1st International Conference New Perspective in
Electrical & Computer Engineering

A New Secure e-Health Structure Based On Mobile Trusted Computing

MohammadAli Doostari [1*], Salimeh Yasari Zare [2]
[1] Department of Computer, University of Shahed, Tehran, Islamic Republic of Iran
[2] Master of IT Engineering, Tehran Regional Electricity Company (TREC)

ABSTRACT

In this research work, a new structure is presented for eHealth in a country. In this structure, patient's Personal Health Records (PHR) is fully stored on the 3 national, provincial, and patient's mobile phone levels. Secure communication between these three levels is provided with safe communications technologies such as NFC, VPN, and SSL/TLS. Security of the 3rd level of the country's structure (patient's mobile phone level), is ensured through integration of the 2 ideas of TPM Mobile and TEE, which together, provide mobile Trusted Computing (TC) objectives. Thus, patient's smart phone can be used as an alternative to health smart card for a secure storage of the entire contents of PHR and patient's identification information and on the basis of which secure communication protocols are designed for this structure. Then, the security of the proposed protocols is analyzed with a protocol analyzer software named Scyther.

Keywords: Mobile security, mobile Health (m-health), TEE, TPM Mobile, eHealth secure protocols

1. INTRODUCTION

Use of digital technology in the field of health, allows all patients to benefit the services of medical centers, anywhere in their home country or abroad, by offering their online personal health records. This means that health records of an individual could be virtually available anywhere only by having a smart phone [1]. Therefore, there is a need to design and implement a proper mobile structure in the whole country for safeguarding patient's privacy and security in collecting the scattered information and storing it in a single medical record for each patient (which is available everywhere).

The purpose of this study is to eliminate the need for a physical smart card for authentication, keeping only part of patient's health record (proposed in most similar studies), and external memory to store patient's health records, and replace them with a smart phone (a mobile device that is with the patient everywhere). However, the problem with mobile operating systems is that they cannot provide adequate level of protection for the stored software or certificates. Even the advanced mobile phone operating systems suffer from inefficiency in protecting against unauthorized manipulation of programs (or even the operating systems themselves) [2]. Thus, it is necessary to use the technologies hidden in the processors of the new smart phones that provide reliability to keep patient's identifiable information, keys, certificates, and PHR. To this purpose, in this research, Trusted Execution Environment (TEE) [3] and Mobile Trusted Platform Module (TPM Mobile) [4, 5] have been employed together and a solution has been proposed to achieve this goal. Then, with regard to the proposed solution, a country-wide

* doostari@shahed.ac.ir

eHealth structure is designed to securely access patient's Personal Health Records (PHR) at the 3 levels: national, provincial, and patient's smart phone level. Also, all communications in this structure are considered, from the country level to the patient's smart phone level and secure protocols are proposed for the communications. To design this structure and present its communication protocols, other relevant research works have been studied and their shortcomings have been resolved using secure communication technologies and proposed mobile solutions.

The present research is constituted of 5 parts. In Section 2, a solution will be proposed to enhance mobile security to protect M-PHR and simulate health smart cards on patient's cell phone. In section 3, the proposed electronic health structure along with their components and connections between them will be introduced. In Section 4, secure communication protocols will be discussed for different scenarios in the proposed structure. Finally, a conclusion will be presented for the current study in Section 5.

2. PROPOSED SOLUTION TO ENHANCE PATIENT MOBILE SECURITY

In this study, a solution has been proposed for Replacing health smart cards and protect patient's confidential mobile software (M-PHR) using the architectural pattern of Global Platform Trusted Execution Environment (GP-TEE) and firmware Trusted Platform Module (TPM) for mobile that means Mobile TPM, that presented by Trusted Computing Group (TCG)). This solution is fully described in details in our other research works in [6].

2.1. The use of TEE and TPM for the proposed solution

In this research work, according to TEE technologies under development (presented by GP) and TPM 2.0 Mobile [4] (presented by TCG), a solution has been proposed for the implementation of health smart cards for patient's smart phone. In addition, the proposed solution is able to securely keep patient's Personal eHealth Records (PHR) and execute his or her M-PHR software.

As the existing solutions to TEE implementation alone are not able to meet all the objectives of Mobile Trusted computing [7] and other existing technologies have not provided perfect TEE solutions and none of them have been able to fully comply with GP-TEE specifications [8], we recommend that a firmware TPM associated with them be used to achieve these objectives. In our proposed solution, we employed firmware TPMs (as TAs in the TEE) to meet 3 objectives:

1. Cryptographic operations (such as key generation, encryption, digital signatures, etc.)
2. Execution of secure and measured boots in the system
3. Binding of encryption keys to the system loading time integrity

The proposed solution to achieve the above-mentioned cases is shown in the architecture of Figure 1.

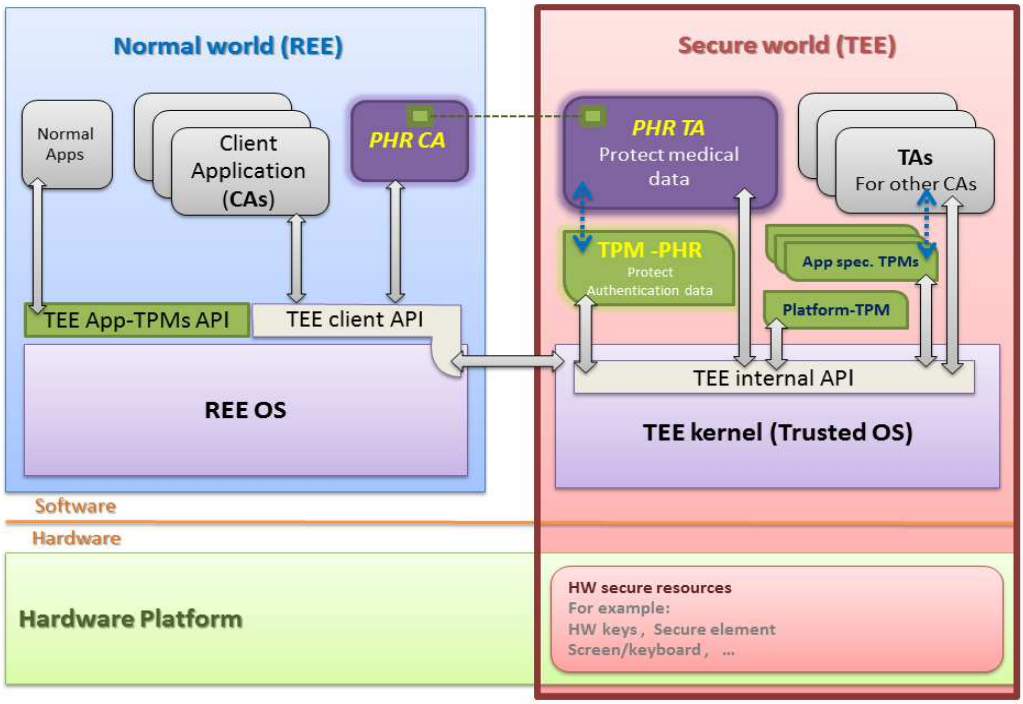

Fig.1. Use of TEE and TPM in the proposed solution

In Figure 1, To meet the objectives behind this study, have been demonstrated that the new TPM components have been added to the basic GP-TEE architecture by using the proposed solutions of "TPM 2.0 Mobile specifications" [4] and [9]. Also, the positions of the two PHR-CA and PHR-TA parts of M-PHR software are shown in this figure.

2.2. The components added to GP-TEE reference architecture

M-PHR Software was developed by a developer (trusted third party) in two PHR-CA and PHR-TA parts, which should have been established in REE and TEE, respectively. It actually contained Patients' Personal Information and their EHR that should have been stored in their mobile device while keeping their confidentiality and integrity. Thus, it was necessary that this information be stored in encrypted form in the memory of the mobile device. The user's public key certificate and encryption keys are protected by TPM-PHR and the encrypted data could be decrypted and recovered with these keys, only if M-PHR system and software was intact and not manipulated (by the patient or an adversary, (the binding concept of TPM). Therefore, it was necessary that the following components be added to GP-TEE reference architecture to meet the objectives of this study

- The different types of TPM present in TEE: A TEE can be simultaneously host several TPMs. This means that each CA may have its own TPM-TA in TEE, as most mobile apps don't need a TA in TEE, they may still need to use some TPM capabilities (such as secure storage, remote attestation, etc.). In such circumstances, a specific TPM for a platform should be created (to provide some operating system services, such as secure boot) within TEE [9]. Figure 1 shows "App spec. TPM" component,

which is a set of TPMs for any software, and "Platform-TPM" components that is a specific TPM for the platform. Also, TPM-PHR component is a special TPM for M-PHR software, which is only accessible by PHR-TA part of the mentioned software. Measured boot operation is carried out by Platform-TPM to ensure the integrity of the system that hosts M-PHR software.

- Normal App: It is software that does not require a TA in TEE, but it may have a special TPM-TA in TEE.

- PHR-CA: It is part of Client App (CA) of the dichotomous M-PHR software in our proposed solution. To run securely, this part of the software needs the security services provided by a TA within TEE.

- PHR-TA: It is part of the Trusted App (TA) of the dichotomous M-PHR software in our proposed solution. Together with its own TPM, this part provides the security services needed for PHR-CA running in REE.

- TEE App-TPMs API: It is a communication interface between "Normal Apps" and their specific "App spec. TPM" in the secure world. In fact, this API displays part of TEE Functional API.

2.3.TEE and TPM: usage on the mobile level of the proposed structure

Based on descriptions given in this section, the following cases of the proposed structure (Figure 2) have been made possible by using patient's smart phone TEE with regard to the objectives of this research work:

1. Secure storage has been provided for storing patient's PHR, passwords, certificates, and keys. For this purpose, patients' PHR is placed in their smart phone's internal memory, which is accessible only through PHR-TA when the device processor is in a TEE mode. PHR is encrypted by a symmetric key that is generated and stored within TPM-PHR and never exits it (the binding key) and placed in the internal memory. Therefore, while protecting the confidentiality of the sensitive information, they can be decoded and used only if Platform-TPM has loaded the system in a secure mode and TPM-PHR has ensured that the integrity of the software has been preserved and not undergone an unauthorized manipulation.

2. The ability to run secure PHR-TA in an environment isolated from PHR-CA has been provided by the innate capability of isolation that TEE creates based on hardware).

3. Using TPM-PHR, a health smart card has been devised on the mobile platform. For this purpose, patient's identifiable information, public key certificate and patient's fingerprint must be stored after digital signature by P-RA, along with patient's P-PHR code, in a secure storage location accessible for TPM-PHR. Also, the hash of these information is saved in one of the Platform Configuration Registers (PCRs) of the mentioned TPM-PHR to prevent manipulation, so that the integrity of the values can be constantly measured and verified when the device is loading. Therefore, the required information can be sent to the smart card reader by NFC from within TPM-PHR whenever identification and authentication of the patient is required by his or her cell phone, as a replacement for health smart card.

3. INTRODUCTION OF THE PROPOSED E-HEALTH STRUCTURE

In this section, the proposed e-health structure, as well as its components and connections between them has been described in details. A visual outline of the proposed eHealth structure is shown in Figure 2. The structure is composed of 3 PHR levels, the original version of which has been stored in the distributed database of each province and its backup exists in the country's centralized database. Also, PHR full version of each patient has been installed on his or her mobile phone. In this architecture, our main focus is on the patient's PHR mobile level that should be protected from both unauthorized access and updatable by PHR provincial level. In addition, patient's cell phone must be able to play the role of a

health smart card in the identification and authentication processes in this architecture. Therefore, to achieve these two goals, a plan based on TEE and TPM Mobile architecture has been presented as explained in section 3.

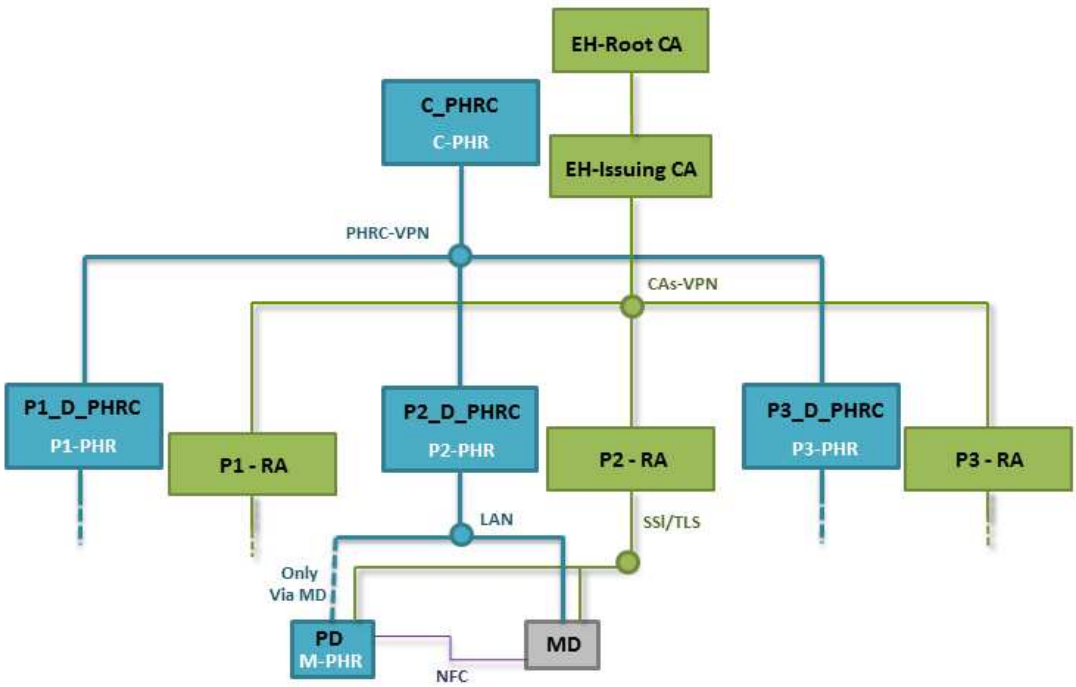

Fig. 2. Outline of the structure of the proposed e-health systems

3.1. Components of the proposed structure

The structure shown in Figure 2 is made up of 3 sub-sets of major components and a number of minor components. The 3 major components include:

1) Patient's Personal Health Record (PHR): In the proposed architecture, the patient's PHR is stored on 3 levels with these titles: C-PHR, P-PHR, and M-PHR.

2) Patient's Personal Health Record Maintenance Centers (PHRCs): In the proposed architecture, patient's personal health records are kept in 2 centers (databases): C-PHRC and P_D_PHRC.

3) Centers for Issuing Certificate Authority (CA): In the proposed system, each patient and authorized medico should have his or her own public key certificate. In the proposed structure, it has been assumed that the root of Public Key Infrastructure lies in EH-ROOT CA. Therefore, after referring to first medical center member of this structure, the patient will registers in the system via the P-RA agent present at the site and receives his or her public key certificate signed by EH- ISSUING CA as the country certificate authority.

In the proposed structure, PKI which is responsible for issuing and preserving public key certificates and other identifying information of the members of the system operates at 3 levels:

Electronic Health-Root Certificate Authority (EH-ROOT CA), Electronic Health-Issuing Certificate Authority (EH- ISSUING CA), and Province Registration Authority (P-RA).

3.2. The relationships between the proposed structure components

At the various levels of the proposed structure, the links between the components have been established in a number of ways that the types of relations have been chosen with regard to security required in the structure. These methods include:

1. Internet communication through SSL/TLS protocol: The patient and the authorized medico communicate with P-RA via the Internet network, the security of which will be provided through SSL/TLS protocol.

2. LAN: The medicos of a medical center can locally communicate with P_D_PHRC province distributed database. In other words, access to patients' P-PHRs is done only via the local networks of the member medical centers of this structure and it is not possible via the Internet. Also, no one except the authorized medicos is able to access this database. Therefore, synchronization of patient's M-PHR with P-PHR available on this database will be only permitted through an authorized medico's device and only at an authorized medical center.

3. Near Field Communication (NFC): NFC communication interface works in 3 modes between the components of "patient's smart phone" and "authorized medico device" of the proposed structure:

- NFC card emulation mode
- NFC reader/writer mode for the smart card
- NFC peer-to-peer mode

4. VPN**:** A Virtual Private Network (VPN) has been used for communications between the components in 3 parts of the proposed structure:

- The communications between all the servers of the provincial distributed database (the database servers at different medical centers that keep patients' P-PHRs)
- A VPN network called PHRC-VPN has been created between PHRCs in this structure.
- In the tree structure of CAs that creates Public Key Infrastructure (PKI) in this structure, that takes place through a VPN network named CAs-VPN.

4. SECURE COMMUNICATION PROTOCOLS FOR DIFFERENT SCENARIOS OF THE PROPOSED STRUCTURE

In this section, the communication protocols plausible for multiple scenarios in the proposed eHealth structure (Figure 2) have been explained and presented by taking into account the level of security required for each scenario. These protocols include:

- ✓ Patient's enrollment protocol in the proposed structure
- ✓ Medicos' registration protocol in the proposed structure
- ✓ Patient's admittance and visiting protocol by the authorized medicos in the intra-provincial medical centers
- ✓ Patient's admittance and visiting protocol at the medical centers of other provinces
- ✓ Patient's visiting protocol in an emergency condition (conscious patients out of authorized medical centers)
- ✓ Patient's visiting protocol in an emergency condition (unconscious patients)
- ✓ Timing-sync protocol of M-PHR with P-PHR information

The internal structure of patient's smart phone has been described for provisioning the purposes of the mentioned protocols in section 3.

4.1. Symbols

The symbols used in the communication protocols of the proposed structure are shown in Table 1.

Table 1: *Symbols and symptoms*

Symbols	Full Name
P	Patient
HP	Healthcare provider *
P-RA	Province- Registration Authority (in a Healthcare center)
RA	Registration Authority (a P-RA agent resident in a Healthcare center)
PD	patient device
M	Medico
MD	Medic device
Sk	Shared key
P_{Id}	Patient Identification
f	Fingerprint (for biometric authentication)
PD_{Id}	Patient Device identification
pr-key	Private key
pu-key	Public key
P_{IC}	Patient insurance code
$P_{\_P\text{-}PHR\ code}$	Patient P-PHR code (in P_D_PHRC)
PK_{cert}	Public key certification
M_{Mc}	Medic medical code
OTP	One Time password
TS	Time stamp
Is.CA	EH- Issuing CA (for a country)
N	Nonce
AC	Access Control

* Authorized medical center (HP): It is the center registered in this structure) and its patients' database is part of P_D_PHRC distributed database.

4.2. Patient's enrollment protocol in the proposed structure

Patient's enrollment phase protocol of the proposed structure is shown in Table 2. For the implementation of this Protocol, the patient is required to install M-PHR software on his or her smart phone beforehand. The patient can only install the insecure part of the software (i.e., PHR-CA) on his or her device, while provisioning the secure part of the software (i.e., PHR-TA) will be handled by P-RA and during the implementation of this scenario.

Table 2: Patient's enrollment protocol

Patient with m-PHR => A HP-RA => B P-RA => C Insurance DB => D P1_D_PHRC => E			
Step 1	A → B	Registration request with P_{Id}+ f + PD_{Id}	Physical + NFC
Step 2	B → C	HP-RA $_{pr\text{-}key}$ (P_{Id} + f + PD_{Id})	CAs-VPN
Step 3	C → D	P-RA $_{pr\text{-}key}$ (P_{IC})	Internet
	D → C	P-RA $_{pu\text{-}key}$ [Verify/Not verify (P_{IC})]	Internet
Step 4	C → B	P-RA $_{pr\text{-}key}$ (P-Pk $_{pu\text{-}key}$)	CAs-VPN
Step 5	B → A	P-RA $_{pu\text{-}key}$	NFC
Step 6	A → C	P-RA $_{pu\text{-}key}$[PD $_{pr\text{-}key}$ (PK_{cert} request) + PD $_{pu\text{-}key}$]	Internet
	C → A	Provision PHR-TA	Internet
Step 7	C ← → A	SK= Diffie-Hellman key exchange	Internet
Step 8	C → A	Sk [(P-Pk $_{cert}$ + P-RA $_{pr\text{-}key}$ (f + P_{Id})]	Internet
Step 9	B → E	BE (P_{Id} + P-Pk $_{pu\text{-}key}$ + Request for Create P-PHR for P)	LAN
	E → B	BE (P_P-PHR code)	LAN
Step 10	B → A	RU $_{pr\text{-}key}$ (P_P-PHR code)	NFC
	B → E	RU $_{pr\text{-}key}$ (P_P-PHR code)	LAN

Security Analysis

Steps 1, 5, and the second part of step 10 are physically conducted, while the physical documents are checked. Also, since at the steps 2, 4, and the first part of step 10, the data are exchanged while encrypted with the public/private key on CAs-VPN virtual private network platform, their securities are provisioned and they are safe from most attacks . In Step 3, message integrity (patient's insurance code) is guaranteed by being signed by P-RA private key. Also, the message of verified/not verified) of the insurance code is preserved from access and manipulation by attackers and its confidentiality is maintained as up to the destination because it has been encrypted with P-RA public key.

However, since the transfer of information at steps 6 and 8 is carried out through the insecure Internet bed, the mentioned processes have been implemented and evaluated using Spdl language in Scyther protocol analyzer software. The results of this implementation are showed in figure 3 and figure 4. The security analyses of these 2 steps have been made within Dolev-Yao model framework [11]. Dolev-Yao is a formal model to prove the properties of interactive cryptographic protocols. In Dolev-Yao model, it is assumed that the network is entirely under the control of adversaries which means that they can see the contents of messages, remove sent messages, add their own messages, or change the routes of their transfers. Therefore, these 3 properties are known to make Dolev-Yao model: 1) Cryptography is perfect, 2) Messages are abstract terms and 3) The network is under full control of the intruder.

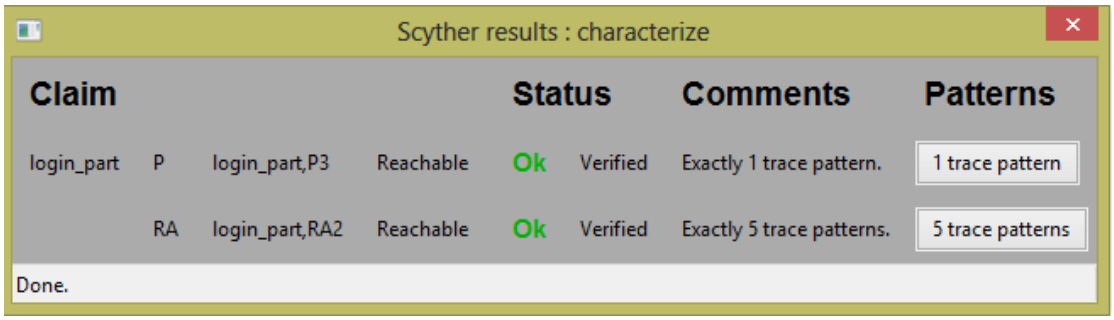

Fig.3. Result of execution steps 6 and 8 of the Patient registration Protocol with six run patterns

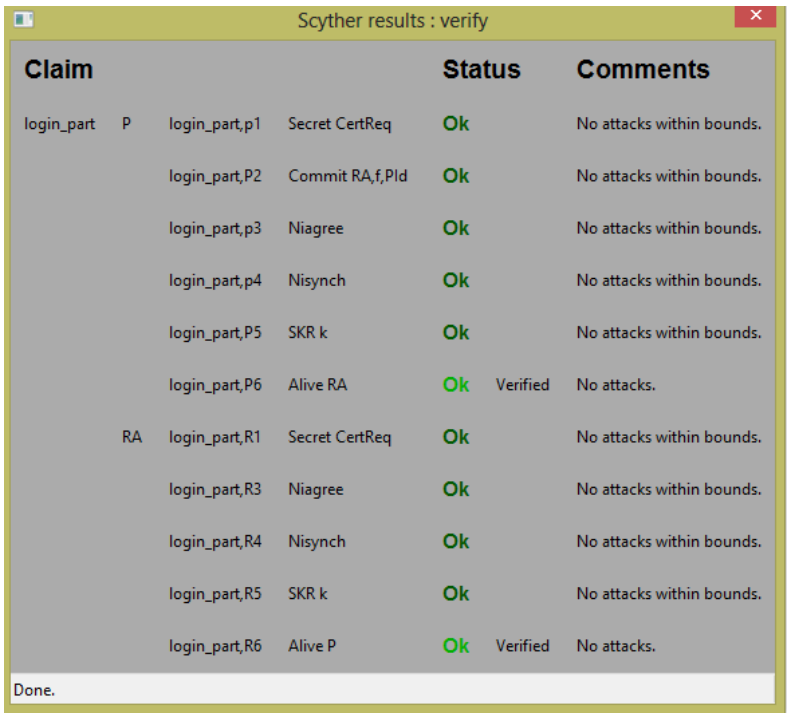

Fig.4. Result of security analysis of steps 6 and 8, in a Bound

Also, in step 9, data transfer is done through the internal LAN of each medical center (in an encrypted form with a pre-shared key between HP-RA and provincial distributed database). At this stage, the confidentiality of the exchanged information will be preserved because the encrypted data with BE symmetric key, is only accessible by the two communicating parties.

4.3. Medicos' enrollment protocol in the proposed structure

The registration process of medicos is similar to that of the patients in this system with the difference that a medico is required to have a medical code instead of an insurance code. Also, a medico's fingerprint will be required to log in to the hospital internal network and connection to P_D_PHRC through an authorized device.

After registration, the medico will be able to see and record the authorized information in the patients' PHRs through their authorized device using PHR-browser software (with regard to a pre-determined access control by the patient). Also, if the authorized medico is an emergency doctor, this device can play the role of his or her smart card to be identified by patients outside of healthcare centers.

4.4. Patient's admission and visiting protocol by an authorized medico within intra-provincial medical centers

Patient's admission and visiting protocol by an authorized medico within intra-provincial medical centers is shown in Table 3. In this protocol, a patient who has attempted to enroll in one of the centers of his or her province in this system refers to an authorized medical center for his or her appointment with the doctor

Table 3: Patient's admission and visiting protocol by an authorized medico within intra-provincial medical centers

Patient with m-PHR => A Medico with PHR-browser => B P1_D_PHRC => C			
Step 1	A → B	send [f + P_{Id} + P_P-PHR code]	NFC
Step 2	B → C	BC (Request (P_P-PHR code))	LAN
Step 3	C → C	Create (OTP + TS)	-
	C → B	OTP $(P\_P\text{-}PHR)^{TS}$, $M_{pu\text{-}key}$ (TS + OTP)	LAN
Step 4	B → C	OTP [$M_{pr\text{-}key}$ (H(new info)) + new info]	LAN
Step 5	C → C	Update P_P-PHR with new info.	-

4.5. Patient's admittance and visiting protocol within the medical centers of other provinces

A patient residing for example in Iranian central city of Yazd can refers to a hospital in Tehran, while he/she has previously enrolled in the Iranian national mobile health system and provisioned Y-PHR in a hospital in Yazd and has a copy of it on his/ her smart phone. The structure in Figure 5 represents the scenario for Iran.

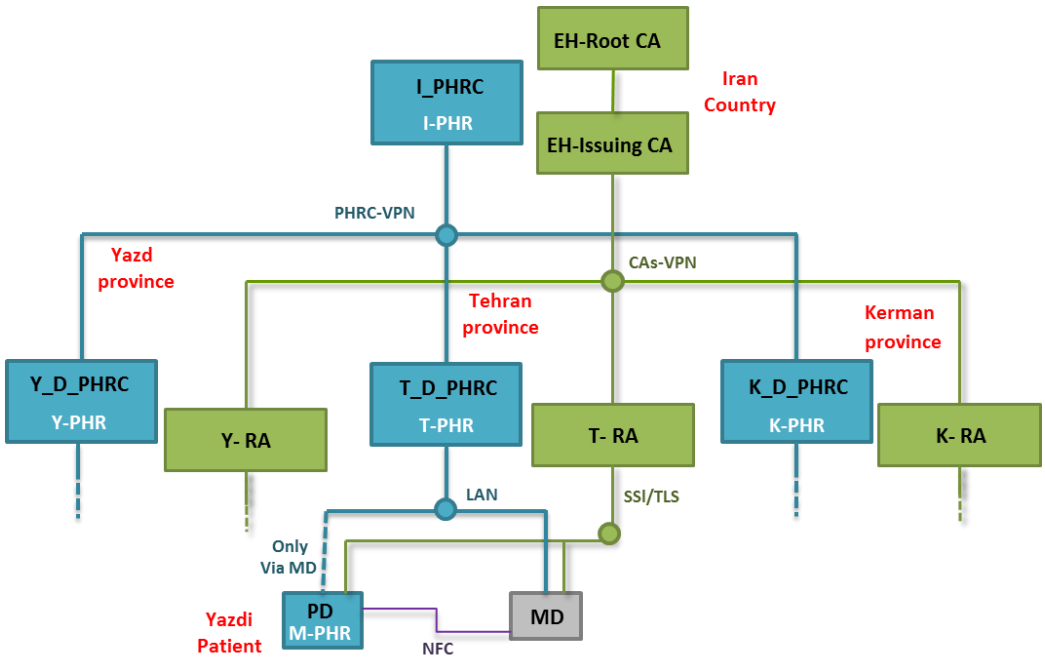

Fig.5. an instance of Figure 2 structure in Iran

Patient's admission and visiting protocol in the medical centers of other provinces is shown in Table 4. For example, a patient with Y-PHR in Yazd City has now referred to a medical center in Tehran province for admittance and treatment.

Table 4: Patient's admission and visiting protocol within the medical centers of other provinces

Patient with m-PHR => A Medico with PHR-browser => B T_D_PHRC => C I_PHRC => D			
Step 1	A → B	send [f + P_{Id} + P_Y-PHR code]	NFC
Step 2	B → C	BC (Request for (P_Y-PHR code))	LAN
Step 3	C → D	(Request (P_{Id} + P_I-PHR code)) TI	PHRC-VPN
Step 4	D → C	TI [$(Y\_PHR)_C$= a copy of I-PHR]	PHRC-VPN
Step 5	C → C	Create (OTP + TS)	-
	C → B	OTP $(P\_(Y\text{-}PHR)_C)^{TS}$, $M_{pu\text{-}key}$ (TS + OTP)	LAN
Step 6	B → C	OTP [$M_{pr\text{-}key}$ (H(new info)) + new info]	LAN
Step 7	C → C	Update $P\_(Y\text{-}PHR)_C$	-
Step 8	C → D	TI $(Y\_PHR)_C$ for update I-PHR	PHRC-VPN
	C → C	Delete $(Y\text{-}PHR)_C$	-

4.6. Patient's visiting protocol in emergency conditions (conscious patients out of authorized medical centers)

Since the Possibility of access to P_D_PHRC database does not exist outside of authorized medical centers through the Internet, in such circumstances, it is imperative that the authorized medico and patient's devices have direct contacts via NFC in a reader/writer mode and authenticate each other.

Table 5: Patient's visiting protocol in emergency conditions

Patient with m-PHR => A Medico with PHR-browser => B			
Step 1	A → B	send [f + signed by P-RA (P_{IC} + f + P_{Id})]	NFC
Step 2	B → A	send [signed by P-RA (M_{Id} + $M_{pu\text{-}key}$) + $M_{pr\text{-}key}$ (N)]	NFC
Step 3	B → A	send (M-PHR + AC)	NFC
Step 4	A → B	$M_{pr\text{-}key}$ (M-PHR new info.)	NFC

4.7. Patient's visiting protocol in emergency conditions (unconscious patient)

In such circumstances, by getting an unconscious patient's fingerprint through an authorized medico's device and sending it to P_D_PHRC (in the case that the patient is present in a health center), the authorized medico is able to recover parts of the patient's P-PHR required in emergency situations (a default access permission.

In such circumstances, the new information will be recorded only in P-PHR with the emergency physician's signature, and later would be recorded in the patient's PHR and then synchronization between M-PHR and P-PHR will take place by the patient himself/ herself in an authorized medical center.

4.8. Sync protocol of M-PHR and P-PHR information

Since an access to P_D_PHRC distributed database outside the member medical centers of this structure is not possible through the Internet, synchronization between M-PHR and P-PHR will be plausible only at the time of the patient's presence at a member health center through an authorized medico's device connected to the internal network of the relevant medical center. Also, given that the database servers of all the medical centers work in a distributed way, the sync can be done through any of the centers (and not necessarily by the same center where the patient has been enrolled and admitted).

1. Upon completion of the meeting with the medico and addition of the new information to the patient's P-PHR by the medico with his/her digital signature, the medico will send the new modifications to M-PHR on the patient's device using NFC of his or her own device.

2. However, to send the new modifications from M-PHR to P-PHR, an attestation should be done by P_D_PHRC to ensure that the changes occurred to M-PHR software are authorized and conducted by authorized people and the software has not undergone an unauthorized manipulation:

- In order to determine that the changes occurred to M-PHR are authorized, M-PHR software integrity should be certified by sending the software hash values placedwithin the PCRs of the patient's device TPM-TA [8].
- To determine the whether changes made in M-PHR has been conducted by an authorized personnel, the digital signature present on each modification must be verified (For example, by adding the new information with the emergency medico's signature at a place outside the member medical centers).

3. After this verification, the authorized changes and modifications made in the patient's M-PHR are sent to P_D_PHRC to be synchronized with P-PHR and in case of detection of unauthorized changes in the software, those changes will be erased and the software returns to its previous trusted mode.

5. CONCLUSION

In this research work, we have proposed use of a mobile phone as a secure alternative to eliminate the need for a smart card to store patients' identity information as well as some part of their health records or an external memory to store the patients' health records. However, the problem existing in mobile operating systems is that they cannot provide an adequate level of protection for the software or the stored certificates. Even the advanced mobile phone operating systems suffer from inefficiency in protecting against unauthorized manipulations of programs (or even the operating systems themselves). Therefore, it is necessary to use the technologies embedded to the processors of new smart phones that provide reliability, to keep patients identifying information, keys, certificates, and PHR. For this purpose, Trusted Execution Environment (TEE) and mobile Trusted Platform Module (TPM Mobile) were used to secure a mobile phone in this study. These two new technologies together provide the trusted computing goals that have been raised by TCG. Thus, by combining these two ideas, an innovative solution was proposed to be used in the mentioned electronic health structure. Then, with regard to the proposed solution, a country structure has presented for secure access to Personal Health Records (PHRs) of patients in 3 national, provincial, and patient levels. Also, all the communications in this structure was considered, from the country to the patient's smart phone level and secure protocols were presented for these communications. Finally, the security of the proposed protocols was analyzed by Scyther protocol analyzer software using SPDL language.

REFERENCES

[1] Yu, W.D. and A. Panova, "An architectural design framework for an Electronic Health Record system with hospice application", in *14th International Conference on e-Health Networking, Applications and Services (Healthcom), 2012 IEEE*..

[2] Dmitrienko, A., et al., "Securing the access to electronic health records on mobile phones", in *Biomedical Engineering Systems and Technologies*. 2011, Springer. p. 365-379.

[3] Global Platform, "The Trusted Execution Environment: Delivering Enhanced Security at a Lower Cost to the Mobile Market", Whitepaper, February, 2011.

[4] TCG Published, "TPM 2.0 Mobile Reference Architecture", *Family "2.0", Level 00 Revision 142*. 16 December 2014.

[5] TCG Published, "Mobile Trusted Module 2.0 Use Cases (Specification Version 1.0)", 4-March-2011.

[6] mohammad ali doostari, e.al., "A review of Trusted Computing new technologies and providing solutions for using these technologies in Electronic Health", in *3rd International Conference on Electrical ,Electronics and Computer Engineering (ICEEECET)*, Aug 2016, norway.

[7] Asokan, N., et al., "Mobile Trusted Computing", Proceedings of the IEEE, 2014. 102(8): p. 1189-1206.

[8] Arfaoui, G., et.al., "Trusted execution environments: a look under the hood". in *2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2014*.

[9] Ekberg, J.-E., et.al., "Trusted execution environments on mobile devices". in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. 2013. ACM.

[10] Isaac, J.T. and S. Zeadally, "Secure Mobile Payment Systems", *IT Professional*, 2014, 16(3), p. 36-43.

[11] Wikipedia. *Dolev–Yao model, Available: https://en.wikipedia.org/wiki/Dolev%E2%80%93Yao_model*. Available from: https://en.wikipedia.org/wiki/Dolev%E2%80%93Yao_model.