and availability of data within a campus system. therefore, ensuring security measures one of the key challenges facing smart campus.

The objective of this paper is to present an overview of smart campus and problems regarding information security in this smart environment. The content of the paper is organized as follows: In Section 2 we present the main application of smart campus. Section 3, describes the technology that proceeds services in the campus. The Vulnerabilities in Smart campus systems are considered in light of the information in Section 4. Section 5 points out the major susceptible attacks on the smart campus. In Section 6 we discuss the main challenges of smart campus. Conclusions are discussed in Section 7 by providing some solutions to encounter the security attacks into a smart campus.

2. SMART CAMPUS APPLICATIONS

Smart campus services are not restricted to the academic aspect, but also the campus' environmental, financial and social aspects based on the six areas mentioned above. In this section, we will present some potential applications of the smart campus.

2.1 Smart learning System

It refers to the use of smart mobile devices and web technologies in the learning system. This service enables lecturers and students to interact directly and indirectly in support of teaching activities (Muhamad et al., 2017). It offers real-time distance learning, automatic attendance monitoring, on-demand course delivery, cross-lecture and online materials, customized course programs, efficient library management and efficient laboratory services (Abuarqoub et al., 2017).

2.2 Smart Building

It is developed with various sensors as an important part of the building automation process. These sensors support the various capabilities of smart services such as temperature adjustment, humidity measurement, switching off of objects (lights, projectors) etc (Muhamad et al., 2017). Smart building services should also be able to generate reports to campus management, such as energy consumption reports, real-time warning, energy and space usage patterns etc.

2.3 Smart Payment Systems

It is a system that improves and facilitates payment services. The money is stored inside the student ID card and the payment is automatically debited when they perform any kind of service, such as reservation of meals, etc (Anirudh et al., 2017).

2.4 Smart Grid

Smart Grid is one of the smart environment area services. The management and deployment of energy on a smart campus are very important, that's why the smart grid is considered to be one of the key components of the Smart Campus (Ijaz et al., 2016). The main aim of this system is to improve energy consumption and reduce monthly bills, allow real-time load analysis on the power system, increase sustainability, energy conservation, enhance reliability and detect potential failures.

2.5 Waste and Water Management

In order to obtain a green environment, the campus has to manage water and waste properly and in real-time (Muhamad et al., 2017) by protecting the environment, detecting water pressure and leakage, detecting waste levels in conditions and optimizing the collection of waste, etc.

2.6 Smart parking system

It consists of cameras, sensors and other devices. These sensors can collect information about the vehicles in the car park and send this information via WIFI or Zigbee to its meter deployed in the nearby area (Anirudh et al., 2017). This system helps to manage the parking space efficiently and to reduce the traffic jams generally seen in front of Campus car parking (Anirudh et al., 2017).

2.7 Smart library System

This system is an intelligent campus application that enables remote control and speed management of the library. Smart libraries use library card with electrical tags, mobile phone and other physical objects (Muhamad et al., 2017). This electronic label (e.g. RFID) can improve several library services such as borrowing and returning the library books, as well as automatically recording the information of shelves, catalogues and books in the database without much human intervention (Anirudh et al., 2017).

2.8 Tracking, Security and Surveillance

This system helps to monitor users and devices inside the campus and track their location in the event of an emergency or evacuation. Sensors may also transmit information to various safety devices, such as motion detectors for the opening and closing of doors and windows, or safety triggering instruments (Anirudh et al., 2017).

3. SMART CAMPUS TECHNOLOGIES & CONNECTIVITY

The technology aims to better meet the needs of users and helps them in performing various tasks on campus. It also provides a high quality of campus services and facilitates communication. in this section, we will illustrate some technologies used in the smart campus:

3.1 Internet of Thing

IoT technology is a wide range of interconnected objects, such as sensors, actuators, digital machines, mobile phones, RFID tags, people and other things that communicate with each other via the Internet to make the system smart. In the smart campus system, this technology is designed to realize intelligent identification, monitoring and tracking. It is also used for automation, data management, green energy, etc.

3.2 Cloud Computing

Cloud computing is generally developed based on virtualization and distributed computing, parallel computing, grid computing

and powerful integrated computing. In the smart campus and other environments, databases and applications should be built on a cloud platform including service levels: PaaS, IaaS and SaaS (Muhamad et al., 2017). Cloud computing is a model, that allows access to services upon request (service on-demand), it can provide high performance, scalability and elasticity. It also offers high powerful data processing to be intelligently stored and used on the smart campus services.

3.3 Automatic Identification Technology

3.3.1 Radio Frequency Identification (RFID): is a technology that uses the radio frequency to communicate with identifiable objects or people in the smart campus. An RFID system consists of a reader, tag, and host computing (Fahmy et al., 2019). Generally, the specific address is given to the tags and then integrated with objects. They contain electronically stored information that can be read by the RFID reader, thus allowing for automatic real-time monitoring without the actual need for a human presence (Anirudh et al., 2017). This technology can also be used in smart campus applications for library management, attendance management, access control, etc.

3.3.2 Near Field Communication (NFC): can be seen as an RFID advancement that allows smartphones and other devices to communicate via radio signals. The idea of working is based on radio waves by bringing mobile phones closer to each other or by touching phones together (Anirudh et al., 2017).

3.3.3 Biometrics: is an automatic recognition of a person by using several metrics related to unique human characteristics. They are of two types: behavioural and biological or physiological characteristics. These two types are obtained by applying proper sensors and the typical features are used to obtain a biometric template in the authentication process (Ijaz et al., 2016).

3.4 Wireless Technology

3.4.1 WIFI: is an IEEE 802.11 standard that is increasingly used, especially in enterprises and campuses with the aim of providing internet access to many devices. WIFI is deployed all over the smart campus to support a huge number of WIFI connections and provide free internet access to users due to high performance, low-cost network and simple technical implementation (Garcia et al., 2018).

3.4.2 ZigBee: is based on the IEEE 802.15.4 standard. Generally, it is used to create personal area networks with applications and devices that require a long battery life, lower data rate and secured networking. So, it is often used in monitoring and control applications where data reliability, power-efficiency, and affordability are crucial. Comparing with other personal area networks, ZigBee is cheaper and simpler(Qadir et al., 2018).

3.5 Mobile technology

Mobile phones, tablets, laptops and other similar devices are becoming one of the most powerful devices used on campus and generally in daily life. This technology can be used in education to improve its quality, meet the needs of campus students and reduce costs (Muhamad et al., 2017). It offers a variety of capabilities to support smart campus services, including accessing the door to enter or exit the room using contactless technology, and developing mobile solutions that allow learning to take place anywhere and at any time, etc (Muhamad et al., 2017).

3.6 Smart Applications

These are a set of web and mobile applications that make the communication between devices on a smart campus easier, by acting an interface between users and devices to simplify sensing and communication (Nathan et al., 2018). They also include Machine to Machine applications that allow communication and information exchange between different devices on the campus without any human manual assistance (Anirudh et al., 2017).

4. SMART CAMPUS VULNERABILITIES

Vulnerabilities are a system, application or service flaws that allow an attacker to have access, take security controls, exploit the system and manipulate it in ways never intended by the developer (Williams et al., 2017).

On smart campus, there are many smart devices and connected components that are involved in diverse services. This increased number of smart devices is a vulnerability that can affect campus security because they can act as entry points of attack into the network. Furthermore, the large scale and complexity of the smart campus network make network monitoring and management extremely difficult (Aloul et al., 2012). Besides, the campus IoT devices and components are vulnerable to many internal and external threats because they are unable to support or implement a complex and robust security mechanism due to their limited resources, including low power, computing capabilities, limited battery power, memory, etc (Abomhara and Ien, 2015).

Software vulnerabilities can be found in operating systems, applications software, databases, communication protocols and device drivers (Abomhara and Ien, 2015). Examples of such software vulnerabilities include lack of ability to securely update the devices or maintain them up to date, lack of notification of security changes due to updates, lack of automatic update system and lack of firmware validation on the device, etc (Paul, 2019). Using unsafe default settings, passwords and default protocols without changing or modifying configurations are also vulnerabilities that allow unauthorized access to the system.
Most devices operate with human assistance, so the technical vulnerabilities usually arise due to human weaknesses, including lack of skills, resources and knowledge to manage and control the system, failure to understand the requirements and lack or poor communication between campus users (developers, staff, etc.). Furthermore, a real lack of qualified cybersecurity staff, absence of continuous training programs and security strategy would make all systems vulnerable and make easy for an attacker to gain access to the devices, control systems and steal data (Abomhara and Ien, 2015).

5. SMART CAMPUS SUSCEPTIBLE ATTACKS

The smart campus is based on a wide range of technologies and equipment including several unsecured devices, systems and applications that transmit information via unsafe media and use weak protocols such as HTTP, FTP, telnet, etc. The attackers can make use of these flaws to gain access to the systems, to retrieve sensitive data and to obtain confidential information for later manipulation (Rehman and Manickam, 2016). He can also damage the life of the devices and stop the functionality of the services. Some major possible attacks on smart campus are listed as follows:

5.1 Physical Attacks

This category of attacks focuses on the hardware devices of the smart campus system, such as controllers, RFID readers, sensors, and all other equipment that are vulnerable to different physical attacks, as well as attacks that harm the lifetime or functionality of smart campus hardware, are also included in this category (Andrea et al., 2015). Some of the physical attacks are described below:

5.1.1 Theft of devices: Campuses are packed with private and public devices (smartphones, laptops, tablets, cameras, etc.) that are deployed throughout the campus and may not be protected. As a result, the theft of these physical objects enables the attacker to gain physical access to the devices and then performs many attacks that violate the privacy of individuals and disrupts the availability and confidentiality of the systems (Aldairi and Tawalbeh, 2017).

5.1.2 Social Engineering: this attack aims to manipulate individuals to divulge confidential and sensitive data (Salahdine, Kaabouch, 2019). It is placed under the category of physical attacks because it is based on human interactions, which means that Social engineers physically interact with campus users to obtain valuable information, which may be used for malicious activities and purposes (Salahdine, Kaabouch, 2019). This type of attack is launched through direct contact with users, using campaign e-mails and phone calls.

5.1.3 Sleep Deprivation Attack: The smart campus uses a lot of IoT devices powered by replaceable batteries to extend their lifetime and ensure high performance, and they are programmed with sleep mode routines. The idea behind this attack is to maximize the power consumption of the sensor nodes in order to reduce their lifetime by keeping the devices awake, which will result in more power consumption and cause the nodes to shut down (Andrea et al., 2015).

5.1.4 Malicious Node Injection: In this case, the attacker physically inserts a new malicious node between two or more sensor nodes to be used as a normal node as shown in (Figure2) to modify, capture, retrieve, process and redirect the incorrect information to the other nodes (Deogirikar, Vidhate, 2017). This attack aims to generate abnormal behaviours on the functionality and services of the campus or to give the attacker full control of the target system.

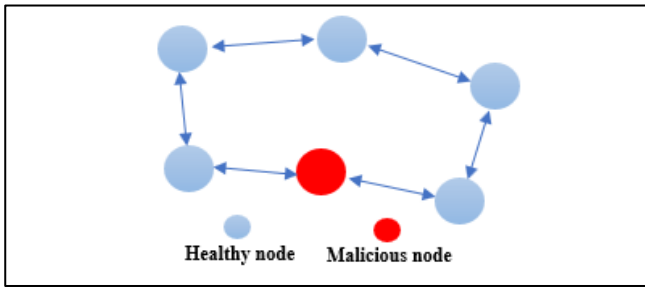

Figure 2. Malicious node injection attack

5.2 Software Attacks

Software attacks exploit the smart campus system by using viruses, malicious programs and scripts that can deny services, steal information, tamper with data, and even damage the smart devices (Andrea et al., 2015). Software attacks are the main source of security vulnerabilities for any computer system and they include:

5.2.1 Virus, Worms, Trojan Horse, Spyware and Aware: are malicious software (malware) used by an attacker to infect the campus system. This malware may spread through downloading files from the Internet, email attachments, etc., and some of them may replicate themselves without any human action or tampering with user's data without the user even knowing it (Deogirikar, Vidhate, 2017).

5.3 Encryption Attacks

This type of attacks is a dangerous threat to the security and privacy of the cryptographic modules. The attacker aims to discover and destroy the cipher key used in the encryption and decryption of protocols, modules, data and devices using special techniques such as:

5.3.1 Cryptanalysis Attacks: this type of attacks is used to break the cryptographic security system by detecting the encryption key used and then gain access to encrypted messages. Various techniques of cryptanalysis attacks are available, such as differential cryptanalysis attacks, cypher-text attacks, Integral cryptanalysis attacks, dictionary attacks, etc (Hamid et al., 2019).

5.3.2 Side-channel Attacks: the attacker collects information about what devices do when performing cryptographic operations, such as the time needed to complete the operation, power consumption, electromagnetic radiation, faults frequency (Figure3), and then uses this side-channel information to detect the encryption key (Deogirikar, Vidhate, 2017).

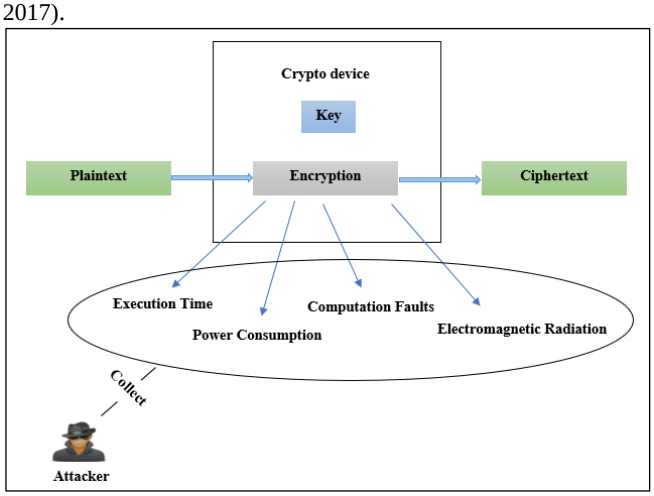

Figure 3. Side-channel attack

5.4 Data privacy attacks

Smart Campus Contains a wide range of devices and applications that produce different types of data that are one of the most important resources on campus. The protection of such data privacy has, therefore, become an important requirement due to the large volume of information that can be easily accessed through remote access mechanisms (Abomhara, Ien, 2015). Data attacks are generally identified as all possible attacks and threats that target the use, collection, deletion and storage of data. Some of these threats are as follows:

5.4.1 Data Breaches: The data breach is the leakage of sensitive campus data to unauthorized persons (Kazim, Zhu, 2015). A data breach occurs as a result of attacks by malicious users accessing in an unauthorized way to the data source on the smart campus by using a variety of techniques to infiltrate data and obtain sensitive information.

5.4.2 Data Loss: it can happen if the data does not have enough security, consequently, that the data can be easily compromised. Data deletion, data corruption, power failures, storage system failures are the most common reason for data loss (Farahat et al., 2019)

5.4.3 Account or Service Hijacking: Account hijacking occurs when the criminal obtains and steals the user credentials to get access to his account, data or other (Figure4). These stolen credentials can be used to access and compromise campus services or modify data, etc (Kazim, Zhu, 2015).

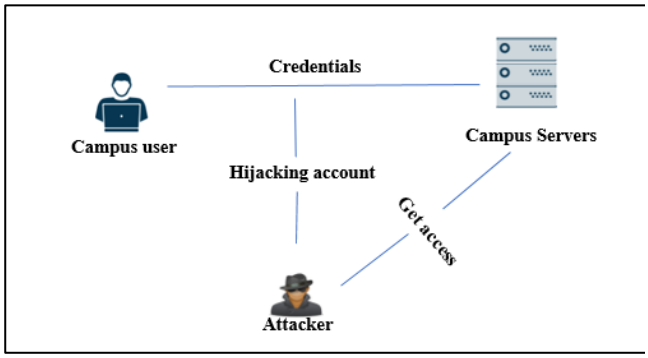

Figure 4. Account hijacking attack

5.5 Network Attacks

Various smart campus objects are linked together through the use of many communication technologies such as WIFI, 4 G, RFID, GSM and others (Aldairi, Tawalbeh, 2017). Due to unauthorized access or network mapping to gather vulnerability information, these technologies may be exposed to several network threats and attacks that could lead to privacy and confidentiality (Figure 5). Some of these network attacks are as follows:

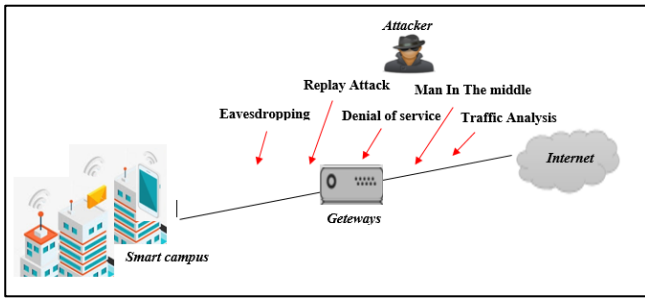

Figure 5. Network attacks in the smart campus

5.5.1 Traffic Analysis Attacks: is based on the interception and examination of network traffic to deduce and gain important information from patterns of communication. In other words, the attacker listens to network communication in order to collect and analyse traffic to determine certain network information which will be used in his attacks, such as the location of key nodes, the routing structure, and even the patterns of application behaviour (Andrea et al., 2015).

5.5.2 Replay Attack: is a network attack in which the attacker receives and transmits data exchange between two legal parties as an authorized element, which leads the participants to believe that the transmission of data has been completed. The intruder can capture and store a copy of a legitimate request for service from a device on the smart campus network. Then, replay it to get services that are only authorized by the smart campus users (Rehman, Manickam, 2016).

5.5.3 Eavesdropping: This attack is against the confidentiality of smart campus environments and it is the most commonly recognized security threat in open systems (Rehman, Manickam, 2016). The idea behind Eavesdropping is that an attacker can monitor all data traffic on smart campus networks without the knowledge of authorized users (Rehman, Manickam, 2016). If we take the example of the RFID system, the readers and tags are wirelessly connected and communicated without any human intervention or encryption technique. As a result, there is a possibility that their communication medium could be eavesdropped to obtain sensitive information and data from RFID tags (Hezam et al., 2018).

5.5.4 Denial of service: in Denial of Service Attack, the attacker aims to make a network service unavailable to its intended users or to reduce the accessibility of such campus services (Rehman, Manickam, 2016). An attacker may send limitless messages or traffic to servers and devices connected to the Internet to over-burden their services and make them inaccessible to users, as well as to restrict traffic transmitted by wired or wireless means inside the smart campus (Rehman, Manickam, 2016).

Table 1 shows a brief description of different smart campus attacks.

Attacks	Description
Physical attacks	Attacks targeting hardware components such as device theft or malicious node injection.
Software Attacks	Exploits systems by using malicious software: worms, viruses etc.
Encryption Attacks	Attacks that use several description techniques to obtain cipher key.
Data privacy attacks	Attacks in which sensitive and protected data are modified, copied or lost.
Network attacks	Unauthorized access or mapping of the campus network to obtain sensitive information.

Table 1. Smart campus attacks

6. SMART CAMPUS CHALLENGES

Like any emerging field, the smart campus faces many real challenges that need to be noted during the development of such campus because they may Affect the evolutions of its areas (Figure1). The implementation costs are one of these challenges because making a campus "smart" required a huge number of smart devices and technologies that necessitate a large investment of money. Also, ensuring the sustainability of these technologies requires high energy consumption, and this is another campus challenge (Ghosal, Halder, 2018).

Moreover, the campus can cover a large area where many users can request several services, which require the transmission of a large amount of data, but there, the quality of the services may be missing (Kamble et al., 2018). Therefore, Certain quality measures must be taken to provide better services (Kamble et al., 2018), to ensure proper functioning and performance of the various campus applications and to adapt all that to the number of campus users.

The smart campus uses several sensors, actuators, and other connected devices which need to be thoroughly investigated (Alghamdi, Shetty, 2016), also it can be very difficult to configure them manually, and that may cause many human faults. So, developing a new system to automatically configure, manage and update all campus system and devices, while maintaining security measures is a real challenge that needs a serious priority.

As mentioned before, the smart campus is highly vulnerable to several cybersecurity threats, so there is a need to take proper security mechanisms to address these attacks (Kamble et al., 2018). Many reasons, such as a heterogeneous environment, the use of some low-energy devices, adopting many technologies, a larger geographical area and intensive communication, make it very difficult to meet security and privacy requirements, and this may be a major challenge for smart campuses (Alghamdi, Shetty, 2016).

7. CONCLUSION

The smart campus is an environment that improves students' and staff experience, ensures service quality and energy efficiency, provides a safe and sustainable environment. It's enhanced by a wide range of smart devices and modern technologies which allows it to be transformed into a digital area.

A general overview of the smart campus environment and its communication technologies used has been introduced in this paper. Besides, several vulnerabilities and security attacks on the smart campus have been investigated. These security issues may put campus privacy and sensitive data at risk, so, there is a need to implement some security solutions and measures based on the primary security goals including authentication, confidentiality, integrity and availability to successfully resolve certain issues and implement effective smart campus security.

The main security mechanisms for making smart campus networks and data secures should be applied by encrypting data with a secret key using powerful cryptographic algorithms and protocols, as a result, even when the exchanged data over the campus network has eavesdropped, the attacker will not be able to view or to access the content of the transited traffic and messages.

We can also protect data integrity through a security strategy based on tracking logging, accesses on all systems, monitor logs and generated events. This will allow us to view and monitor all changes and have the history of transactions applied on the system, so, we can easily determine the origin of an unauthorized update of the data.

Furthermore, it is necessary to test the availability of the system regularly by checking devices and applications status, have a redundancy system of telecommunications lines, have a reliable backup system, as well as hosting data in several remote datacentres.

Additionally, the use of systems, databases and applications hardening is mandatory to ensure the security of configuration and system updates in order to avoid any vulnerabilities associated with the use of an unsafe package, minimize system exposure to threats and mitigate potential risks.

Also, another very important element that needs to be adopted and applied on smart campus is the management of security audits, the planning of regular vulnerability tests with the internal and external network and system scans, as well as penetration tests.

In parallel with all that the use of intrusion detection systems (IDS) and Intrusion Prevention Systems (IPS) is required to detect and block threats and intrusion attempts with malicious actions, also, it is necessary to deploy Unified Threat management firewalls (UTM) and web application firewall (WAF) with advanced features such as DLP (data loss protection), APT Blocker, Antivirus, proxies and others to control traffic and secure the network, the systems and server databases and applications.

REFERENCES

Abomhara, M., Ien, G.M.K., 2015. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. Journal of Cyber Security and Mobility 4, 65–88. https://doi.org/10.13052/jcsm2245-1439.414

Abuarqoub, A., Abusaimeh, H., Hammoudeh, M., Uliyan, M., Abu-Hashem, M., Murad, S., Al-Jarrah, M., Alfayez, F., 2017. A Survey on Internet of Things Enabled Smart Campus Applications. pp. 1–7. https://doi.org/10.1145/3102304.3109810

Ahmed, E., Yaqoob, I., Gani, A., Imran, M., Guizani, M., 2016. Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges. IEEE Wireless Communications 23, 10–16. https://doi.org/10.1109/MWC.2016.7721736

Aldairi, A., Tawalbeh, L., 2017. Cyber Security Attacks on Smart Cities and Associated Mobile Technologies.

Alghamdi, A., Shetty, S., 2016. Survey Toward a Smart Campus Using the Internet of Things. pp. 235–239. https://doi.org/10.1109/FiCloud.2016.41

Aloul, F., Al-Ali, A.R., Al-Dalky, R., Al-Mardini, M., El-Hajj, W., 2012. Smart Grid Security: Threats, Vulnerabilities and Solutions. International Journal of Smart Grid and Clean Energy 1, 1–6. https://doi.org/10.12720/sgce.1.1.1-6

Andrea, I., Chrysostomou, C., Hadjichristofi, G., 2015. Internet of Things: Security vulnerabilities and challenges. pp. 180–187. https://doi.org/10.1109/ISCC.2015.7405513

Anirudh, A., Pandey, V.K., Sodhi, J.S., Bagga, T., 2017. Next generation indian campuses going SMART. International Journal of Applied Business and Economic Research 15, 385–398.

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

Fahmy, A., Altaf, H., Al Nabulsi, A., Al-Ali, A., Aburukba, R., 2019. Role of RFID Technology in Smart City Applications, in: 2019 International Conference on Communications, Signal Processing, and Their Applications (ICCSPA). Presented at the 2019 International Conference on Communications, Signal Processing, and their Applications (ICCSPA), pp. 1–6. https://doi.org/10.1109/ICCSPA.2019.8713622

Farahat, I.S., Tolba, A.S., Elhoseny, M., Eladrosy, W., 2019. Data Security and Challenges in Smart Cities, in: Hassanien, A.E., Elhoseny, M., Ahmed, S.H., Singh, A.K. (Eds.), Security in Smart Cities: Models, Applications, and Challenges, Lecture Notes in Intelligent Transportation and Infrastructure. Springer International Publishing, Cham, pp. 117–142. https://doi.org/10.1007/978-3-030-01560-2_6

Fernández-Caramés, T., Fraga-Lamas, P., 2019. Towards Next Generation Teaching, Learning, and Context-Aware Applications for Higher Education: A Review on Blockchain, IoT, Fog and Edge
Computing Enabled Smart Campuses and Universities. Applied Sciences 9, 4479. https://doi.org/10.3390/app9214479

Friess, K., Herwig, P., Leo, A., 2017. CLASSIFICATION OF SCENARIOS WITH A HUMAN WEARABLE-ENVIRONMENT BY THE KIND OF INTERACTION AND REACTION OF THE SMART ENVIRONMENTS 9, 2017.

Garcia, L., Jimenez, J., Taha, M., Lloret, J., 2018. Wireless Technologies for IoT in Smart Cities. Network Protocols and Algorithms 10, 23. https://doi.org/10.5296/npa.v10i1.12798

Ghosal, A., Halder, S., 2018. Building Intelligent Systems for Smart Cities: Issues, Challenges and Approaches. pp. 107–125. https://doi.org/10.1007/978-3-319-76669-0_5

Hamid, B., Jhanjhi, N., Humayun, M., Khan, A., Alsayat, A., 2019. Cyber Security Issues and Challenges for Smart Cities: A survey, in: 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS). Presented at the 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), pp. 1–7. https://doi.org/10.1109/MACS48846.2019.9024768

Hezam, A., Konstantas, D., Mahyoub, M., 2018. A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Mode. International Journal of Advanced Computer Science and Applications Vol. 9. https://doi.org/10.14569/IJACSA.2018.090349

Ijaz, S., Shah, M., Khan, A., Ahmed, M., 2016. Smart Cities: A Survey on Security Concerns. International Journal of Advanced Computer Science and Applications 7. https://doi.org/10.14569/IJACSA.2016.070277

Kamble, S., Borkar, M., Nakhwa, A., Mukadam, S., Mayekar, S., 2018. An IoT Based Smart Campus 4.

Kazim, M., Zhu, S.Y., 2015. A survey on top security threats in cloud computing. International Journal of Advanced Computer Science and Applications 6. https://doi.org/10.14569/IJACSA.2015.060316

Muhamad, W., Kurniawan, N.B., Suhardi, Yazid, S., 2017. Smart campus features, technologies, and applications: A systematic literature review, in: 2017 International Conference on Information Technology Systems and Innovation (ICITSI). Presented at the 2017 International Conference on Information Technology Systems and Innovation (ICITSI), pp. 384–391. https://doi.org/10.1109/ICITSI.2017.8267975

Nathan, N., Gambo, Y., Joel, N., Davwar, P., 2018. Smart Technologies for Smart Campus Information System. Asian Journal of Research in Computer Science 1–7. https://doi.org/10.9734/ajrcos/2018/v2i228738

Paul, F., 2019. Top 10 IoT vulnerabilities [WWW Document]. Network World. URL https://www.networkworld.com/article/3332032/top-10-iot-vulnerabilities.html (accessed 4.22.20).

Qadir, Z., Tafadzwa, V., Rashid, H., Batunlu, C., 2018. Smart Solar Micro-Grid Using ZigBee and Related Security Challenges, in: 2018 18th Mediterranean Microwave Symposium (MMS).Presented at the 2018 18th Mediterranean Microwave Symposium (MMS), pp. 299–302. https://doi.org/10.1109/MMS.2018.8611886

Rehman, S., Manickam, S., 2016. A Study of Smart Home Environment and it's Security Threats. International Journal of Reliability, Quality and Safety Engineering 23. https://doi.org/10.1142/S0218539316400052
Salahdine, F., Kaabouch, N., 2019. Social Engineering Attacks: A Survey. Future Internet 11, 89. https://doi.org/10.3390/fi11040089

Williams, R., McMahon, E., Samtani, S., Patton, M., Chen, H., 2017. Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach, in: 2017 IEEE International Conference on Intelligence and Security Informatics (ISI). Presented at the 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), pp. 179–181. https://doi.org/10.1109/ISI.2017.8004904