УДК: 004.7:37

Velev D. G.
Prof. Dr.,
University of National and World Economy,
Bulgaria; e-mail:dgvelev@unwe.bg

SECURITY ASPECTS OF CLOUD-BASED MOBILE LEARNING

Abstract. The paper attempts to outline the security issues in the development and application of cloud-based mobile learning. A brief definition of the mobile learning, its components and related technologies and devices is given. The specific characteristics of social media, big data and cloud computing are summarized in relation with their integration in the mobile learning and its transformation to a cloud-based environment. The main security threats to this type of learning are pointed out and some recommendations for providing security learning are given are given.

Keywords: Mobile learning, Cloud computing, Social media, Big data, Security.
Formulas: 0; fig.: 0, tabl.: 0, bibl.: 39
JEL Classification: D 83, C 80.

Велєв Д. Ж.
доктор, професор,
Університет національної та світової економіки,
Болгарія; e-mail:dgvelev@unwe.bg

ПІДХОДИ ДО БЕЗПЕКИ ХМАРО-ОРІЄНТОВАНОГО МОБІЛЬНОГО НАВЧАННЯ

Анотація. У статті робиться спроба окреслити проблеми безпеки при розробці та застосуванні мобільного навчання з застосуванням хмарних технологій. Зроблено коротке визначення мобільного навчання, його компонентів, супутніх технологій та пристроїв. Підсумовані особливості соціальних медіа, великих данних та хмарних технологій у відношенні до їх інтеграції у мобільне навчання та трансформацію в хмарному середовищі. Визначені основні загрози для безпеки такого виду навчання та надані деякі рекомендації для забезпечення безпеки навчання.

Ключові слова: мобільне навчання, хмарні обчислення, соціальні медіа, великі данні, безпека.
Формул: 0; рис.: 0, табл.:0, бібл.: 39

Велев Д. Ж.
доктор, профессор,
Університет национальной и мировой экономики,
Болгария;e-mail:dgvelev@unwe.bg

ПОДХОДЫ К БЕЗОПАСНОСТИ ОБЛАЧНО-ОРИЕТИРОВАННОЙ МОБИЛЬНОЙ УЧЕБЫ

Аннотация. В статье делается попытка выделить проблемы безопасности при разработке и применении мобильной учебы с применением облачных технологий. Сделано короткое определение мобильной учебы, ее компонентов, сопутствующих технологий и устройств. Обобщены особенности социальных медиа, больших данных и облачных технологий в отношении к их интеграции в мобильную учебу и трансформацию в облачной среде. Определены основные угрозы для безопасности такого вида учебы и предоставлены некоторые рекомендации для обеспечения безопасности учебы.

Ключевые слова: мобильная учеба, облачные вычисления, социальные медиа, большие данные, безопасность.

Формул: 0; рис.: 0, табл.:0, библ.: 39

Introduction. The mobile platforms have already become the dominant communications and interaction platforms by early-adopting and best-practice organizations. The capabilities of smartphones and tablet devices grow immensely day-by-day. Tablets will become the virtual classroom, and an emerging class of tools will let students and employees manage digitally almost every aspect of their educational and professional life.

The new ICT devices transforming education and business are characterized by [1]:

- Volume – more than 1,3 billion mobile phones on the market today;
- Increased volume of tablets – 55 million tablets sold in 2011 vs. 409 million PCs;
- Constant use - 34% of mobile phone users under the age of 34 are permanently in touch with their devices;
- Video content – social network sites deliver more hours of video each day that all the traditional networks combined, which is 69% of all web traffic;
- Domination of mobile platforms – Android and Apple have seized 73% of all mobile phone browsing;
- Gamification – Games are the fastest growing application on mobile devices;
- Consumerization – employees expect the consumer experience they have at home at work.

Learning is acquiring new and modifying existing, knowledge, behaviors, skills, values or preferences and involves synthesizing different types of information. Learning may be viewed as a process, rather than a collection of factual and procedural knowledge [2]. Research unanimously proves the significance of the mobile learning [3, 4]. It is known that 28 % of smartphone owners use their devices as their primary way to access the Internet [5]. This fact supports the tendency of moving learning content in scope of mobile learning.

The term mobile learning has different meanings for different communities. Although related to e-learning and distance education, it is distinct in its focus on learning across contexts and learning with mobile devices. One definition of mobile learning is: Any sort of learning that happens when the learner is not at a fixed, predetermined location, or learning that happens when the learner takes advantage of the learning opportunities offered by mobile technologies. In other words mobile learning decreases limitation of learning location with the mobility of general portable devices [6].

Mobile learning includes portable devices and related technologies such as handheld computers, MP3 players, notebooks, netbooks, ultrabooks, tablets and mobile phones. Recently there is a new trend in mobile learning which adds mobility of the instructor and includes creation of learning materials "on-the-spot" using mainly smartphones with special software. Using mobile tools for creating learning aides and materials becomes an important part of informal learning.

Mobile learning is convenient since it is accessible from virtually anywhere. It has a high collaboration and it provides for an instantaneous sharing among everyone using the same content, which leads to the reception of instant feedback and tips, as well as for a strong portability by replacing traditional textbooks.

In recent years, the mobile learning has grown from a minor research interest to a set of significant projects in schools, workplaces, museums, etc. around the world with different national perspectives, differences between academia and industry, and between the school, higher education and lifelong learning sectors. Current areas of growth include: Testing, surveys, job aids and just-in-time learning; Location-based and contextual learning; Social-networked mobile learning; Mobile educational gaming; Mobile learning through bidirectional SMS messaging; Mobile storage; Mobile voting; Mobile contests.

New technologies in help of mobile learning

The advent of newest information and communication technologies such as social media, big data and cloud computing and the wide-spread increase of smaller and more portable computers and Internet-capable devices makes it possible focusing on mobile learning through mobile devices, allowing learners to move about in a classroom or remotely learn from any location of their choice.

A. Social networking services

Nowadays the terms Social Media, Social Software and Social Networking Services are quite often used, sometimes mistakenly, in Internet interaction between different users.

A social networking service (SNS) is an online service, platform, or site that focuses on facilitating the building of social networks or social relations among people who, for example, share interests, activities, backgrounds, or real-life connections. A social network service consists of a representation of each user through a profile, his/her social links, and a variety of additional services. Most social network services are web-based and provide means for users to interact over the Internet, such as e-mail and instant messaging. Online community services are sometimes considered as a social network service, though in a broader sense, social network service usually means an individual-centered service whereas online community services are group-centered. Social networking sites allow users to share ideas, activities, events, and interests within their individual networks [7]. Most sites support existing networks, but others help people connect based on their shared interests, political views or activities. SNS also vary in the extent to which they use new information and communication tools, such as mobile connectivity, blogging and photo/ video-sharing.

The term Social Software is used for software systems that are utilized for group communication and collaboration which thus foster building and managing social networks or publishing information and its dissemination [8]. Blogs, discussion groups, Wikis, music streams with rating features, social networking platforms or picture sharing are examples of Social Software. SNS emulate real social networks in a virtual environment. Each member is encouraged to expand the current network by inviting others to join and connecting with others. Links that are made with existing users of platforms and added to ones network can also be controlled. Besides these functions, SNS might offer newsgroups around one or more sets of topics usually managed by members of the community, a personal blog, calendar, RSS, chat, classifieds and picture sharing functionality.

The term Social Media is content creation and distribution. The ability to create, post and share content is a major component of many SNS. Social media has already surpassed that workhorse of the modern enterprise, e-mail. Increasingly, the world is using social networks and other social media-based services to stay in touch, communicate, and collaborate [9]. The Social function is one of the most compelling examples of how consumerization drives ICT practices. It includes personal activities of sharing comments, links and recommendations with friends. There are many benefits - from being able to communicate and collaborate easily with extended networks of employees, partners, customers, across internal and external social networks. Social technologies both drive and depend on other factors [10]:

- Social provides an important need for mobility: Accessing social networks is one of the primary uses of mobile devices and social interactions have much more value when they are possible wherever the user is located.
- Social depends on cloud for scale and access: Social networks benefit from scale, the kind of scale that is really only practical through cloud deployment.

- Social feeds and depends on deep analysis: Social interactions provide a rich source of information about connections, preferences and intentions. As social networks get larger, participants need better tools to be able to manage the growing number of interactions, which drives the need for deeper social analytics.

Mining social media networks for data around customers' habits is a huge opportunity. Successful organizations are starting to leverage this information to listen to their customers and engage with them in a more appropriate and interactive way. Government agencies, manufacturers, vendors regard social media sites as a new channel to engage and interact with their customers. Incorporating social media information when collaborating with both internal employees and external customers and partners is an essential element in resolving any business problem. A consumer information is already easily available to organizations to leverage that will allow them to make more informed decisions to better serve their customers.

B. Big Data

The concept of information known as Big data is not only managing large volumes of data, but also controlling the velocity and variety of data that exists nowadays. It is expected data will continue to grow exponentially in future. Velocity defines the speed with which customers and employees expect information to be available to them and how fast they are able to generate and consume data. Variety deals with the type of data (structured or unstructured data, data captured from social media sites, machine data, etc.) and how this information could be used to obtain competitive advantage. The ability to extract data from different sources to perform a specific task and the ability to provide information in real-time with the right context is essential. Information is stored everywhere. Social, mobile and cloud make information accessible, shareable and consumable at anytime and anywhere. The term "big data" is to describe new technologies and techniques that can handle an order of magnitude or two more data than enterprises are today. Big data offers the promise of better ROI on valuable datasets while being able to tackle entirely new learning problems that were previously impossible to solve with existing techniques.

The emergence of big data is causing deep technology and business transformation worldwide. Technically, the large data conventional manner to extract information from the data, which has changed. In the field of technology, ever more rely on the model, we can now borrow massive data based on statistical methods, is expected to make the speech recognition, machine translation technology to make new progress in the era of big data [11].

C. Cloud Computing

Cloud computing is an on-demand service model for IT provision based on virtualization and distributed computing technologies [12], [13], [14]. Typical cloud computing providers deliver common business applications online as services, which are accessed from another web service or software like a web browser, while the software and data are stored on servers. The abstraction of computing, network and storage infrastructure is the foundation of cloud computing. The infrastructure is a service, and its components must be readily accessible and available to the immediate needs of the application stacks it supports. Cloud computing removes the traditional application silos within the data center and introduces a new level of flexibility and scalability to the IT organization.

The following cloud computing categories have been identified and defined in the process of cloud development:

- Infrastructure as Service (IaaS): provides virtual machines and other abstracted hardware and operating systems, which may be controlled through a service Application Programming Interface (API). IaaS includes the entire infrastructure resource stack from the facilities to the hardware platforms that reside in them. It incorporates the capability to abstract resources as well as deliver physical and logical connectivity to those resources. IaaS

provides a set of APIs which allow management and other forms of interaction with the infrastructure by consumers.

- Platform as a Service (PaaS): allows customers to develop new applications using APIs, implemented and operated remotely. The platforms offered include development tools, configuration management and deployment platforms. PaaS is positioned over IaaS and adds an additional layer of integration with application development frameworks and functions such as database, messaging, and queuing that allow developers to build applications for the platform with programming languages and tools are supported by the stack.
- Software as a Service (SaaS): does a third party provider, available on demand, usually through a Web browser, operating in a remote manner, offer software. Examples include online word processing and spreadsheet tools, CRM services and Web content delivery services. SaaS in turn is built upon the underlying IaaS and PaaS stacks and provides a self-contained operating environment used to deliver the entire user experience including the content, its presentation, the applications and management capabilities.
- Multi-Tenancy: the need for policy-driven enforcement, segmentation, isolation, governance, service levels and billing models for different consumer constituencies. Consumers might utilize a public cloud provider's service offerings or actually be from the same organization, but would still share infrastructure.

The cloud services can be implemented in four deployment models:

- Public Cloud. The cloud infrastructure is made available to the general public or large industry group and is owned by an organization selling cloud services.
- Private Cloud. The cloud infrastructure is operated entirely for a single organization. It may be managed by the organization or a third party, and may exist on-premises or off-premises.
- Community Cloud. The cloud infrastructure is shared by several organizations and supports a specific community. It may be managed by the organizations or a third party, and may exist on-premises or off-premises.
- Hybrid Cloud. The cloud infrastructure is a composition of two or more clouds (private, community or public) that are bound together by standardized or proprietary technology that enables portability of data and application.

The cloud computing environment usually consists of the following components [13], [15]:

- Servers - Hosting servers in the cloud using the corresponding services means operating those servers a safe distance from any disaster. Cloud hosting providers generally have more redundancy of network connections, mirrored sites and other precautions to ensure access under adverse conditions.
- Applications - People that use cloud-based applications like Google Apps or Microsoft Office 365 can log in and be productive from virtually anywhere and any mobile device.
- Online data - Users will tend to keep their data stored remotely in the cloud. It is available from everywhere, and like cloud applications and it can be accessed from any device capable of connecting to the web.
- Cloud backup - Many companies fail to backup critical systems on a periodic basis at all, but it is even more severe when an organization has taken the time to create the backups, but the backups end up getting destroyed at the same time as the servers and data their backing up. Using a cloud-based backup solution provides for rebuilding the systems and resuming normal operations.

Under some circumstances, virtual appliances or virtual machine images of existing workloads can be created in the data center and stored in a cloud data center. In the event of a

failure of the former, the virtual machines serve as recovery mechanisms that can be reactivated in the cloud.

Mobile Cloud Computing is the combination of mobile computing, cloud computing, and wireless networks aiming to enhance computational capabilities of resource-constrained mobile devices towards rich user experience.

Cloud-Based Mobile Learning

M-learning design presents a unique set of challenges [16]:

- Device variability;
- Slow download speed and limited Internet access;
- Small screen sizes with poor resolution, color, and contrast;
- Awkward text input;
- Limited memory.

One of the biggest issues in mobile application development is how to build mobile apps that are applicable to many mobile devices [17]. This issue is being escalated with the advent of bring your own device (BYOD), a policy that many organizations favored. Developing a mobile app that runs on many devices provides the cross-platform capability to make more mobile apps available to users, but it creates a lot of work for developers. Mobile cloud computing can be viewed as a cloud infrastructure enhanced to provide a mobile ecosystem for mobile apps and to allow access to business apps from mobile devices. The data processing and the data storage happen outside the mobile device, and results are displayed through the mobile device screen or speakers. There are additional advantages to running mobile applications on a mobile cloud:

- Mobile devices can be allowed access to powerful, back-end business apps, if sufficient security is provided.
- More mobile apps can be made available to a broader audience.
- Multiple security apps that check mobile device security can be run on the mobile cloud, providing much broader and more comprehensive security checking for mobile devices.
- Running mobile apps on a mobile cloud makes many more apps available for organization users.
- Use of the mobile cloud allows mobile devices to be included in the centralized security scheme of the cloud.

The information gathered in this immersive world will have tremendous value. Ultimately, the lasting relationship will be between a user and a cloud-based ecosystem [18].

Cloud computing represents the binding substance for all the forces of the Nexus [19]. This is the model for delivery of whatever computing resources are needed and for activities that grow out of such delivery. Without cloud computing, social interactions would not to happen, mobile access would fail to be able to connect to a wide variety of data and functions, and information still would be stuck inside internal systems. Many cloud services have become so inexpensive or even free that users try out multiple services before picking the one they like the most. Utilizing these cloud services also has benefits to companies as well. They drive down costs, create greater focus on core business and increase deployment speed [20]. There is a natural tendency for combining social media, mobile computing and cloud computing into mobile learning [21], [22], [23]:

- Cloud offers the promise of faster development and delivery of services. It provides for cost savings and faster iteration of new delivery services. Clouds computing seamlessly deliver services to multiple end-points such as tablets and PCs.
- Cloud Computing could guarantee mobile delivery of enterprise email, calendar and other critical applications is a basic necessity.
- Social collaboration is best conducted by Cloud computing – blogs, wikis, file sharing, and social document collaboration create great opportunities for productivity.

- Anywhere, anytime access to learning applications.
- Instant scalability to meet growing learner populations.
- Seamless compatibility with social and collaborative tools and features.
- Streamline learning delivery.
- Enhance video and mobile learning access.
- Improve management costs and efficiency.
- Provide autonomy to the user and learning organization.
- Strengthen content security.
- The cloud grants more autonomy to individuals and the organization.
- The cloud creates relevant, tailored user content, without IT's help. There is no need to modify, update or implement the delivery platform.
- The cloud uses an open source environment where group collaboration enriches the learning ecosystem and applications.

The architecture of the cloud-based mobile learning should be built on the following groups [24]:

Cloud Learning Devices - mobile and tablet computing corresponds to distribute learning resources from human and non-human appliances since the input and access devices are becoming context sensitive and location independent. This enables the devices to be adapted to the individual needs and the content to be delivered in a contextual way. Learners will combine various applications on their mobile devices to form a personalized cloud-learning environment, consisting of interconnected software applications utilizing content and services available from the cloud for their individual learning needs.

Cloud Learning Services - the social technologies allow for new modes of collaboration and learning and in real life, they deploy a network of globally connected participants. Such services will provide means for asking questions and getting answers from experienced users who would increase the spectrum of conversations.

Cloud Learning Environments - the traditional classroom model is obsolete, since it limits our access to other people, content and new learning tools. Internet reduces the transaction costs of learning, which leads to a situation where learning happens in a distributed and decentralized manner.

It is obvious that the primary interface will be based on mobile cloud-based devices. Some principles could be applied to this architecture and its functionality [24]:

- Learning content - Content needs to be presented in various different forms and mediums from dynamic conversation-based streams to well thought out narratives and information visualization dashboards.
- Learning locations - Learning should take place in different locations during the day. Material under study would connect with the objects in the environment.
- Storage of learning content - Content will be organized in an associative way through tagging and could potentially use the possibilities offered by the semantic web. Cloud computing will provide a distributed and efficient way to store and access this information.
- Organization of learning content and collaboration - Content and teachers will be available on-demand from anywhere in the world through the network. Various new search engines will provide relevancy and accuracy for finding suitable learning content.

Security Issues of Cloud-Based Mobile Learning

D. Cloud Computing

There are certain requirements that should be taken into account on the utilization of cloud computing in mobile learning [25]:

- The cloud provider must be responsible for data confidentiality, integrity and availability. This should be a complete detailed controllership and accountability at each point (and each vendor they use) within the cloud. It would mean authentication, transmission, processing, storage, recovery and destruction.
- Specifications must be prepared regarding ways how the cloud provider will preserve and produce data from requests. Depending on the compliance and legal objectives, this can extend to a few more providers within the cloud and can influence systems that are shared with other cloud clients.
- Data encryption must be considered. The geographical and logical location of its use must be taken into account, the minimum and maximum levels required, laws that may impact use, and if encryption will block the ability to monitor and track the data and threats.
- The cloud provider must possess a crisis management process that will have the appropriate technical, organizational and procedural measures. This could include financial crisis such as vendor bankruptcies, mergers, etc.
- Since cloud is not in one place only, the risk of systems failures substantially decreases. In the case of cloud-based mobile learning the recovery costs are considerably lower since only the local cloud environment, used to access the Internet, is at risk and user data and cloud servers are protected with a high degree of security and reliability.

E. Social networks

Nowadays Web content is highly dynamic, which requires the need for security solutions that are capable of real-time assessment, categorization, and threat control. Recent research shows that [26]:

- 87% of office workers access Web 2.0 & Social Media sites/week, with 63% accessing the sites one or more times/day
- 51% of office workers spend one or more hours a week using & accessing Social Media sites when at work
- 46% of office workers have discussed work-related issues on social media websites
- 71% of office workers use Web-based email at work for personal reasons
- A growing number of organizations (60%) are using Web 2.0 apps (blogs, Wiki's, RSS feeds, social media) to improve collaboration & facilitate participation across the enterprise.
- Users are still mostly using Web 2.0 apps without any filtering or monitoring, creating a legitimate security threat.

While social media can bring benefits to common users and businesses, they can also bring in lots of trouble as far as security issues. Social networks became the main targets for hackers, a situation which is made worse by the prevalence of mobile devices. According to many reports mobile device continue to attract malicious code writers [27]. Even though the volume of threats facing these devices grows quickly, they are still a small minority out of all the threats and vulnerabilities discovered so far. Less than 30% of documented mobile vulnerabilities had malicious codes that targeted and actively abused them. The growing popularity of Android devices led to the appearance of malicious code that focuses on them.

The biggest enemies of users of social networking platforms are spammers, scammers and cybercriminals that want to hijack your social accounts. Many businesses regard the move to on-line phishing as a natural response to the growth in the user communities of the main social networking sites. Regardless online phishing attacks remain a clear and present threat to businesses with the arrival of social networking in the workplace presenting phishers with a bigger pond to phish in.

Many attackers take advantage of users and webmasters who neglect and disregard basic security regulations. One such attack targets servers hosting a large number of websites stored on them, and the people who access these websites. After hacking into the server, it can be used

to spread malicious code to other websites – or even relatively sophisticated users, who usually avoid phishing attacks. Other advanced attacks target branches of international organizations. The attackers infiltrate branches with relatively simple security measures and through them gain access to the networks of the main organization.

Security experts also report more sophisticated attacks on entry points to organizational networks through web servers. Other attacks abuse the basic trust exhibited by typical users when visiting social network websites, or harm users through the use of fake identities on the same websites. A recent survey of executives puts the concerns into four categories: disclosure of confidential information; damaged brand reputation; ID theft; and legal and compliance violations [28].

In publications one can probably find a great variety of solutions to these threats, but in general the recommendations for securing social network sites could be summarized as follows [29, 30]:

- Most social networks offer privacy as a global setting to make a profile public or private, it is important to review and keep track of these settings before posting as most of these platforms encourage users to share updates publicly.
- Personal Info, such as place of birth, address, phone number, etc. are not pieces of information that need to be broadcasted over any networking site.
- Applications that request access to social networking sites upon download are dangerous and should be canceled.
- Suspicious links should be avoided since the chance for a user to be scammed is high.
- Photos could pose a danger when posted and shared in SNS, especially photos from mobile phones coming with geotags. Geotags can show where the photo was taken. Geotags should be turned off and shared photos should be filtered.
- Posts and content. Always remember that you are accountable for what you post. Posts that reflect poorly on your company reflect poorly on you. If you would not say it to someone's face, do not say it to the internet.
- Strong passwords – this means a case-sensitive combination of letters, numbers and special characters. The reuse of passwords across different social media platforms should be avoided.
- Setting up two-factor authentication is recommended - Facebook offers two-factor authentication as an added measure of security for any account. Using two-factor authentication introduces a randomly generated number or token that can deliver to the mobile phone through SMS or a number generator within the mobile application.

F. Mobile Security

More and more users and businesses use smartphones as communication tools but also as a means of planning and organizing their work and private life. Within companies, these technologies are causing profound changes in the organization of information systems and therefore they have become the source of new risks. Mobile security involves protecting both personal and business information stored on and transmitted from smartphones, tablets, laptops and other mobile devices. All smartphones and computers are preferred targets of attacks. These attacks exploit weaknesses related to smartphones that can come from means of communication like SMS, MMS, wireless networks and smart mobile devices.

The term mobile security is a broad one that covers everything from protecting mobile devices from malware threats to reducing risks and securing mobile devices and their data in the case of theft, unauthorized access or accidental loss of the mobile device [31], [32]. Mobile security also refers to the means by which a mobile device can authenticate users and protect or restrict access to data stored on the device through the use of passwords, personal identification

numbers or more advanced forms of authentication such as fingerprint readers, eye scanners, biometric readers, etc.

Research has identified an impressively long list of threats to mobile computing [33], [34]:

- Malware, Trojans and other attacks;
- Key loggers;
- Compromised Wi-Fi hotspots;
- Poisoned DNS;
- Malicious and privacy leaking apps;
- Jail broken and rooted devices;
- Unpatched OS versions;
- Spear phishing;
- Advanced persistent threats.

Recommended prevention measures to them could be [33, 35]

- Securing mobile communications - all mobile device communications be encrypted, any communications between a mobile device and a cloud system/service require should use a VPN access. This will provide opportunities for logging, management and strong authentication of clients using a mobile device to access applications and services.
- Requiring strong authentication and using password controls - besides simple account and password, mobile devices should be used with multiple forms of authentication in order to guarantee that using a mobile device does not grant access to important information and systems by default.
- Password protection and management - protecting against phishing scams and re-direct attacks using real-time website blacklists and whitelists.
- Compliance and risk management - built-in password protection and management, content loss prevention, and centralized control over remote devices helps reduce risk and achieve regulatory compliance.
- Data loss prevention - Policy management by user, device and content to control copying, pasting, and printing over the network.
- Controlling third-party software - policies must be established to limit or block the use of third-party software. This is the best way to prevent possible compromise and security breaches.
- Choosing secure mobile devices - mobile devices should be configured to avoid unsecured wireless networks, and Bluetooth should be hidden from discovery.
- Unified user experience - working similarly across all devices, with the same interface for desktop and mobile devices, regardless of platform.
- Performing regular mobile security audits and penetration testing - At least once a year organizations should conduct a security testing to audit their mobile security and conduct penetration testing on the mobile devices they use.

G. Big Data

Data security rules have changed in the age of big data. Organizations are collecting, analyzing and making decisions based on analysis of massive amounts of data sets from various sources such as web logs, clickstream data and social media content to gain better insights about their customers. Their business and security in this process are becoming increasingly more important [36].

In the early days of big data, storage security was less of an issue, as the only organizations collecting and storing it were large corporations and government agencies with proprietary infrastructures isolated from the operational networks. As cloud storage became

available, these organizations were able to transition to private clouds without needing to make too many adjustments to their data protection practices [37]. Nowadays even small companies are collecting huge amounts of data about customer behavior, marketing campaign responses, market trends, and more. Such companies are storing their data in public cloud environments, where security is a completely different matter. The traditional security systems smaller companies use to secure static data on semi-isolated networks are not up to the task of securing big data in a public cloud.

A Forrester report, the "Future of Data Security and Privacy: Controlling Big Data," observes that security professionals apply most controls at the very edges of the network [38]. However, if attackers penetrate the perimeter, they will have full and unrestricted access to the data. The report recommends placing controls as close as possible to the data store and the data itself to create a more effective line of defense. Thus, if the priority is data security, then the cluster must be highly secured against attacks. One of the greatest obstacles to conquering cybersecurity is the challenge of analyzing the enormous amount of data that is required to adequately handle specific threats

The volume of data created, sent, stored and needing protection will also continue to grow at more than 40 per cent each year, which means it will double every two years. Around 80 per cent of that new data will be unstructured [39]. Organizations that have moved their data to the cloud will also understand that e-discovery and investigation efforts need to be applied in the same cloud as the data. With the volume of data involved in these tasks, it is simply not practical to copy it from one data center to another, as some cloud e-discovery and investigation providers require.

Conclusion. The increased use of tablets and smartphones for mobile-specific applications, extended use of digital textbooks and online instructional materials as a main learning resource, growth in preparation and use of open source materials providing for greater collaboration and cross-device use, further integration of social networking integrated into the learning process for increasing learners' collaboration and connections with instructors, the movement to cloud computing and online classroom management systems that gather student achievement data and allow for more personalized instruction will bring new meaning and content to education as a whole, as well as new possibilities to provide for a higher educational level.

However, each of the four components of this type of learning – cloud computing, social networks, mobile computing and big data bring new security issues alone, and their combination could be too complex to handle at first. Therefore, new recommendations must be provided and new multi-faceted rules should be followed to keep the cloud-based mobile learning secure.

References

1. Bersin, J. (2012). *From e-Learning to We-learning and m-Learning*. Available at http://www.slideshare.net/jbersin/mobile-and-informal-learning-trends-for-2012.
2. *Learning*. Available at http://en.wikipedia.org/wiki/Learning
3. Trucano, M. *What do we know about using mobile phones in education?* Available at http://blogs.worldbank.org/edutech/videos/what-do-we-know-about-using-mobile-phones-in-education-0.
4. Weiss, C. (2012). *State of the LMS 2012*. Available at http://elearninfo247.com/2012/02/16/state-of-the-lms-2012/
5. *InteSolv*. (2012). Five eLearning Trends to Watch in 2012. Available at http://intesolv.com/details/tabid/552/listingkey/2725/five_elearning_trends_to_watch_in_2012.aspx.
6. *Mlearning*. Available at http://en.wikipedia.org/wiki/MLearning
7. *Wikipedia*. Social networking service. Available at http://en.wikipedia.org/wiki/Social_networking_service
8. *Gartner*. Gartner Says Nexus of Forces Social, Mobile Cloud and Information - Is the Basis of the Technology Platform of the Future. Available at http://www.gartner.com/it/page.jsp?id=2097215
9. Hinchcliffe, D. *The "Big Five" IT trends of the next half decade: Mobile, social, cloud, consumerization, and big data*. Available at http://www.zdnet.com/blog/hinchcliffe/the-big-five-it-trends-of-the-next-half-decade-mobile-social-cloud-consumerization-and-big-data/1811
10. Pavlenyi, J. (2012). *Social + Mobile + Cloud = The New Paradigm for Midsize Business*. Available at http://www.wired.com/cloudline/2012/05/social-mobile-cloud/

11. *Mobile Learning Course Development Blog*. The rise of big data and cloud computing mutually indispensable. Available at http://blog.dianlake.com/the-rise-of-big-data-and-cloud-computing-mutually-indispensable.html
12. *Cloud Computing*. Available at http://en.wikipedia.org/wiki/Cloud_computing
13. Reese, G. (2009). *Cloud Application Architectures: Building Applications and Infrastructure in the Cloud*. O'Reilly Media.
14. Rittinghouse, J. W. & Ransome, J. F. (2009). *Cloud Computing: Implementation, Management and Security*. CRC Press.
15. Bradley, T. (2011). Embrace the cloud for natural disaster recovery; *PC World*. Available at http://www.computerworlduk.com/advice/infrastructure/3265771/
16. Tanya, E. *Universal instructional design principles for mobile learning*. Available at http://www.irrodl.org/index.php/irrodl/article/view/965/1675
17. Educational Publishing, (June, 2012). 10 Mobile Learning Trends for 2012. Available at http://edpublishing.wordpress.com/2012/01/06/mobile-learning-in-education-10-trends-to-track-in-2012/
18. Weiss, C. (2012). *State of the LMS 2012*. Available at http://elearninfo247.com/2012/02/16/state-of-the-lms-2012/
19. *Gartner*. Gartner Says Nexus of Forces Social, Mobile Cloud and Information - Is the Basis of the Technology Platform of the Future. Available at http://www.gartner.com/it/page.jsp?id=2097215
20. *Symantec*. As the cloud, social media and mobile come together, IT is becoming a service organization. Available at www.symantec.com/connect/blogs/cloud-social-media-and-mobile-come-together-it-becoming-service-organization
21. Pavlenyi, J. (May, 2012). *Social + Mobile + Cloud = The New Paradigm for Midsize Business*. Available at http://www.wired.com/cloudline/2012/05/social-mobile-cloud/
22. Ramani, R. *Six Ways Cloud Technology Will Impact Learning*. Available at http://clomedia.com/articles/view/six-ways-cloud-technology-will-impact-learning
23. Taylor, C. *Integration is Everything in a Mobile, Social, Cloud and Big Data World*. Available at http://cloud.dzone.com/articles/integration-everything-mobile-0
24. Teemu, A. (2011). *Cloud Learning as Universal Primary Education*. Available at http://tarina.blogging.fi/2011/11/12/cloud-learning-as-universal-primary-education/
25. Lawhorn, R. (2010). *Tarantino-Style Approach to Secure Cloud Computing; Sec Techno*. Available at http://www.sectechno.com/2010/09/18/tarantino-style-secure-cloud-computing/
26. *InfoSight*. Web 2.0 & Social Media Security. Available at http://www.infosightinc.com/IT-Security/web2_security.php
27. *iHLS*. (2013). Cyber security report: Social networks – a favorite target for hackers. Available at http://i-hls.com/2013/10/cyber-security-report-social-networks-a-favorite-target-for-hackers/.
28. Siciliano, R. *7 Small Business Social Media Risks*. Available at http://www.huffingtonpost.com/robert-siciliano/7-small-business-social-m_b_4846083.html
29. Hunt, G. How to Protect your Data Privacy on Social Networks. *Web Security*. Available at http://solutions.webtitan.com/blog/bid/157016/How-to-Protect-your-Data-Privacy-on-Social-Networks-Web-Security
30. Reese, R. (2014). *10 Steps to Help Your Users Secure Their Online Presence*. Available at http://broadcast.oreilly.com/2014/01/10-steps-help-users-secure-online-presence.html
31. *Wikipedia*. Mobile security. Available at http://en.wikipedia.org/wiki/Mobile_security.
32. *Webopedia*. Mobile Security. Available at http://www.webopedia.com/TERM/M/mobile_security.html
33. *Marble*. Nine Critical Threats Against Mobile Workers, WhitePaper. Available at http://go.marblesecurity.com/NineThreatsWPwebsite_Marblelandingpage052013.htm
34. John, K. *Higgins,Feds' Shift to Mobile Creates Security Cracks*. Available at http://www.ecommercetimes.com/story/79918.html
35. Tittel, E. *7 Enterprise Mobile Security Best Practices*. Available at http://www.cio.com/article/748142/7_Enterprise_Mobile_Security_Best_Practices
36. Gelgon, S. (2014). Big Data: new challenges for information systems security. Available at http://news.bull.com/bulldirect/2014/02/03/big-data-new-challenges-for-information-systems-security/
37. Benz, J. (2014). *Building the foundation for Big Data – Security*, Part 1. Available at http://blog.code-n.org/2014/01/27/building-foundation-big-data-security-part-1/
38. Pramanick, S. Adressing *Big Data Security*. Available at http://www.ibmbigdatahub.com/blog/addressing-big-data-security
39. Sheehey, E. (2014). *Five information security and big data forecasts for 2014*. Available at http://www.cso.com.au/article/536875/five_information_security_big_data_forecasts_2014.

Received 30.09.2014 *© Velev D. G.*
Стаття надійшла до редакції 30.09.2014 *© Велєв Д.Г.*