Interdiscip J Virtual Learn Med Sci. 2017 September; 8(3):e64233. doi: 10.5812/ijvlms.64233.

Published online 2017 September 30. **Research Article**

Proposing a Secure Architecture for Mobile-Learning Environments and Investigating Teachers' Attitude

Seyed Hassan Sadeghzadeh,[1,*] and Ali Nakhaei[1]

[1]Department of Information and Communication Technology, Payame Noor University, IR Iran

[*]*Corresponding author*: Seyed Hassan Sadeghzadeh, Department of Information and Communication Technology, Payame Noor University, IR Iran. E-mail: sadeghzadeh@pnu.ac.ir

Received 2017 July 05; **Accepted** 2017 August 22.

Abstract

Background: The next generation of learning called mobile learning (m-learning) provides education to people through mobile devices. The security of mobile systems is an important issue due to users' mobility and use of various devices and different ways of connecting to the network. Therefore, the current study aimed at providing a secure architecture as the basis for use in m-learning software to improve the security of such systems and investigate professors' satisfaction with this architecture.
Methods: The current applied study was conducted in 2014. Statistical population included all professors using m-learning in Tabas, Firdaus, and Birjand cities, Southern Khorasan, Iran (26 participants). The purposive sampling method was used. The reliability of the questionnaire was measured using Cronbach's alpha (94%) and the validity based on factor validity (explained percentage of variance) was 63%. According to the use of the web-based e-learning service in Southern Khorasan Payam-e-Noor University (PNU), it was attempted to write a mobile application to provide the use of this service on mobile devices. The difference between the current study provided app and other mobile apps is based on using the proposed secure architecture. To measure the satisfaction of users with the study app, a researcher-made questionnaire was distributed among the professors using the app. Data analysis was performed with SPSS 16 by t test and the one-way analysis of variance (ANOVA).
Results: Findings showed that the professors using m-learning application of Southern Khorasan PNU had a positive attitude towards it with the average satisfaction of 80%. The most important factor for this satisfaction was the safety of the presented architecture, while avoiding complex and time-consuming control mechanisms.
Conclusions: In the current study a secure architecture was provided for mobile system that was simple, fast, and applicable on all mobile network operators. Given the positive perspectives of professors, this architecture can be a good solution to secure m-learning environments.

Keywords: Learning, Distance Learning, Professor, Mobile Learning, Telecommunications, Data Security, Cryptography

1. Background

By the increasing use of the internet and modern communication technologies, electronic learning (e-learning) and mobile learning (m-learning) are the highlighted words. E-learning uses information and communication technologies such as internet, multimedia, and hypermedia systems to improve the quality of learning by facilitating the access to resources and educational services, and provides tools such as distance interaction and participation (1). The ability to learn at any time and place that has the characteristics of e-learning is up-to-date with the advancement of wireless technology and m-learning. In fact, m-learning is a model of e-learning carried out through mobile technologies such as mobile phones, personal digital assistant (PDA), audio players, electronic books, etc. M-learning provides people with learning through mobile devices. And as observed in Figure 1, m-learning can be considered a combination of distance education and e-learning (1).

Similar to distance learning, there is a separation between the faculty and the learner, and similar to e-learning; m-learning provides learning through electronic devices with more advanced technologies (1). In a more precise definition, Brown suggests m-learning position in the field of distance learning and e-learning, as shown in Figure 2 (2).

M-learning, as noted above, eliminates the location restriction and enables the person to benefit from this kind of learning at any place, during travel, or even trapped by the traffic gam. Table 1 presents some of the m-learning goals (3).

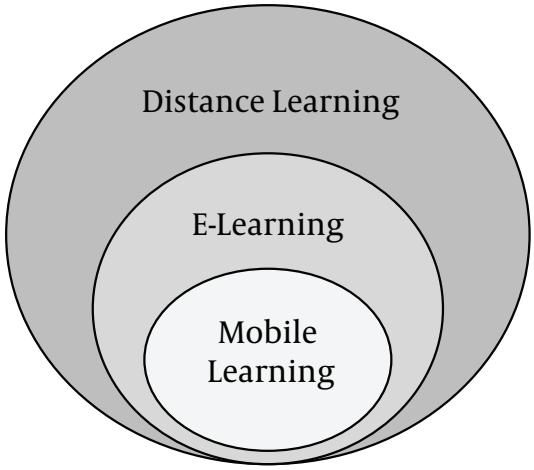

Figure 1. Status of Mobile Learning as a Part of Distance and E-Learning (1)

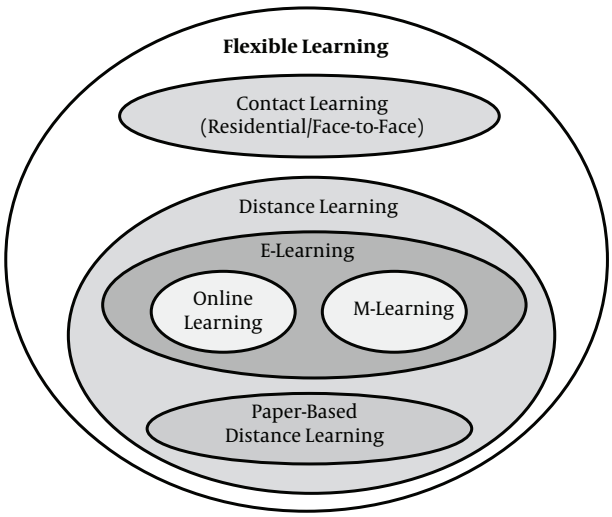

Figure 2. The Subsets of Flexible Learning (2)

1.1. Security: The Main Challenge in m-Learning

Devices used in m-learning such as mobile phones, tablets, and other similar devices benefit from a high degree of security, which allows data interception, copying, and sharing (4). The increasing threats to data and privacy in mobile communication raised concern for teachers, learners, and educational institutions as most students are often allowed to use their own mobile devices to access m-learning services and resources (5). So far, most advancements in m-learning focus on the development, deployment, and delivery of training courses, and little attention is also paid to security and privacy.

Table 1. M-Learning Goals (3)

Goals of M-Learning	Description
To learn from worldwide	In m-learning, students can learn from diverse sources around the world.
To maintain physical and mental health	M-learning can reduce the physical pressures caused by carrying heavy school bags; in addition, educators can change the environment and view the educational environment and benefit from various educational experiences.
To learn at any time and place, in order to optimize the management of time	M-learners can set their own time and place of learning. M-learning has benefits for students and they can chose the time and place of learning.
To diminish infrastructure costs	Unlike traditional learning, m-learning does not require physical classroom facilities.
To prepare people for the future communication and computer technologies	The high availability of m-learning can provide users updated information about communication technologies in order to make them ready for change.

For example, the authors (6) reviewed the latest frameworks and middleware developed to facilitate m-learning and U-learning, and concluded that further development of privacy and security is needed to enable m-learning systems guarantee the users' rights. It is not correct to use e-learning security mechanisms in m-learning, since m-learning is directly affected by mobile technologies and is more about interacting with information at the moment they are needed and/or in a specific use context. Therefore, it is expected that issues in the field of security and privacy in m-learning are investigated in a completely different way from those of the e-learning systems (7). For example, when the privacy issue is highlighted, individuals, groups, and organizations that are somehow engaged in may be particularly concerned about indirect access (e g, without user consent) to personal information such as mobile phone numbers, IP (internet protocol) addresses, user locations, the international mobile equipment identities (IMEIs), mobile hardware codes, etc. (8).

There are similar concerns for securityin typical e-learning activities such as participating in the electronic tests; it is likely that under such conditions m-learning settings are completely uncontrollable. In response to the aforementioned needs, so far, several researchers identified security and privacy issues especially for m-learning ecosystem (8). Figure 3 provides a schematic overview of the challenges for clarification and easy referencing (8).

In the field of m-learning, 3 of its constituent parts:

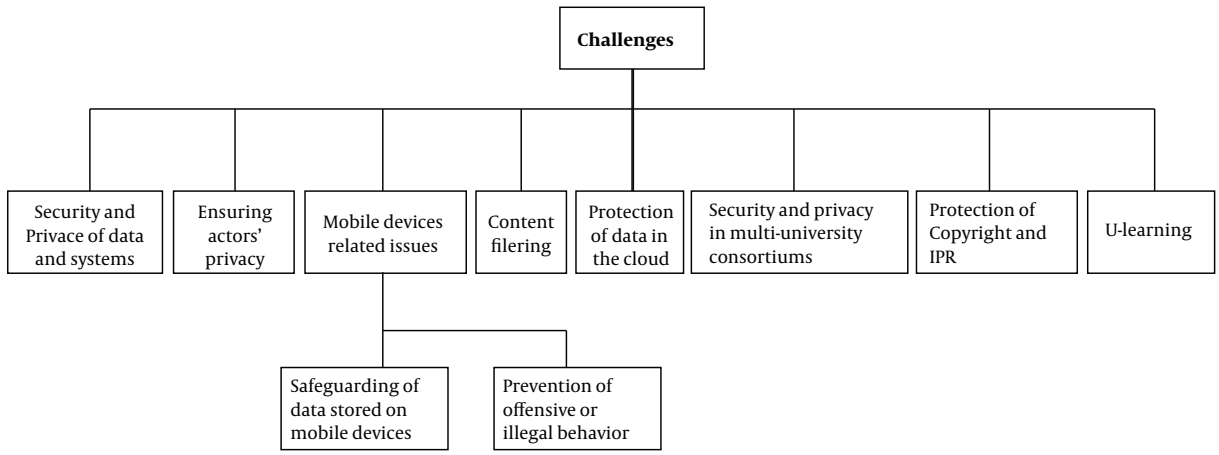

Figure 3. Security and Privacy Challenges in m-Learning and Beyond (8)

learner, educator, and online educator organization should have resources and software to ensure that they can verify the accuracy of the communication with the expected party (9). The main purpose of the architecture presented in the current study is security issues, along with a lightweight solution dealt with in fewer articles.

In recent years problems related to service authentication in mobile environments are studied and some methods are proposed to improve them. In all of them, the proposed 2-way authentication protocols normally require heavy operating charges, especially on the mobile side (10-13).

In general, the main purpose of current paper is to provide a secure mobile system that uses a lightweight encryption system instead of commonly used cryptographic methods in authentication protocols requiring heavy calculations.

The proposed architecture has simplicity and speed and boosts the process of double-sided security and security of the system and provides all the services of an m-learning system.

2. Methods

The current applied study aimed at developing the applied knowledge in a specific context to provide a secure architecture for m-learning environments and assess the satisfaction of instructors with this architecture. As Payame Noor University (PNU) of Southern Khorasan province, Iran, employed the web-based e-learning service, it began to program a mobile application to provide using this service on mobile devices.

The main difference between this app and other m-learning apps is using a secure architecture to create a sense of trust and satisfaction with users while using the m-learning services on their mobile phones.

2.1. The Main Steps in Designing the Proposed Strategy

- Selection of an appropriate basis

Various applications are used by software developers to deliver m-learning both in commercial and free licenses (14). Since the e-learning services are available to all students of PNU of Southern Khorasan on www.lms.skpnu.ac.ir, it was necessary to program an app that allow the students to communicate with e-learning web services of the university, pick up the courses, and use teachers' information service database.

Programming and developing of this app were based on the Semertzidis successful experience presented in his Master's thesis (15). To better understand the entire project of architecture, Figure 4 shows the component view of the system.

- Choosing the right encryption method

In an application, an innovative and successful encryption algorithm was used to secure data (16).

Choosing an appropriate encryption method:

To secure data, an innovative and successful encryption algorithm used in electronic payment applications was employed (16). In this model, a hybrid application of elliptical bending algorithms and a message summary of the BLAKE 2.0 was used.

Its features are fast and responsive and require little memory usage, and its implementation was easy with Android APIs programming.

2.2. Review of the Proposed Scheme

Data confidentiality prevents unauthorized access. In other words, only authorized personnel can access the data

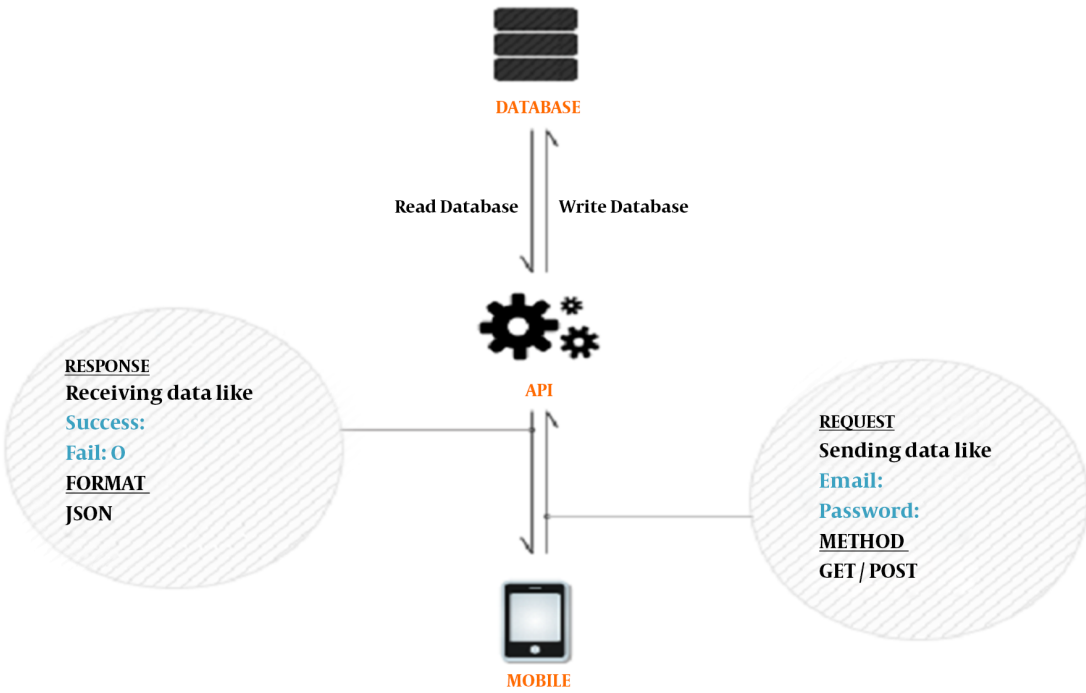

Figure 4. Component View of the System (16)

and unlicensed personnel cannot access the data (17).

The factors that influence the success of data confidentiality in the proposed architecture were: user authentication, identity verification, double-checking authenticity, and non-denial service. Therefore, by analyzing these factors, it was demonstrated that it covered all the security needs:

- Given that the advanced encryption standard (AES) algorithm and a 128-byte key as well as RSA algorithm and a 1024-byte key were used for coding of user and organization information and these algorithms had acceptable security, the information confidentiality was obtained.

- Given that each user had a unique PIN and this PIN was placed inside organization database, after receiving the demand, the organization could decode the related PIN sent with information package including the demand, and match it with PIN existed in the organization, and confirm user identity if they were similar.

- By the PIN, the user could be quite sure about communication with the desired organization. PIN was registered at the time of user's registration and only the user and organization knew it. It could be in any forms (such as favorite movie star) and ensured the user on communication with the desired organization and the organization's identity was confirmed this way.

- For the confirmation of mutual identity, SHA-1 hash function was used. Service receiver program prepares a summary of the sent information using this function and then, encoded it using organization's public key and sent along with other information. At the organization, after receiving the information package, the encoded summary was decoded using organization's private key. Then information summary was recalculated using the function, after being matched and if similar, mutual identity confirmation was ensured.

- Given that information packages sent to the organization by service receiver contained user PIN, if the PIN was confirmed, the carrier of PIN was accounted for the related transactions and the user could not deny sending the demand, because he/she had sent the demand or the PIN was used by another person. Therefore, undoubtedly the customer cannot deny sending the demand received by the organization and this showed non-repudiation feature in the proposed design.

To measure the satisfaction of users, the questionnaire was distributed among the PNU of Southern Khorasan professors. Data collection was conducted in a survey method.

Statistical population included all professors using m-learning in Tabas, Firdaus, and Birjand cities (26 participants). Given the small size of the population, all of the

participants were included in the research. Data collection tool was a researcher-made questionnaire. Reliability of the questionnaire was 94% using Cronbach's alpha. The validity of the questionnaire was verified by the recruited professors and the factor's validity of the questionnaire was calculated 63% based on the factor validity (explained percentage of variance). Data analysis was performed with SPSS version 16 by t test and the one-way analysis of variance (ANOVA).

3. Results

Table 2 shows the result of the questionnaires.

Demographic variables including age, experience, city, and gender are represented in Table 2 part A. Statistical population included 26 people, 13 females and 13 males, and the research was conducted in 3 cities.

Table 2 part B shows professors' satisfaction based on gender. The mean satisfaction in both genders was 80%. Mean parameter showed that professors had positive perspectives toward the new architecture. The level of satisfaction between the 2 groups was almost equal. There was no significant difference between the groups based on P value. Table 2 part C represents professors' satisfaction. According to part C, the mean for minimum and maximum satisfaction was 80% that represented professors' satisfaction with this architecture and the main reason was its security.

The Kolmogorov-Smirnov test was used to investigate normal distribution of professors' satisfaction. The level of significance of satisfaction for both female (0.211) and male professors (0.167) was more than 0.05, and therefore; normal distribution of variable was confirmed. ANOVA was used to evaluate the differences in the level of satisfaction among the professors in Tabas, Ferdows and Birjand (Table 3).

According to the results of Table 3 part B, P value was more than 0.05 (0.136), and therefore; there was no significant difference between the average satisfaction of professors among cities. To evaluate the difference between the professors' satisfaction in terms of gender, the independent t test was used (Table 4 part A). Given the significance (0.172) of Levene test (sig > 0.05), the variance equality was achieved; therefore, the basis of t test analysis was the first row (assumption of variance equality). Given the significance (0.075) of t test (sig > 0.05), lack of difference between mean satisfaction of professors based on gender was achieved. Moreover, the results of mean satisfaction of professors based on work experience are presented in Table 4 parts B & C using the independent t test.

According to Table 4 part C given significance (0.697) of Levene test (sig > 0.05), variance equality was achieved; therefore, the basis of t test analysis was the first row (assumption of variance equality). Given the significance (0.001) of t test (sig > 0.05), lack of difference between mean satisfaction of professors based on gender was achieved.

Given the positive mean difference (1.224), it was obvious that the first group including people with low experience had a higher satisfaction compared with the other group. Table 5 represents factors influenced professors' satisfaction with this architecture using factor analysis.

According to factor analysis (main components), 4 subgroups were obtained based on the above table.

4. Discussion and Conclusions

With the development of internet-enabled facilities and the provision of wireless connectivity, cell phones entered the market and provided the platform for the emergence of a new generation of education called m-learning. Since the security of mobile systems, due to the mobility of users, is a critical issue, the app presented in current study, which was provided to activate the e-learning system of Southern Khorasan PNU on smart phones and tablets, proposed a secure architecture to use a lightweight encryption system instead of the most widely used encryption methods, which simplified and speeded up the process of double-sided authentication and security of the system. The app also had all the services of an m-learning system and can be implemented on all GSM (global system for mobile communications) supported networks. The encryption system used in this application had many advantages such as support for user anonymity, local authentication, robustness against common security attacks; e g, repetition, change, server forgery, and other types of attacks.

Statistical analysis showed that the use of lightweight architecture along with the reduction of hardware and software resources was the most important factor to motivate and assure users in this m-learning app.

The average satisfaction of users with this software in both genders was 80%. The parameters of satisfaction, ease of use, motivation, cost-efficacy, and security were studied based on factor analysis. Regarding the fact that the mean difference (224/1) was positive, it is evident that the first group, the less experienced professors, had a higher mean satisfaction than the highly experienced ones.

Footnote

Conflict of Interest: None declared.

Table 2. Statistical Results of the Questionnaires

	A) Description of Demographic Variables in the Study Population				
Variables	**Subgroups**	**Number**	**Percentage/Age Range**		
Age	-	-	33.34 ± 3.66		
Experience	-	-	9.15 ± 4.23		
City	Tabas	9	34.6		
	Firdaus	8	30.8		
	Birjand	9	34.6		
Gender	Male	13	50		
	Female	13	50		
B) Comparison of the Mean Satisfaction of Professors Based on Gender					
		Number	**Mean**	**SD**	**Mean Standard Error**
Male		13	79.0283	6.77377	1.87871
Female		13	80.9717	9.61360	2.66633
Significance = 0.55 Degree of freedom = 24; T = 0.59					
C) Score of Professors' Satisfaction					
	Number	**Minimum**	**Maximum**	**Mean**	**SD**
Satisfaction	26	65.26	100	80	8.20783
Reliable data	26				

Table 3. Results of ANOVA and Descriptive Statistics

	A) Descriptive Statistics of Satisfaction Based on the Cities				
City	**Number of Teachers**	**Average**	**Variance**		
Tabas	9	4.11	0.601		
Firdaus	8	3.75	1.165		
Birjand	9	3	1		
Total	26	3.62	1.023		
B) Results of ANOVA Regarding the Mean Difference of Professors' Satisfaction in the Cities					
	Sum of Squares	**Degree of Freedom**	**Mean of Squares**	**F Value**	**P Value**
Between two Groups	4.168	2	2.084	2.	0.136
In each group	21.99	23	0.956	1	
Total	26.15	25		80	

References

1. Barzegar R. From electronic learning to mobile learning: theoretical principles. *Interdisciplinar J Virtual Learn Med Sci.* 2012;**3**(2):35–41.
2. Georgiev T, Georgieva E, Smrikarov A. M-learning-a New Stage of -Learning. International conference on computer systems and technologies. *CompSysTech.* 2004;**4**(28):1–4. doi: 10.1145/1050330.1050437.
3. Mohammadi H. Social and individual antecedents of m-learning adoption in Iran. *Comput Human Behav.* 2015;**49**:191–207. doi: 10.1016/j.chb.2015.03.006.
4. Thompson N, McGill TJ, Wang X. "Security begins at home": Determinants of home computer and mobile device security behavior. *Comput Secur.* 2017;**70**:376–91. doi: 10.1016/j.cose.2017.07.003.
5. Pachler N, Bachmair B, Cook J. Mobile Devices as Resources for Learning: Adoption Trends, Characteristics", Constraints and Challenges, In Mobile Learning. Springer; 2010.
6. Zhang B, Yin C, David B, Xiong Z, Niu W. Facilitating professionals' work-based learning with context-aware mobile system. *Sci Comput Program.* 2016;**129**:3–19. doi: 10.1016/j.scico.2016.01.008.
7. Sarrab M, Elbasir M, Alnaeli S. Towards a quality model of technical aspects for mobile learning services: An empirical investigation. *Comput Human Behav.* 2016;**55**:100–12. doi: 10.1016/j.chb.2015.09.003.
8. Kambourakis G. Security and Privacy in m-Learning and Beyond: Challenges and State-of-the-art. *Int J u-e-Serv Sci Technol.* 2013;**6**(3):67–84.

Table 4. Results of the Independent t Test

	A) Results of the Independent t Test for the Mean Satisfaction of Professors Based on Gender					
	Levene Test		t Test			
Professors' Satisfaction	F Value	Sig	T Value	Degree of Freedom	Sig	Mean Difference
Assumption of variance equality	1.99	0.172	2.284	23	0.075	0.154
Assumption of variance inequality	-	-	2.318	21.39	0.076	0.154
B) Descriptive Statistics of Satisfaction Based on Work Experience						
Experience	Number of Teachers	Average	Variance			
Low experience	15	4.13	0.743			
High experience	11	2.91	0.944			
C) Results of the Independent t Test on Mean Satisfaction of Professors Based on Work Experience						
Professors Satisfaction	Levene Test		t Test			
	F Value	Sig	T value	Degree of Freedom	Sig	Mean Difference
Assumption of variance equality	0.155	0.697	3.704	24	0.001	1.224
Assumption of variance inequality	-	-	3.567	18.44	0.002	1.224

Table 5. Determination of Effective Factors on Professors' Satisfaction With the Architecture Using Factor Analysis

Variable	Factor			
	Ease of Using the Architecture	Professors Motivation in Using the Architecture	Reduction of Software and Hardware Resources	System Security
q18	0.894			
q19	0.827			
q4	0.797			
q7	0.720			
q17	0.574			
q14	0.573			
q10		0.844		
q16		0.759		
q12		0.719		
q15			0.787	
q5			0.787	
q6			0.716	
q9				0.658
Variance	32.89	18.07	16.66	9.98

9. Al-Hunaiyyan A, Alhajri RA, Al-Sharhan S. Perceptions and challenges of mobile learning in Kuwait. *J King Saud Univ Comput Inf Sci.* 2016 doi: 10.1016/j.jksuci.2016.12.001.
10. Bahry FDS, Anwar N, Amran N, Rias RPM. Conceptualizing Security Measures on Mobile Learning for Malaysian Higher Education Institutions. *Proc Soc Behav Sci.* 2015;**176**:1083–8. doi: 10.1016/j.sbspro.2015.01.582.
11. Emmanouilidis C, Koutsiamanis RA, Tasidou A. Mobile guides: Taxonomy of architectures, context awareness, technologies and applications. *J Network Comput Applicat.* 2013;**36**(1):103–25. doi: 10.1016/j.jnca.2012.04.007.
12. Tully S, Mohanraj Y. In: Mobile Security and Privacy. Tully S, Mohanraj Y, editors. ; 2017. pp. 5–55.Mobile Security: A Practitioner's Perspective.
13. Shuib L, Shamshirband S, Ismail MH. A review of mobile pervasive learning: Applications and issues. *Comput Human Behav.* 2015;**46**:239–44. doi: 10.1016/j.chb.2015.01.002.
14. Digital Trends Staff . Get smart: The 25 best educational apps for iPhone and Android 2017. Available from: https://www.digitaltrends.com/mobile/best-educational-apps/#ixzz4g5WaCyhA.
15. Semertzidis K. Mobile application development to enhance higher education lectures. The University of York; 2013.

16. Pokharel S, Choo KKR, Liu J. Mobile cloud security: An adversary model for lightweight browser security. *Comput Standards Interfaces.* 2017;**49**:71–8. doi: 10.1016/j.csi.2016.09.002.

17. Kim HJ, Lee JM, Rha JY. Understanding the role of user resistance on mobile learning usage among university students. *Comput Educ.* 2017;**113**:108–18. doi: 10.1016/j.compedu.2017.05.015.