JOURNAL OF E-LEARNING AND KNOWLEDGE SOCIETY
Vol. 16, No. 01 (2020), pp. 01-10

A Holistic Model for Security of Learning Applications in Smart Cities

Luca Caviglione[a], Mauro Coccoli[b,1]

[a]*Institute for Applied Mathematics and Information Technologies, National Research Council of Italy – Genoa (Italy)*

[b]*University of Genoa, Department of Informatics, Bioengineering, Robotics, and Systems Engineering – Genoa (Italy)*

(submitted: 28/10/2019; accepted: 11/02/2020; published: 30/04/2020)

Abstract

Modern learning frameworks take advantage of the interconnection among individuals, multimedia artifacts, places, events, and physical objects. In this perspective, smart cities are primary providers of data, learning stimuli and realistic hands-on laboratories. Unfortunately, the development of smart-city-enabled learning frameworks leads to many privacy and security risks since they are built on top of IoT nodes, wireless sensors networks and cyber-physical systems. To efficiently address such issues, a suitable holistic approach is needed, especially to reveal the interdependence between different actors, e.g., cloud infrastructures, resource-constrained devices and big data sources. Therefore, this paper introduces a model to help the engineering of novel learning frameworks for smart cities by enlightening the problem space characterizing security.

KEYWORDS: e-learning, smart cities, privacy and security, big data, model-driven design

DOI
https://doi.org/10.20368/1971-8829/1135031

CITE AS
Caviglione L., Coccoli M., (2020) A holistic model for security of learning applications in smart cities.Journal of E-Learning and Knowledge Society, 16(1), 01-10. https://doi.org/10.20368/1971-8829/1135031

1. Introduction

The implementation of the smart city paradigm requires deploying emergent technologies to better manage the finite resources of modern urban areas (Allwinkle & Cruickshank, 2011). In essence, the main goal of a smart city is the enhancement of the quality of life of citizens, mainly by optimizing aspects related to healthcare, bureaucracy, public transportation and commerce, just to mention some. To pursue such vision, relevant advancements in several fields are required, including ICT, humanities and social sciences, architecture and environment protection.

With reference to our country, one of the most important drivers to pursue the smart city vision is the European Union. In fact, its policies provide several funding schemes to improve nine dimensions defining the quality of life, which complete the more aseptic gross domestic product indicator used to measure the economic and social development of a country. However, the dimension of education has been often neglected in favor of environmental challenges, pollution prevention, energy efficiency, and safety. Indeed, smart cities and learning can be merged as to pursue new, interactive and efficient frameworks. This requires bringing both learners and learning platforms into an interactive environment populated with wireless sensors, portable devices, and nodes of the IoT. Alas, the pervasive nature of smart paradigms demands for mechanisms to handle user mobility, manage big data sources, offload devices with constrained capabilities, and mitigate communication issues due to intermittent network coverage (Caviglione, 2006).

In such a scenario, privacy and security of the entire architectural blueprint become critical aspects, which are the topics of this paper. In fact, the perception of a

[1] corresponding author - email: mauro.coccoli@unige.it – address: DIBRIS, University of Genoa - Viale Causa, 13 - 16145, Genova (Italy)

"secure" environment is crucial for its acceptance. As an example, see the work by Wilkowska and Ziefle (2011) for a detailed study on the case of medical assistive technologies. Unfortunately, guaranteeing the security and privacy of users requires searching for a complex and fragile trade-off. For instance, learners cannot be completely anonymous and some information about their actions should be collected by the platform or by the supervisor in order to evaluate progresses, adapt the learning curve and draw reasonable assessments (Borcea et al., 2005). Moreover, the increasing personalization of the learning experience by means of big data sources, possibly enriched with bits gathered from social media, may open several opportunities to undertake attacks via social engineering techniques (Manca et al., 2016).

Even if issues caused by the merge of learning platforms with smart city environments have not been explicitly discussed in the literature, several works already investigated trust, privacy and security features of e-learning frameworks. For instance, Anwar and Greer (2012) focused on trust, which is a core aspect for distance learning or for remotely interact with the software artifacts provided by a smart city. In fact, while in a classroom the authenticity is guaranteed by the physical presence, in a virtualized environment, other techniques have to be used. The work of Caviglione and Coccoli (2018) deals with smart learning platforms fed with big data generated by sensors, buildings and appliances deployed in a smart city, but does not offer a solution to protect the bulk of information or to prevent security flaws caused by improper access rights, incorrect mappings and conversions, de-anonymization attacks and steganographic threats. A possible solution is to deploy some layers for removing personal information, promote privacy awareness and provide context separation (Anwar et al., 2006). Alas, this is not a trivial task, especially in smart cities, where data are provided by different, heterogeneous sources and the volumes of information could not allow a fine-grained management (Hashem et al., 2016).

Even if limited to legacy client-server frameworks, Miguel et al. (2012) discuss requirements to avoid attacks like spoofing, unauthorized accesses, fraudulent alteration of learning materials, injection of virus or malicious code, and Denial of Service (DoS). The work of Bdiwi et al. (2018) partially addresses smart cities as it investigates intelligent classrooms equipped with IoT nodes, smart devices and connected objects. In essence, authors propose to use blockchain technologies to guarantee security and authenticate data as to prevent misuses and attacks. A specular problem, i.e., authenticating users, is addressed by Kang and Kim (2015).

Concerning mobile and ubiquitous frameworks, the work of Kambourakis (2013) surveys several security and privacy issues of mobile-learning and ubiquitous-learning, but does not cover the use of smart or emerging paradigms, such as the Bring Your Own Device (BYOD) one (Miller et al., 2012). Lastly, the work of Neila and Rabai (2014) proposes a matrix-driven design approach to quantify the security issues of e-learning platforms, especially technology-dependent attacks, such as cross site request forgery, buffer overflows and DoS.

To sum up, all the aforementioned works do not consider the issues, both in terms of security hazards or privacy leaks, arising from the use of smart cities to enhance learning frameworks. Additionally, the resulting complexity demands for a holistic approach, instead of solely considering an aspect at time, e.g., the guest operating system running core services or the user behavior. In this perspective, along the lines of Caviglione et al. (2014), this work introduces a holistic model to describe the privacy and security issues characterizing cutting-edge learning applications leveraging smart cities. In this respect, Zuev (2012) proposes a model for e-learning systems but it concentrates on the didactic risk, and hazards caused by the learning material and the delegation of responsibility from the teacher to the electronic Learning Management System (LMS). Thus, at the best of the authors' knowledge, this is the first work dealing with security aspects of e-learning exploiting smart cities.

The main contributions of this work are: *i)* a model to classify and organize security and privacy aspects of the joint use of smart city and learning environments, and *ii)* a methodology to isolate hazards of future learning applications and to reveal new ones.

The remainder of the paper is structured as follows. Section 2 presents the proposed functional model. Section 3 deals with learner space, Section 4 discusses the hazards caused by data, and Section 5 showcases risks due to the mix of technologies implementing the learning infrastructure and the smart city. Section 6 provides examples on how to exploit the modeling approach, while Section 7 concludes the paper and proposes some possible future extensions.

2. Privacy and Security: A Holistic Model

As hinted, the interplay among social, educational and technological aspects characterizing learning applications in smart cities leads to a very composite set of privacy and security issues. To understand and enlighten possible cause-effect relations including potential hazards, we introduce the model illustrated in Figure 1.

As depicted, each space contains a homogenous set of entities implementing coherent and recognizable

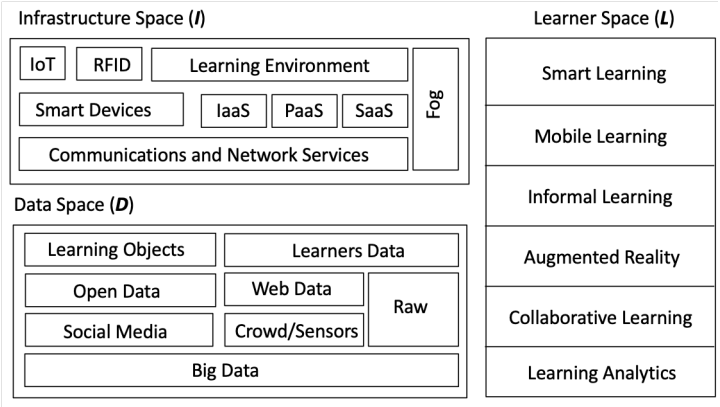

Figure 1 – The three spaces characterizing learning applications in smart-city environments.

aspects of the learning process. For the sake of clarity, Figure 1 only contains the most popular architectural components and technologies as well as learning models. Each space should be considered as a sort of base, which can be used to describe privacy and security within a well-given functional scope. In more detail, the model is articulated as follows:

- **Infrastructure Space**: it groups all the software and hardware entities composing the smart-city-learning paradigm, i.e., from user devices to server farms. In general, the resulting space is highly composite and complex as modern learning frameworks support on-the-road and hands-on didactics, hence mixing many technologies, including wireless communications, mobile agents, and cloud architectures (Caviglione et al., 2011a).
- **Data Space**: it groups all the functionalities related to the creation, collection, processing and storage of data. It considers issues ranging from those characterizing standard learning objects to leakage of information in social network sites and Intelligent Tutoring Systems (ITS) as well (Riccucci et al., 2007). This space also describes attacks that can be developed by considering novel sources, such as those exploiting unknown relations nested within big data (Bertino & Ferrari, 2018) or weaknesses of crowd-based schemes collecting measures from the field (Ganti et al., 2011).
- **Learning Space**: it groups the different learning methodologies that can be used in the smart-city-capable scenario. For instance, it considers issues arising from interlinking of learning resources (Carbonaro, 2012) or from "interpersonal" relations, like bullying, lack of anonymity or the need of enforcing a rigorous execution of assessments (Marais et al., 2006).

The three aforementioned spaces can be used as "bases" to describe the security and privacy features of learning applications in a holistic manner. For instance, an unsecure wireless channel could allow to collect insights from the data space or to infer some habits of the learner. Similarly, the data space can be used to attack the learner, even physically, e.g., by disclosing his/her geographical location. Another example deals with implementation-specific issues such as Web-based technologies prone to weaknesses identified by the Open Web Application Security Project, or misconfigured databases vulnerable to SQL injection (Caviglione et al., 2014).

To discuss such relationships and dependencies, let us denote with $\boldsymbol{I}$, $\boldsymbol{D}$, and $\boldsymbol{L}$ the infrastructure, data, and learning space, respectively. Each one represents a collection of hazards related to the specific technological components of that space. More precisely, $\boldsymbol{I}=\{i_1, i_2, \ldots, i_N\}$, $\boldsymbol{D}=\{d_1, d_2, \ldots, d_M\}$, and $\boldsymbol{L}=\{l_1, l_2, \ldots, l_K\}$, where N, M, and K are the amount of threats of each space. Vulnerabilities of $\boldsymbol{I}$, $\boldsymbol{D}$, and $\boldsymbol{L}$ have to be addressed during the design and engineering of the learning application or mitigated at runtime with proper countermeasures.

The interplay of the various techniques will result into a complete security and privacy space denoted with $\boldsymbol{C}$ and defined as:

$$\boldsymbol{C} = f(\boldsymbol{I}, \boldsymbol{D}, \boldsymbol{L}),$$

where, $f(\cdot)$ is a design-dependent function. Unfortunately, defining a unique $f(\cdot)$, possibly analytical, could be unfeasible, but some relations can be empirically derived (Ten et al., 2010). Instead, we aim at defining a framework for quantitatively

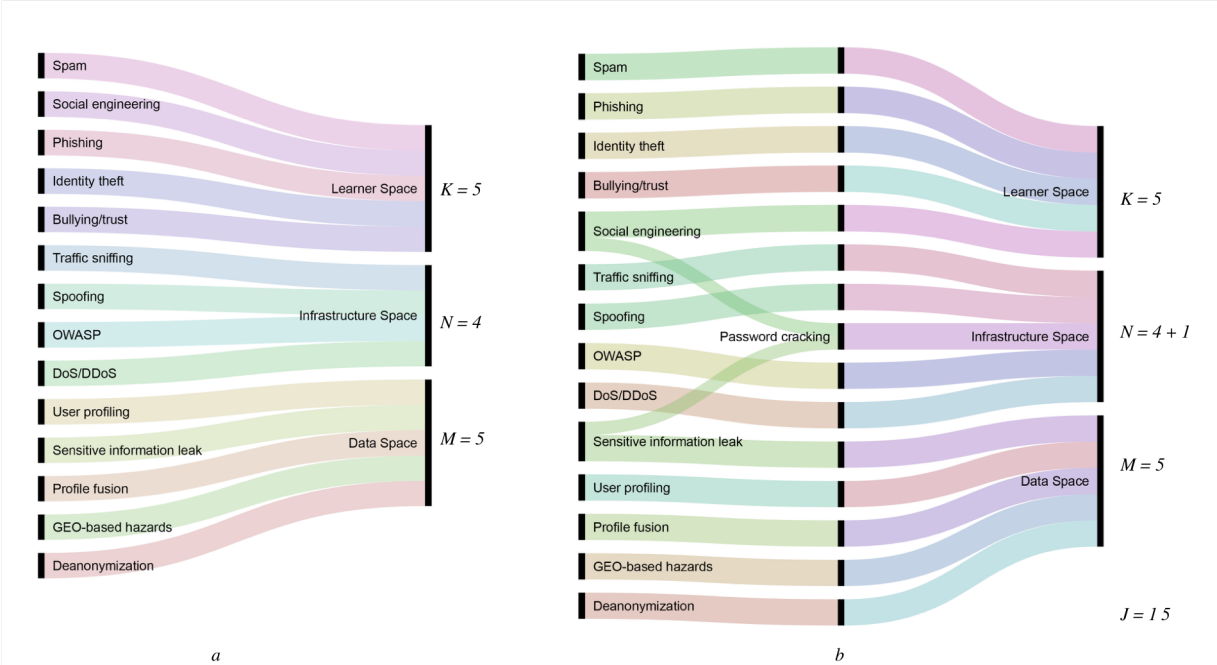

Figure 2 – Toy example: the different security issues in the relevant spaces.

investigate vulnerabilities. Let us introduce with $|\cdot|$ a pseudo-cardinality operator, i.e., a measure of the impact of all the components of a space. As discussed by Caviglione et al. (2014), the complex mix of behaviors of learners, smart environments and ICT techniques can "amplify" the number of hazards and weaknesses of the entire framework. The combination of multiple vulnerabilities across different spaces can cause new threats, i.e.:

$$|\boldsymbol{C}| \geq |\boldsymbol{I}| + |\boldsymbol{D}| + |\boldsymbol{L}| \quad (1)$$

By defining $|\boldsymbol{C}| = J$, Equation (1) leads to $J \geq N+M+K$. To clarify this, let us introduce a toy example considering a learning application enhanced via social media. A possible visual representation can be obtained by using alluvial diagrams as depicted in Figure 2 showcasing the mappings of security risks for each space.

According to our model, Figure 2*a* shows that both learner and data spaces are characterized by five different vulnerabilities or attacks, hence $K=M=5$, whereas the infrastructure space is characterized by $N=4$. We point out that not all the vulnerabilities can be feasible for an attacker, e.g., due to a lack of skills. However, when blended in the learning application, an attacker can "move" through spaces to find an exploitable vulnerability. As an example, penetrating into a host to exfiltrate sensitive data requires to being able to attack the ***I*** space, i.e., to void the security framework of the operating system. The attacker can act on ***D*** by collecting data from social media and obtain sensitive bits via social engineering on ***L***. The leaked information can be used to craft a dictionary to make password cracking feasible (Bonneau, 2012), hence granting access to an inaccessible *i*-th component of the ***I*** space as shown in Figure 2*b*. We point out that this corresponds to mix different privacy and security threats and leads to an attack only feasible in the space ***C***. In our model, this is quantitatively denoted as considering $J=15$, which is greater than the sum of the pseudo-cardinality of each space owing to the password cracking attack. In real-world usages, J should be considered as a sort of weight, rather than a strict indicator of the number of real vulnerabilities. In fact, precisely enumerating all the threats affecting a given module or technology is usually unfeasible. In practice, at design time, J has to be considered carefully by both instructional designers and developers. It can help to quantify the (in)security of the applications and, for example, reserve an adequate budget.

In the following, we will characterize each space by surveying the related literature with emphasis on hazards addressing the joint usage of learning applications and smart city technologies. For the sake of brevity, this paper does not cover "plain" cybersecurity threats, which have been already investigated, see, e.g., the recent work by Humayed et al. (2017) on issues of cyber-physical systems and IoT technologies.

3. Learner Space

The learner space ***L*** is where the learning process happens. It can rely upon mobile and ubiquitous learning paradigms as well as lifelong learning strategies, or exploit novel solutions such as augmented reality.

Even if not specifically addressing a smart city scenario, the work by Bellekens et al. (2016) confirms that the majority of e-learning users do not have a clear understanding of risks and threats associated with the use of computing and network technologies. This may lead to major pitfalls, as users can be prone to social engineering attacks, poorly configure their accounts, introduce additional fragilities due to a BYOD policy or being target for technology-specific attacks as it happens in developing countries where satellites are often used (Caviglione, 2009).

Scientific training is a very important application of e-learning and can show major benefits if applied to smart cities, as they offer the access to complex infrastructures, collections of raw data coming from the field as well as the possibility of observing cause-effect relations, e.g., the trend of temperature and humidity in a building when parameters of heating, ventilation and air conditioning plants are changed. However, data must be protected with policies to guarantee the ownership while enabling some form of linkage and archiving (Demchenko et al., 2013).

An important advancement made possible by IoT technologies concerns the case-based learning and its pollination with flipped learning approaches. The smart city offers a wide variety of use-cases helping students to evaluate data and draw conclusions. This, for instance, can be the scenario of using measurements from IoT nodes to investigate the impact of pollutants on the health of citizens. To this aim, the work by Ali et al. (2017) offers many insights applied to the medical scenario also highlighting the pervasive nature of security. However, this requires to engineer privacy and security techniques able to scale from a datacenter dimension to the single user device. Unfortunately, full scalability properties are difficult to achieve and pose different challenges, for instance excessive resource requirements or energy drains (Caviglione et al., 2017).

As envisioned in the work by Coccoli et al. (2017), one of the ultimate goals of a smarter university is the deployment of ICT solutions to let individuals collaborate and cooperate. By using technologies *à la* Industry 4.0, universities can manage assets and resources (Coccoli et al., 2016), develop proper access information, and design safer campuses and buildings (Aldowah et al., 2017). At the same time, this causes additional vulnerabilities, as the entire university becomes part of the smart city.

Concerning mobile and ubiquitous learning approaches, their adoption in a smart city scheme could expose devices of users (e.g., smartphones and tablets) to many attacks, including data exfiltration of biometric information or geo-tagged data, colluding applications and energy draining attacks, DoS, zombification and cycle stealing threats, for instance for mining crypto currencies (Cabaj et al., 2018).

As a concluding remark, the plethora of IoT nodes, smart devices, home appliances and wireless sensors potentially account for a "security tsunami" (Dragoni et al., 2016). Indeed, this heavily impacts on the technological infrastructure (as discussed in Section 5), but also shifts part of the responsibility on students and teachers. Therefore, training and technological awareness of individuals should be considered a prime countermeasure.

4. Data Space

The data space ***D*** is where information relevant to the learning activities circulate. In general, accounts and achievements of users are managed by the LMS, while learning objects, learning analytics and interactions among students have not clear boundaries. For instance, measurements coming from sensors network as well as open data published by the municipalities can be mixed in a smart city. Therefore, data should support standard formats for both store and exchange purposes. This allows accessing a vast scientific literature and software libraries, while reducing vulnerabilities caused by poor design or implementations. For instance, the work by Bartoli et al. (2011) reviews the different actors that concur for the security of a "smart" scenario: the resulting technological space is very mixed and requires a meticulous management. The work of Gharaibeh et al. (2017) offers a holistic view of the lifecycle of data within a smart city. In more detail, authors observe that interconnected objects demand for security and network technologies able to handle data collection, processing and dissemination. This poses several cross-layer challenges and their negligence may

have catastrophic outcomes. In fact, overlaying a learning application on a smart city worsens the resulting data space, which can be also cross-pollinated with bits of information gathered from sources linked with the account of the learner. As a consequence, leakage of data or functionalities belonging to the learning application should not impact on the city or partially void the physical security of citizens and users. In this vein, a major risk deals with de-anonymization attacks and vulnerabilities of users at a physical level. Multiple profile fusion attacks can be done in social media, and gathered data can be used to empower social engineering threats. Attackers posing as a learner or as a teacher can manipulate the data from the smart city or leak sensitive information such as the physical location of hands-on laboratories, or preferred smart devices used to perform assignments.

Another relevant risk concerns data, which could be vast and contain composite and untrusted information coming from sensors, devices and crowds. Specifically, it can be used to hide communication channels, which can be used to exfiltrate sensitive bits (e.g., identity of learners or their credentials), or to perform profiling campaigns, to transform portions of the software architecture in elements of a botnet (Wendzel et al., 2014).

Concerning multimedia data, a variety of IoT nodes and smart devices exploit video information to automatically recognize patterns, objects, or shapes. Usually, this is done to enforce security or to perform some optimizations, for instance by counting people or vehicles using a portion of the street. Indeed, video is also important for learning purposes and it is a valuable tool to quantify the attention of the learner as well as to adapt the material or re-think some learning strategies (Farhan et al., 2018). The collected information has to be properly secured and anonymized as it can leak many privacy bits, as well as it can be exploited for different attacks, including to feed machine learning algorithms to produce fake identities or fraudulent photomontages.

As regards possible pollinations with other applications interacting with IoT or wearable sensors, smart e-learning frameworks share many concerns and pitfalls with the e-health universe. Specifically, it is very hard to develop a platform able to exercise suitable control on the entire "information chain" and security and privacy requirements should be properly standardized, especially to enforce a privacy and security by design approach (Guadagni et al., 2015).

Lastly, when in the presence of a balkanized space like the one characterizing smart city used for learning purposes notions dealing with cybersecurity should be precisely clarified. For instance, Heath (2014) indicates that privacy is an ill-defined concept subject to different interpretations causing misbehaviors due to incompatible software implementations or unclear settings.

5. Infrastructure Space

The interactions within the infrastructure space ***I*** vary according to the specific learning needs. A major driver is the LMS, and its evolution from a closed system to a more distributed form heavily influences the security models to be adopted. In fact, legacy LMSs used walled-garden architectures, which handled the mere delivery of learning material. In this case, learners access the platform via web-based clients retrieving data through secured Internet connections or intranet accesses. In contrast, today many activities involve entities and systems outside the platform and may rely on very different technological solutions. In this perspective, the most significant is cloud/fog computing, which is crucial to develop future e-learning applications, since it is fundamental to implement sensor fusion in a fully connected city (Schaffers et al., 2011).

Cloud and fog computing approaches to support e-learning applications, including learning analytics services, are becoming ubiquitous and populate the toolbox of many course architects and software developers (Manca et al., 2016; Fernández et al., 2014; Caviglione et al., 2011a). Therefore, Education-as-a-Service or Smart-City-as-a-Service will become relevant paradigms in the next future, thus requiring proper security levels, including enforcing privacy of users and protection of information, typically spread over different nations with different laws and requirements.

The e-learning community should also focus on cloud security to borrow pros and evaluate cons. For instance, Jeong et al. (2013) underline the need of developing suitable techniques to encrypt the learning context of students and to retain backup data. This accounts for ad-hoc security policies, and mechanisms to enforce data preservation, service availability, reliability, and resiliency. Fortunately, such properties are often built-in and can be shifted from the e-learning framework towards the cloud via proper delegation schemes. At the same time, this could lead to additional vulnerabilities caused by unsecure network connections or Man-in-the-Middle (MitM) attacks. Security and privacy concerns of the joint use of cloud and e-learning are also relevant among students (Arpaci et al., 2015), thus the introduction of the smart city factor may lead to their exacerbation and should be planned carefully.

6. Examples

In this section, we present three toy examples describing how the proposed holistic model can be used to drive the evaluation of security and privacy risks of a learning applications interacting with the smart city. We underline that our approach allows rating the overall learning framework to have a guideline for its deployment.

6.1 Example: Real vs Synthetic Data

Let us consider an application enriching the learning experience with data from the field. To this aim, two possible paradigms can be used (Caviglione & Coccoli, 2018): *i*) the information is made available in an asynchronous manner, for instance by the municipality via open data, or *ii*) data is collected "live" with ad-hoc devices, such as, sensors and IoT nodes.

For the case *i*), risks are primarily limited to the data space ***D***. For instance, data can be altered with fake information (d_1='data corruption'), contain hidden information (d_2='steganography attack') or be not properly anonymized thus including sensitive data (d_3='privacy leak'). Obtaining open data usually requires downloading some files from a host operated by the municipality, hence MitM attacks targeting the ***I*** space are not likely. Instead the learner can be attacked in his/her space ***L*** by using corrupted data to alter the behavior of the host (e.g., by exploiting a l_1='buffer overflow'). Merging the two spaces can increase the number of vulnerabilities, hence making the space ***C*** less secure. For instance, if the learning application implements a hands-on laboratory, the physical security of the user can be endangered by poisoning ***D***, i.e., by exploiting d_1='data corruption', and ask the user to move in an unsafe physical space location. This corresponds to a new l_2 ='physical security' threat. As a result, J=2+3=5, instead of the original J=4.

Instead, for the case *ii*), additional attacks can happen in ***I***, which is a relevant part of the overall learning experience. In fact, data can still be corrupted or manipulated as in the previous case, but also spoofed or reduced by making a sensor unreachable, i.e., i_1='spoofing', or the user can be deceived by injecting fake GPS data, hence leading to i_2='GPS manipulation'. Therefore, the overall space ***C*** can be further augmented with joint threats like, d_2+i_1 in which data is manipulated to exfiltrate information through a covert channel (l_3='exfiltration of data'), or l_1+i_1 leading to DoS by means of ad-hoc crafted packets generated via IoT nodes. Nevertheless, physical space can be also endangered as in the previous case by using "live" data instead of static entries in the file. As a result, J =(2+3+ 2)+2=9. The course architect can then use this indicator to evaluate if his/her team, the budget, or the skills of the teacher/learners are adequate with respect to the resulting complete space ***C***.

6.2 Example: Virtualized Environments

In this example, we consider a learning application based on the Platform-as-a-Service paradigm. As described by Coccoli et al. (2015), students from different universities interact with remote virtual machines to complete assessments or to emulate a laboratory or hardware facilities not available locally. Let us focus on the infrastructure space ***I***. In general, for the case of cloud, it is partially outside the control of the developer of the learning experience. As a consequence, virtual machines can collude to exfiltrate data via a local covert channel or exploit shared portion of the hypervisor or of the underlying hardware to exchange information (Cabaj et al., 2018). This leads to a vulnerability i_1='unintended exchange of data' and it is limited to the PaaS provider. Let us now also consider the data space ***D***. A possible implementation of the learning experience can use a mixed public/private cloud scenario, where personal information of learners is locally stored. Another idea could rely upon a fully public framework. However, information is stored in the cloud and can be exfiltrated by using the vulnerability i_1. For instance, information to be processed by learning analytics algorithms or data to perform authentication and accounting may reside in a virtual machine and can be leaked towards another one under the control of the attacker. Accordingly, this may lead to a d_1=leak of sensitive data or login credentials. As a result, ***C*** is characterized by J=2, whereas the mixed public/private solution by J=1. Hence, a sort of trade-off among fine-grained control of data, complexity and cost of the platform has been made. space ***C***.

6.3 Example: Contactless Data

Another possible example of the interplay among different technologies considers the interaction of annotated objects (Coccoli & Torre, 2014), which are often accessed via RFID, for instance in cultural heritage applications or in smart museums (Caviglione et al., 2011b). In this case, the museum has to be considered a portion of the smart city, and similar usage paradigms can be envisaged in other scenarios, e.g., when the Near Field Communication (NFC) technologies are deployed. By considering our modelling, the usage of contactless communications may cause additional fragilities in the ***I*** space, as the data can be intercepted via a MitM attack, i_1='MitM'. This can be mixed with the vulnerabilities in the data space, for instance d_1='plain data', which happens when the information is not properly encrypted. Such a case characterizes LMS not supporting end-to-end

cyphering of flows, or developers not considering as sensitive some bits of information. Hence, d_1 can be mixed with privacy leaks of the learning space $\boldsymbol{L}$ (such as l_1='learning objects enriched with personal information') and the attacker can exploit $i_1+d_1+l_1$ to perform a user profiling by means of a fusion of all the data sensed, including information on "when" and "where" it has been collected. As a consequence, $J=(1+1+1)+1=4$, thus: course developers should understand the security requirements of data, limit the amount of unneeded information exchanged, and avoid to allow personal details to travel through the smart learning infrastructure.

7. Conclusions and future work

In this paper, we have introduced a holistic model to identify and classify threats and vulnerabilities characterizing e-learning frameworks taking advantage of smart cities. As shown, the resulting space is very complex and the combination of a multifaceted set of technologies multiplies the risks impacting over the entire architecture.

The issues presented for each space, as well as toy examples, demonstrated that emerging paradigms and applications require to not neglect the complex interplay between security and privacy requirements. This is especially true for the case of smart cities, since it is composed of entities like buildings, which are very attractive targets for cybercriminals. Therefore, the e-learning applications should be hardened as to not represent an entry point for the attack or to not behave as a trojan. Besides, the impact of IoT is cross-space, i.e., it affects all the functional layers. Learners and teachers should be also educated in the risks and fragilities arising from the use of information coming from realistic setups or when interacting with software artifacts beyond the control of the course architect. Future work aims at refining the model, possibly by using formal methods. A relevant part of our research deals with the development of suitable algorithms to automate the detection of privacy leaks and security hazards during the design phase of a smart-capable course.

References

Aldowah, H., Rehman, S. U., Ghazal, S., and Umar, I. N. (2017). Internet of Things in higher education: a study on future learning. In Journal of Physics: Conference Series, 892(1), 12-17.

Ali, M., Bilal, H. S. M., Razzaq, M. A., Khan, J., Lee, S., Idris, M., Aazam, M., Choi, T., Han, S. C., and Kang, B. H. (2017). IoTFLiP: IoT-based flipped learning platform for medical education. Digital Communications and Networks, 3(3), 188-194.

Allwinkle, S. and Cruickshank, P. (2011). Creating smart-er cities: an overview. Journal of Urban Technology, 18(2), 1-16.

Anwar, M. M., Greer, J., and Brooks, C. A. (2006). Privacy enhanced personalization in e-learning. In Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services.

Anwar, M. and Greer, J. (2012). Facilitating trust in privacy-preserving e-learning environments. IEEE Transactions on Learning Technologies, 5(1), 62-73.

Arpaci, I., Kilicer, K. and Bardakci, S. (2015). Effects of security and privacy concerns on educational use of cloud services. Computers in Human Behavior, 45, 93-98.

Bartoli, A., Hernández-Serrano, J., Soriano, M., Dohler, M., Kountouris, A., and Barthel, D. (2011). Security and privacy in your smart city. In Proceedings of the Barcelona smart cities congress, 292.

Bdiwi, R., de Runz, C., Faiz, S., and Cherif, A. A. (2018). A blockchain based decentralized platform for ubiquitous learning environment. In Proceedings of the 2018 IEEE 18th International Conference on Advanced Learning Technologies (ICALT), 90-92.

Bellekens, X., Hamilton, A., Seeam, P., Nieradzinska, K., Franssen, Q., and Seeam, A. (2016). Pervasive eHealth services a security and privacy risk awareness survey. In Proceedings of the 2016 IEEE International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 1-4.

Bertino, E. and Ferrari, E. (2018). Big data security and privacy. In A Comprehensive Guide Through the Italian Database Research Over the Last 25 Years, 425-439, Springer, Cham.

Bonneau, J. (2012). The science of guessing: analyzing an anonymized corpus of 70 million passwords. In Proceedings of the 2012 IEEE Symposium on Security and Privacy (SP), 538-552.

Borcea, K., Donker, H., Franz, E., Pfitzmann, A., and Wahrig, H. (2005). Towards privacy-aware elearning. In Proceedings of the International Workshop on Privacy Enhancing Technologies, 167-178.

Cabaj, K., Caviglione, L., Mazurczyk, W., Wendzel, S., Woodward, A., and Zander, S. (2018). The new

threats of information hiding: the road ahead. IT Professional, 20(3), 31-39.

Carbonaro, A. (2012). Interlinking e-learning resources and the web of data for improving student experience. Journal of E-Learning and Knowledge Society, 8(2), 33-44.

Caviglione, L. and Coccoli, M. (2018). Smart e-learning systems with big data. International Journal of Electronics and Telecommunications, 64(4), 445-450.

Caviglione, L., Gaggero, M., Cambiaso, E., and Aiello, M. (2017). Measuring the energy consumption of cyber security. IEEE Communications Magazine, 55(7), 58-63.

Caviglione, L., Coccoli, M., and Merlo, A. (2014). A taxonomy-based model of security and privacy in online social networks. International Journal of Computational Science and Engineering, 9(4), 325-338.

Caviglione, L., Coccoli, M., and Gianuzzi, V. (2011). Opportunities, integration and issues of applying new technologies over e-learning platforms. In Proceedings of the 3rd International Conference on Next Generation Networks and Services (NGNS), 12-17.

Caviglione, L., Coccoli, M., and Grosso, A. (2011). A framework for the delivery of contents in RFID-driven smart environments. In Proceedings of the IEEE International Conference on RFID Technologies and Applications, 45-49.

Caviglione, L. (2009). Can satellites face trends? The case of Web 2.0. In Proceedings of the International Workshop on Satellite and Space Communications, 446-450.

Caviglione, L. (2006). Introducing emergent technologies in tactical and disaster recovery networks. International Journal of Communication Systems, 19(9), 1045-1062.

Coccoli, M., Maresca, P., and Stanganelli, L. (2017). The role of big data and cognitive computing in the learning process. Journal of Visual Languages and Computing, 38(1), 97-103.

Coccoli, M., Maresca, P., and Stanganelli, L. (2016). Cognitive computing in education. Journal of E-Learning and Knowledge Society, 12(2), 55-69.

Coccoli, M., Maresca, P., Stanganelli, L., and Guercio, A. (2015). An experience of collaboration using a PaaS for the smarter university model. Journal of Visual Languages and Computing, 31, 275-282.

Coccoli, M. and Torre I. (2014). Interacting with annotated objects in a semantic web of things application. Journal of Visual Languages and Computing, 25(6), 1012-1020.

Demchenko, Y., Grosso, P., De Laat, C., and Membrey, P. (2013). Addressing big data issues in scientific data infrastructure. In Proceedings of the 2013 International Conference on Collaboration Technologies and Systems (CTS), 48-55.

Dragoni, N., Giaretta, A., and Mazzara, M. (2016). The Internet of hackable things. In Proceedings of the International Conference in Software Engineering for Defence Applications, 129-140.

Farhan, M., Jabbar, S., Aslam, M., Hammoudeh, M., Ahmad, M., Khalid, S., and Han, K. (2018). IoT-based students interaction framework using attention-scoring assessment in e-learning. Future Generation Computer Systems, 79, 909-919.

Fernández, A., Peralta, D., Benítez, J. M., and Herrera, F. (2014). E-learning and educational data mining in cloud computing: an overview. International Journal of Learning Technology, 9(1), 25-52.

Ganti, R. K., Ye, F., and Lei, H. (2011). Mobile crowdsensing: current state and future challenges. IEEE Communications Magazine, 49(11), 32-39.

Gharaibeh, A., Salahuddin, M. A., Hussini, S. J., Khreishah, A., Khalil, I., Guizani, M., and Al-Fuqaha, A. (2017). Smart cities: a survey on data management, security, and enabling technologies. IEEE Communications Surveys & Tutorials, 19(4), 2456-2501.

Guadagni, F., Scarpato, N., Patrizia, F., D'Ottavi, G., Boavida, F., Roselli, M., Garrisi, G., and Lisi, A. (2015). Personal and sensitive data in the e-health-IoT universe. In International Internet of Things Summit, 504-514.

Hashem, I. A. T., Chang, V., Anuar, N. B., Adewole, K., Yaqoob, I., Gani, A., Ahmed, E., and Chiroma, H. (2016). The role of big data in smart city. International Journal of Information Management, 36(5), 748-758.

Heath, J. (2014). Contemporary privacy theory contributions to learning analytics. Journal of Learning Analytics, 1(1), 140-149.

Humayed, A., Lin, J., Li, F., and Luo, B. (2017). Cyber-physical systems security - A survey. IEEE Internet of Things Journal, 4(6), 1802-1831.

Jeong, J. S., Kim, M., and Yoo, K. H. (2013). A content oriented smart education system based on cloud computing. International Journal of Multimedia and Ubiquitous Engineering, 8(6), 313-328.

Kambourakis, G. (2013). Security and privacy in m-learning and beyond: challenges and state of the art. International Journal of u-and e-Service, Science and Technology, 6(3), 67-84.

Kang, B. H. and Kim, H. (2015). Proposal: a design of e-learning user authentication system. International Journal of Security and Its Applications, 9(1), 45-50.

Manca, S., Caviglione, L., and Raffaghelli, J. (2016). Big data for social media learning analytics: potentials and challenges. Journal of e-Learning and Knowledge Society, 12(2), 27-39.

Marais, E., Argles, D., and von Solms, B. (2006). Security issues specific to e-assessments. In Proceedings of the 8th Annual Conference on WWW Applications.

Miguel, J., Caballé, S., and Prieto, J. (2012). Providing security to computer-supported collaborative learning: an overview. In Proceedings of the 2012 4th IEEE International Conference on Intelligent Networking and Collaborative Systems (INCoS), 97-104.

Miller, K. W., Voas, J., and Hurlburt, G. F. (2012). BYOD: security and privacy considerations. It Professional, 14(5), 53-55.

Neila, R. and Rabai, L. B. A. (2014). Deploying suitable countermeasures to solve the security problems within an e-learning environment. In Proceedings of the 7th International Conference on Security of Information and Networks, 33-38.

Riccucci, S., Carbonaro, A., and Casadei, G. (2007). Knowledge acquisition in intelligent tutoring system: A data mining approach. In Proceedings of the 6th Mexican International Conference on Artificial Intelligence, 1195-1205. Springer, Berlin, Heidelberg.

Schaffers, H., Komninos, N., Pallot, M., Trousse, B., Nilsson, M., and Oliveira, A. (2011). Smart cities and the future Internet: Towards cooperation frameworks for open innovation. In The future Internet assembly, 431-446. Springer, Berlin, Heidelberg.

Ten, C. W., Manimaran, G., and Liu, C. C. (2010). Cybersecurity for critical infrastructures: attack and defense modeling. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 40(4), 853-865.

Wendzel, S., Mazurczyk, W., Caviglione, L., and Meier, M. (2014). Hidden and uncontrolled - On the emergence of network steganographic threats. In ISSE 2014 Securing Electronic Business Processes, 123-133. Springer Vieweg, Wiesbaden.

Wilkowska, W. and Ziefle, M. (2011). Perception of privacy and security for acceptance of e-health technologies: exploratory analysis for diverse user groups. In Proceedings of the 2011 5th International Conference on Pervasive Computing Technologies for Healthcare, 593-600.

Zuev, V. I. (2012). E-learning security models. Management Information Systems, 7(2), 24-28.