

Towards secure smart campus: security requirements, attacks and counter measures

Ahmed Srhir, Tomader Mazri, Mohammed Benbrahim

Department of Electrical Engineering, Networks, and Telecommunication Systems, National School of Applied Sciences, Ibn Tofail University, Kenitra, Maroco

Article Info

Article history:

Received Jun 23, 2023

Revised Jul 20, 2023

Accepted Jul 27, 2023

Keywords:

Attacks

Internet of thing

Security issues

Smart campus

Smart system

Vulnerabilities

ABSTRACT

The internet of things (IoT) has the potential to significantly impact growth due to the technological revolution, widespread dissemination of information, and emergence of events. Intelligent housing, urban centers, and educational systems are all forms of intelligence. The IoT has garnered significant attention from researchers, who claim that this technology will play a pivotal role in determining the future of the Internet, as per the reports of Cisco Inc., in this context, the concept of a smart campus refers to the establishment of a durable and interconnected setting that enhances learning, efficiency, and the overall living experience. Similar to other intelligent environments, the smart campus is susceptible to a variety of risks and threats this situation presents important security-related challenges that have an influence on the advancement of the campus. This article presents an overview of intelligent campuses by emphasizing the primary applications and technologies utilized. It provides an examination and evaluation of the primary security concerns associated with smart campuses, classified based on their respective types and levels of significance, and determines the security requirements, current threats and attacks, and the state of the art in terms of architectural solutions and the prevention of security vulnerabilities.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Ahmed Srhir

Department of Electrical Engineering

Networks and Telecommunication Systems National School of Applied Sciences, Ibn Tofail University

Kenitra, Maroco

Email: ahmed.srhir1@uit.ac.ma

1. INTRODUCTION

The integration of the internet of things (IoT) is a fundamental aspect of the smart campus, and its implementation is an unavoidable eventuality [1]. The IoT, also known as the IoT, is a communication paradigm that has gained significant traction due to its capacity to link a diverse range of objects to the internet. The aforementioned items encompass a range of technologies including sensors, safety mechanisms, alarm systems, unmanned aerial vehicles, automated machines, household appliances, intelligent power grids, office machinery, and additional devices. The IoT is a nascent field that requires the implementation of various applications and standardization measures, such as home automation, water and waste control, traffic control, smart vehicles, smart campus, and smart grids, among others [2].

A smart campus is a campus environment that is equipped with the technology and infrastructure to support and enhance the teaching process, research, and student experience. Students, stakeholders, and the surrounding environment that communicate intelligently with the campus constitute a smart campus [3]. The smart campus is characterized by three approaches [4], [5]: technology-driven, adoption of the smart city concept, and implementation of an organization or business process, it's referring to both an ecosystem and the

main standards that are related to “smart campus” in particular. Associated applications, utilities, and use cases are included in this category [6], [7]: i) education, ii) energy, iii) urban planning, iv) healthcare, and v) transport. Educational institutions are increasingly embracing the idea of a “smart campus” which aims to improve communication, efficiency, and safety among students, staff, and faculty by utilizing the most recent technologies. However, the adoption of these technologies may also entail security risks that must be considered. The problem addressed in this article focuses on security issues on smart campuses, where IoT devices, cloud computing, and wireless technologies are transforming networked ecosystems and environments. Smart campuses may be susceptible to various types of threats, including breaches of data confidentiality, physical security breaches, network security breaches, and challenges related to the integration of legacy systems. Understanding security requirements, potential attacks, and countermeasures is crucial for protecting sensitive data and infrastructure.

Extensive research has been conducted to address security challenges in the IoT ecosystem paradigm and smart environment. Certain methodologies prioritize the resolution of security concerns within a particular layer, while others aim to provide comprehensive end-to-end security for the entire IoT layer. Security issues are classified based on application, architecture, communication, and data, with traditional layered designs differing from the suggested topology for IoT security [8] subsequently, the threats posed by the hardware, network, and application components are examined. Alzoubi *et al.* [9] discuss security challenges in fog computing, privacy, and blockchain technology for low latency IoT applications. Granjal *et al.* [10] examines security risks with IoT protocol definitions, while the research in [11] reviews IoT privacy, security, access control, confidentiality contributions, and cross-software security. Atiqur *et al.* [12] present an overview of IoT privacy preservation strategies, highlighting secure multi-party computations and attribute-based access control mechanisms. Additionally, Zhou *et al.* [13] examine security risks in cloud-based IoT systems, including key management, node compromise, identity and location privacy, and node compromise. Zhang *et al.* [14] highlight security concerns in IoT, including lightweight cryptographic protocols, privacy, unique object identification, authentication, authorization mechanisms, malware threats, and software susceptibility.

While these contributions provide valuable information, there are still unresolved issues and areas requiring improvement to guarantee security in the overall IoT as well as on smart campuses. In this context, safeguarding the privacy of individuals and sensitive data is of paramount importance. Physical security systems are crucial in ensuring that only authorized individuals have access to sensitive areas. The security of networks is also a crucial element of smart campus security, as wireless networks are utilized to connect devices and provide access to the internet. Due to a lack of adequate security, these networks may be exposed to vulnerabilities that pirates may exploit, which could result in the compromise of sensitive data or the disruption of campus activities. For this purpose, the educational institutions must pay particular attention to security in the context of the smart campus, implement best practices in terms of security, and conduct regular risk audits to identify potential vulnerabilities and ensure that systems are secured against known threats. In order to guarantee the security of a smart campus, it is imperative to prioritize the security of the IoT technologies that are utilized or implemented [15], [16]. This paper presents a comprehensive examination of security methodologies and prerequisites, potential threats and risks, and recommended preventative measures to achieve optimal security. Compared to previously published survey studies, the following are our primary contributions and methodologies:

- Parametric analysis of security concerns associated with IoT applications and domains, with a focus on the smart campus and their compatibility with potential IoT solutions.
- Classification and categorization of smart campus security difficulties with respect to tiers, as well as the security requirements and solutions used.
- Potential perspectives providing pragmatic resolutions to the challenges of smart campus security in the context of the IoT and providing practical solutions to enhance the overall security level on smart campuses.

The subsequent sections of the manuscript are structured in the following manner: The section 2 explains the various applications of the IoT, including its implementation in the context of smart campuses. In section 3, the main security requirements and issues for smart campuses are categorized. It also explores common security threats faced by smart campuses, including attack scenarios and schematizations for each identified attack. In section 4 provides an analysis of different types of attacks, their fundamental characteristics, and their nature, and presents a map of possible remedies for mitigating these attacks, while section 5 concludes the paper.

2. IOT APPLICATIONS

The IoT is a technological revolution that connects physical objects to the internet, enabling them to exchange data and communicate with each other. This interconnection offers immense potential for improving

our daily lives, transforming businesses, and opening up new opportunities in a variety of fields. IoT applications cover a wide range of sectors, offering innovative solutions that simplify tasks, optimize processes, and create smarter, more efficient environments. In this section, we will provide an overview of the various applications of the IoT, describing each application area and including how it is employed in the context of the smart campus.

2.1. IoT applications domaine

The IoT has the potential to be utilized in a variety of industries, such as home automation, healthcare, industrial applications, transportation, agriculture, smart cities, energy production systems, and other related functions. The advancement of technology and the expansion of the IoT may lead to novel applications and use cases in the future.

The applications of the IoT are multifaceted and extend to a range of sectors such as healthcare, manufacturing, transportation, agriculture, and others. The main applications of the IoT are examined, as shown in Figure 1:

- Smart city: Smart cities are characterized as metropolitan regions that employ information and communication technology to raise the standard of living for their citizens, make the most use of their resources, and simplify interactions different city actors. Smart street lighting, smart surveillance, smart parking, and waste and water management are all examples of IoT-based smart city solutions [17].

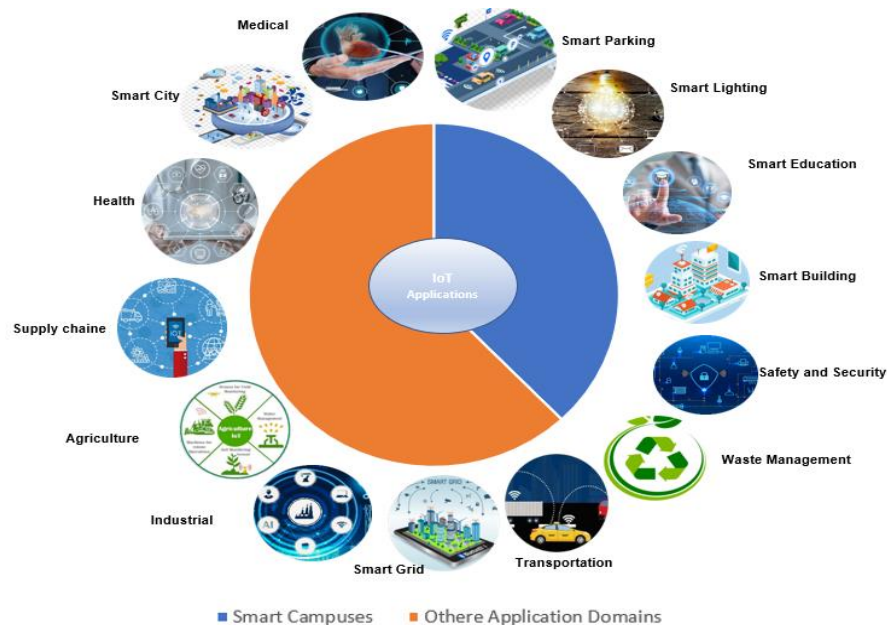


Figure 1. Major IoT application areas

- Manufacturing industry: IoT sensors may be used to track machinery and equipment, enhancing performance and reducing downtime.
- Healthcare: The domain of smart healthcare focuses on the comprehensive health considerations of the campus community. To provide information on the state of health, offer proactive and preventative healthcare services, and maintain records of health status, an intelligent system is built [18]. Remote control system enables online appointment scheduling for doctors, saving time and effort [3].
- Transportation: Real-time traffic updates, improved route planning, and increased safety may all be achieved with IoT-enabled cars and infrastructure.
- Smart grid: IoT sensors may be used to track energy use, improve efficiency, and save expenses.the implementation of a smart grid presents a potential for the utilization of novel information and communication technologies (ICTs) to transform the electrical power system [19].
- Smart supply chain: A smart supply chain is an integration of advanced technologies and data analytics to optimize the flow of goods and services from origin to consumption. It aims to improve efficiency, transparency, and sustainability by leveraging real-time data, automation, and artificial intelligence.

- Smart farming: IoT technology can optimize resource utilization and increase efficiency, resulting in reduced waste and improved productivity for farmers.

Technology advancements, internet connectivity, smart home adoption, industrial IoT applications, and integration in industries like healthcare, agriculture, and transportation have all contributed to the IoT significant growth in recent years. This evolution is expected to continue as new technologies develop and IoT devices continue to evolve. According to Alam [20], the estimated number of IoT-connected devices is predicted to exceed 75 billion by 2025, based on statistics' projections and the current rate of expansion, as illustrated in Figure 2.

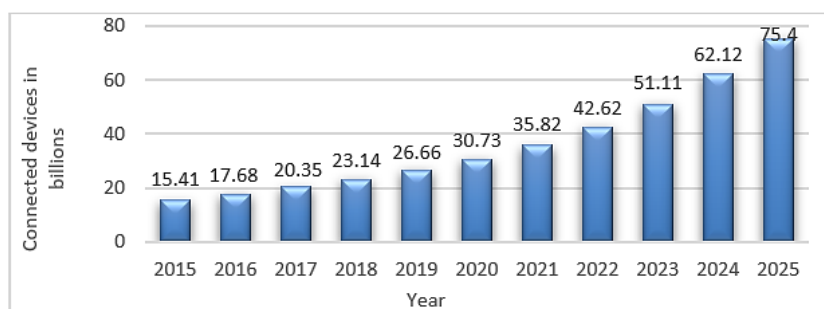


Figure 2. IoT connected devices estimated by 2025

2.2. IoT in smart campus

IoT applications are being used more and more on smart campuses to increase operational effectiveness, improve service quality, and enhance the user experience for teachers, staff, and students. The current research on smart campuses may be divided into four main categories: intelligent buildings, an intelligent campus network, an educational environment, and other applications. The areas of a smart campus are depicted in Figure 1, along with several examples of IoT applications, as shown in:

- Smart lighting: IoT-enabled lighting systems may modify the brightness and color of the lights automatically depending on the number of occupants in the space, the time of day, and the quantity of available natural light. This enhances passenger comfort while reducing energy usage.
- Smart parking: IoT-enabled parking systems may make it simple and quick for drivers to identify open places, easing traffic congestion and enhancing the parking experience in general. A central system may show real-time availability information to drivers after receiving the information from sensors put in parking lots that can identify the presence of automobiles.
- Smart building management: IoT sensors can be deployed all across the campus to keep an eye on things like temperature, humidity, air quality, and energy usage. This information may be utilized to enhance occupant comfort, optimize heating, ventilation, and air conditioning (HVAC) systems, and cut down on energy waste [21].
- Safety and security: By offering real-time monitoring of video feeds, access control mechanisms, and intrusion detection sensors, IoT-enabled security systems may increase campus safety. Machine learning algorithms may be used to evaluate the data from these devices to detect possible dangers and automatically notify security staff [22].
- Smart waste management: IoT sensors may be used to monitor trash cans all over a campus and notify maintenance staff when they need to be emptied. As a consequence, fewer pickups are needed, which saves money and has a less negative impact on the environment. Several recent publications in the field of waste management propose the implementation of sensor technology at waste bins and collection trucks to gather real-time data for analysis [23].
- Smart campus transportation: By providing real-time data on vehicle whereabouts, arrival times, and traffic conditions, IoT-enabled transportation systems can increase the effectiveness of campus transportation. For students, instructors, and staff, this information may be utilized to streamline routes and shorten wait times. It may also be used to monitor traffic dynamics, such as road map development, real-time traffic flow monitoring, traffic congestion prediction, traffic accident detection, incorrect driving behavior alerts, and intelligent navigation [24].
- Smart education: The goal of intelligent education is to improve teaching and learning in universities, primary schools, colleges, and high schools by modernizing network infrastructure, data processing, and storage, as well as by using technological platforms, supporting students' independent learning using an

“e-learning platform” [3], the creation and recording of courses as well as instructional and pedagogical content via a “smart classroom” [25], developing a variety of teaching and learning methods that are not constrained by geography or time, and offering assessments based on students’ proficiency in learning. Several academic institutions have implemented the virtual learning environment (VLE) system within their campus premises to improve favorable attitudes towards knowledge acquisition and promote active learning within the campus area [26].

3. RESEARCH METHOD

In this section, an overview of smart campus design and security requirements for IoT deployment and systems is discussed and provided, focusing on data confidentiality, integrity, availability, authentication, and authorization. It also addresses security threats and challenges specific to IoT systems on smart campuses. The text highlights the potential impact of threats and attacks on data confidentiality, integrity, and availability. It also covers prevalent security threats encountered by smart campuses, including various attack scenarios and schematizations of each attack.

3.1. Security requirement for smart campus

The development of the smart campus is among the innovative initiatives underway at the university. The smart campus infrastructure is a subject of significant consideration in its development. In light of this, we propose a technical architecture for the smart campus and recommend a local operational model. In order to ensure adequate campus security, it is necessary to establish a convergence infrastructure [27] that comprehensively addresses all relevant aspects and satisfies the requisite security standards. The smart campus architecture, as depicted in Figure 3, covers three fundamental areas of a smart campus:

- The concept of smart education involves the integration of various technological components such as e-learning, radio frequency identification (RFID) tags, and virtual classrooms to create a comprehensive educational system.
- Smart parking is a system that offers location tracking information for vehicles and provides details about the availability of parking spaces. This technology has received substantial research in the literature [28].
- The smart building is a comprehensive system that offers insights into the monitoring of building temperature, power, and illumination systems.

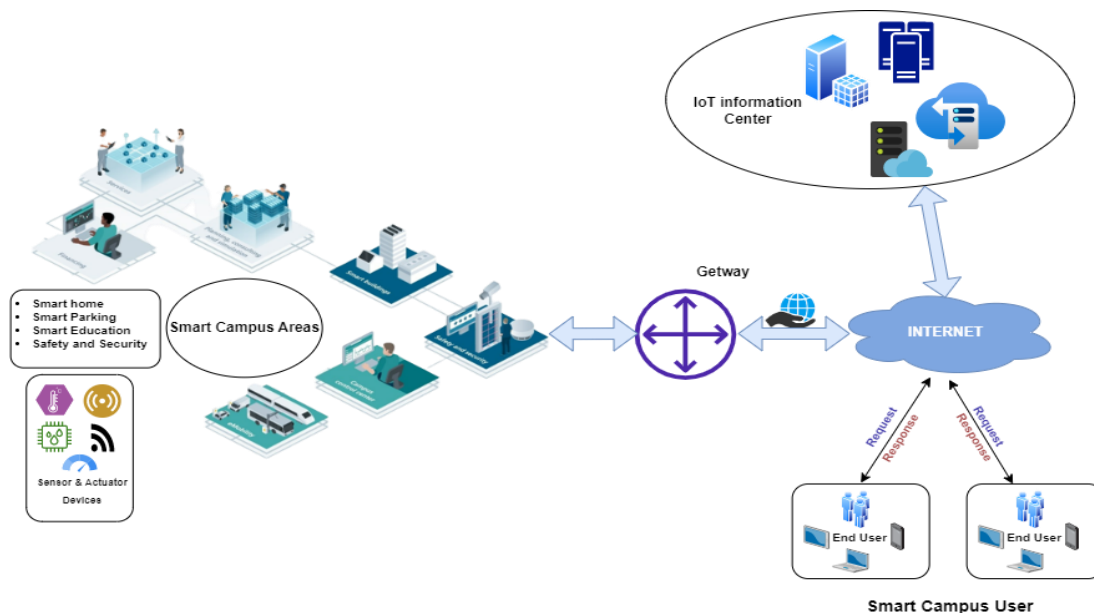


Figure 3. Smart campus design

3.1.1. Security requirement for IoT deployment

The deployment of a large-scale IoT infrastructure presents a significant risk as it exposes numerous devices and networks to potential vulnerabilities. The establishment of security requirements in the deployment

of IoT is imperative in order to safeguard sensitive data, protect user privacy, and maintain service availability. In this context, the protection of data, systems, and users against cyber threats is of paramount importance in guaranteeing the comprehensive security of the implementation architecture of the IoT on smart campuses. The implementation of certain security measures, as described in Figure 4, can prove pivotal in safeguarding against potential threats in IoT deployment.

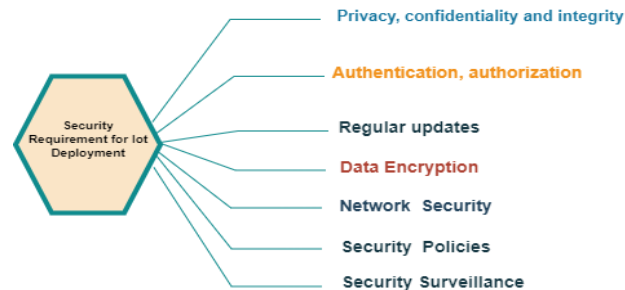


Figure 4. Security requirement for IoT deployment

- Privacy, confidentiality and integrity: Organizations, including smart campuses, must address privacy, confidentiality, and integrity requirements to protect sensitive information and maintain trust with stakeholders. Privacy measures include data minimization, consent, anonymization, access controls, and privacy policies. Confidentiality measures include encryption, access controls, secure communication, and data segregation. Integrity measures ensure data accuracy, completeness, and consistency throughout its lifecycle.
- Authentication and authorization: All IoT devices, sensors, gateways, and users must meet authentication and authorization procedures prior to accessing campus systems and data. The authentication and authorization protocols, such as OAuth, OpenID connect, and security assertion markup language (SAML), can be employed to ensure secure access.
- Data encryption: Data in transit and at rest must be encrypted to protect against interception or theft attacks. Encryption protocols such as secure sockets layer (SSL)/transport layer security (TLS), advanced encryption standard (AES), and Rivest-Shamir-Adleman (RSA) can be utilized for safeguarding data.
- Network security: The security of networks is a crucial aspect that must be taken into consideration during the design phase of communication networks. The networks should be designed in a manner that guarantees secure and reliable connectivity. Various security protocols, including Wi-Fi Protected Access 2 (WPA2), 802.1X, and virtual private networks (VPN), can be employed to enhance the security of computer networks.
- Security surveillance: the monitoring of security is facilitated through the use of security surveillance systems including firewalls, intrusion prevention systems (IPS), and security information and management of events systems (SIEM). These systems are capable of monitoring suspicious activities and detecting potential attacks.
- Regular updates of operating systems, applications, and security software can aid in eliminating known vulnerabilities and enhancing overall security.
- Security policies: The implementation of clear security policies, user training and awareness, continuous security monitoring, and system maintenance are crucial in reducing the risks of cyberattacks and ensuring the protection of data and users on campus.

3.2. IoT security issues, privacy, and threats

Smart campuses are becoming increasingly connected and automated, offering benefits such as cost optimization, improved student and staff experiences, and operational efficiency. However, this also entails challenges in terms of cybersecurity, as interconnected infrastructures are more susceptible to attacks. Smart campuses face a range of security threats, including distributed denial of service (DDoS) attacks, phishing attacks, ransomware, intrusions, and data breaches [29]. They also store a significant amount of sensitive data, including students' personal information, medical records, and research data, making them particularly attractive to cybercriminals.

The safeguarding of smart campuses necessitates an exhaustive approach to cybersecurity, encompassing the establishment of security policies and procedures, as well as the implementation of technical security measures such as network monitoring, data security, physical security, and IoT device protection.

Institutions are also required to raise awareness among users regarding appropriate information security practices and train their personnel in detecting and responding to security incidents. In summary, smart campuses must address the challenge of securing their infrastructure while continuing to provide an optimal user experience.

3.2.1. Security threats and attacks in smart campus

Smart campus security attacks can be categorized into different types based on their characteristics and consequences. Presented is a comprehensive categorization of security breaches that may occur within the context of smart campuses.

- Physical attacks: The smart campus is susceptible to physical attacks that aim to compromise its physical infrastructure, which encompasses a range of components such as servers, data centers, access points, and IoT devices [30]. The aforementioned attacks have the potential to encompass various forms of malicious activity such as theft, vandalism, tampering, or unauthorized access to areas of high sensitivity.
- Network attacks: The objective of these attacks is to disrupt communication, intercept data, or gain unauthorized access by targeting the network infrastructure of the smart campus [31]. Examples include network scanning, port scanning, packet sniffing, and man-in-the-middle attacks as illustrated in Figure 5.

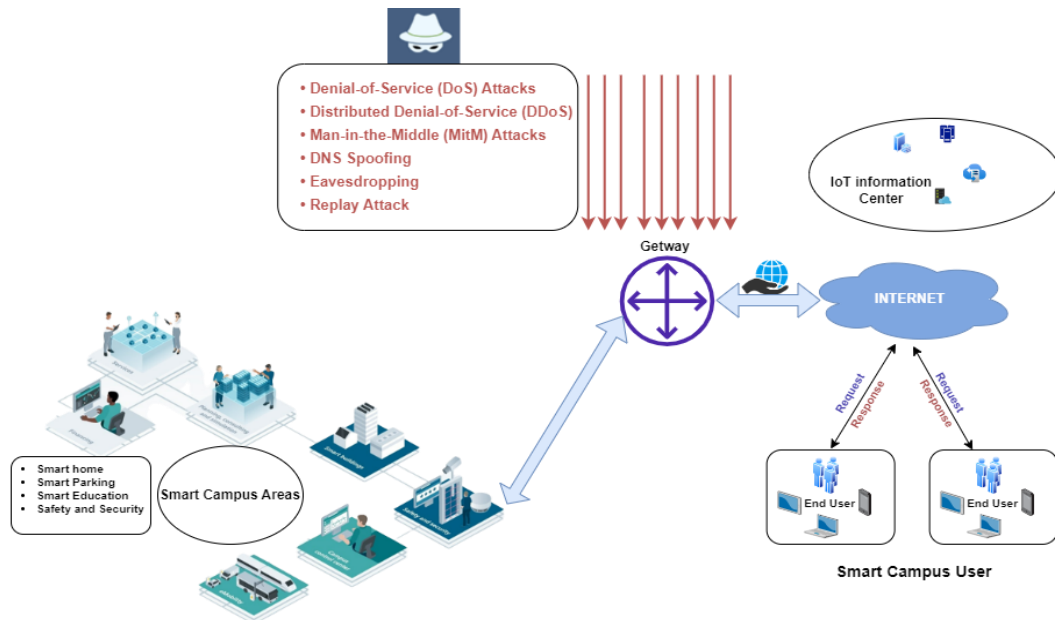


Figure 5. Network attacks in the smart campus

- Malware attack: Smart campus systems and devices are susceptible to infection by various forms of malware, including but not limited to viruses, worms, trojans, and ransomware [30] which is characterized by malicious programs that encrypt the user's files and demand payment in ransom in order to decrypt them. The aforementioned attacks have the potential to result in various negative consequences such as loss of data, disruption of system operations, unauthorized entry, or financial detriment.
- Social engineering attack: Social engineering attacks leverage human susceptibilities to deceive individuals and gain unauthorized entry. Phishing, pretexting, baiting, and tailgating are prevalent methods employed to deceive users into divulging confidential data or providing entry to systems. This type of attack attempts to influence people into revealing sensitive information [32]. As a human interaction-based attack, it falls under the category of physical attacks since social engineers physically contact students to gather useful information that might be utilized for illicit activities [33].
- Application layer attacks: Web applications are frequently employed for diverse objectives on smart campuses. Web applications are vulnerable to various types of attacks, including SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF), which have the potential to undermine the security and integrity of the systems.

- IoT-based attacks: Due to the increasing number of interconnected devices and sensors that exploit IoT infrastructure vulnerabilities, IoT-based attacks on smart campuses present a security challenge. Here are some common IoT-based attack vectors on smart campuses: i) Exploiting vulnerable IoT devices: Targeting vulnerabilities in IoT devices to gain unauthorized access or control; ii) IoT botnets refer to the exploitation of IoT devices to establish a network of bots that can be utilized for launching DDoS attacks or other malicious activities; iii) Device spoofing refers to the act of impersonating authentic internet; and iv) Physical security exploitation: In a smart campus, attackers can exploit vulnerabilities in IoT devices to obtain unauthorized access to such devices as door locks, alarms, or surveillance systems, disable security measures, or manipulate their functionality. By attacking a smart access control system, unauthorized individuals may gain access to restricted areas.
- Data privacy attacks: The smart campus is a significant resource on campus, comprising diverse devices and applications that generate various forms of data. The safeguarding of data privacy has emerged as a crucial necessity owing to the considerable amount of information that can be readily retrieved via remote access mechanisms [34]. Data attacks cover a range of potential threats and attacks that are directed toward the manipulation, deletion, storage, collection, and utilization of data. Some of the noted threats include (data breaches, data loss, and service hijacking) [35].

3.2.2. Attack scenario in smart campus

Smart campuses are subject to a variety of security threats and attacks, from external ones like DDoS and phishing attacks to internal ones like employee or student negligence or malicious acts. Here are a few of the most prevalent security threats that smart campuses must deal with:

- Attacks through DDoS: As illustrated in Figure 6 DDoS attacks aim to disrupt normal network operation by overloading servers with malicious traffic coming from several computers [36].

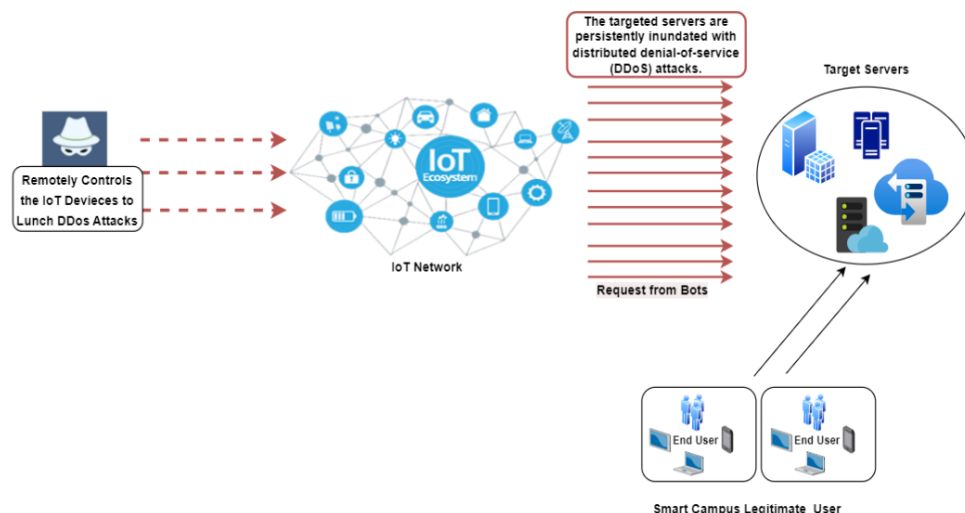


Figure 6. DDoS attack scenario in IoT networks

- Phishing attacks aim to persuade users to click on malicious links or download malicious software as shown in Figure 7 in order to reveal their sensitive personal information or identity information, the attacker gains access to sensitive information such as passwords and credit card details [37].
- Session hijacking attack in the context of systems, services, and networks, it is possible for an adversary to obtain unauthorized access to data and applications by acting as a proxy and acquiring a compromised session key or token. Conventionally, servers employ session tokens to identify and authenticate the ongoing connections of active users. Figure 8 illustrates the overall attack scenario. The adversary has the capability to execute the aforementioned attack through the act of either purloining or forecasting a legitimate session token, thereby obtaining illicit entry to the server [38].
- Replay attack: It is a form of the man-in-the-middle (MITM) attack, in which the attackers intercept packets transmitted through a communication channel and subsequently retransmit valid packets that have been modified. This is done with the intention of pretending to be an authentic node, as documented by Syverson [39]. on the smart campus the reader and RFID tag's communication is frequently the target of this attack, according to [40], the prevalence of this attack vector is observed in cases where the authentication protocol

employs authentication keys that are reusable. Figure 9 illustrates the overall attack scenario. The outcome of this attack could potentially result in malevolent entities gaining unapproved access to network assets. This particular method of attack aids in evaluating the feasibility of employing the suggested scheme for the purpose of authentication within network topologies.

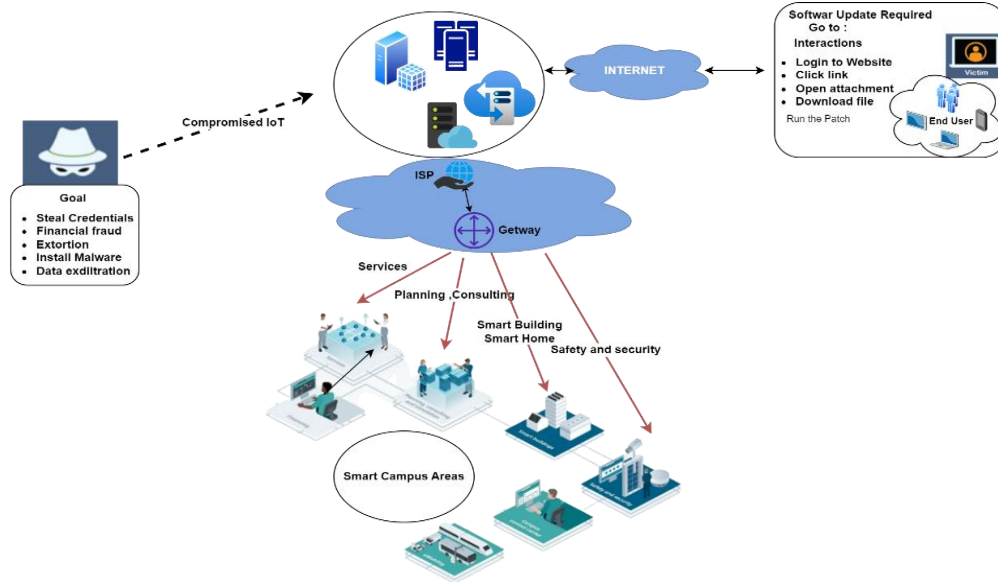


Figure 7. Fishing attacks

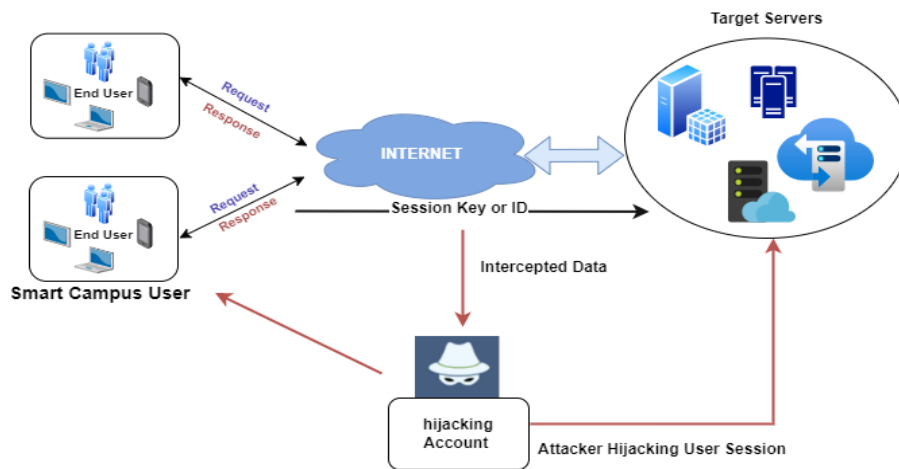


Figure 8. Scenario of session hijacking attack

- RFID spoofing, RFID coning, RFID unauthorized access an attacker spoofs an RFID signal in order to read and record data sent from an RFID tag. Then, the attacker can send his own data that includes the original tag ID, making it look like it's valid. By claiming to be the original source, the attacker gets full access to the system [41]. In the case of RFID cloning, the attacker clones the RFID tag by inserting the information from the target's RFID tag on another RFID tag as illustrated in Figure 10. Similarly, the absence of adequate authentication mechanisms in RFID systems results in unrestricted and unauthorized access to tags, which makes it possible for illicit actors to gain unauthorized access to nodes and manipulate, modify, or delete data [42].

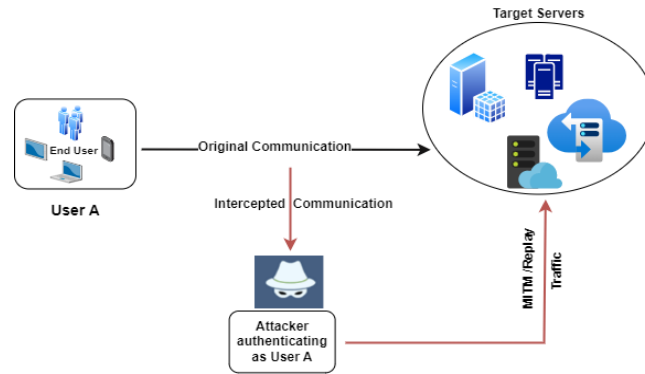


Figure 9. Scenario of session replay attack

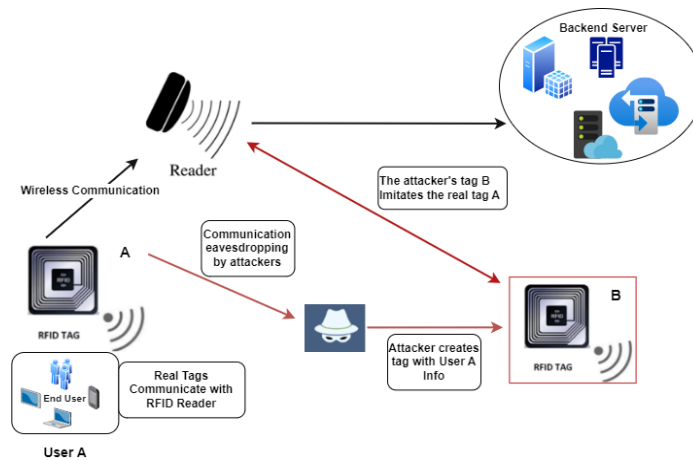


Figure 10. Scenario of RFID tags cloning attack

4. RESULTS AND DISCUSSION

This section provides results and analysis of attack characteristics and severity, classifying them into four distinct categories: low-level, medium-level, high-level, and extremely high-level. It highlights various attack types, their threat levels, fundamental characteristics, and potential solutions for mitigating them. The section also proposes defensive measures to effectively counter these threats.

4.1. Analysis of various attack types and potential solutions

The IoT is susceptible to a multitude of attacks, encompassing both active and passive forms of assault that have the potential to significantly compromise the operational capacity of an object. There exist active and passive components that have the potential to rapidly impede the functioning of a system and nullify the advantages of its offerings. Passive attacks refer to intrusions that aim to steal information or detect a threat without resorting to physical attacks [43].

However, it is imperative to refrain from engaging in any form of physical aggression. In contrast, active attacks entail the physical disruption of performances. The active attacks can be classified into two distinct categories, namely internal attacks and external attacks [44]. The lack of strength in these attacks could potentially hinder their ability to engage in effective communication. In order to mitigate the risk of malevolent intrusions, it is imperative to establish security constraints for the devices.

This section provides an analysis of attack characteristics and severity. In addition, attack levels are classified into four distinct groups, as seen each delimited by its behavioral attributes and their nature. In addition, defensive measures and solutions are proposed to effectively counter the associated threats and attacks.

- Low-level: In the event of an unsuccessful attempt by an attacker to compromise a network, it can be classified as a low-level attack.
- Medium-level: In the context of cybersecurity, a medium-level attack refers to a scenario in which an unauthorized individual, such as an attacker, intruder, or eavesdropper, is able to access and monitor a communication medium without compromising the integrity of the transmitted data.

- High-level: A high-level attack is defined as an attack on a network that results in the compromise or modification of data integrity.
- Extremely high-level: A severe form of cyber-attack involves an unauthorized individual gaining access to a network and engaging in illicit activities such as rendering the network inaccessible, transmitting a large volume of messages, or disrupting network functionality.

The IoT is rapidly enhancing everyday experiences through connected devices, but it is also presenting security issues and raising concerns about data privacy and protection. Understanding these issues is crucial to implementing proper protocols, protecting equipment, and safeguarding valuable data. Table 1 in APPENDIX [45]–[54] illustrates a variety of attack types, their corresponding levels of threat, their fundamental characteristics, nature, or behaviors, and potential solutions for mitigating these attacks.

5. CONCLUSION

The digital revolution has significantly altered cybersecurity requirements for industrial and academic fields, making it crucial to secure computer and data resources. The deployment and implementation of diverse security mechanisms and solutions will enable us to manage user access in a secure manner, reduce the vulnerabilities caused by IoT, mobile, and network devices, prevent unavoidable security gaps from acting as an attack vector, and still allow users access to all of their data. To increase overall security, it is necessary to secure the whole architecture of the implementation of the IoT on the smart campus and to put in place clear security measures like authentication and authorization, data encryption, network security, security monitoring, routine security updates, security policies, and user education and sensitization. Additionally, a proactive approach is required to monitor and identify vulnerabilities, implement the proper countermeasures, and maintain a high level of security for IoT systems. Finally, it is imperative to highlight that in the context of the continually changing nature of threats, the maintenance of security must remain a perpetual and persistent priority for the operators and administrators of intelligent campuses. In order to ensure user trust and dependability and enable the realization of the benefits provided by IoT systems on intelligent campuses. In the future, we might expand this work with regard to IoT domains and work on the limitations of the proposed solutions. Each IoT application area will have its own unique level of security risk, and as a result, the most pressing security concerns will vary from one domain to another, requiring a different prioritization of the problems to be addressed.

APPENDIX

Table 1. Summary of different types of attacks and their nature, their threat levels and suggested solutions

Attack type	Nature	Threat level	Behavior	Suggested solution
Passive	Passive	Low	In a smart campus, a passive attack is when an unauthorized person tries to access the network or data without making any changes to it. In other words, the attacker simply listens to or watches the data being transferred without making any changes to it. Since the attacker is not changing the data, passive attacks can be difficult to spot, and it can be difficult to tell which users are legitimate and which are not.	In order to mitigate passive attacks within a smart campus, a number of security measures may be employed, including but not limited to data transmission encryption, virtual private network (VPN) utilization, and intrusion detection system (IDS) deployment. Furthermore, access control mechanisms can be employed to limit unapproved entry to the network, while periodic security audits can be executed to detect possible susceptibilities and deficiencies in the system.
Sniffing	Passive	Low to high	The attacker eavesdrops on device communication by intercepting network traffic. Sniffing attacks can be used on a smart campus to gather sensitive data, including login passwords, private information, and secret information. Sniffing assaults can range in severity from low to high, depending on the resources and expertise of the attacker. High-intensity sniffing attacks can be carried out by internal attackers who have access to the network and network equipment. However, external attackers might need to employ more advanced methods, such as ARP spoofing or DNS spoofing, to carry out a sniffer assault [45].	To protect against sniffer attacks, it is advisable to use encrypted communication protocols like HTTPS, SSH, and VPN. The ability of an attacker to move laterally inside the network and get access to sensitive data may be restricted by the segmentation [46] and access control systems of the network. Setting up intrusion detection and prevention systems can also aid in identifying and halting real-time sniffing assaults.

Table 1. Summary of different types of attacks and their nature, their threat levels and suggested solutions (continued)

Attack type	Nature	Threat level	Behavior	Suggested solution
Spoofing	Passive	Low to high	An adversary has the ability to impersonate a legitimate IoT device by claiming the media access control (MAC), internet protocol (IP) address or RFID signal of the legitimate user. Once the attacker has gained unauthorized access, they are able to launch attacks on the smart campus network.	Measurements of the signal intensity and channel estimation, signature authentication using elliptic curve cryptography (ECC) [47]. network segmentation isolate IoT devices into separate network segments to reduce the potential for spoofing attacks [46].
Side-channel attacks	Passive	Medium	Side-channel attacks are a category of attacks that aim to extract sensitive information by exploiting the physical or electrical properties of a system. They include Timing, power analysis, electromagnetic, and acoustic attacks. Timing attacks exploit the time taken by cryptographic operations to infer information, while power analysis attacks measure the power consumption of a device to deduce sensitive data. Electromagnetic and acoustic attacks use device emissions to extract sensitive information.	To prevent side-channel attacks on smart campuses, it is crucial to implement appropriate hardware and software security measures. Hardware solutions include the utilization of tamper-resistant chips, shielding, and filtering to mitigate the susceptibility of devices to side-channel attacks. Software solutions encompass the implementation of secure coding practices, encryption, and randomization techniques to impede the extraction of sensitive information by attackers.
Active	Active	High	An active cyberattack is characterized by the intentional modification or manipulation of data that is being transmitted within a network or system by the attacker. In contrast to passive attacks that solely involve the monitoring of communication, active attacks entail the attacker's active participation in the communication process with the intention of manipulating it to their benefit.	Symmetric encryption can be utilized as a means of preserving data confidentiality. The implementation of an authentication mechanism can restrict data access only to individuals who have been granted authorization. Robust firewalls and intrusion prevention systems can serve as effective measures to prevent active attacks.
Man in the Middle	Active	Low to medium	Man-in-the-Middle (MitM) attacks are active attacks that intercept communication between two parties, such as in a smart campus environment when an attacker gains access to the network and positions themselves between a device and its intended recipient. Allowing them to intercept, alter, or even inject new data into the communication [48].	Using encryption protocols and algorithms like https and SSL/TLS, AES/DES to protect connections and making sure that devices and apps are set up to only communicate with trustworthy organizations are crucial for preventing MitM attacks [49]. access restrictions and network segmentation can help prevent an attacker from moving laterally through the network and gaining access to sensitive data. regular vulnerability assessments and security audits can help find and fix possible system vulnerabilities before they can be exploited [50].
Session hijacking	Active	High	Session hijacking is a type of attack that happens when an attacker gets unauthorized access to a user's session on a website or application. This can happen when an attacker intercepts a user's session ID and takes control of their session. The attacker can intercept session data, change it, and inject their own commands, which gives them control over the user's session.	It is imperative to employ secure session management mechanisms, such as using https. https encrypts user-server traffic, making session cookies harder to steal. Setting session waiting times: limit each session's duration. Thus, sessions will automatically end after a certain amount of inactivity, decreasing pirate infiltration. Implementing multi-factor authentication, such as two-factor authentication, to increase user authentication security monitoring.
Imitation	Active	High	Imitation attacks on the smart campus are a form of active attack in which an attacker takes on a legitimate user or device in order to obtain unauthorized access or conduct malicious actions. These attacks, also known as spoofing attacks, aim to convince the system that the attacker is a trusted user. There are several types of imitation attacks that can occur on a smart campus, including IP, DNS, and Mac spoofing.	To avoid spoofing and cloning attacks, apply identity-based authentication protocols. Physically unclonable functions are a countermeasure to cloning attacks. The implementation of robust authentication mechanisms, such as two-factor authentication, is of paramount significance.
Malware attack	Active	Extremely high	Malware attacks can have major consequences, such as data loss, confidentiality violations, and service disruption. They can be spread through IoT devices, phishing emails, and malicious software downloads. Malware can take many forms, such as viruses, Trojans, worms, ransomware, and spyware. On smart campuses, malware attacks can target various devices and	Security measures such as firewalls, antivirus software, intrusion detection systems, regular updates, and patches should be applied to all software and devices to address known vulnerabilities and prevent attackers from exploiting them. Network traffic should also be monitored and analyzed to detect suspicious activity that may indicate a

Table 1. Summary of different types of attacks and their nature, their threat levels and suggested solutions (continued)

Attack type	Nature	Threat level	Behavior	Suggested solution
Malware attack	Active	Extremely high	systems, such as computers, servers, routers, and IoT devices. It can be used to steal sensitive data, disrupt services, or take control of systems for malicious purposes.	malware infection or other security threat [51]. Last but not least, it's critical to regularly backup data to minimize losses in the event of a successful attack.
Fabrication	Active	Extremely high	Fabrication attacks refer to the deliberate generation of spurious data or information with the intent of deceiving or manipulating the system. The aforementioned attacks pertain to the fabrication of spurious data, procedures, correspondences, or any other form of operation within the system, the introduction of false data by a hostile entity can compromise the authenticity and integrity of information.	The application of data authenticity can serve as a means of verifying that data remains unchanged throughout its transmission.
DOS and DDOS	Active	Extremely high	A DoS attack is a type of attack in which an adversary floods a system, network, or application with traffic or requests to overwhelm and exhaust its resources, preventing it from responding to legitimate requests. DoS attacks could target various systems or services on a smart campus, including network infrastructure, communication systems, and IoT devices [52]. DoS attacks can have devastating effects on a smart campus, including disruption of vital services, loss of data, and even physical damage to devices or infrastructure.	Implementing multiple security measures, such as firewalls, intrusion detection systems, load balancers, and traffic filtration, is typical for preventing DoS attacks. Apply cryptographic techniques to secure networks, apply authenticity to detect malicious users. Prevent their access permanently [53], [54]. In this way, the network is protected from damage. In addition, ensuring system availability via redundant infrastructure and capacity planning can mitigate the effects of DoS attacks.

REFERENCES




- [1] N. Lee, H. Lee, H. Lee, and W. Ryu, "Smart home web of object architecture," in *International Conference on ICT Convergence 2015: Innovations Toward the IoT, 5G, and Smart Media Era, ICTC 2015*, Oct. 2015, pp. 1212–1214, doi: 10.1109/ICTC.2015.7354777.
- [2] A. Lazakidou, K. Siassiakos, and K. Ioannou, *Wireless technologies for ambient assisted living and healthcare: Systems and applications*. IGI Global, 2010.
- [3] E. M. Malatji, "The development of a smart campus - African universities point of view," in *2017 8th International Renewable Energy Congress, IREC 2017*, Mar. 2017, pp. 1–5, doi: 10.1109/IREC.2017.7926010.
- [4] W. Muhamad, N. B. Kurniawan, S. Suhardi, and S. Yazid, "Smart campus features, technologies, and applications: a systematic literature review," in *2017 International Conference on Information Technology Systems and Innovation, ICITSI 2017 - Proceedings*, Oct. 2017, vol. 2018-January, pp. 384–391, doi: 10.1109/ICITSI.2017.8267975.
- [5] J. W. P. Ng, N. Azarmi, M. Leida, F. Saffre, A. Afzal, and P. D. Yoo, "The intelligent campus (iCampus): end-to-end learning lifecycle of a knowledge ecosystem," in *Proceedings - 2010 6th International Conference on Intelligent Environments, IE 2010*, Jul. 2010, pp. 332–337, doi: 10.1109/IE.2010.68.
- [6] A. Abdullah, M. Thanoon, and A. Alsulami, "Toward a smart campus using IoT: Framework for safety and security system on a university campus," *Advances in Science, Technology and Engineering Systems*, vol. 4, no. 5, pp. 97–103, 2019, doi: 10.25046/aj040512.
- [7] S. Ahmed and T. Mazri, "Security approaches for smart campus," in *Lecture Notes in Networks and Systems*, vol. 629 LNNS, 2023, pp. 196–205.
- [8] M. A. M. Sadeeq, S. R. M. Zeebaree, R. Qashi, S. H. Ahmed, and K. Jacksi, "Internet of things security: a survey," in *ICOASE 2018 - International Conference on Advanced Science and Engineering*, Oct. 2018, pp. 162–166, doi: 10.1109/ICOASE.2018.8548785.
- [9] Y. I. Alzoubi, A. Al-Ahmad, and A. Jaradat, "Fog computing security and privacy issues, open challenges, and blockchain solution: an overview," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 6, pp. 5081–5088, Dec. 2021, doi: 10.11591/ijece.v11i6.pp5081-5088.
- [10] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the internet of things: a survey of existing protocols and open research issues," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015, doi: 10.1109/COMST.2015.2388550.
- [11] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: the road ahead," *Computer Networks*, vol. 76, pp. 146–164, Jan. 2015, doi: 10.1016/j.comnet.2014.11.008.
- [12] R. Atiqur, G. Wu, and A. M. Liton, "Mobile edge computing for internet of things: security and privacy issues," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 18, no. 3, pp. 1486–1493, Jun. 2020, doi: 10.11591/IJECS.V18.I3.PP1486-1493.
- [13] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: challenges," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 26–33, Jan. 2017, doi: 10.1109/MCOM.2017.1600363CM.
- [14] Z. K. Zhang, M. C. Y. Cho, C. W. Wang, C. W. Hsu, C. K. Chen, and S. Shieh, "IoT security: Ongoing challenges and research opportunities," in *Proceedings - IEEE 7th International Conference on Service-Oriented Computing and Applications, SOCA 2014*, Nov. 2014, pp. 230–234, doi: 10.1109/SOCA.2014.58.

- [15] M. Hager, S. Schellenberg, J. Seitz, S. Mann, and G. Schorcht, "Secure and QoS-aware communications for smart home services," in *2012 35th International Conference on Telecommunications and Signal Processing, TSP 2012 - Proceedings*, Jul. 2012, pp. 11–17, doi: 10.1109/TSP.2012.6256188.
- [16] Microsoft, "Smart and secure campus," *Microsoft*, 2018. <https://edudownloads.azureedge.net/msdownloads/MS-SmartSecureCampus-eBook.pdf>.
- [17] V. Sandeep, P. V. Honagond, P. S. Pujari, S. C. Kim, and S. R. Salkuti, "A comprehensive study on smart cities: Recent developments, challenges and opportunities," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 20, no. 2, pp. 575–582, Nov. 2020, doi: 10.11591/ijeecs.v20.i2.pp575-582.
- [18] O. Ali, W. Abdelbaki, A. Shrestha, E. Elbasi, M. A. A. Alryalat, and Y. K. Dwivedi, "A systematic literature review of artificial intelligence in the healthcare sector: Benefits, challenges, methodologies, and functionalities," *Journal of Innovation and Knowledge*, vol. 8, no. 1, p. 100333, Jan. 2023, doi: 10.1016/j.jik.2023.100333.
- [19] P. Soni and J. Subhashini, "Future smart grid communication-deployment of IoT: opportunities and challenges," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 23, no. 1, pp. 14–22, 2021, doi: 10.11591/ijeecs.v23.i1.pp14-22.
- [20] T. Alam, "A reliable communication framework and its use in internet of things," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2018 IJSRCSEIT*, vol. 5, no. 10, pp. 450–456, 2018, doi: 10.36227/techrxiv.12657158.
- [21] C. Del-Valle-Soto, L. J. Valdivia, J. C. López-Pimentel, and P. Visconti, "Comparison of collaborative and cooperative schemes in sensor networks for non-invasive monitoring of people at home," *International Journal of Environmental Research and Public Health*, vol. 20, no. 7, 2023, doi: 10.3390/ijerph20075268.
- [22] W. Villegas-Ch, X. Palacios-Pacheco, and S. Luján-Mora, "Application of a smart city model to a traditional university campus with a big data architecture: a sustainable smart campus," *Sustainability (Switzerland)*, vol. 11, no. 10, p. 2857, May 2019, doi: 10.3390/su11102857.
- [23] T. Anagnostopoulos, A. Zaslavsky, A. Medvedev, and S. Khoruzhnicov, "Top - k Query based dynamic scheduling for IoT-enabled smart city waste collection," in *Proceedings - IEEE International Conference on Mobile Data Management*, Jun. 2015, vol. 2, pp. 50–55, doi: 10.1109/MDM.2015.25.
- [24] P. S. Saarika, K. Sandhya, and T. Sudha, "Smart transportation system using IoT," in *Proceedings of the 2017 International Conference On Smart Technology for Smart Nation, SmartTechCon 2017*, Aug. 2018, vol. 10, no. 5, pp. 1104–1107, doi: 10.1109/SmartTechCon.2017.8358540.
- [25] R. S. Abd-Ali, S. A. Radhi, and Z. I. Rasool, "A survey: the role of the internet of things in the development of education," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 19, no. 1, p. 215, Jul. 2020, doi: 10.11591/ijeecs.v19.i1.pp215-221.
- [26] R. Charanya and M. Kesavan, "Analysis of factors influencing the virtual learning environment in a Sri Lankan higher studies institution," in *2019 International Research Conference on Smart Computing and Systems Engineering (SCSE)*, Mar. 2019, pp. 240–244, doi: 10.23919/SCSE.2019.8842719.
- [27] R. Jurva, M. Matinmikko-Blue, V. Niemelä, and S. Nenonen, "Architecture and operational model for smart campus digital infrastructure," *Wireless Personal Communications*, vol. 113, no. 3, pp. 1437–1454, 2020, doi: 10.1007/s11277-020-07221-5.
- [28] L. Wang, K. Li, and X. Chen, "Internet of things security analysis of smart campus," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11067 LNCS, 2018, pp. 418–428.
- [29] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017, doi: 10.1109/JIOT.2017.2694844.
- [30] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of things: Security vulnerabilities and challenges," in *2015 IEEE Symposium on Computers and Communication (ISCC)*, Jul. 2015, vol. 2016-Febru, pp. 180–187, doi: 10.1109/ISCC.2015.7405513.
- [31] A. Aldairi and L. Tawalbeh, "Cyber security attacks on smart cities and associated mobile technologies," *Procedia Computer Science*, vol. 109, pp. 1086–1091, 2017, doi: 10.1016/j.procs.2017.05.391.
- [32] F. Salahdine and N. Kaabouch, "Social engineering attacks: a survey," *Future Internet*, vol. 11, no. 4, p. 89, Apr. 2019, doi: 10.3390/FI11040089.
- [33] S. Colabianchi, F. Costantino, G. D. Gravio, F. Nonino, and R. Patriarca, "Discussing resilience in the context of cyber physical systems," *Computers & Industrial Engineering*, vol. 160, p. 107534, Oct. 2021, doi: 10.1016/j.cie.2021.107534.
- [34] H. Tao, M. Z. A. Bhuiyan, A. N. Abdalla, M. M. Hassan, J. M. Zain, and T. Hayajneh, "Secured data collection with hardware-based ciphers for IoT-based healthcare," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 410–420, Feb. 2019, doi: 10.1109/JIOT.2018.2854714.
- [35] M. Abomhara and G. M. Köien, "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks," *Journal of Cyber Security and Mobility*, vol. 4, no. 1, pp. 65–88, 2015, doi: 10.13052/jcsm2245-1439.414.
- [36] N. Kumar, J. Madhuri, and M. Channegowda, "Review on security and privacy concerns in internet of things," in *IEEE International Conference on IoT and its Applications, ICIOT 2017*, May 2017, pp. 1–5, doi: 10.1109/ICIOTA.2017.8073640.
- [37] K. Chen *et al.*, "Internet-of-things security and vulnerabilities: taxonomy, challenges, and practice," *Journal of Hardware and Systems Security*, vol. 2, no. 2, pp. 97–110, Jun. 2018, doi: 10.1007/s41635-017-0029-7.
- [38] A. K. Baitha and P. S. Vinod, "Session hijacking and prevention technique," *International Journal of Engineering & Technology*, vol. 7, no. 2.6, p. 193, Mar. 2018, doi: 10.14419/ijet.v7i2.6.10566.
- [39] P. Syverson, "A taxonomy of replay attacks [cryptographic protocols]," in *Proceedings of the Computer Security Foundations Workshop*, 1995, pp. 187–191, doi: 10.1109/CSFW.1994.315935.
- [40] D. Zhen-Hua, L. Jin-Tao, and F. Bo, "A taxonomy model of RFID security threats," in *International Conference on Communication Technology Proceedings, ICCT*, Nov. 2008, pp. 765–768, doi: 10.1109/ICCT.2008.4716242.
- [41] D. Braganza and B. Tulasi, "RFID security issues in IoT: a comparative study," *Oriental journal of computer science and technology*, vol. 10, no. 1, pp. 127–134, Mar. 2017, doi: 10.13005/ojcsst/10.01.17.
- [42] G. Tuna, D. G. Kogias, V. C. Gungor, C. Gezer, E. Taşkın, and E. Ayday, "A survey on information security threats and solutions for machine to machine (M2M) communications," *Journal of Parallel and Distributed Computing*, vol. 109, pp. 142–154, Nov. 2017, doi: 10.1016/j.jpdc.2017.05.021.
- [43] M. Abomhara and G. M. Koien, "Security and privacy in the internet of things: current status and open issues," in *2014 International Conference on Privacy and Security in Mobile Systems, PRISMS 2014 - Co-located with Global Wireless Summit*, May 2014, pp. 1–8, doi: 10.1109/PRISMS.2014.6970594.
- [44] M. Keerthika and D. Shanmugapriya, "Wireless sensor networks: active and passive attacks - vulnerabilities and countermeasures," *Global Transitions Proceedings*, vol. 2, no. 2, pp. 362–367, Nov. 2021, doi: 10.1016/j.gltp.2021.08.045.




- [45] B. Prabadevi and N. Jeyanthi, "A review on various sniffing attacks and its mitigation techniques," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 12, no. 3, pp. 1117–1125, Dec. 2018, doi: 10.11591/ijeecs.v12.i3.pp1117-1125.
- [46] M. N. Dazhara, F. Elmariami, A. Belfqih, and J. Boukherouaa, "A defense-in-depth cybersecurity for smart substations," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, no. 6, p. 4423, Dec. 2018, doi: 10.11591/ijece.v8i6.pp4423-4431.
- [47] S. Koppula and J. Muthukuru, "Secure digital signature scheme based on elliptic curves for internet of things," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 6, no. 3, p. 1002, Jun. 2016, doi: 10.11591/ijece.v6i3.pp1002-1010.
- [48] M. U. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A critical analysis on the security concerns of internet of things (IoT)," *International Journal of Computer Applications*, vol. 111, no. 7, pp. 1–6, Feb. 2015, doi: 10.5120/19547-1280.
- [49] E. R. Arboleda, C. E. R. Fenomeno, and J. Z. Jimenez, "KED-AES algorithm: combined key encryption decryption and advance encryption standard algorithm," *International Journal of Advances in Applied Sciences*, vol. 8, no. 1, pp. 44–53, Mar. 2019, doi: 10.11591/ijaas.v8.i1.pp44-53.
- [50] A. Srhir, T. Mazri, and M. Benbrahim, "Security in the IoT: State-of-the-art, issues, solutions, and challenges," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 5, pp. 65–75, 2023, doi: 10.14569/IJACSA.2023.0140507.
- [51] A. Wani and S. Revathi, "Ransomware protection in IoT using software defined networking," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 3, pp. 3166–3174, Jun. 2020, doi: 10.11591/ijece.v10i3.pp3166-3175.
- [52] R. Khader and D. Eleyan, "Survey of DoS/DDoS attacks in IoT," *Sustainable Engineering and Innovation*, vol. 3, no. 1, pp. 23–28, Jan. 2021, doi: 10.37868/sei.v3i1.124.
- [53] I. Cvitić, D. Peraković, M. Periša, and M. Botica, "Novel approach for detection of IoT generated DDoS traffic," *Wireless Networks*, vol. 27, no. 3, pp. 1573–1586, Apr. 2021, doi: 10.1007/s11276-019-02043-1.
- [54] M. A. Naagas, E. L. Mique, T. D. Palaoag, and J. S. D. Cruz, "Defense-through-deception network security model: securing university campus network from DOS/DDOS attack," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 7, no. 4, pp. 593–600, Dec. 2018, doi: 10.11591/eei.v7i4.1349.

BIOGRAPHIES OF AUTHORS






Ahmed Srhir    Ph.D. candidate at Ibn Tofail University, holding a state engineering degree in networks and information systems in 2015 at the National School of Applied Sciences in Kenitra, Morocco, have a particular interest in the internet of things, network security and machine learning as well as cloud architectures. currently working on the implementation of smart systems and its security in IoT platforms, focusing on several approaches and multi-agent methodologies as well as ensuring coherence with the Architecture and its implementations, currently hold the position of head of IT infrastructure and digitalization at CRI-RSK. Certified Azure Solutions Architect Expert, Oracle cloud infrastructure architect professional and Juniper JNCIA-DevOps. He can be contacted at email: ahmed.srhirl@uit.ac.ma.



Prof. Tomader Mazri    received her HDR degree in Networks and Telecommunication from Ibn Tofail University, Ph.D. in Microelectronics and Telecommunication from Sidi Mohamed Ben Abdellah University and INPT of Rabat, Master's in Microelectronics and Telecommunication Systems, and Bachelor's in Telecommunication from the Cadi Ayad University. She is currently a Professor at the National School of Applied Sciences of Kenitra, a permanent member of AS Laboratory, author and co-author of 20 articles journals, 40 articles in international conferences, 3 chapter and three books. Her major research interests are on microwave systems for mobile and radar, smart antennas and mobile network security. She can be contacted at email: tomader.mazri@uit.ac.ma.



Prof. Dr. Mohammed Benbrahim    professor of Higher Education at Ibn Tofail University. He holds a Ph.D. in Physical Sciences from the Faculty of Science, Rabat, culminating in a Doctorate from the University of Bordeaux I in 1989, specializing in instrumentation and measurement. He also completed a Master's degree (DEA) in Instrumentation and Measurement at the University of Bordeaux I, France, in 1987. currently hold the position of Deputy Director in Charge of Educational Affairs at the National School of Applied Sciences (ENSA) in Kenitra and served as Head of the Department of Electrical Engineering, Networks, and Telecommunication Systems (GERST) at ENSAK (National School of Applied Sciences). Her major research interests are in the physical sciences, systems, microelectronics, applied microwaves, and networks for telecommunications. He can be contacted at email: mohammed.benbrahim@uit.ac.ma.