A Secure Mobile Learning Framework based on Cloud

Dr. Mohammad Al Shehri
CCIS, Majmaah University,
Al Majmaah
Kingdom of Saudi Arabia

***Abstract*—With the rising need for highly advanced and digital learning coupled with the growing penetration of smartphones has contributed to the growth of Mobile Learning. According to Ericsson's forecast, 80% of the world's population (6.4 billion people) will be Smartphone users by 2021. But the existing Mobile Learning Frameworks has some limitations that need to be addressed for mass adaptation, limitations include device compatibility and security. In this paper we propose a Secure Mobile Learning Framework (SMLF) based on TPM in the cloud. SMLF is supported by three layers Communication Module (CM) which helps in ensuring end to end security. In addition to this we propose a procedure for personalizing mobile learning applications of the student and instructors. We also propose a secure mobile learning protocol in SMLF framework. Proposed SMLF ensures mutual authentication of all the stakeholders, privacy of the message, integrity of the message, and anonymity of the student from the instructor and non-repudiation and is free from known attacks. Our proposed SMLF framework is successfully verified using BAN logic.**

Keywords—Trusted Platform Module (TPM); Communication Module (CM), anonymity; non-repudiation; personalized; BAN logic

I. Introduction

Mobile learning combines electronic content with learning support and services. Mobile learning systems requires specialized infrastructure but this infrastructure cannot be afforded by universities. Cloud provides a novel opportunity for these universities which is based on the distributed computing, parallel computing, grid computing and virtualization technologies. When adopting cloud technology in the realm of Mobile learning customers are not ready to deploy their applications in the cloud as security and data privacy are the main concerns in the cloud. Popularity of Mobile learning system should contain the following features L. Gouveia (1999) [8]:

a) Rich content and curriculum approved by experts.

b) Convenient & Flexible for all the stakeholders.

c) Continuous improvement.

d) Rich simulation with threaded discussion.

e) Should ensure Security and privacy in delivering.

Following are the requirements for mobile learning framework:

1) Authentication of Stakeholders: Student / Instructor / University identifications should ensure strong mutual authentication properties for all the stakeholders in the framework.

2) Privacy of the Message: Message privacy should be ensured among the messages exchanged among the stakeholders.

3) Integrity of the Message: Messages exchanged among the stakeholders should not be altered, so Message integrity property should be ensured for all the messages exchanged among the stakeholders.

4) Non-Repudiation: Non-repudiation property should be ensured in the framework to avoid stakeholders denying their involvement in the communication.

5) Anonymity of the student from the instructor: Anonymity of the student from the instructor should be ensured while submitting feedback for the instructor i.e. the real identity of the student should not be known to the instructor.

6) Unauthorized access to the stakeholder's credentials and private resource or information: No intruder or stakeholder in the framework should be able to access other stakeholder's credentials and private resource or information.

The rest of the paper is organized as follows: In Section 2 we present Related Work, in Section 3 we present our proposed mobile learning framework based on Cloud, in Section 4 we provide formal verification of SMLF protocol using BAN logic, Section 5 presents Comparative Analysis of our proposed framework with Related Works, and Section 6 concludes our work.

II. Related Work

Existing mobile learning solutions based on cloud such as [1]-[3] does not ensure non repudiation, mutual authentication, integrity properties. So this paper overcomes all the flaws of the existing solutions, by proposing a Secure Mobile Learning Model (SMLF) based on TPM in the cloud. SMLF is supported by three layers Communication Module (CM) and a novel procedure is proposed for personalizing mobile learning applications of the student and instructors. Proposed SMLF ensures authentication of all the stakeholders, privacy of the message, integrity of the message, and anonymity of the student from the instructor and non-repudiation and is free from known attacks.

III. Proposed Mobile Learning Framework

A. Proposed Four Layer Mobile Learning Model

In order to ensure success and to maintain the efficiency of the services, all the stakeholders must cooperate and stay open-minded to the development of new technologies, protocols and frameworks. We propose a four-layer mobile learning model involving stakeholders used to understand the functions and analyze the relationship among the stakeholders.

a) Mobile Learning Layer: The student, the University and the Instructor are the Stakeholders involved in this mobile learning layer. University acts as a Registration Authority (RA) by offering Mobile PKI services of registration to both students and instructors.

b) Communication Layer: A mobile learning framework is based on a wireless network, which is maintained by the mobile network operator. The mobile network operator is a part of communication layer and is responsible for carrying the data Over The Air (OTA).

c) Technology Layer: The software provider, Mobile device manufacturer, Secure Element (SE) manufacturer, Trusted Platform Module (TPM) manufacturer, and the Cloud provider are located in the Technology Provider layer. The software provider produces software components that connect different stakeholders in the Mobile Learning layer, while the Mobile device manufacturer provides the mobile devices to students and Instructors; the Secure Element (SE) manufacturer provides SE’s to students and Instructors; the Trusted Platform Module (TPM) manufacturer provides TPM’s to University, Cloud Provider, Mobile Network Operator (MNO) and Certifying Authority (CA) and finally Cloud Provider provides cloud services to mobile learning framework.

d) Supervision Layer: Certifying Authority (CA), Regulator (Department of Higher Education) and the Central Government are a part of this layer. Certifying Authority (CA) is responsible for issuing certificates, binds public keys and revokes certificates of all the stakeholders in the Mobile Learning framework. It issues X.509 version 3 and Short Lived Certificates (SLC) for all the stakeholders in the framework. It also acts as a Trusted Service Manager (TSM) which establishes an important link among Regulator, MNO and the Central Government. Department of Higher Education acts as a Regulator for all the universities in the country it frames and implements the policies for mobile learning framework from time to time. Regulator submits reports to the Central Government Time Stamping Authority (TSA).

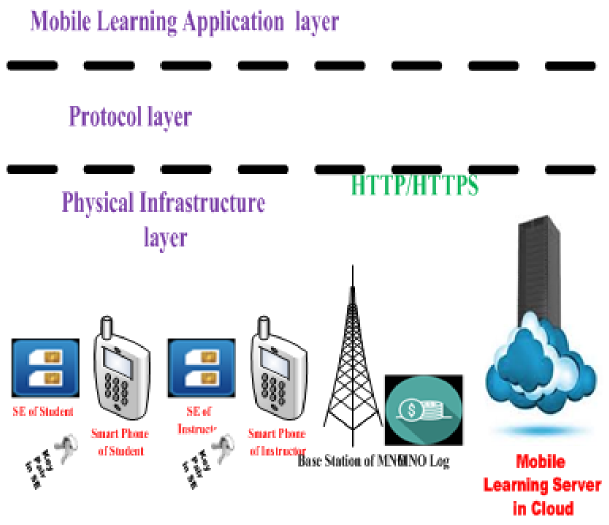

Fig. 1. Communication module of SMLF.

B. Proposed Communication Module

Student, Instructor and University are the three stakeholders involved in a normal mobile learning environment. Both Student and Instructor have a smart mobile phone with a Secure Element (SE) which connects with the cloud Over The Air (OTA) provided by MNO using wireless networks. Our proposed model is designed for the application layer so it focuses on the security of the business application layer in the three layer network model for mobile learning so we do not make any change in the protocol layer and physical infrastructure layer. Fig. 1 depicts the communication module of SMLF.

C. Proposed Procedure for Personalization

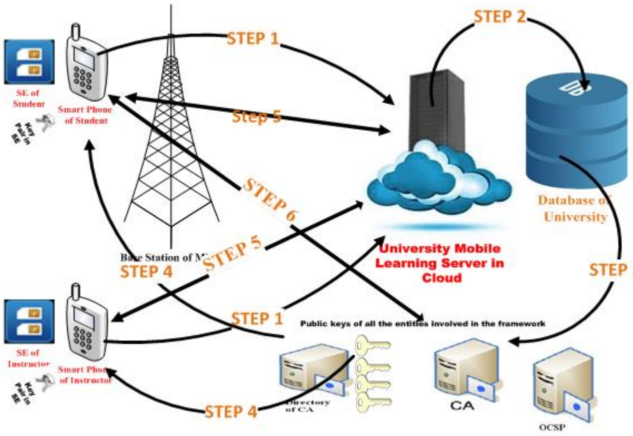

Fig. 2. Procedure for personalization of SMLF.

In this section we propose a procedure for personalization of SMLF, Fig. 2 depicts the procedure for personalization of SMLF.

1) Step 1: University acts as a Registration Authority (RA) for both Students and Instructors for issuing certificates. Certification Authority (CA) issues both X.509 and Short Lived Certificates (SLC) to all the stakeholders. CA issues Anonymous X.509 Certificates to all the students in order to ensure anonymity from instructors during the process of evaluating instructors (by the students). RA checks the certificate of the SEs of each and every student & instructor and maps the serial number and SE certificate to the user's national identity. All the stakeholders in the proposed mobile learning framework generate their credentials in the tamper resistant hardware such as Secure Element (Students & Instructors) and the Trusted Platform Module (TPM) of the University in the cloud.

2) Step 2: Trusted Platform Module (TPM) of the University in the cloud builds the database of the registered students and the instructors.

3) Step 3: All the students will be issued anonymous certificates in order to ensure anonymity of students during evaluating the instructor.

4) Step 4: Students and instructors will be asked to download mobile learning application which will be uploaded by the university in the cloud, before downloading the mobile learning application students and instructors will check the authenticity of the mobile learning application by downloading the certificate. If the checking is successful they accept the mobile learning application or report it to the university.

5) Step 5: Students and instructors will check the certificate of TPM of the university which is in the cloud. If the checks are successful they can start using Mobile learning application.

a) Students and instructors validates platform certificate of TPM of the university which is in the cloud using Certificate Validation Procedure given in (D.R. Stinson 2006) [7].

b) Validation of Students and instructors certificates is done by OCSP using Algorithm 1. $S \,\&\, I \rightarrow OCSP: U_{mla}$

c) /* C_{mla} is Mobile Learning Application Certificate */

d) Upon receiving positive response from OCSP, TPM installs Mobile Learning Application on the SE. /* this is the provisioning step */

e) University TPM personalizes Mobile Learning Application which is in the SE's of Students and instructors.

D. Proposed Secure Mobile Learning Protocol (SMLP)

$\boldsymbol{Step\ 1: Ins\ \rightarrow UMLS: \{MS1\}_{SYYKEY_{InsUMLS}}}$

$$\boldsymbol{MS1: \{UN, PW, DS(MS)_{Ins_{UMLS}},}$$

$$\boldsymbol{InsID, MS, SYYKEY_{InsULMS}\ , T_{Ins}, N_{Ins}\}}$$

Instructor sends $\boldsymbol{\{MS1\}_{SYYKEY_{InsUMLS}}}$ to University Mobile Learning Server containing files to be uploaded (i.e. MS) and digitally signing the message $\boldsymbol{DS(MS)_{Ins_{UMLS}}}$.

University Mobile Learning Server receives $\boldsymbol{\{MS1\}_{SYYKEY_{InsUMLS}}}$ from the Instructor and verifies the files to be uploaded (i.e. MS) and verifies the digital signature of the message $\boldsymbol{DS(MS)_{Ins_{UMLS}}}$, if the verification of digital signature is successful it uploads the (MS) message in the University Community Cloud.

$\boldsymbol{Step\ 2: S\ \rightarrow UMLS: \{MS2\ \}_{SYYKEY_{SUMLS}}}$

$\boldsymbol{MS2: \{UN, PW, SID, MS, SYYKEY_{SULMS}\ , T_S, N_S\}}$

Student gets authenticated by the UMLS and is allowed to download the files uploaded by the instructor.

IV. Formal Verification of srpf Protocol using BAN Logic

A security protocol is a communication protocol which exchanges encrypted messages by using cryptographic mechanisms [4] (Muhammad et al., 2006). Popular and carefully designed protocols were found out to have security breaches (Muhammad et al., 2006) [4]. We have analyzed the protocol using BAN logic [5] ((Abadi, M. et al. 1993) & [6] (Burrows,M. et al. 1990)).

A. Assumptions for the Analysis and Verification of the Proposed Protocol

1) Assumptions about keys and secrets:

'S' is a set of stakeholders containing {Ins, UMLS and S}. These assumptions gives a brief overview of public and private keys possessed by all the stakeholders. CA certifies all the certificates and knows all the public keys of the stakeholders (**AS1, AS2)**.

AS1. CA **believes** $(\forall S \in \{\text{Ins, UMLS and S}\} \overset{K_s}{\underset{}{\mapsto}} S)$ Certification Authority CA believes that all the stakeholders have their own public keys to communicate.

AS2. $S \in \{\text{Ins, UMLS and S}\}$ S believes $\overset{K_{ca}}{\mapsto} CA)$. All the stakeholders in the framework knows the public key and certificate of the certification authority CA.

2) Assumptions about freshness:

Assumption **AS3** specifies freshness of quantities. For instance, if the Instructor Ins sees quantity ($\boldsymbol{N_{Ins}}$) in a message then the Instructor Ins can conclude that it is a replay message.

AS3. Ins believes freshness ($\boldsymbol{N_{Ins}}$, S believes freshness ($\boldsymbol{N_s}$).

Every stakeholder believes nonce generated by him/her is fresh

Assumption **AS4** is about validity time of certificates and timestamps which ensures timeliness.

AS4. TS_x & TS_y are the timestamps generated by the stakeholders X and Y ({Ins, UMLS, S and CA}) which ensures **timeliness** of the messages exchanged.

3) Assumptions about trust:

These assumptions gives a brief overview of trust level on each stakeholder.

AS5. $(\forall S, Q \in \{\text{Ins}, \text{UMLS}, S \text{ and CA}\}$, S **believes** CA **controls** $\overset{K_{ca}}{\mapsto Q}$. Every stakeholder trusts the Certification Authority CA.

AS6. $\forall$ belief X, CA **believes** (W **controls** (P **believes** X)). The Certification Authority CA trusts the Student S that UICC or Secure Element (SE) (W) to relay Instructor Ins's beliefs.

B. Verification of our Proposed Protocol using BAN logic

$$\boldsymbol{Step\ 1: Ins\ \rightarrow UMLS: \{MS1\}_{SYYKEY_{InsUMLS}}}$$

$$\boldsymbol{MS1: \{UN, PW, DS(MS)_{Ins_{UMLS}},}$$

$$\boldsymbol{InsID, MS, SYYKEY_{InsULMS}\ , T_{Ins}, N_{Ins}\}}$$

UMLS decrypts the received $\{\boldsymbol{MS1}\}_{\boldsymbol{SYYKEY_{InsUMLS}}}$ from the assumptions AS1, AS2, AS5, AS6 & AS7.

UMLS believes $\{\boldsymbol{MS1}\}_{\boldsymbol{SYYKEY_{InsUMLS}}}$ statement (1)

UMLS verifies the public key of Ins (**AS7**) received from Ins which mainly includes [7] (D.R. Stinson 2006):

If the verification of certificate is successful then:

UMLS believes Ins said $\{\boldsymbol{MS1}\}_{\boldsymbol{SYYKEY_{InsUMLS}}}$statement (2)

UMLS believes **fresh** T_{Ins} from **AS3** statement (3)

UMLS **believes fresh** N_{Ins} from **AS4** statement (4)

So from the statements 1 to 4

UMLS **believes** $\{\boldsymbol{MS1}\}_{\boldsymbol{SYYKEY_{InsUMLS}}}$

$$\boldsymbol{Step\ 2: S\ \rightarrow UMLS: \{MS2\ \}_{SYYKEY_{SUMLS}}}$$

$$\boldsymbol{MS2: \{UN, PW, SID, MS, SYYKEY_{SULMS}\ , T_S, N_S\}}$$

UMLS decrypts the received $\{\boldsymbol{MS2}\}_{\boldsymbol{SYYKEY_{SUMLS}}}$ from the assumptions AS1, AS2, AS5, AS6 & AS7 UMLS **believes** $\{\boldsymbol{MS2}\}_{\boldsymbol{SYYKEY_{SUMLS}}}$ statement (5)

UMLS verifies the public key of Ins (**AS7**) received from Ins which mainly includes [8] (D.R. Stinson 2006):

If the verification of certificate is successful then

UMLS believes S said $\{\boldsymbol{MS2}\}_{\boldsymbol{SYYKEY_{SUMLS}}}$ statement (6)

UMLS believes **fresh** T_S from **AS3** statement (7)

UMLS **believes fresh** T_S from **AS4** statement (8)

So from the statements 5 to 8:

UMLS believes $\{\boldsymbol{MS2}\}_{\boldsymbol{SYYKEY_{SUMLS}}}$

V. Security Analysis

a) End to End Security: Proposed SMLF ensures End to End Security, i.e. SMLF ensures authentication, integrity, confidentiality and non-repudiation properties.

b) Key pair generation and storage at the User side in secure element: UICC is used at student which is a secure element. UICC is used for generating and storing student's credentials**.**

c) Identity protection (Anonymity) of Student from Instructor: Student enrolls for anonymous identity with CA and University, both CA and University know the original identity of student. So the instructor will not be able to know the real identity of student.

d) Withstands well known attacks: Timestamps and nonce are included in the messages exchanged thereby avoiding replay attacks in our protocol. An intruder (In) cannot impersonate as student to CA and University because intruder (In) is not in possession of Student's private key, so impersonation attack is not possible in our protocol. Intruder (In) is not in possession of receiver's private key so man in the middle attack is not possible in our protocol.

VI. Comparative Analysis of the Proposed Solution with the Existing Solutions

In this section we present a comparative analysis of SMLF with related works. Table 1 depicts the comparative analysis of SMLF with related works.

TABLE I. Comparative Analysis of SMLF with Related Work

	NAAP [2]	**KAAP [3]**	**AUTHMAC_DH [1]**	**SMLF (Proposed)**
Message Privacy	No	No	No	Yes
Message Integrity	No	No	No	Yes
Non-Repudiation	No	No	No	Yes
Authentication	No	No	No	Yes
Message Privacy	No	No	No	Yes
Anonymity	No	No	No	Yes
Unauthorized access to the stakeholder's credentials and private resource	Yes	Yes	Yes	No
Proposed protocol is formally verified	No	No	No	Yes
MITM Attack	No	No	No	Yes
Replay Attack	No	No	No	Yes
Impersonation Attack	No	No	No	Yes

VII. Conclusions and Future Work

This paper proposes a Secure Mobile Learning Framework (SMLF) based on TPM in the cloud. SMLF ensures end to end security using Communication Module (CM), SMLF proposes a procedure for personalizing mobile learning applications of the student and instructors. We also propose a secure mobile learning protocol in SMLF framework. Proposed SMLF ensures mutual authentication of all the stakeholders, privacy of the message, integrity of the message, and anonymity of the student from the instructor and non-repudiation and is free from known attacks. Our proposed SMLF framework is successfully verified using BAN logic. Our future work is to verify the proposed mobile learning protocol using advanced formal tools (i.e. in simulation environment) such as AVISPA and Scyther tools in order to verify that it can withstand all the known attacks.

References

[1] Alsan, H. K. "AUTHMAC_DH: A New Protocol for Authentication and Key Distribution," in 7th IFIP conference on Communications and Multimedia Security, Italy, 2003, pp.14–26, 2003

[2] Lirong He, Lisha He, Ian Rogers, "New Security Protocol For M-Learning," [Online], Available: https://www.researchgate.net/publication/228742605_New_security_protocol_for_m-learning%27

[3] Yeh, H.-T., Sun, H.-M. (2004), "Password-based User Authentication and Key Distribution Protocols for Client server Applications", Journal of Systems and Software, 72, 97-103, 2004.

[4] Muhammad, S., Furqan, Z. and Guha, R.K, "Understanding the intruder through attacks on cryptographic protocols", in Conf. 44th ACM Southeast Conference, Florida,USA, 2006, pp.667–672, 2006.

[5] Abadi, M., Burrows, M., Kaufman, C. and Lampson, B. (1993), "Authentication and delegation with smart-cards", Science of Computer Programming, 21(2), 93–113, 1993.

[6] Burrows, M., Abadi, M. and Needham, R. (1990), "A logic of authentication", ACM Transactions on Computer Systems, 8(1), pp.18–36, 1990.

[7] D.R. Stinson (2006), "Cryptography-Theory and Practice", 3rd edition, Chapman & Hall/CRC.

[8] Gouveia, L. (1999, "On education, learning and training: Bring windows where just walls exist", UFP Journal, 3 (May), 223-227, 1999.