Security and Privacy in m-Learning and Beyond: Challenges and State-of-the-art

Georgios Kambourakis

Laboratory of Information and Communications Systems Security (Info-Sec-Lab)
Department of Information and Communication Systems Engineering
University of the Aegean
Karlovassi, Samos, GR-83200, Greece
gkamb@aegean.gr

Abstract

Mobile learning is constantly evolving, following the shift of mobile technologies from laptops to handheld devices and smartphones. Indeed, the opportunities for innovation in this area are numerous and constantly under the focus of all the parties involved, ranging from traditional schools and universities to individual learners. However, mobile technology brings along increased threats to system and data security and privacy, given the fact that learners and educators are mobile, and in most cases, permitted to use their own mobile devices to access resources and services. After identifying the challenges, this paper provides a comprehensive review and classification of the state-of-the-art research on security and privacy in the m-learning realm and beyond. As far as we are aware of, this is the first time an exhaustive and detailed survey of this kind is attempted.

Keywords: *m-learning; security; privacy; survey*

1. Introduction

During the last decade, mobile learning (m-learning) has established itself as a way to constitute learning more accessible, personalized and flexible for students everywhere [1-2]. This is mainly thanks to the mushrooming of mobile devices and services, and the increasing capabilities of modern smartphones. Obviously, m-learning, whether formal or informal, has significantly evolved over the years passing from the laptop era to the current generation of ultramodern smartphones and beyond to the so called context-aware ubiquitous learning (u-learning) [3]. It is also for certain that m-learning is not just a descendant or extension of e-learning, but rather a quite different learning philosophy and practice. This is self-evident when considering that we do not utilize our mobile devices in the same way we use our desktop or even laptop machines. In fact, the differences between the *e-* and *m-* in regards to learning are so prominent that it imposes an entirely different path to be followed towards information presentation, instructional design, graphic and user experience design, to name just a few.

However, apart from the native educational issues revolving around m-learning, there exist several other concerns that stem from the misuse of the mobile technology and may affect negatively m-learning adoption [4-6]. For instance, educational institutions, educators, and individual learners may be deeply concerned about the growing threats to data security and privacy [7-8], given that in most cases learners are allowed to use their own mobile devices to access m-learning services and resources. Indeed, several projects [9-10], as well as other

works [11], come to the same conclusion. Such concerns can hamper the penetration of mobile technologies into the education realm, and hence prevent stakeholders from capitalizing on the benefits that these technologies bring along.

Until now, most m-learning advances have focused on course development, deployment and delivery, paying little attention to security and privacy. For instance, the authors in [12] investigate the state-of-the-art in frameworks and middleware for facilitating mobile and ubiquitous learning (u-learning) development, and conclude that further development is needed in the privacy and security field to build systems that guarantee user's rights. In several cases, security and privacy concerns have been downplayed, considered and conceptualized in a similar way as in the context of e-learning. However, as already pointed out, this is actually not the proper way to do so, as m-learning is directly influenced by mobile technologies and is more about interacting with information at the moment they are needed and/or in a specific use context. Therefore, the issues of security and privacy in the m-learning realm are expected to be quite different from those confronted in legacy e-learning systems. For example, when focusing on privacy, the involved parties may be especially worried about the use of sensitive personal data collected indirectly (*e.g.*, without the implicit user's consent) such as mobile phone number, IP address, location data, International Mobile Equipment Identity (IMEI), unique phone ID, and so forth. Similar concerns, but for security, apply to usual learning activities like those of e-examination which may be totally uncontrollable under the m-learning setting. Responding to the aforementioned needs, so far, several researchers have identified security and privacy issues especially for the m-learning ecosystem.

Our contribution: The contribution of this paper is twofold. First, it identifies challenges germane to security and privacy in the m-learning setting and beyond. Naturally, several of these challenges can be identified for e-learning in general, but here effort is put to examine them solely under the m-learning prism. Second, a comprehensive review of literature addressing security and privacy in the m-learning ecosystem is attempted. After briefly analyzing each work, we classify them with reference to the challenges identified as well as other general criteria that help us to draw a clearer picture of the on-going research in this particular area. To the best of our knowledge, it is the first time an exhaustive and detailed survey of this kind is attempted.

The remainder of this paper is organized as follows: The next section identifies challenges in the m-learning ecosystem pertinent to security and privacy. Section 3 reviews the state-of-the-art in the area and provides a categorization of the various works based on the challenges identified and other related factors. The last section concludes the paper and suggests a way forward.

2. Challenges: Now and beyond

As already pointed out, apart from pedagogical issues regarding ways the mobile technology can be exploited to support teaching, organizations involved in the provision of m-educational services need to cope with a variety of technical, administrative, and in some cases, legal challenges [6]. This section identifies challenges germane to security and privacy as a first step prior to analyzing the state-of-the-art in the area. Figure 1 provides a schematic overview of these challenges for clarity and easy reference.

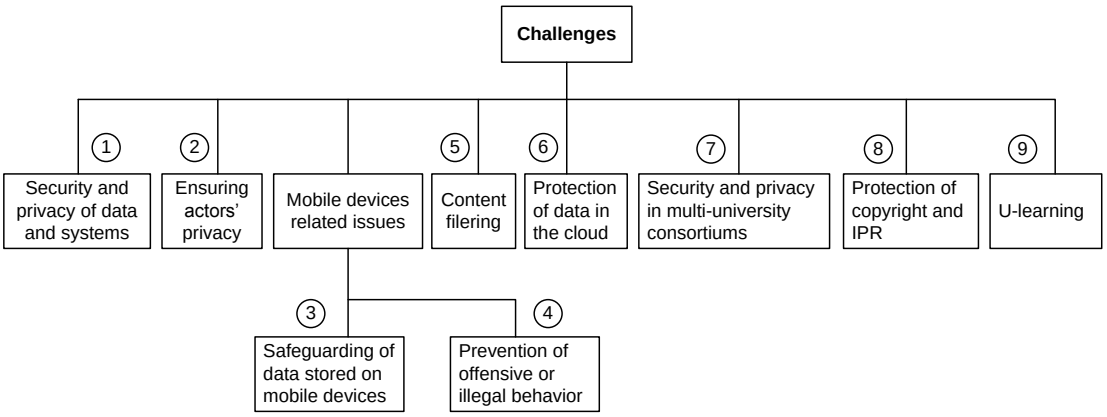

Figure 1. Security and Privacy Challenges in m-learning and beyond (the number of each Challenge is given with Reference to Table1)

2.1. System and Data Security and Privacy

Without doubt, the protection of systems - either on the client or server side - for running smoothly and being capable of providing their services to the legitimate user is crucial for any educational realm. This challenge has to do with securing the systems and deploying proper security policies and procedures so as to be able to deter and repel attacks. It also requires insuring the integrity, privacy and confidentiality of the data stored and transferred for the needs of the educational process. Therefore, the provision of robust mechanisms to support learner authentication, authorization, non-repudiation, management of data, content copying, editing and downloading, and safeguarding learner examination and assessment processes from attackers and impostors are only some prerequisites for the e-learning arena.

Especially for m-learning, some - if not all - of the aforementioned needs become even more sophisticated because learners are constantly on the move, they use a diversity of out-of-control devices, and they usually connect via wireless interfaces. For instance, connecting to an unsecured wireless network increases the risk of connection hijacking, meaning that it automatically puts personal data at risk. Therefore, educators and learners should be alarmed of the potential risk of automatically connecting to potentially rogue wireless access points controlled by attackers. Overall, the use of mobile technologies it is for sure to pose the confidentiality, integrity and privacy of the data involved in the educational process for both the learners and the service at stake [13]. In this regard, student records, e-portfolio data, assessment data, are only some examples of sensitive information that need to be protected.

On the service side, legacy protection mechanisms such as firewalls and anti-malware software compile a common solution. However, as already pointed out, mobile technologies augment the risk of ill-motivated or even casual users trying to get access to restricted resources, download content without having the authorization, inject malware, and clogging server and network performance. On the learner's side, the utilization of common-sense mechanisms such as passwords is imperative. Other, more advanced solutions may involve biometric security mechanisms, encryption and the installation of firewall and anti-malware software for mobile platforms. However, even in such cases, nothing is guaranteed. For instance, mobile firewalls typically inspect all IP interfaces, but they often neglect the Bluetooth interface. Several other attack incidents especially reported for mobile services [14] suggest that educators and learners should be extremely concerned about the safety of their data stored on the device and communicated over the air.

A last topic in this group of challenges has to do with e-examination procedures carried out in non- or semi-supervised way. Without doubt, this is one of the hardest challenges within the m-learning context. This issue can be quite complex and it is better to be dealt on a case by case basis, *e.g.*, proportional to the strictness of the e-examination procedures imposed by the organization. In any case, proper confidentiality, integrity, non-repudiation - and some time anonymity mechanisms - may need to be in place in order to preserve security and privacy during different examination stages.

2.2. User Privacy

When it comes to the protection of user privacy, mobile technologies provide several possibilities for constantly monitoring the behavior of learners. Nevertheless, while such a possibility is claimed to be used for the protection of the learner itself (*e.g.*, as a means to deter cyber-bullying) and the safeguarding and easy administering of educational assets, it may sometimes be regarded as violating or trampling on user's privacy sphere. Also, collecting and evaluating personal data such as information about user's preferences and goals is essential in order to be able to provide assistance for learners, achieve assessment, or ease collaboration between users. This is actually a tradeoff between preserving user's privacy and monitoring and controlling learner's behavior. For example, the monitoring of learners content of communication, geographic location, and/or browsing behavior may be easily assumed to lead to profiling the user in the mid or long term. So, for example, a privacy-preserving mechanism is needed to enable users to be identifiable only if necessary or they wish to, say, for enabling debates with others on a certain subject, arrange a meeting with certain classmates that roam near to them, or letting the tutor to assist them. Moreover, users must be able to create their own reputation in class by revealing certain pieces of information but not everything. In this way, upon registering to a new class, learners feel comfortable to work in a non-prejudiced environment, that is, independently of outcomes of previous classes.

Mobile devices have been long criticized for leaking the location of its user and consequently tracking their movement in space. Thus, location tracking is generally considered unacceptable not only for learners, but anyone. On the other hand, as already mentioned, there exist some cases where device tracking may be handy. For example, when trying to locate a stolen device, a missing person, or deny access to a device reported stolen. In fact, this may be compulsory in case where the mobile devices provided to learners for supporting the educational process are property of the educational institution. The latter has put in place a Mobile Device Management (MDM) system for administering the devices in real-time. That is, locate, track and gather information on the movement of devices, with the aim to remotely diagnose and fix software problems, install and update software on devices, erase data from lost or stolen devices etc.

Personal mobile numbers are also a private piece of information and if used by the institution, this must happen only for supporting the provision of learning (*e.g.*, informing a student about an urgent event). Privacy is also closely related to biometric-based authentication schemes enforced by mobile devices and used in many educational contexts to authenticate students and academic personnel, say, upon laboratory entry.

From the above it becomes obvious that, in the context of m-learning, the provision of privacy-preserving mechanisms is very important for safeguarding private sensitive data. These may include: name, gender, birth data, address, credit card details, biometric characteristics of a person, mobile phone number, email address, location data, IP address, IMEI, location data, service usage data, e-mail, call record and web-browsing log files and history, security credentials, *etc*.

2.3. Mobile Device Related Issues

In many cases, especially in those the learning institution supplies young learners with special mobile equipment, there exist concerns about making learners attractive to thieves. This is however a general problem considering the fact that especially in developed countries virtually all young people carry at least one mobile device. When properly utilized, user/device post-authentication solutions based on the behavior of the user and contextual data (e.g., the place the user roams) as well as MDM systems could also be of particular help in this case. Another solution to this problem could be the marking of devices with large and easy notable organization logos. This issue is also related with the safeguarding of data stored on mobile devices. In the m-learning context this data might relate to the user of the device (*e.g.*, personal data or data about their learning curve and assessments), an employer of the learner (*e.g.*, corporate sensitive data), a client of the organization the learner works for (*e.g.*, think of medical education - sensitive data about patients). Passwords, biometric security mechanisms and encryption are some methods towards combating this threat.

Some other concerns stem from the functionalities that mobile devices incorporate. For instance, social networking websites and the use of high resolution cameras in mobile devices give rise to worries about bullying or embarrassing learners or educators. Naturally, mobile technology has augmented the risks for abusing behavior as it is easy to capitalize on the functionality of mobile technologies to photograph or capture on tape individuals for posting and making fun of them. However, it is not clear if the use of mobile technologies in the m-learning context increases that risk or not. This also applies to m-learning scenarios destined to employees. So, for example, in such setting the use of camera embedded in mobile devices may be forbidden due to the possibility of corporate information leaks.

2.4. Content Filtering

Another challenge has to do with controlling and restricting access to improper, and in some cases, illegal online content. This means that m-learners, especially the younger and naive ones, should be obstructed from accessing websites or other online content that is characterized as either illegal (*e.g.*, illegal file sharing and downloading websites) or inappropriate for (young) people (*e.g.*, gambling sites). Among others, such sites are also known to be used by attackers for spreading malware. Entry to online communication tools (*e.g.*, chat-rooms) that may be used by perpetrators for grooming or other offensive actions targeting children must also be banned. Access to other websites, like those of social networks, also need to be controlled as it may hamper or obstruct the learning process.

Security policies and hardware and software systems (firewalls, filtering, anti-malware) are usually utilized toward tackling this issue. However, this is not enough in the case of m-learning because learners use their devices outside the organization premises. So, in addition to standard mechanisms for controlling access to the institution's wired and wireless network, extra protection measures need to be implemented and installed in the device. Excluding user discontent, this option requires a lot of administration effort to constantly deal with installing and maintaining software on (possibly) different mobile platforms and handling user complaints. Stakeholders, including mobile operators, service providers, governments etc can also help in increasing the effectiveness of any conjunctionally deployed countermeasure by providing additional network security and monitoring mechanisms and specifying policies, regulations and laws related to this particular problem.

2.5. Cloud Education and Cross-educational realms

In the recent years, the cloud computing paradigm has emerged as an attractive solution for education realms. For example, think of an educator wishing to share several large files with mobile learners. This could be easily attained thanks to a cloud storage service such as Dropbox. Of course, cloud computing brings several goodies to the m-learning ecosystem including: (a) virtually unlimited storage capacity, (b) defend against data loss in case of lost or stolen devices, (c) automatic, continuous and reliable backup of data, (d) access to resources and collaboration on content in real-time from anywhere, (e) reduced costs for organizations, and (f) easy sharing of information amongst devices. Thus, especially in the case of m-learning, cloud-based device management solutions may facilitate organizations to accommodate the management of disparate mobile platforms, *e.g.*, when supporting a diverse range of mobile devices and operating systems [15].

Nevertheless, security-savvy stakeholders have expressed concerns that this outsourcing may negatively affect the level of security and privacy for any sensitive piece of data stored and administered externally [16-17]. Such worries have gained ground after major attack incidents such as the well-known Sony PlayStation Network security outage in April 2011. Even worse, the employment of mobile learning services on cloud-based infrastructures introduces additional and more complex security and privacy concerns, since no one has the complete control over the whole infrastructure where the services are running. This is due to the: (a) complexity, heterogeneity in terms of network access technology, security and privacy policies, *etc.*, of the involved systems, and (b) diversities in legislation considering the fact that providers act in the global sphere. So, although the cloud providers offer some kind of confidentiality mechanism to protect the data of their customers, the storage of student data imposes special precautions and must be in line with international data protection and privacy laws and regulations.

Another emerging issue related to e-learning in general, and cloud education, at least to some extent, is how to protect data in a cross-institutional collaborative environment that among others support m-learning activities. This issue has been given little attention so far (mostly in the context of e-learning) but studies like [18] report interesting findings regarding security and privacy. Specifically, it is argued that due to the heterogeneity and sometimes complexity of security and privacy policies across realms, systems that support teaching and learning are proved inadequate since they are not properly integrated and provide little access control or privacy of data. For instance, it is highlighted that due to the poor support given to the types of activities of disparate user roles in different phases of the educational process, the available security models used in multi-university consortiums obstruct the management of learning and associated materials.

2.6. Content's Copyright and IPR

Excluding that being purchased by the organization, m-learning material including text, pictures, videos, audio, *etc*., is created by different stakeholders, which may be individual teachers, learners, hobbyists, *etc*. However, often, to ensure fast access in locations where wireless network is unavailable or the service is of low quality, m-learning material may be pre-installed on learner's mobile equipment. This may require protecting the content's copyright and Intellectual Property Rights (IPR) on a case by case basis. To this end, many educators and learners may be unaware of or not paying enough attention to the implications of using and sharing material that comes under some kind of IPR.

2.7. The Shift Towards u-learning

During the last few years we are witnessing a growing interest in context-aware ubiquitous learning (u-learning), which can be conceptualized as a direct descendant of m-learning. So far, in practice, u-learning is realized by capitalizing on the use of advanced forms of mobile technology including GPS, sensor devices, and Radio-frequency identification (RFID) [19]. Near Field Communication (NFC) technology also seems to gain momentum over the last few years. Mobile devices equipped with this technology are able to transmit information through physical proximity to receivers and other devices. It is thus straightforward that this technology, already used for making e-payments, will most likely be used in smartphones and tablets to transfer files, hyperlinks and other information. Therefore, in the near future, the emergence of NFC-driven applications for the m-learning realm it is deemed highly probable. In the same context one can identify other trends like those based on Augmented Reality (AR) and Spatial AR (SAR). For example, we are already witnessed prototypes and other more mature products (see Google Glass) of highly portable devices which combine a camera and wireless connectivity to offer contextual information to users about places, experiences and activities. In the mid or long run, such devices may even replace legacy smartphones at least to some extent.

Such technologies are posed to enhance the learning experience by putting users in position to learn via their interaction with smart objects scattered in the environment [3, 19, 20]. This enables the system to actively provide personalized services to the learners based on the learner's context(s), where the term *context* refers to any information about the user needs and operating environment. For example, think of the case of a museum where each exhibit has been labeled with an RFID tag. It is also assumed that students carry mobile devices equipped with an RFID reader. So, during roaming within the learning area, the system can detect their location by reading and analyzing the data stemming from the nearest RFID tag.

Therefore, in addition to the previously mentioned challenges, u-learning is sure to introduce some interesting directions regarding security and privacy. Without doubt, the tradeoff between the preservation of user's privacy and the enhanced learning experience receives the majority of focus here. This is because as the user constantly interacts with their environment when on the move, several personal information are revealed (*e.g.*, location, history of movement in space, history of interaction with smart objects, preferences *etc*.). This requires the tight coupling of security and privacy with user's current situation (reflected to contextual attributes) in an automatic and continuous manner, and calls for security and privacy policies that are able to offer advanced context-aware information control. Such concerns have already started to attract attention in the general literature [21-24], but as discussed further in the next section have not been yet addressed specifically for u-learning.

2.8. Remarks

As already stated, while m-learning is generally conceived simply as a subset of e-learning it presents certain particularities that constitute it a quite different approach both from a pedagogical and technological point of view. So, each of the above challenges has to be dealt proportional to the needs and constraints of the situation in hand. For example, in an m-learning course running in the context of a lifelong learning adult education program the needs are sure to be substantially different from another designed to complement and enhance formal schooling.

Also, as a general remark, it can be said that the nature of each of the challenges analyzed in this section as well as the way of confronting them profoundly depends on whether the learners (and sometimes tutors) are allowed to use their own mobile equipment (known also

with the term *bring-your-own-device*) for participating in the m-learning activities. One the other hand, mostly due to reasons of homogeneity and easy administration of the mobile assets, several institutions mandate the use of pre-selected hardware and software for enabling access to m-learning classes. Each option has its advantages and disadvantages [6], but it is sure to severely impact the way security and privacy mechanisms and policies are conceptualized and deployed.

3. State-of-the-art and Classification

Until now, a considerable number of works in the literature have been devoted to the issues of security and/or privacy in the context of e-learning. A good overview of this topic can be obtained from [25-34]. As already pointed out, it is not the intention of this paper to delve into the e-learning literature but rather focus primarily on works addressing security and privacy in the m-learning terrain. Nevertheless, proposals been given for e-learning but also touch upon m-learning - due to, for example, their lightweight nature that may allow them to run on mobile devices - will also be analysed. This also means that works based on the use of resource demanding cryptographic schemes on the client-side (*e.g.*, impose some short of Public Key Infrastructure (PKI)) [35-36], have been intentionally neglected, expect if they proposed and tested specifically for m-learning services.

So far, the only works that examine security and privacy issues in the m-learning arena *in toto* are those in [37, 38]. The author in [37] analyzes the weaknesses inherent to mobile devices, aiming to propose methods of addressing risks specific to mobile e-learning. The same applies for the second but most recent work in [38]. While both the aforementioned studies correctly pinpoint threats stemming from the ubiquitous nature of m-learning and the use of mobile devices, identify affected user groups and propose corresponding solutions, do not occupy themselves in providing a comprehensive review and taxonomy of existing solutions. They also mix up proposals and guidelines given for e-learning in general with others formed specifically for m-learning. In the meanwhile, literature in this field has grown. Therefore, to fill this gap, the current paper attempts to systematically review and categorize solutions and proposals explicitly defined for m-learning or others that can be straightforwardly applied to such a context. In the following, we analyze each of them under the prism of Section 2. For helping the reader to grasp a better view of the findings, we use another two criteria for each work. These are: if the proposed solution is based on legacy and/or custom technologies and mechanisms, and on symmetric and/or asymmetric key technology. All the works are summarized in chronological and thematic order in Table 1. Note that security and privacy could also be discussed in a hierarchical way, meaning at infrastructure level, OS level, transmission level, application level, organizational level, user level and so forth. This is however left for future work.

3.1. Review of Works

The works addressed in this section are organized into four groups, *i.e.*, those that: (a) deal with the challenge of system and data security and privacy, (b) address multiple challenges, (c) occupy themselves with the issue of user's privacy, and (d) cope with issues within the scope of (a) but employ biometrics.

Table 1. Listing of Literature Proposals in Chronological and Thematic Order

Work(s)	Challenge					Legacy(L)/Custom(C) solution	Symmetric (S) / Asymmetric (A) cryptography	Specifically defined for m-learning
	1	2	6	7	8			
[39]	√					C (IDS)	N/A	Yes
[40]	√					C	S	Yes
[41]	√					Both (XML)	N/A	Yes
[42]	√					C (Ajax, XML)	N/A	No
[43]	√					Both (XML)	Both	Yes
[44]	√					C	S	Yes
[28]	√					C	A	Yes
[45]	√					C (Bluetooth)	S	Yes
[46]	√	√				C (Digital identity)	N/A	Yes
[47]	√	√	√		√	N/A	N/A	Yes
[48]	√	√				C	Both	No
[49]	√				√	C	N/A	Yes
[18, 50]	√			√		C (RBAC, XML)	N/A	No
[51, 52]	√				√	L (DRM)	Both	Yes
[9]		√				C (Partial identities & aliases/pseudonyms)	N/A	No
[53]		√				C (Pseudonymity)	N/A	No
[54-56, 59-62]	√					Biometrics	N/A	Only for [61, 62]

Works Addressing the Challenge of System and Data Security and Privacy

The work in [39] deals with Mobile Collaborative Learning (MCL). The authors observe that while several supporting architectures and frameworks have been introduced to enhance MCL, so far, no literature is devoted to enhancing the security of these frameworks with the intention to provide secure MCL services to learners. Motivated by this fact, they propose a way to handle the incidents of rogue Dynamic Host Configuration Protocol (DHCP) server that can be used by attackers to release incorrect IP addresses to users, and thus enable eavesdropping on the communication line. To do so, they employ an anomaly-based Intrusion Detection System (IDS) towards detecting malicious attacks and blocking the activity of such rogue network elements.

The authors in [40] highlight that due to its low cost, availability, and wide coverage of mobile networks, several m-learning services use Short Message Service (SMS) to deliver sensitive content. Motivated by this fact they propose a lightweight solution that is able to secure the SMS content with minimal impact on the device performance. The solution is based on symmetric encryption and is assumed to be used in the context of a distributed m-learning architecture. The authors provide implementations of their scheme in .NET and Java ME platforms and correctly conclude that the basic shortcoming of such an approach is the way the secret key is transmitted to the communication parties.

The work in [41] capitalizes on XML and Java and presents a proof-of-concept implementation used to assess the potential of mobile devices in testing (computer-assisted assessment) as compared to legacy web-based assessment systems. The authors also describe an authoring tool to build adaptable and adaptive computerized tests that can be executed on different platforms ranging from personal computers to mobile phones. They highlight on security issues revolving around their system in an effort to prevent students from cheating when using their mobile device during testing.

The contribution presented in [42] tries to tackle the issue of arbitration in e-learning contestation processes and propose a non-repudiation system for student evaluation based on web services. They capitalize on Asynchronous JavaScript (AJAX) frameworks aiming to implement Extensible Markup Language (XML) security standards to provide improved user experience, asynchronous data exchange and message authentication for on-line test papers. While this work is defined for the e-learning realm, the fact that it is based on XML security makes it appropriate for m-learning. The work in [43] also utilizes XML security standards such as XML Encryption and Signature in an effort to provide secure mobile Wiki services in the context of m-learning. The authors argue that the proposed scheme, offering end-to-end confidentiality, integrity and non-repudiation services, can be applied selectively and only to sensitive parts of Wiki content, thus diminishing by far computational resources needed at both ends; the server and the client.

The work in [44] points out that current m-learning systems are mainly based on HTTP. However, as HTTP is static and limits in Web access constitutes m-learning systems incapable of supporting the various modern mobile device platforms and wireless access methods. Compelled by this fact, the authors explore the possibility of using Session Initiation Protocol (SIP) as a basis for developing an optimized m-learning system architecture. They argue that by introducing SIP, personal mobility and service mobility for m-learning systems can be dramatically improved. Security is of peripheral interest in this paper. It is suggested that Transport Layer Security (TLS) could be used to protect SIP signaling. For the protection of messages at application layer the authors suggest the use of the standard HTTP digest mechanism as currently employed by SIP for authentication and authorization.

An approach for enabling fine-grained and robust access control in e/m-learning environments is proposed in [28]. More specifically, the authors argue that PKI and Attribute Certificates (AC) can provide the appropriate framework to effectively support authentication and authorization services in the e/m-learning context, and examine the use of ACs in a proposed trust model. The application of ACs to support m-learning is also presented and evaluated through an experimental test-bed setup using the General Packet Radio Service (GPRS) network. The work in [45] introduces a Bluetooth-based system in support of m-learning. By using this system the instructor can receive instant feedback from the learners and check their performance at any time. Learners are also able to participate in the class and answer instructor's questions with the help of the same system. The authors discuss system's architecture and deal with user authentication by means of username/password. Bluetooth standard security mechanisms are also employed for protecting the communication link between devices.

Proposals Addressing Multiple Challenges

The work in [46] discusses security and privacy concerns for mobile e-learning systems and proposes a generalized architecture consisting of five layers. The authors comment that digital identity attributes can be introduced to portable devices to strengthen the security and privacy of mobile e-learning systems. Specifically, they suggest that upon registration with the e-learning system, each learner would be assigned a unique digital identity. After that, any portable device will be registered as one attribute associated with its owner's digital identity. The system will be responsible to manage the association between each user and multiple devices they may possess. From the technical analysis the author provides, it is assumed that such a scheme can be used to enhance the level of privacy provided to learners because only the system is in position to know the relationship between the digital identity of a given user and the identities of the devices they use during m-learning transactions.

The authors in [47] highlight the opportunities for cloud-based education. They describe the issues that need to be solved in order to fulfill this goal, including integration, ownership (of work), security and assessment, and attempt to offer a holistic approach to cloud education. Among others, the paper addresses the issues of security and privacy, and the concepts of identity and ownership for cloud-based m-learning environments. In particular, the authors do not propose novel solutions but discuss possible ways of dealing with the aforementioned issues in forthcoming implementations.

Another proposal for coping with the issue of e-examinations is given in [48]. The authors propose a cryptographic scheme that fulfills several security properties, namely authenticity, anonymity, secrecy, robustness, correctness. This solution also provides students with a receipt (proof of successful submission), and makes use of anonymous return channels to offer anonymity for both the tutor and student. While this proposal is defined for e-examinations in general, makes use of PKI only for authenticating the participating entities, and assumes the existence of an examination center controlled by a supervisor for monitoring the examinee, it can be qualified for m-learning as it does not impose the existence of a Trusted Third Party (TTP). The work in [49] proposes a new model for securing mobile phone learning systems. The aim is to protect the m-learning material from unauthorized distribution, the e-course material from being modified, and to authenticate the messages transmitted between the communication parties. The proposed model, namely SmLS, is argued to constitute m-learning processes more secure for both the organization and learners.

The authors in [18] observe that existing software systems designed to support e-learning are not sufficient for the needs of vicarious learning (*i.e.*, learning by overhearing or observation rather than by direct participation) in a cross-institutional collaborative environment. To cope with this issue they develop an architecture based on Role-Based Access Control (RBAC), namely RAED (Role-Based Access Control for the Evolution of Distributed courseware) which provides a role-based access secured infrastructure for globally distributed electronic courseware. The work in [50] is a direct descendant of [18]. More precisely, similarly to [18], the authors in [50] cope with the challenge of digital information sharing in multi-university e-learning environments. They propose a new rule-based framework to identify and address issues of content sharing in such environments via the use of RBAC management. The proposed framework includes a role-based group delegation granting model, group delegation revocation model, authorization granting and revocation. Overall, by extending what is proposed in [18] the authors provide several options that are able to cope with delegation, authorization, and revocation. Note that while both of these works are about e-learning in general, they can straightforwardly be used for m-learning realms as the solution proposed by the authors is XML-based, and thus lightweight in the general case.

The authors in [51, 52] examine the potential of Digital Rights Management (DRM) technology for contents protection in m-learning environment. DRM is defined as a class of access control technologies that are used by various parties such as publishers and copyright holders aiming to limit the use of digital content and devices after sale. While the goals of paper are not quite clear, to our understanding, the authors propose a DRM-based m-learning system and focus on contents protection as well as other basic procedures of m-learning that can be secured via the use of the aforementioned technology.

Proposals Addressing User's Privacy

The authors in [9] observe that in e-learning contexts, where users work under one login, all their actions within that application can be linked. This is however hazardous in terms of privacy because learners can be easily profiled in the mid- or long-term. This stands true

especially after collecting data about which classes a learner attends, learner's actions within a class or group, regularity of learning sessions, duration of processing learning modules, and even results of tests. It is also pointed out that learners may also lose reputation due to failures done during the learning process. Overall, it is argued that privacy issues are not sufficiently considered in current e-learning environments and especially within collaborative e-learning. Motivated by this fact, they present a proof-of-concept implementation of a privacy-enhanced collaborative e-learning application called BluES'n that makes use of partial identities and aliases/pseudonyms to deliver privacy-preserving services to learners. This work also presents some enhancements of access control based on policies and anonymous user credentials as well as the realization of a privacy-aware user interface. Once more, this work is not defined specifically for m-learning. However, its properties make it directly applicable to such a context.

The work in [53] systematically identifies privacy risks for students using an e-learning system. It is argued that the main threat to privacy is that the contributions of learners are preserved in the system much longer than required. This means that, in most cases, students can be easily identified. The authors also describe some improvements they made using the well-known open-source Learning Management System (LMS) Moodle towards solving this problem. While this study focuses on e-learning in general it can be also easily realized in the context of m-learning. This is because the privacy problems identified by the authors are also inherent to many similar m-learning systems (*e.g.*, Moodle affords *MLE-Moodle* as a plugin, which is an out-of-the-box system designed for use with mobile phones).

Proposals Based on Biometrics

The use of biometrics (keystroke dynamics, voice, dynamic signature features, facial features, iris, fingerprint) in e-learning and m-learning arena is an aspect that has not been completely ignored by researchers, especially for combating e-cheating [54]. For example, the works by [55, 56] describe some possibilities of using biometric features and solutions in the field of e-learning and propose to combine several different biometric methods toward this goal. Indeed, biometrics can be very handy in m-learning for enabling security services like (post)authentication and non-repudiation, especially when assuming the use of ultramodern mobile devices equipped with full QWERTY keyboards, cameras, touch-screens, and sometimes, fingerprint readers. Hence, while the use of biometrics specifically for the m-learning setting is still in its infancy, in the following, we review some works that may be used as a basis for fostering further research on this topic. In addition to those referenced previously in this subsection, we include works that either specifically address biometrics for enabling security in m-learning, or in e-learning in general, but the solution proposed can be realized for m-learning. The interested reader can also refer to the general literature on *e.g.*, keystroke dynamics analysis conducted for hardware keyboards on mobile devices [57, 58] for further exploring the potential of such a solution.

The authors in [59] suggest the use of random fingerprint biometrics user authentication during e-examination procedures. The work in [56] argues that multi-biometrics can be proved very handy for improving the reliability of biometrics authentication when a single biometrics authentication technology is not sufficient. Hence, the authors propose an authentication system that exploits multi-biometrics to support various services in e-learning where user authentication is required. Also, the authors in [60] introduce a biometric scheme for providing continuous user authentication in e-examination through keystroke dynamics. The authors in [61] deal with the problem of tracking individuals accessing the learning materials, and more specifically that of monitoring the true identity of the examination attendees, and propose a multimedia-enriched interactive non-repudiation system involved in

an m-learning environment. They developed an application layer non-repudiation system based on a person's single biometric information (*e.g.*, iris, fingerprint, face, or voice), which resulted in the generation of a unique digital ID per user. After that, digital signatures were created based on the digital IDs to provide message integrity and non-repudiation. Another work that specifically evaluates the potential of the biometric modality called dynamic signature in touch-screen mobile devices in an effort to offer post-authentication and non-repudiation in the m-learning setting is given in [62]. Based on a prototype implementation the authors demonstrate that such a solution can be very accurate in correctly classifying a dynamic signature, and thus providing strong evidences that a given transaction has been performed by the legitimate user. The dynamic signature data on the client-side are recorded and securely transmitted to the server as plain text, thus contributing to the lightweight nature of the proposal.

3.2. Discussion

In this section we discuss the results of the above analysis from both a quantitative and qualitative point of view. First off, it is clear that there exist significant active research on the topic under the focus of this paper. Most of the works address the challenge of systems and data security, occupying themselves with core security services like authentication, authorization, non-repudiation, confidentiality and integrity. Three of them also examine user's privacy issues, while another two specifically engage in the problem of securing examination processes [42, 48]. An entirely different approach is given in [39] where the authors propose an IDS to combat rogue entity attacks in such environment. Two works [9, 53] are found to concentrate solely on user's privacy issues. Three works investigate copyright and/or IPR issues in m-learning [49, 51, 52]. Security in multi-university e-learning environments is a topic investigated by two works [18, 50] so far. Note that due to cross-certification, the proposal in [28] can be also classified into this topic although not included as such in Table 1. Also, as observed, [47] is the only work to put in the foreground some security and privacy aspects under the prism of cloud-based mobile education. Following the general trends, in the last few years, this topic is found to attract the interest of the education community [63] - and especially that of m-learning [64] - but regarding the security and privacy aspect is still in its infancy.

A growing tendency towards biometric-based solutions is witnessed in Table 1. We think that this research field will flourish in the years to come because, as already mentioned, mobile devices embed several functionalities and features that can be exploited for implementing such solutions. Another interesting observation is that, so far, challenges #3 to #5 and #9 as depicted in Figure 1 are not found to be tackled. For these challenges one can find peripheral literature such as [65] for challenge #3, [66-68] for #4, and [22-24] for #9, but for the time being no work addresses them specifically for m-learning.

Overall, the aforementioned analysis reveals that there are several uncharted areas that surround the topic of security and privacy in m-learning. Several of the issues pointed out in Section 2, while addressed in the general literature in a considerable amount, for m-learning seem still at their infancy, if not completely undiscovered.

From a qualitative point of view, we can argue that some of the abovementioned works try to tackle security and privacy in the m-learning setting by only employing legacy security and privacy solutions borrowed from the standard security arsenal and amended for m-learning needs. However, such standard approaches to security and privacy were built up when users were typically interacting with computers in a static environment, thus ignoring the special needs of mobile users. Hence, security and privacy-related judgments were taken based on static characteristics such as user's identity or role. Nevertheless, when considering a nomadic

computing environment of mobile learners, and the shift towards u-learning, security and privacy needs vary drastically. That is, one must take into account several important factors including: (a) the use of a plethora of mobile devices/platforms having different configurations, (b) the fact that learners are able to connect over various networks, (c) the usual case of a mobile learner being in different physical environments when attempting access to remote resources, (d) the norm that mobile devices are basically learning assets usually incorporating advanced capacities that can be used either productively or harmfully, and store private information about the owner and others, (e) the interaction with smart objects scattered in space. As a result, to effectively fulfill security and privacy requirements in this dynamic computing environment, choices regarding security must take into account the user's different contextual attributes which may vary frequently and rapidly. For instance, in terms of access control this means not only regulating users' permissions on-the-fly, but also the policies based on contextual data.

All the above requirements stem directly from the mobile and sometimes spontaneous nature of m-learning. However, this is not enough. After all, in the literature of mobile and wireless computing there are several solutions that tackle the above issues in great detail, diversity and depth. So, in addition to these requirements, any solution proposed must also take into serious consideration the special needs of the all the actors involved depending on the scenario (formal, informal, blended learning) as well as the fundamental pedagogical differences that constitute the m-learning style very different from that of e-learning. For example, the work in [9], while not defined specifically for m-learning, fulfills the aforementioned goal. On the other hand, work in [39] concentrates solely on the technical details of the solution, thus remaining loosely anchored to the specific needs of mobile collaborative learning.

4. Conclusions

Mobile learning is a growing trend as it can be exploited to respond to the challenges of particular educational contexts, complement and enhance formal schooling, improve and assist learning for people across age and income spectrums, augment learning opportunities principally in communities where educational opportunities are limited, and so forth. However, along with opportunities come several challenges that need to be addressed. For instance, the pervasive use of mobile technologies for the needs of m-learning may entail, among others, loss of privacy and attacks on personal and institutional security.

Compelled by this fact, in this paper, we examined challenges revolving around security and privacy issues in the m-learning setting and beyond. Based on these challenges we classified all works found in the literature and somehow address directly (or indirectly) security and/or privacy in the m-learning realm. We also considered works that may not be specifically defined for m-learning but have the potential to be characterized as such. From the analysis becomes clear that several poorly discovered areas exist that call for further investigation. Also, while there is a critical mass of works in this particular area, further research effort is required in order the characteristics of each solution to be tightly coupled with that of learners, tutors, and educational institutions depending on the case. The current work can be used as a reference to anyone interested in better understanding the facets of this fast evolving area. It is also expected to foster research efforts to the development of fully-fledged solutions that put emphasis not only to the technological aspect, but also to human factor.

References

[1] E. D. Wagner, "Realizing the promises of mobile learning", J. Computing in Higher Education, vol. 20, no. 2, **(2008)**, pp. 4-14.
[2] J. Lam, J. Yau and S. Cheung, "A Review of Mobile Learning in the Mobile Age", In Hybrid Learning, Lecture Notes in Computer Science, Edited by Tsang P, Cheung S, Lee V, Huang R, Springer Berlin / Heidelberg, vol. 6248, **(2010)**, pp. 306-315, [http://dx.doi.org/10.1007/978-3-642-14657-2 28].
[3] G. J. Hwang, C. C. Tsai and S. J. H. Yang, "Criteria, Strategies and Research Issues of Context-Aware Ubiquitous Learning". Educational Technology & Society, vol. 11, no. 2, **(2008)**, pp. 81-91.
[4] R. Beale, "How to enhance the experience without interfering with it?", Big Issues in Mobile Learning: Report of a workshop by the Kaleidoscope Network of Excellence, Edited by Sharples M, Nottingham: Learning Sciences Research Institute, **(2007)**.
[5] N. Pachler, J. Cook, B. Bachmair, N. Pachler, B. Bachmair and J. Cook, "Mobile Devices as Resources for Learning: Adoption Trends, Characteristics", Constraints and Challenges, In Mobile Learning, Springer US, **(2010)**, pp. 73-93, [http://dx.doi.org/10.1007/978-1-4419-0585-7 3].
[6] GSMA: Safeguarding, Security and Privacy in Mobile Education. Tech. rep., GSMA Connected Living programme: mEducation, **(2012)**, [http://www.gsma.com/connectedliving/gsma-safeguarding-security-and-privacy-in-mobile-education-whitepaper-2/].
[7] S. Gritzalis, "Enhancing Web privacy and anonymity in the digital era", Inf. Manag. Comput. Security, vol. 12, no. 3, **(2004)**, pp. 255-287.
[8] A. Ruiz-Martinez, "A survey on solutions and main free tools for privacy enhancing Web communications", Journal of Network and Computer Applications, vol. 35, no. 5, **(2012)**, pp. 1473-1492, [http://www.sciencedirect.com/science/ article/pii/S1084804512000665].
[9] K. Liesebach, E. Franz, A. K. Stange, A. Juschka, K. Borcea-Ptzmann, A. Bottcher and H. Wahrig, "Collaborative E-Learning", Digital Privacy, Lecture Notes in Computer Science, Edited by Camenisch J, Leenes R, Sommer D, Springer Berlin / Heidelberg, vol. 6545, **(2011)**, pp. 657-677, [http://dx.doi.org/10.1007/978-3-642-19050-624].
[10] D. Frohberg, C. Goth and G. Schwabe, "Mobile Learning projects - a critical analysis of the state of the art", J. Comp. Assisted Learning, **(2009)**, vol. 25, no. 4, pp. 307-331.
[11] G. Walton, S. Childs and E. Blenkinsopp, "Using mobile technologies to give health students access to learning resources in the UK community setting", Health Info Libr J, 22 Suppl., **(2005)**, no. 2, pp. 51-65, [http://dx.doi.org/10.1111/ j.1470-3327.2005.00615.x].
[12] S. Martin, G. Diaz, I. Plaza, E. R. Larrocha, M. Castro and J. Peire, "State of the art of frameworks and middleware for facilitating mobile and ubiquitous learning development", Journal of Systems and Software, vol. 84, no. 11, **(2011)**, pp. 1883-1891.
[13] A. Charlesworth, "Code of Practice for the Further and Higher Education Sectors on the Data Protection Act 1998", Tech. rep., JISC Legal, **(2009)**, [http://www.jisclegal.ac.uk/Portals/12/Documents/PDFs/ DPACodeofpractice.pdf].
[14] D. Damopoulos, G. Kambourakis, M. Anagnostopoulos, S. Gritzalis and J. Park, "User privacy and modern mobile services: are they on the same path?", Personal and Ubiquitous Computing, **(2012)**, pp. 1-12, [http://dx.doi.org/10.1007/s00779-012-0579-1].
[15] H. T. Dinh, C. Lee, D. Niyato and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches", Wireless Communications and Mobile Computing, **(2011)**, [http://dx.doi.org/10.1002/wcm.1203].
[16] D. Zissis and D. Lekkas, "Addressing cloud computing security issues", Future Generation Comp. Syst., vol. 28, no. 3, **(2012)**, pp. 583-592.
[17] D. Teneyuca, "Internet cloud security: The illusion of inclusion", Information Security Technical Report **(2011)**, vol. 16, no. 3-4, pp. 102-107, [http://www.sciencedirect.com/science/article/pii/S1363412711000501].
[18] S. Neely, H. Lowe, D. Eyers, J. Bacon, J. Newman and X. Gong, "An architecture for supporting vicarious learning in a distributed environment", Proceedings of the 2004 ACM symposium on Applied computing, SAC '04, New York, NY, USA: ACM, **(2004)**:963-970, [http://doi.acm.org/10.1145/967900.968095].
[19] G. Z. Liu and G. J. Hwang, "A key step to understanding paradigm shifts in e-learning: towards context-aware ubiquitous learning", British Journal of Educational Technology, vol. 41, no. 2, **(2010)**, pp. E1-E9, [http://dx.doi.org/10.1111/j.1467-8535.2009.00976.x].
[20] T. D. Jong, M. Specht and R. Koper, "Contextualised Media for Learning", Educational Technology & Society, vol. 11, **(2008)**, pp. 41-53.
[21] G. Johnson, P. Shakarian, N. Gupta and A. K. Agrawala, "Towards Shrink-Wrapped Security: Practically Incorporating Context Into Security Services", Procedia CS, Elsevier, vol. 5, **(2011)**, pp. 782-787.

[22] S. Hallsteinsen, K. Geihs, N. Paspallis, F. Eliassen, G. Horn, J. Lorenzo, A. Mamelli and G. Papadopoulos, "A development framework and methodology for self-adapting applications in ubiquitous computing environments", Journal of Systems and Software, **(2012)**, [http://www.sciencedirect.com/science/article/pii/S0164121212002245].
[23] E. Rekleitis, P. Rizomiliotis and S. Gritzalis, "How to protect security and privacy in the IoT: a policy-based RFID tag management protocol", Security and Communication Networks, **(2011)**, Wiley, [http://dx.doi.org/10.1002/sec.400].
[24] E. Toch, Y. Wang and L. Cranor, "Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems", User Modeling and User-Adapted Interaction, vol. 22, **(2012)**, pp. 203-220, [http://dx.doi.org/10.1007/s11257-011-9110-z].
[25] S. Furnell, U. Bleimann, J. Girsang, H. Rder, P. Sanders and I. Stengel, "Security considerations in online distance learning", Proceedings of Euromedia 99, Edited by W Hahn EWK, Knop J, **(1999)**, pp. 31-35.
[26] K. El-Khatib, L. Korba, Y. Xu and G. Yee, "Privacy and Security in E-Learning", International Journal of Distance Education, Idea Group Publishing, vol. 1, no. 4, **(2003)**, pp. 1-15.
[27] E. Weippl, "Security in E-Learning", Advances in Information Security, Springer, vol. 16, **(2005)**.
[28] G. Kambourakis, D.-P. Kontoni, A. N. Rouskas and S. Gritzalis, "A PKI approach for deploying modern secure distributed e-learning and m-learning environments", Computers & Education, Elsevier, vol. 48, **(2007)**, pp. 1-16.
[29] J. Yong, "Security modelling for e-Learning", Proc. First IEEE Int. Symp. Information Technologies and Applications in Education ISITAE '07, **(2007)**, pp. 1-5.
[30] J. Mwakalinga, S. Kowalski and L. Yngstrom, "Secure e-learning using a holistic and immune security framework", Proc. Int. Conf. for Internet Technology and Secured Transactions ICITST 2009, **(2009)**, pp. 1-6.
[31] H. M. A. Najwa and F. Ip-Shing, "E-Learning and Information Security Management", International Journal of Digital Society, vol. 1, no. 2, **(2010)**, pp. 148-156.
[32] P. R. L. Eswari, "A process framework for securing an e-Learning ecosystem", Proc. of Conf. for Int Internet Technology and Secured Transactions (ICITST), **(2011)**, pp. 403-407.
[33] J. C. Granda, P. Nuno, D. F. Garcia and F. J. Suarez, "Security Issues in a Synchronous e-Training Platform", Proc. Sixth Int Availability, Reliability and Security (ARES) Conf., **(2011)**, pp. 485-492.
[34] D. C. Luminita, "Information security in E-learning Platforms", Procedia - Social and Behavioral Sciences, **(2011)**, vol. 15, no. 0, pp. 2689-2693, 3rd World Conference on Educational Sciences [http://www.sciencedirect.com/science/ article/ pii/S1877042811007178].
[35] J. Castella-Roca, J. Herrera-Joancomarti and A. Dorca-Josa, "A secure e-exam management system", Proc. First Int. Conf. Availability, Reliability and Security ARES, **(2006)**.
[36] T. De Medeiros Gualberto and S. D. Zorzo, "Service for secure and protected applications in Collaborative Learning Environments", Proc. IEEE Int Systems Man and Cybernetics (SMC) Conf., **(2010)**, pp. 2419-2426.
[37] E. R. Weippl, "Security considerations in m-learning: threats and countermeasures", Advanced Technology for Learning, **(2007)**, vol. 4, no. 2, pp. 99-105.
[38] Z. Ugray, "Security and privacy issues in mobile learning", International Journal of Mobile Learning and Organisation, vol. 3, no. 2, **(2009)**, pp. 202-218.
[39] A. Razaque and K. Elleithy, "Restoring privacy of users to foster Mobile Collaborative learning (MCL)", ASEE Northeast Section Conf., **(2012)**, pp. 1-10.
[40] C. Boja, P. Pocatilu and A. Zamroiu, "Secure SMS communications for M-learning services", Proceedings of the 5th European conference on European computing conference, ECC'11, Stevens Point, Wisconsin, USA: World Scientic and Engineering Academy and Society (WSEAS), **(2011)**, pp. 480-484, [http://dl.acm.org/citation.cfm?id=1991016.1991097].
[41] C. Romero, S. Ventura and P. de Bra, "Using mobile and web-based computerized tests to evaluate university students", Computer Applications in Engineering Education, **(2009)**, vol. 17, no. 4, pp. 435-447, [http://dx.doi.org/10.1002/ cae.20242].
[42] R. A. Buchmann and S. Jecan, "An arbitration web service for e-learning based on xml security standards", W. Trans. on Comp., **(2008)**, vol. 7, no. 10, pp. 1742-1751, [http://dl.acm.org/citation.cfm?id=1486693.1486713].
[43] C. Kolias, S. Demertzis and G. Kambourakis, "Design and implementation of a secure mobile wiki system", Proceedings of the Seventh IASTED International Conference on Web-based Education, WBE '08, Anaheim, CA, USA: ACTA Press, **(2008)**, pp. 212-217, [http://dl.acm.org/citation.cfm?id=1722815.1722860].
[44] S. Fan, J. Fan, Y. Zhang and Z. He, "An Optimized Scheme for Mobile Learning on IP-Based Network Using SIP", Proceedings of the 7th international conference on Advances in Web Based Learning, ICWL '08, Berlin, Heidelberg: Springer-Verlag, **(2008)**, pp. 541-551, [http://dx.doi.org/10.1007/978-3-540-85033-5_53].
[45] Y. Zhang, S. Zhang, S. Vuong and K. Malik, "Mobile learning with Bluetooth-based e-learning system", Proc. 2nd Int Mobile Technology, Applications and Systems Conf, **(2005)**.

[46] J. Yong, "Security and Privacy Preservation for Mobile E-Learning via Digital Identity Attributes", Journal of Universal Computer Science (J. UCS), vol. 17, no. 2, **(2011)**, pp. 296-310.
[47] B. Hirsch and J. W. P. Ng, "Education beyond the cloud: Anytime-anywhere learning in a smart campus environment", Proc. of Int Conf. for Internet Technology and Secured Transactions (ICITST), **(2011)**, pp. 718-723.
[48] A. Huszti and A. Petho, "A secure electronic exam system", Publ. Math. Debrecen, vol. 77, no. 3-4, **(2010)**, pp. 299-312.
[49] K. M. Titi and O. A. Marie, "Protecting E-courses Copyright in M-learning Process", Proc. of Int. Conf. Future Computer and Communication ICFCC 2009, **(2009)**, pp. 636-640.
[50] H. Wang and Q. Li, "Secure and Efficient Information Sharing in Multi-university E-Learning Environments", Advances in Web Based Learning ICWL 2007, Lecture Notes in Computer Science, Edited by Leung H., Li F., Lau R., Li Q., Springer Berlin / Heidelberg, vol. 4823, **(2008)**, pp. 542-553, [http://dx.doi.org/10.1007/978-3-540-78139-4-48].
[51] J. Song, M. Kang and S. Kim, "Study on Contents Protection in M-Learning Environment", Computational Science and Its Applications ICCSA, Lecture Notes in Computer Science, Edited by Gavrilova M., Gervasi O, Kumar V., Tan C., Taniar D., Lagan A., Mun Y., Choo H., Springer Berlin / Heidelberg, vol. 3984, **(2006)**, pp. 575-583, [http://dx.doi.org/10.1007/11751649-63].
[52] M. Kang, S. Kim, G. C. Park, G. Lee and M. Kil, "Design of DRM-LMS Model in M-Learning Environment", Knowledge-Based Intelligent Information and Engineering Systems, Lecture Notes in Computer Science, Edited by Gabrys B., Howlett R., Jain L., Springer Berlin / Heidelberg, vol. 4253, **(2006)**, pp. 1075-1082, [http://dx.doi.org/10.1007/11893011-136].
[53] E. R. Weippl and A. M. Tjoa, "Privacy in e-learning: anonymity, pseudonyms and authenticated usage", Inter- active Technology and Smart Education, vol. 2, no, 4, **(2004)**, pp. 247-256.
[54] G. Qinghai, "Online teaching, Do you know who is taking the final exam?", In Mid-Atlantic ASEE Conference, **(2010)**, pp. 1-6.
[55] K. Rabuzin, M. Baca and M. Sajko, "E-learning, Biometrics as a Security Factor", Proc. Int. Multi-Conf. Computing in the Global Information Technology ICCGI '06, **(2006)**.
[56] S. Asha and C. Chellappan, "Authentication of e-learners using multimodal biometric technology", Proc. Int. Symp. Biometrics and Security Technologies ISBAST 2008, **(2008)**, pp. 1-6.
[57] N. L. Clarke and S. Furnell, "Authenticating mobile phone users using keystroke analysis", Int. J. Inf. Sec., vol. 6, **(2007)**, pp. 1-14.
[58] S. Hwang, S. Cho and S. Park, "Keystroke dynamics-based authentication for mobile devices", Computers & Security, Elsevier, **(2009)**, vol. 28, no. 1-2, pp. 85-93.
[59] Y. Levy and M. M. Ramin, "A Theoretical Approach for Biometrics Authentication of e-Exams, **(2007)**. [http://telem-pub.openu.ac.il/users/chais/2007/morning 1/M1 6.pdf].
[60] E. Flior and K. Kowalski, "Continuous Biometric User Authentication in Online Examinations", Proc. Seventh Int Information Technology: New Generations (ITNG) Conf., **(2010)**, pp. 488-492.
[61] A. Sasan, "A remote interactive non-repudiation multimedia-based m-learning system", Telematics and Informatics **(2010)**, vol. 27, no. 4, pp. 377-393. [http://www.sciencedirect.com/science/article/pii/ S073658531000002X].
[62] G. Kambourakis and D. Damopoulos, "A competent post-authentication and non-repudiation biometric scheme for mLearning", Proceedings of the 10th IASTED International Conference on Web-based Education, IASTED, ACTA Press, **(2013)**, pp. 821-827.
[63] H. Mousannif, I. Khalil and G. Kotsis, "Collaborative learning in the clouds", Information Systems Frontiers, **(2012)**, pp. 1-7, [http://dx.doi.org/10.1007/s10796-012-9364-y].
[64] S. Kitanov and D. Davcev, "Mobile Cloud Computing Environment as a Support for Mobile Learning", In The Third International Conference on Cloud Computing, GRIDs, and Virtualization, IARIA, **(2012)**, pp. 99-105, [http://www.thinkmind.org/index.php?view=article&articleid=cloud computing 2012 4 40 20097].
[65] D. Damopoulos, S. A. Menesidou, G. Kambourakis, M. Papadaki, N. Clarke and S. Gritzalis, "Evaluation of anomaly-based IDS for mobile devices using machine learning classifiers", Security and Communication Networks, vol. 5, **(2012)**, pp. 3-14. [http://dx.doi.org/10.1002/sec.341].
[66] M. Valcke, B. D. Wever, H. V. Keer and T. Schellens, "Long-term study of safe Internet use of young children", Computers & Education, Elsevier, vol. 57, **(2011)**, pp. 1292-1305. [http://www.sciencedirect.com/science/article/pii/ S0360131511000273].
[67] R. Cohen-Almagor, "Fighting Hate and Bigotry on the Internet", Policy & Internet, vol. 3, no. 3, **(2011)**, pp. 1-26, [http://dx.doi.org/10.2202/1944-2866.1059].
[68] S. J. Delany, M. Buckley and D. Greene, "SMS spam filtering: Methods and data", Expert Systems with Applications, vol. 39, no. 10, **(2012)**, pp. 9899-9908, [http://www.sciencedirect.com/science/article/ pii/S0957417412002977].

Author

Georgios Kambourakis was born in Samos, Greece, in 1970. He received the Diploma in Applied Informatics from the Athens University of Economics and Business and the Ph.D. in Information and Communication Systems Engineering from the Department of Information and Communications Systems Engineering of the University of Aegean. He also holds a Master's of Education (Ed.M.) degree from the Hellenic Open University. Currently, Dr. Kambourakis is an Assistant Professor at the Department of Information and Communication Systems Engineering of the University of the Aegean, Greece. His research interests are in the fields of mobile and wireless networks security and privacy, VoIP security, Public Key Infrastructure, DNS security, and mLearning and he has more than 80 publications in the above areas. He has guest edited special issues of several journals including Computer Standards & Interfaces, ACM/Springer Mobile Networks and Applications, IEEE Computer magazine, Information Sciences. He has been involved in several national and EU funded R&D projects in the areas of Information and Communication Systems Security. He is a reviewer of several IEEE and other international journals and has served as a technical program committee member for more than 100 international conferences in security and networking.