# Exploring Risk Analysis Methods in IoE Projects: A Smart Campus Use Case

Henrique Santos(✉) and Tiago Pereira

Universidade do Minho, Centro Algoritmi, Guimarães, Portugal
{hsantos,tcpereira}@dsi.uminho.pt

**Abstract.** The IoT is an ICT development paradigm based on technological evolution. The underlying vision is an increasingly sensorized world, where all phenomena can be virtually digitised and processed by machines, interacting to improve humanity's quality of life. This transformation has taken place at breakneck speed. In a few years, the Internet began to be mainly used by machines, whose number and variety have increased exponentially, in symbiosis with humans, giving rise to the Internet of Everything (IoE) concept. Among the challenges in pursuing this primary objective, information security is one of the most relevant. Security flaws imply a loss of trust, compromising the acceptance and use of the entire system. Analysing risks and anticipating problems is imperative for any project in this field. However, the traditional risk analysis (RA) methods aiming at isolated Information Systems must be revised, given the complexity and dependence between systems in the IoE. Furthermore, traditional RA is performed periodically, usually annually, while the threat landscape linked to IoE changes more rapidly, demanding new approaches. This paper presents a survey of RA methods that have been applied in this context, justifying and demonstrating their adjustments to a particular case of a Smart Campus project. The results demonstrate the method's usefulness for planning adequate techniques to achieve the security-by-design and by-default principle.

**Keywords:** IoT · IoE · Risk Analysis · Risk Assessment · Smart Campus · Cybersecurity

## 1 Introduction

With the accelerated evolution of ICT in the last decade, we have witnessed many notable evolution. Computer networks, computing systems and intelligent software platforms have generated an ecosystem that today creates the illusion that we have the best and most accurate information available, anywhere and whenever we need it. The Internet of Things (IoT) was a term coined in first place

Supported by Lab4U&Spaces – Living Lab of Interactive Urban Space Solution, Ref. NORTE-01-0145-FEDER-000072, financed by community funds (FEDER), through Norte 2020.


T. Pereira et al. (Eds.): IOECON 2023, LNICST 551, pp. 76–91, 2024.
https://doi.org/10.1007/978-3-031-51572-9_7

to describe a view of this evolution, emphasising that the Internet space, until then focused on use by humans, was beginning to be exposed to use by machines, thanks to a set of emerging specific protocols, called machine-to-machine (M2M) [2,5,8,15]. In fact, according to well-known surveys, sometime in mid-2018, the number of 'things' using the Internet surpassed the number of human beings, and since then, it has grown in a sustained way without indications of slowing down [42]. One of the key transformations in this process was the adoption of the IPv6 protocol, which makes it possible to extend the Internet to millions of devices per square centimetre of the Earth's surface [39].

A natural next step was to merge both worlds, taking advantage of AI techniques and a massive amount of information, as well as processing and storage power, opening doors to adopting the term Internet of Everything (IoE). The vision is to have machines and humans cooperating to improve the quality of life on the planet. Some other terms emerged, such as the Internet of Nano Things (IoNT), to highlight the possibility of integrating sub micron-scale devices, which IPv6 allows and promotes [35]. One of the most prominent applications is in the health area, with the so-called Body Area Networks (BAN) [16].

Among the vast range of applications, the smart spaces has deserved much attention. The tendency to increase the concentration of people in urban spaces and the need to guarantee high quality of life standards pose serious challenges, mainly at the policy and government levels. Additionally, the need to better manage spaces has been markedly evidenced by the most recent COVID-19 pandemic crises and extreme weather events [25]. In the space of supporting solutions ICT and AI play a crucial role. The increase in research works and projects in Smart Cities, Smart Agriculture, and Smart Industries, among many other smart-like applications, is a clear sign of this [19,21,31]. Academic campuses are no exception. Following the generalised trend, some research works have been addressing the issues of this specific type of space, referred to as Smart Campus (SCampus). Concerning technological infrastructure shares identical solutions type with, for instance, Smart Cities. The main differences are in the focus and specific functions implemented. Most proposed models define six development dimensions: environment, energy, management, social, educational services, and utilities. Applications in each domain handle data from myriad linked sensors and sources, perform some intelligent analysis, and output results to proper operators' dashboards to better support decision-making [14,34].

SCampus involves innovative technology and people (students, staff, and general public), which are crucial for its main operation and (in)success. In most studies related to smart space challenges, security and privacy emerge as fundamental properties demanding proper management [11,17]. In addition to the different, complex and new technology stacks that support IoE and SCampus, we have a vast universe of very heterogeneous users regarding ICT awareness and expertise in its use. Even with the best security and privacy controls in place, uncertainty and mistrust can compromise the functional goals of any SCampus project. Thus, risk and trust assume a particularly relevant role and must be

adequately addressed, on an ongoing basis, throughout the project's entire life cycle [13,41].

Security and privacy impositions are non-functional requirements for projects. By definition, this type of requirement imposes restrictions on flexibility and general functional requirements, which are the base of the business model and, at large, of its success. So, in general, security and privacy may limit the exploitation of a product to the limit of making it unusable. Nevertheless, ignoring security and privacy issues can definitely damage the product's reputation, with the same final consequence. Finding the right balance is a challenging goal defined under a risk management process [39]. Each application domain and deployment restrictions imply different approaches concerning both technology and human resources. Furthermore, the risk perception of different communities makes it even harder to find some widely accepted security solutions. This is why the security area has been supported mainly by standards, sometimes focused on specific domains, trying to capitalise on the knowledge of experts to find a good solution. Smart Cities are no exception being possible to identify a framework of dedicated standards [32]. The number of security and privacy standards available is already significant, making it difficult to decide which ones to use [40]. Nevertheless, most standards and good practices guides defend an approach based on the Risk Management process. In this paper we will address the issues of trying to apply a Risk Analysis approach, and in particular Risk Assessment, to a project within the SCampus domain, named Lab4USpaces.

The paper is structured as follows: Sect. 2 present the fundamental concepts related to Information Security that are used along the paper, including the Risk Analysis model; Sect. 3 discuss the related work, emphasising the use of the ATT&CK matrix for threat modelling; Sect. 4 describes in detail each of the three steps of the proposed model (system description, threat modelling, and impact assessment), using as a case study a research project aiming at developing a Smart Campus – Lab4USpaces; finally, Sect. 5 draws some conclusions related to the applicability of the proposed model and refer the future work.

## 2 Fundamental Concepts

Before approaching the models and techniques already developed for risk management in the environment in question, it is convenient to define some fundamental concepts. We will use the ISO/IEC 27000 standard as a reference, although any text that addresses this topic presents similar definitions. The main concepts (in a simplified way) are [39]:

**Information Security** It is a process aiming to preserve a given set of properties or objectives relevant to information security; more specifically, it aims at the "*preservation of confidentiality, integrity and availability of information*" [27, pp. 6]:

- **Integrity**, to ensure information **is not modified** or **created** in an undesirable way;

- **Confidentiality**, to ensure information **is available only** to legitimate subjects;
- **Availability**, to ensure information **is available** whenever we need it; and
- **Others**, which is a placeholder for properties deriving from the above three, whenever security objectives are more specific; this is particularly relevant with integrity and confidentiality since the concepts are too abstract (e.g., assuring ownership and authenticity is probably critical for healthcare information, and both are related to integrity).

**Threat** A **possible cause of damage** in one or more security properties. When analysing threats it is possible not be aware of their origin, or how an accident might occur. Threats are frequently linked to security properties. However, they can also arise from the perception of the existence of an Information System's weaknesses, or even dangerous situations from the environment.

**Attack** Any malicious action or group of actions, intentional or not, that will **offend one or more security properties**, causing some harm to the Information System. Attacks may be executed by external or internal agents. When analysing possible attacks, we usually start with a relevant threat and in all possible ways it can be came into effect.

**Vulnerability** Any **flaw** or **weakness** existing in the Information System, which can be explored by a possible attack.

**Resource** Any asset that has **value** to the organisation. Knowing that value is crucial to define the impact of a total or partial loss. With intangible resources it is a considerable challenge to define it.

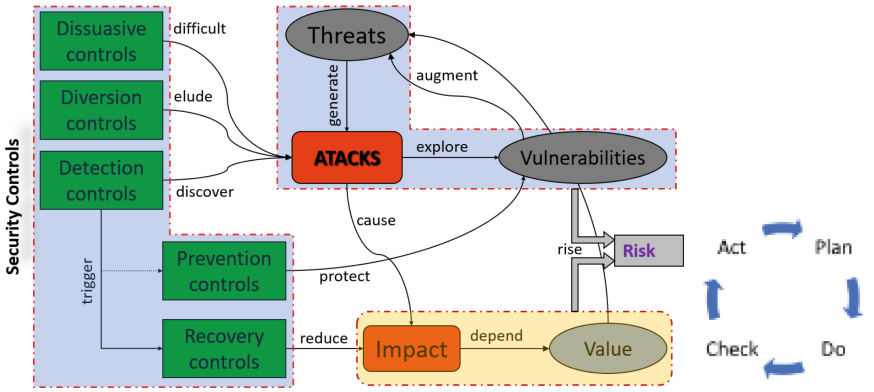
**Risk** Result of **uncertainty on security objectives**, when the Information System faces deviations from the correct behaviour. Uncertainty is related to a deficit of knowledge about events, their consequences or likelihood. Given the nature and variety of the events, that deficit may be impossible to overcome.

**Security Controls** All the measures we can take to **manage the risk**. It includes **policies, guidelines, procedures, and practices**. Their nature can be **administrative, technical, management, or legal**. Frequently, they are also referenced by safeguards or countermeasures. The ISO/IEC Standard 27001 [26] defines 14 security controls' classes, linked to 34 security objectives and a total of 124 specific controls. About half of those controls address technical issues, while the other group address organisational issues. Despite the relevance of this standard, there is no general consensus about its benefits. Frameworks like the SP 800-53 [36], or the CIS Critical Security Controls (CIS Controls) [1], among a few others usually promoted by specific companies selling security related services, are frequently considered useful alternatives.

### 2.1 Risk Analysis Model

The relationships between those concepts are highlighted in Fig. 1a, and establish a simple Risk Analysis model [39]. While the detailed analysis of this model is out of scope, it is important to highlight some aspects. The three elements

related to hazards (threats, attacks, and vulnerabilities) should allow us to derive the likelihood of any malicious action. Combining it with the resources' impact value, allows us to assess the risk, which must be the basis to choose the proper security controls. While impact value is intrinsic to each organisation and must be agreed upon within it, the threat landscape, particularly the attack techniques diversity, presents a primary challenge to recognise the second risk component. Attack modelling has been the target of several studies and solutions, but even so, it is still missing a practical approach limiting applicability in real world [10].




(a) Information Security model (b) PDC model

**Fig. 1.** Basic models for Information Security

Despite the simplicity of the above model, the lack of systematised knowledge regarding security and privacy threats and objectives, or even about security controls' efficiency, raises many uncertainties ameliorated only by the adoption of a continuous cycle model aiming to improve the security function over time – usually referred as the PDC (Plan, Do Check, and Act) model shown in Fig. 1b. This model characterises the Information Security function as a **management process**, referred by ISMS (Information Security Management System) [27]. Behind this simple formulation lies a considerable difficulty in finding the appropriate metrics to assess security (phase Check) with a view of its management. Finally, and still looking at Fig. 1a, the classification adopted for the security controls only partially aligns with the abovementioned standards. It focuses on the purpose towards threats from five alternative perspectives: deterrence, illusion, detection, prevention and recovery [39]. Each class exhibits a particular level of implementation cost and efficacy expectation, impacting the required monitoring level and the linked metrics.

Although it may currently be considered unthinkable not to implement an ISMS in any organisation that depends minimally on its IS, several factors condition its implementation. In [22], the authors suggest that limited resources and the need for alignment with business goals can make it challenging to establish

and operate all involved processes at the same level of maturity. In [45], the authors refer to top management support, resource planning, competency development, and awareness as critical points. The main difficulties can be attributed to the need for more preparation and awareness or less commitment from the people involved. Nevertheless, the increasing complexity of IT systems makes it also challenging for security practitioners to filter out the noise and focus on the essential threats, impacting their apparent competency [18] – in this last work, the authors also suggests that a systematic approach to identifying and documenting security threats is necessary.

## 3 Related Work

Risk Analysis, particularly Risk Assessment, is always hard to perform in any environment. In some cases, it is imperative to do so (e.g., critical systems or health systems); in others, there may even be regulatory or legal impositions (e.g., financial sector, in the USA), but in the vast majority of applications, it ends up being the market and users that may demand more or less in terms of security and privacy. A SCampus fits this last perspective. Some standards can be followed, but there are no mandatory rules or system certifications [3]. There are some system design recommendations, but typically they are not intended to be used by such heterogeneous communities, where some individuals are aware of the hazards and others are not. Even so, some interesting works focus on Risk Analysis in that environment type.

Towards an effective Risk Analysis process, the first step consists of identifying and characterising the threat landscape (if we cannot identify what can damage our IS, we cannot defend it), the main assets, and deriving a risk value (Risk Assessment). In [29], the authors discuss several types of attacks that can threaten a Smart Environment based on IoT. However, there are no clear security objectives or indicators allowing detection and effect measuring, limiting the practicability of the approach. Exploring different approaches, [44] proposes using the EBIOS methodology to identify weaknesses and vulnerabilities in IoT architectures, while [43] presents a survey and proposes a taxonomy of security Risk Assessment methodologies. In [30], the authors propose a multi-dimensional security Risk Assessment model based on three elements: assets, threats, and vulnerabilities. In a bottom-up approach, [33] conducts a systematic literature review to analyse the security of IoT devices and proposes using mobile computing to address security challenges and provide potential solutions. Overall, all these works suggest that traditional security Risk Assessment methodologies may not be effective in the IoT and SCampus context, and that new approaches are needed to address the unique challenges.

More specifically oriented to SCampus (or Smart Cities), but clearly still in a generalist approach, [9] propose some Risk Assessment techniques, including risk prediction and evaluation based on ISO27001 standards. It also suggests using data mining to identify information security threats in campus networks, such as database-related attacks. In [7], the authors focus on surveillance systems in IoT-enabled Smart Campuses, proposing a taxonomy and weighted scoring model

to assess the state-of-the-art systems. Meanwhile, in [24], the authors propose an information security Risk Assessment model, which includes 20 risk factors from five domains: infrastructure, data service, information content, information management, and public literacy. The model uses the decision tree algorithm to assess information security risks. Additionally, [28] proposes a comprehensive method for automatic security management of smart infrastructures using attack graphs and risk analysis. In synthesis, most of the above works assume that security objectives and threats are well-known or easy to identify, which is a fallacy as this knowledge can rarely be consolidated in the community of all stakeholders (including users).

There are already well-known models for studying attacks. However, these models are very focused on the study of attacks rather than their role in Risk Analysis, where the concern is not how the attack is executed but more on the effects and exploitation opportunities that can impact the system. A possible approach to address this gap is to use the MITRE ATT&CK matrix (Adversarial Tactics, Techniques, and Common Knowledge). In simple terms, it is a database with strategies (attacker goals), techniques and effects of cyberattacks, to which is added information on how to detect, mitigate, and even some examples of its use and groups of hackers that use or have used it. The matrix has been built by an open community, and has become a useful conceptual tool across many cybersecurity disciplines to convey threat intelligence, perform testing through red teaming or adversary emulation, and improve network and system defenses against intrusions [12].

Concerning specifically Risk Assessment, the ATT&CK matrix has already shown some virtues. In [20], the authors present research results on associating a comprehensive set of organisational and individual culture factors with security vulnerabilities mapped to specific adversary behaviour and patterns. Other relevant results are reported in [6] that proposes a new risk assessment approach based on a Failure Modes Effects and Criticality Analysis (FMECA) that is enriched with selected semantics and components of the MITRE ATT&ACK framework; [37] applies the framework to assess security risks of an integrated navigation system (INS) on a vessel; and [23] proposes an IS risk assessment method based on the ATT&CK model, which can calculate the risk value of security threats caused by various attack tactics and techniques, to effectively determine the risk indicator that should be paid attention to when the information system is under security threat.

The works mentioned above demonstrate the usefulness of the ATT&CK matrix and several ways it can be used for Risk Assessment. Nevertheless, there are some works whose results influence more directly the work described in this paper. In [38], the authors provide an extensive systematic review and a taxonomy of the applications and research on ATT&CK. Concerning Risk Assessment – one of the approached use cases – it identifies some works where the authors complement other frameworks (e.g., ISO/IEC 27005, NIST SP800-30) with ATT&CK to enrich the risk perception and impact effectively. Notwithstanding, it also highlights the need for more research on the practical implementation

and evaluation of ATT&CK. A relevant example of the complimentary between Risk Analysis frameworks and the ATT&CK matrix is given in [4]. The authors begin by identifying implementation models defined by the reference frameworks and then explore the semantic richness of the ATT&CK matrix to conduct the risk assessment. Among the implementation models, the Asset/Impact-centric approach assumes particular relevance here. It is used when adversaries, vulnerabilities and group threats are challenging to recognise or when assets are considered more critical. As will be seen, this is the most appropriate framework for the Lab4USpaces project.

## 4 Proposed Solution

This section describes the work carried out to perform a Risk Analysis process on the Smart Campus research project called Lab4U&Spaces[1]. The project's primary goal is to explore innovative technologies to increase the university campus's quality of life. We decided to follow a similar method to the one adopted by [4], but without a deeper attack analysis since we envisage a limited exposition and a low level of interest for sophisticated attackers, being enough a qualitative estimation for risks. The focus is on understanding the threats and impacts, not on the attack variants and their mitigation. The Risk Analysis framework used is described in Sect. 2.1, complemented with the MITRE ATT&CK to deduce the qualitative risk level, as described next.

### 4.1 Step 1: System Description

The general system architecture proposed for the Lab4USpaces platform is organised in four layers, as usually adopted for this type of system. Figure 2 shows a high-level version of the architecture, highlighting the role of the four layers and the main components of each, with enough detail to understand their function, the relevant assets, and the subjects involved. When describing a system this way, we may expect to identify the main threats and probability of success to emerge, even if that is not the primary objective.

The physical layer encompasses several sensors and actuators, which generally interact with the environment. Here we can categorise the device types:

- Resource-limited devices, whose function cannot be modified on the fly; reprogramming demands special equipment or physical access, meaning there is no way of accessing them remotely. They are connected to the upper layer by wireless networks, and to preserve battery life, usually, they do not perform complex authentication and ciphering operations. The main threats are usually related to rogue devices and the openness of wireless networks. In the case of actuators controlling critical operations, or sensors capturing critical information, such as private data (e.g., health data), those threats can raise higher risks. Otherwise, risk should be low.

[1] https://transparencia.gov.pt/pt/fundos-europeus/beneficiarios-projetos/projeto/NORTE-01-0145-FEDER-000072.

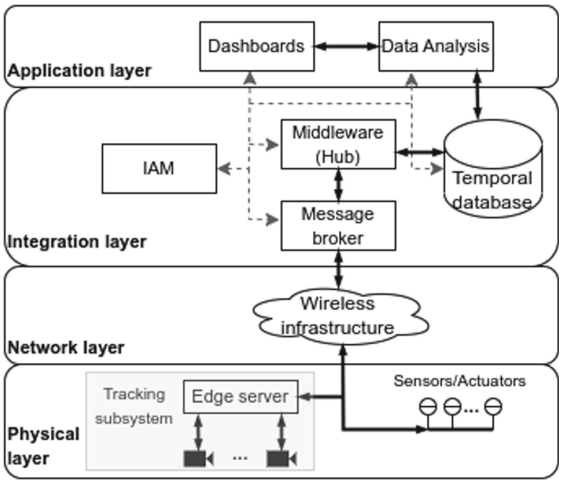



**Fig. 2.** Lab4USpaces platform general architecture

- Resource-limited programmable devices, whose function can be modified on the fly; this is a variant of the above, using powerful micro-controllers (e.g., ESP-32) that can be programmed remotely, through wireless, being exposed to malware; since they do not have an Operating System their functional capacity is limited, but so it is the support for any anti-malware or high sophisticated defence mechanism. Concerning security risks, the rationale above also applies, adding the exposition to remote tempering and abuse, with impact both at the data and network levels.
- Fully-capable computerised devices, like smartphones or laptop computers, serving as sensors or actuators, usually through dedicated applications. These devices face all the usual cyberthreats, possibly even being infected and abused. In the case of mobile devices using cellular communication technology, there is an additional threat related to exploiting that second channel as a gateway for networks outside our architecture.
- Edge computers, working as a hub for a set of related low-level devices, providing data pre-processing operations and/or a network node switching function for optimisation reasons. These are full-capable computers with the usual cyberthreats worsened by the use of wireless networks. Another aggravating factor is the non-interactive way it is used, making it difficult to observe anomalous behaviours that could trigger an alarm.

The network layer encompasses all the wireless access points, besides the network switches, firewalls and Intrusion Detection Systems that filter the traffic towards the upper level. Assuming they are properly configured, the main threat at this level is the wireless network and all its inherent vulnerabilities.

The integration layer resides in a private network and encompasses four main blocks:

- a message broker to properly organise the communication with the different low-level device classes;
- a temporal database as the central data repository;
- a middleware platform (at the moment, we are using Home Assistant) to provide sensors and actuators integration, visualisation, and simple data analysis functions; and
- an identity and access control management software (IAM) to implement Access Control functions for all users and devices capable of using OpenID connect and OAuth2 protocols. At the moment, we are using Keycloak.

All these components are isolated from the Internet, and all accesses are controlled using the best well-known protocols. So, even if we can consider a minimum risk, this is where the most valuable data is stored. Privacy issues can also become critical, as well as insider threats, since administrators and system operators will have access to the core components.

The application layer includes all software dedicated to high-level data analysis and dashboards. This is the only level within the architecture accessible to external users. Eventual external attacks will try to explore the link entry points at this level. Besides the user authentication and authorisation provided by the IAM, all system request should be filtered by a proxy or similar device at the entrance of the integration layer (not shown in Fig. 2).

From the above description and considering the role of each component, it is possible to identify the main assets and their potential impact on security properties. Table 1 synthesises that information. The impact is measured in three levels since it seems unnecessary to distinguish further the assets with higher impact at this stage. However, these assumptions may be reviewed later if necessary. The 'Exposition' column highlights the medium by which the assets can be reached, being the primary source of attacks. As expected, the wireless networks represent the main source of threads in the Lab4USpaces project. Still, to undertake a more accurate Risk Assessment, the threats must be explored more deeply.

### 4.2 Step 2: Threat Modelling

Threat modelling is an activity aiming to understand threats better. Most proposed methods focus on discovering how the related attacks are deployed, the tools used, and the explored vulnerabilities. This information is essential for mitigation purposes. However, from the initial Risk Assessment point of view, the main question is: How likely will it affect our system?

The ATT&CK matrix (see also Sect. 3) is a database that aggregates information about **tactics** (goals), **techniques**, **procedure examples**, **software tools**, **threat groups and campaigns**, **mitigation actions**, and **detectors' data sources**. The MITRE organisation also provides a front-end tool named ATT&CK Navigator[2] to explore the matrix and all the correlations between the

[2] https://mitre-attack.github.io/attack-navigator/.

**Table 1.** Asset/Impact synthesis.

| Asset | Exposition | Impact | Notes |
|---|---|---|---|
| Resource-limited devices | None | Low | Should not be used with critical data/processes |
| Small programmable devices | Wireless | **High** | Remote control and data injection |
| Computer-like nodes | Wireless and cellular com | **High** | Data injection |
| Edge nodes | Wireless | Medium | Sensor devices integration |
| Network nodes | Wireless | **High** | Network devices integration |
| Message Broker | Limited | Low | Data publish and subscribe |
| Temporal Database | None | **High** | Central repository for all data |
| Middleware platform | None | Low | Integration rules and data filtering |
| IAM | None | Low | Authentication and authorisation information |
| Web applications | Internet | **High** | APIs for web applications |

different dimensions. The Navigator allows extraction of partial views, named layers, based on a subset of tactics or techniques and using one of three domains: Enterprise, ICS (Industrial Control Systems), and Mobile. The first includes all tactics and techniques, while the others include a subset matching the indicated contexts. For illustration, the following steps describe how we approached the matrix, starting with the broader domain and searching for the Risk Assessment related details for some of the assets enumerated in Table 1:

1. In the architectural study, the wireless medium appears linked to the resources with the most significant impact. Using 'Wireless' as the search term, only three related techniques appear:
   - **Network Sniffing**, used for **Discovery** and **Credential Access** goals; reading the technique description and denoting a large number of Procedure Examples, it is evident that the medium and supporting protocols themselves are inherently vulnerable; we avoid credential abuse and data leakage by using cypher-based protocols; even so, the probability of a successful Network Sniffing attack is **very high**.
   - **Hardware Additions**, used for **Initial Access** goal; it consists of adding devices into the system or network; the Procedure Examples indicates just one case consisting of the addition of small computers, like Raspberry Pi, in a local network; looking into Fig. 2, especially at the physical layer and giving the sensors' diversity without the capacity to implement robust authentication mechanisms, the success of this attack is **very high**; at higher levels, the implementation of proper access control policies reduces the probability of successful attacks, but does not mitigate the threat.

- **Brute Force: Password Guessing**, used for (tactic or goal) Credential Access; the description and the high number of Procedure Examples reveal a severe challenge, mainly at the application layer, since at lower levels, most devices use tokens instead of passwords; as we will be using exposed protocols like SSH and HTTPS (despite being secure by robust ciphering techniques and a password policy) the success of these attacks are **high**.

2. The central repository also shows a high impact if it is possible to improperly take data (exfiltration) or to mess up data (manipulation).
   - Starting with **Exfiltration**, the ATT&CK includes a specific tactic for that goal, with nine techniques and some sub-techniques; one, in particular, is relevant in the context of the identified assets, **Exfiltration Over Web Service**, consisting of exploring eventual Web services' vulnerabilities; in this case, the Procedure Examples refer to existing cloud services, but giving the shared libraries, modules used, and server side languages when building Web services, most likely they will suffer from similar weaknesses, resulting in a **significant success probability** for this technique.
3. For the second data threat, searching the ATT&CK matrix for the term 'manipulation' within the description field returns 21 attack techniques; most of them are related to control operations, account abuse, or network and specific applications vulnerabilities, which do not fit the central repository case, but one technique stands out for the correspondence: **Data Manipulation: Stored Data Manipulation**; the corresponding tactic is **Impact**, denoting the destructive nature of the technique, but the limited Procedure Examples reveals its inherent limited efficacy; giving its potential impact, the probability of a successful attack is **very high**.

### 4.3 Step: 3: Impact Assessment

The final step consists on determining the risk value for each asset. The objective is to find a qualitative value, and define a decision point for mitigation purposes. In this case, this task is straightforward, just combining the impact and probability values. The final result appears in Table 2, where all elements with at least one High or greater value occurrence are considered. Analysing the table shows that counterfeit devices and Web applications are the resources considered most critical regarding security and on which further mitigation actions should be studied.

In this simple analysis, we deliberately ignore the important domino effect that results from exploiting one threat having an impact on another resources. This is the case of the Temporal Database, which, as it is not directly exposed to the Internet, shows a lower probability of attack success. However, attacks on Web applications will most certainly target this database (or even other components). The same rationale can be applied to fraudulent devices that could contaminate the same database. This is why we need to resort to more elaborate

attack analysis techniques. However, in the first phase, this simple model helps better to contextualise information security with the most critical resources.

**Table 2.** Critical Asset/Impact and Threat success probability list.

| Asset | Impact | Success Probability |
|---|---|---|
| Small programmable devices | **High** | **Very High** |
| Computer-like nodes | **High** | Low |
| Network nodes | **High** | Low |
| Temporal Database | **High** | **High** |
| Web applications | **High** | **Very High** |

## 5 Conclusion

Cybersecurity is currently an essential management process that must be part of any ICT project from the start. This process is very complex, with Risk Assessment being one of its essential elements. In its application, in addition to recognising the security objectives of the project in question, a demanding reflection on threats and attacks is required. Several models have been applied in the most diverse projects, but no solution can be considered a winner. This paper describes an alternative method that uses the ATT&CK matrix to provide information about threats and attacks.

This method is applied to a project under development, Lab4USpaces, which aims to build a framework to support a Smart Campus. The application of the model proved to be quite effective, allowing the identification of the most critical resources and a qualitative estimate of the risks. However, it was also possible to identify some limitations. When consulting the ATT&CK matrix, some keywords extracted from the description of the project's architecture were used. The use of different terms naturally results in different outcomes, revealing uncertainty due to the absence of an adequate taxonomy, which needs further investigation.

On the other hand, it was decided to avoid a deeper analysis of attacks in identifying threats and for the sake of simplicity. This option aimed to streamline the process but hid cascading effects related to attacks that affect risk assessment results. When knowledge about threats is limited and in an early stage of development, the solution is quite helpful. However, it should be further developed in subsequent iterations of the risk management process. These issues will be further investigated in future work on the model.

## References


1. CIS controls. https://www.cisecurity.org/controls
2. Miorandi, D., Sicari, S., De Pellegrini, F., Chlamtac, I.: Internet of things: vision, applications and research challenges. Ad Hoc Netw. **10**, 1497–1516 (2012). https://doi.org/10.1016/J.ADHOC.2012.02.016
3. Smart city standards - an overview (2017). https://urbanopus.net/smart-city-standards-an-overview/
4. Ahmed, M., Panda, S., Xenakis, C., Panaousis, E.: MITRE ATT&CK-driven cyber risk assessment, pp. 1–10. ACM (2022)
5. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: Internet of things: a survey on enabling technologies, protocols, and applications. IEEE Commun. Surv. Tutorials **17**, 2347–2376 (2015). https://doi.org/10.1109/COMST.2015.2444095
6. Amro, A., Gkioulos, V., Katsikas, S.: Assessing cyber risk in cyber-physical systems using the ATT&CK framework. ACM Trans. Priv. Secur. **26**(2), 1–33 (2023). https://doi.org/10.1145/3571733
7. Anagnostopoulos, T., et al.: Challenges and solutions of surveillance systems in IoT-enabled smart campus: a survey. IEEE Access **9**, 131926–131954 (2021)
8. Atzori, L., Iera, A., Morabito, G.: The internet of things: a survey. Comput. Netw. **54**, 2787–2805 (2010). https://doi.org/10.1016/j.comnet.2010.05.010
9. Awang, N., Xanthan, A., Samy, L.N., Hassan, N.H.: A review on risk assessment using risk prediction technique in campus network. Int. J. Adv. Trends Comput. Sci. Eng. **9**(3) (2020)
10. Ayrour, Y., Raji, A., Nassar, M.: Modelling cyber-attacks: a survey study. Netw. Secur. **2018**(3), 13–19 (2018)
11. Babun, L., Denney, K., Celik, Z.B., McDaniel, P., Uluagac, A.S.: A survey on IoT platforms: communication, security, and privacy perspectives. Comput. Netw. **192**, 108040 (2021). https://doi.org/10.1016/j.comnet.2021.108040. scholar: 2 cit 4/2021
12. Strom, B.E., Applebaum, A., Miller, D.P., Nickels, K.C., Pennington, A.G., Thomas, C.B.: MITRE ATT&CK®: design and philosophy (2020). https://www.mitre.org/news-insights/publication/mitre-attck-design-and-philosophy
13. Brand, B.S., Rigo, S.J., Figueiredo, R.M., Barbosa, J.L.V.: Sapientia: a smart campus model to promote device and application flexibility. Adv. Comput. Intell. **2**, 18 (2022). https://doi.org/10.1007/s43674-022-00032-0
14. Chagnon-Lessard, N., et al.: Smart campuses: extensive review of the last decade of research and current challenges. IEEE Access **9**, 124200–124234 (2021). https://doi.org/10.1109/ACCESS.2021.3109516
15. Cisco: The internet of things reference model (2014). http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf
16. Elhayatmy, G., Dey, N., Ashour, A.S.: Internet of things based wireless body area network in healthcare. In: Dey, N., Hassanien, A.E., Bhatt, C., Ashour, A.S., Satapathy, S.C. (eds.) Internet of Things and Big Data Analytics Toward Next-Generation Intelligence. SBD, vol. 30, pp. 3–20. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-60435-0_1
17. Elmaghraby, A.S., Losavio, M.M.: Cyber security challenges in smart cities: safety, security and privacy. J. Adv. Res. **5**, 491–497 (2014). https://doi.org/10.1016/j.jare.2014.02.006

18. Fielding, J.: Back to basics: tackling security threats in an increasingly complex world. Comput. Fraud Secur. **2019**, 6–8 (2019)
19. Friha, O., Ferrag, M.A., Shu, L., Maglaras, L., Wang, X.: Internet of things for the future of smart agriculture: a comprehensive survey of emerging technologies. IEEE/CAA J. Automatica Sinica **8**, 718–752 (2021)
20. Georgiadou, A., Mouzakitis, S., Askounis, D.: Assessing MITRE ATT&CK risk using a cyber-security culture framework. Sensors **21**(9), 3267 (2021). https://doi.org/10.3390/s21093267
21. Gomez, C., Chessa, S., Fleury, A., Roussos, G., Preuveneers, D.: Internet of things for enabling smart environments: a technology-centric perspective. J. Ambient Intell. Smart Environ. **11**, 23–43 (2019)
22. Haufe, K.: Maturity based approach for ISMS governance (2017)
23. He, T., Li, Z.: A model and method of information system security risk assessment based on MITRE ATT&CK. In: 2021 2nd International Conference on Electronics, Communications and Information Technology (CECIT). IEEE (2021). https://doi.org/10.1109/cecit53797.2021.00022
24. Hui, P.: Construction of information security risk assessment model in smart city. In: 2020 IEEE Conference on Telecommunications, Optics and Computer Science (TOCS). IEEE (2020). https://doi.org/10.1109/tocs50858.2020.9339614
25. Hussain, A.A., Bouachir, O., Al-Turjman, F., Aloqaily, M.: Notice of retraction: AI techniques for COVID-19. IEEE Access **8**, 128776–128795 (2020)
26. ISO/IEC: Iso/iec 27001:2013, information technology - security techniques - information security management systems - requirements (2013). https://www.iso.org/standard/54534.htmlhttps://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en
27. ISO/IEC: Information technology-security techniques-information security management systems-overview and vocabulary (international standard ISO/IEC 27000) (2016). https://www.iso.org
28. Ivanov, D., Kalinin, M., Krundyshev, V., Orel, E.: Automatic security management of smart infrastructures using attack graph and risk analysis. In: 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4). IEEE (2020). https://doi.org/10.1109/worlds450073.2020.9210410
29. Kalinin, M., Krundyshev, V., Zegzhda, P.: Cybersecurity risk assessment in smart city infrastructures. Machines **9**, 78 (2021). https://doi.org/10.3390/machines9040078
30. Kang, W., Deng, J., Zhu, P., Liu, X., Zhao, W., Hang, Z.: Multi-dimensional security risk assessment model based on three elements in the IoT system. In: 2020 IEEE/CIC International Conference on Communications in China (ICCC), pp. 518–523. IEEE (2020)
31. Kirimtat, A., Krejcar, O., Kertesz, A., Tasgetiren, M.F.: Future trends and current state of smart city concepts: a survey. IEEE Access **8**, 86448–86467 (2020)
32. Lea, R.: (2016). https://urbanopus.net/smart-city-standards-an-overview/
33. Liao, B., Ali, Y., Nazir, S., He, L., Khan, H.U.: Security analysis of IoT devices by using mobile computing: a systematic literature review. IEEE Access **8**, 120331–120350 (2020)
34. Min-Allah, N., Alrashed, S.: Smart campus-a sketch. Sustain. Cities Soc. **59**, 102231 (2020). https://doi.org/10.1016/j.scs.2020.102231. scholar: cit 95 4/2023
35. Miraz, M.H., Ali, M., Excell, P.S., Picking, R.: A review on internet of things (IoT), internet of everything (IoE) and internet of Nano things (IoNT). In: 2015

Internet Technologies and Applications, ITA 2015 - Proceedings of the 6th International Conference, pp. 219–224 (11 2015). https://doi.org/10.1109/ITECHA.2015.7317398
36. NIST: SP 800–53 rev. 5 security and privacy controls for information systems and organizations (2020). https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
37. Oruc, A., Amro, A., Gkioulos, V.: Assessing cyber risks of an INS using the MITRE ATT&CK framework. Sensors **22**(22), 8745 (2022). https://doi.org/10.3390/s22228745
38. Roy, S., Panaousis, E., Noakes, C., Laszka, A., Panda, S., Loukas, G.: SoK: the MITRE ATT&CK framework in research and practice (2023). https://doi.org/10.48550/ARXIV.2304.07411
39. Santos, H.M.: Cybersecurity: A Practical Engineering Approach. CRC Press, Boca Raton (2022)
40. Stallings, W.: Effective Cybersecurity: A Guide to Using Best Practices and Standards. Addison-Wesley Professional, Boston (2018)
41. Tewari, A., Gupta, B.: Security, privacy and trust of different layers in internet-of-things (IoTs) framework. Future Gener. Comput. Syst. **108**, 909–920 (2020). https://doi.org/10.1016/j.future.2018.04.027
42. Vailshery, L.S.: IoT connected devices worldwide 2019–2030 (2022). https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/. Accessed 10 Apr 2023
43. Yassine, I., Halabi, T., Bellaiche, M.: security risk assessment methodologies in the internet of things: survey and taxonomy. In: 2021 IEEE 21st International Conference on Software Quality, Reliability and Security Companion (QRS-C), pp. 668–675. IEEE (2021)
44. Zahra, B.F., Abdelhamid, B.: Risk analysis in internet of things using EBIOS. In: 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), pp. 1–7. IEEE (2017)
45. Zammani, M., Razali, R., Singh, D.: Factors contributing to the success of information security management implementation. Int. J. Adv. Comput. Sci. Appl. (2019)