Smart Health 13 (2019) 100063

Contents lists available at ScienceDirect

Smart Health

journal homepage: www.elsevier.com/locate/smhl

Smart health record management with secure NFC-enabled mobile devices

Divyashikha Sethia [a,*], Daya Gupta [a], Huzur Saran [b]

[a] Department of Computer Science and Engineering, Delhi Technological University, India
[b] Department of Computer Science and Engineering, Indian Institute of Technology, Delhi, India

ARTICLE INFO

Article history:
Received 3 September 2017
Received in revised form
8 October 2018
Accepted 11 November 2018
Available online 22 November 2018

Keywords:
Portable health records
NFC
HL7
Secure Element
Mobility
Selective access

ABSTRACT

Patients with dispersed health records face the challenge of accessing readily available health history and mobility across different hospitals. It can hinder timely diagnosis and treatment, especially in the case of an emergency or for travellers. Cloud-based solutions have open challenges of interoperability and integration, higher challenges for security and privacy and may lack 24/7 support for the high availability of health history. Existing portable systems store limited health information for only a specific hospital and do not support mobility of patients across different hospitals.

In this paper, we propose a next-generation portable Smart Health Record Management system with secure Near Field Communication (NFC)-enabled mobile devices to retain the dispersed health records on an S-MAPLE (Secure Mobility-Assisted PortabLE) health folder. It provides secure yet easy access to up to date health history and assists patient mobility across hospitals. An NFC-based Host Card Emulation (HCE) mode maintains a software-based contactless mobile-based health wallet on the patient's mobile device. An authorized medical professional can access it directly and selectively with their mobile devices, over low energy wireless interfaces of NFC and Bluetooth. NFC provides secure proof-of-locality and ease of access. A tamper-resistant storage Secure Element (SE), end-to-end mutual authentication with attestation scheme, variant of the Ciphertext-policy Attribute-based encryption (CP-ABE) scheme and backup on a secure digital vault further secure the S-MAPLE health folder.

We present the system requirements, system architecture and security requirements with a brief overview of the security solutions for the proposed health system. The implementation and performance of the system prototype using mid-range Android-based mobile devices has acceptable results.

1. Introduction

For robust and efficient healthcare, a patient must have ready access to the complete health history. However, it is difficult to maintain it if a patient has to visit several hospitals with dispersed health records. Some hospitals may adopt paper-based health record management, and others may use a digitized Health Information System (HIS) for record management. There are open challenges of syntactic and semantic interoperability and integration of health records

* Corresponding author.
E-mail address: divyashikha@dtu.ac.in (D. Sethia).

https://doi.org/10.1016/j.smhl.2018.11.001
2352-6483/

between several HIS, due to the differences in health formats, policies and laws such as Health Insurance Portability and Accountability Act (HIPAA) in the US and the European regulations for healthcare data protection (The new, 2018).

People in emerging countries such as India face the challenges of dispersed health record management since they do not have proper healthcare policies and infrastructure for a centralised health system. They visit various hospitals for seeking specialised consultations in urban cities and also to take second opinions for a reliable diagnosis from hospitals with specialisations.

The challenges of dispersed health records is also an issue for the developed countries where global citizens may seek treatment from different hospitals. Such as the case of the citizens of the European countries, who relocate to different states and countries for work and tourism. Additionally, in an emergency, patients may land in a hospital which is not under their health policy, and hence the hospital cannot access their health records. Although the health record management systems in developed countries may be advanced and well established with patients registered to a specific hospital or insurance policy such as the NPfIT system in U.K (NHS, 2018) and Taiwan Electronic Medical Record Template (TMT) (Chen et al., 2010), they lack the syntactic and semantic interoperability of health records.

Hence the patients who visit several hospitals, face the burden of maintaining the dispersed health records such as medical prescriptions, lab tests and medications for complete health history, as well as financial records for payment of medical bills. In most cases, patients end up retaining paper-based health records which are less efficient than the Electronic Health Records (EHR)s (Fernandez-Aleman et al., 2013). They are also cumbersome to maintain especially in the case of chronic patients.

The advanced digitized HIS may provide access to detailed health information to patients on cloud-based systems or basic health information on a portable health device such as a smart card or a USB stick. However, most such systems are for a particular hospital or a nationwide system, and other health systems cannot access them. Some cloud-based solutions such as the Cloud Health Information Systems technology architecture (CHISTAR) scheme proposed by Bahga and Madisetti (2013) offer integration of dispersed health records. However, the issue of interoperability and integration has open challenges. Moreover, the cloud-based systems are not 24/7 available in the disconnected networks and remote regions and have higher risks for security and privacy (Abbas & Khan, 2014). Third-party cloud-based services may take away control of data from hospitals and patients, cause data accessibility for data mining applications with legal and privacy issues such as identity theft (Kotz et al., 2016).

Hence, a patient must have a portable device to retain the dispersed health records for readily available health history. Although the smart card-based portable devices are secure, they usually have limited space and can store only basic health information. The USB-based portable devices have larger storage space. However, they can infect a hospital computer with malware.

With the growing penetration of mobile devices across the globe including developing countries such as India, they can be used to retain secure portable health records. However, as per the previous research work (Akinyele, Pagano, & Green, 2011; Doukas, Pliakas, & Maglogiannis, 2010; Dmitrienko et al., 2010), the mobile devices have been used only for the backup of health records and offline access. All records are updated directly on the cloud and not on the mobile device. Hence records on the mobile device cannot be up to date, especially in a disconnected network. With the improvement in the computational and storage capabilities on the mobile devices, they can assist for a portable smart health record management system for patient mobility across different hospitals, emergency care, and travellers with readily available up to date health history. It must provide secure and trustful access along with provenance of health records so that the records may be considered reliable by the physicians across different hospitals.

Near Field Communication (NFC) (Coskun, Ozdenizci, & Ok, 2013) **(NFC)** has been used for improving several healthcare applications (Marcus et al., 2009; Lahtela, Hassinen, & Jylha, 2008; Vergara et al., 2010). It can also be used for ease of access to health records from a portable device and assist patient mobility across hospitals. NFC provides proof-of-locality, assures that only the two devices interface and makes threats such as Man-In-the-middle (MITM) attack and eavesdropping difficult. However, it does not provide a secure channel, authentication and trustful states of the devices. Hence there must be a bidirectional security handshake between the devices that communicate over the NFC tap.

The NFC-enabled Android mobile devices can operate in several modes. However, the Host Card Emulation (HCE) mode has several advantages as discussed in Section 5. HCE has only been used for financial applications, and its use for healthcare for secure NFC-based ease of access has not been explored to the best of our knowledge. HCE-based authentication and attestation with end-to-end secure computations on the Secure Elements(SE) on the devices can assist secure access between a portable card and reader devices (Sethia, Gupta & Saran, 2018a) as discussed in Sections 3 and 5.

Ciphertext Attribute-based encryption (CP-ABE) (Bethencourt, Sahai, & Waters, 2007) Since health records can be accessed by various health professionals such as a physician, nurse, pharmacist and a lab technician, it is essential that they may access information selectively based on their roles, for the privacy of patient and health records. Many cloud-based health record management systems use CP-ABE (Bethencourt et al., 2007) scheme which is a variation of Attribute-based encryption (ABE) for fine-grained access control and selective Role-based Access Control (RBAC). Although CP-ABE uses pairing-based cryptography which is computationally expensive, with the recent advancement in computational capabilities of the currently available mid-range priced mobile devices, Bethencourt et al.'s CP-ABE (Bethencourt et al., 2007) scheme and its variations have been implemented and proved feasible for deployment (Ambrosin, Cont, & Dargahi, 2015; Sethia, Gupta, & Saran, 2016, Sethis, Gupta, & Saran, 2018b) on mobile devices. We have previously proposed an improved CP-ABE scheme which can secure health records on mobile-based devices with selective access (Sethia et al., 2018b) and scalable

revocation, as discussed in Section 5. Hence it can assist in scalable sharing of health records across hospitals and assist in patient mobility.

Contribution. In this paper for the first time, we propose the requirements and design architecture for a novel next-generation portable Smart Health Record Management system with mobile devices for providing patient mobility across hospitals and up to date health history. A secure NFC-enabled mobile device aggregates the dispersed health records on an S-MAPLE (Secure Mobility-Assisted PortabLE) health folder as an HCE-based contactless card. It can be accessed by the mobile device of an authorised medical professional over low energy wireless interfaces such as NFC and Bluetooth and locally by the patient as well. NFC-based proof-of-locality, SEs, end-to-end mutual authentication with attestation protocol (Sethia et al., 2018a) and a variation of the CP-ABE (Bethencourt et al., 2007) scheme secure the proposed system. A cloud-based service provides data aggregation, translation of health records, management of credentials and a secure digital vault for backup.

We identify the security requirements for the proposed system and briefly present their solutions. We also present the implementation of a prototype for the proposed health record system on mid-range priced Android-based mobile devices with acceptable performance results.

Organization of the paper: The rest of the paper, consists of Section 2 in which we describe the system requirements for patient mobility across hospitals and the proposed system design for the Smart Health Record Management system with secure NFC-enabled mobile devices. Section 3 presents the security requirements and their solutions in brief. We then describe the implementation and performance evaluation in Section 4 followed by Related work in Section 5 and the conclusion and future work in Section 6.

2. System requirements and proposed solution

We identify the following requirements for a portable health records system for patient mobility across different hospitals with up to date health records:

- **R1: Aggregation**: It must retain the dispersed health records of a patient from different hospitals in a standard health format and maintain a complete health history of the patient.
- **R2: Up to date**: Besides maintaining a copy of the health record on the local HIS, the medical professional must also directly update it on the portable device and keep it up to date.
- **R3: Usability across hospitals** A patient must be able to present the portable device in different hospitals for direct reading and writing of health records and aggregate them for maintaining a complete health history of a patient.
- **R4: Availability** The complete health history must readily be available with the patient. It must be directly accessible by an authorized medical professional for the timely medical diagnosis and treatment especially in the case of emergency, chronic ailments and a traveller.
- **R5: Easy Accessibility** The health records must be accessible directly from portable devices. The communication must initiate as soon as there is proximity between the reader and portable health devices.
- **R6: Selective Access** The portable device must retain different types of health records. They must be accessible for direct read and write by authorized medical professionals, based on their roles using selective RBAC.
- **R7: Security and Privacy**: As per the previous review papers (Fernandez-Aleman et al., 2013; Haasa et al., 2011; Abbas & Khan, 2014) it is essential to secure the health records and retain the privacy of the patient. All credentials must reside on secure storage. It must satisfy different laws for security and privacy to aggregate the various health formats (Wuyts, Scandariato, Joosen, & Dumortier, 2012). It is also essential to maintain the provenance of health records so that medical professionals can refer to them reliably. The portable device must reliably identify the authorized patient and medical professional devices. The security framework must provide confidentiality, integrity and availability.

2.1. Proposed system design for the Smart Health Record Management system

In the following subsections, we describe the details of the Smart Health Record Management system with secure NFC-enabled mobile devices to retain an S-MAPLE (Secure Mobility-Assisted PortabLE) health folder. It retains aggregated dispersed health records as a mobile-based contactless health wallet. It assists in patient mobility across hospitals and up to date aggregated health history. Table 1 summarizes how the S-MAPLE health folder fulfils the various requirements *R1-R7* to provide patient mobility across hospitals.

2.1.1. Health folder organization

The portable NFC-based healt folder retains the different health records from various hospitals using the standard HL7 (Hapi, 2018) health format and fulfils requirement *R1* for aggregation. It maintains the health folder as a JavaScript Object Notation (JSON) file which is lightweight and fast to access as compared to the traditional XML file format. Since the HL7 format is cumbersome to parse, we pre-parse the health records with the HL7 application programming interface (HAPI) parser (Hapi, 2018) and also retain the pre-parsed health data separately to assist for efficient health data visualisation for the user. The JSON file maintains two arrays one for the HL7 data and the other for the pre-parsed non-HL7 data. Table 2

illustrates the layout of a sample health folder for two departments oncology and cardiology and the access rights for different medical professionals. Each subsection of the department record is encrypted using a variation of the CP-ABE scheme (Bethencourt et al., 2007) previously proposed by us called *Scalable Proxy-based Immediate Revocation for CP-ABE (SPIRC)* (Sethia et al., 2018b) for confidentiality and selective RBAC. Hence it satisfies requirement *R6* for selective access.

Physicians can access the S-MAPLE health folder by tapping their mobile device over NFC to read the past health records as well as a summary of the old health records. In the case, they require much older health records they may access them from the digital vault using delegation of cryptographic keys for CP-ABE (Bethencourt et al., 2007). A physician can diagnose the patient's health problem with the current symptoms as well as the previous history and tap to write the new prescription on the health folder.

With the size of 10 health records on a JSON file, around 57KB, an X-ray report around 2MB and MRI scan report around 200 MB, the S-MAPLE health folder can easily store most recent health records on the current mid-ranged priced mobile devices. Even with 100 records (OPD and lab tests), 10 XRay images and 2 fMRI scans, the space required is less than 1 GB. We feel that modern mobile devices have a minimum of 16 to 32 GB of RAM which is adequate to store few years of records and summary information. Hence it can provide readily available past health information for the patient and satisfies requirement *R4* for availability. It can be presented as a mobile-based health wallet and accessed by various authorised health professionals across different hospitals. Hence it satisfies requirement *R3* for usability across hospitals.

2.1.2. System model

Let us consider the scenario where patients with dispersed health records visit a hospital to seek treatment. They must register with the administrator before they can consult a physician for an Out Patient Department (OPD) session.

Fig. 1 demonstrates the system which involves a Patient mobile device **P** that retains the S-MAPLE health folder **F** with dispersed health records in HL7 format. **P** maintains a software-based contactless card using NFC-based HCE mode, which can access the health folder **F** internally as well as support the exchange of health information with the reader device over the NFC tap. NFC provides ease of access and hence helps satisfy requirement *R5*. The CP-ABE-based SPIRC scheme (Sethia et al., 2018b) encrypts the health folder for confidentiality, selective RBAC and scalable revocation. A medical professional can tap the card device using the NFC interface and directly read and write to it using the reader application **R** on the mobile device **M**. Multiple stakeholders can access each section with selective RBAC. The card and reader applications support the HL7 health format. A Cloud-based HealthSecure service **HSS** provides data aggregation and translation of health records, management of cryptographic credentials and a secure digital vault for backup of the health folder. All devices store cryptographic credentials on a Secure Element (SE), which provides tamper-resistant storage and performs secure

Table 1
Requirements fulfilled by the S-MAPLE Health folder Architecture.

Requirements	Method
R1:Aggregation	Storage of health records in a standard HL7 format and data aggregation and translation
R2:Up to date	New records written directly to the S-MAPLE health folder as well as on the local HIS
R3:Usability across hospitals	Direct access to the S-MAPLE health folder in different hospitals
R4:Availability	Storage of recent few years of health records and past health summary
R5:Easy Accessibility	Ease of access with NFC tap between the devices
R6:Selective Access	Selective RBAC with the SPIRC scheme based on CP-ABE
R7:Security and Privacy	Secure storage on SE; NSE-AA protocol (Sethia et al., 2018a) for end-to-end mutual authentication with attestation; SPIRC Sethia et al. (2018b) for confidentiality, selective RBAC and scalable revocation; NFC for proof-of-locality and Digital vault to refurbish lost health folder

Table 2
JSON Health Folder HL7 Health Records.

Depart.	Roles	Basic Vitals	Allergies/ Diseases	Advan. Vitals	Drugs	Lab Tests/ Immuniz.	Emerg/ Admin Data
Oncology	Doctor	RW	RW	RW	RW	RW	R
	Nurse	RW	R	R	R	R	R
	Pharm.	–	–	–	RW	–	R
	Lab Tech	–	–	–	–	RW	R
	Emerg.	RW	RW	RW	RW	RW	R
	Patient	R	R	R	R	R	R
	Admin	R	R	R	R	R	W
Cardiology	Doctor	RW	RW	RW	RW	RW	R
	:	:	:	:	:	:	:

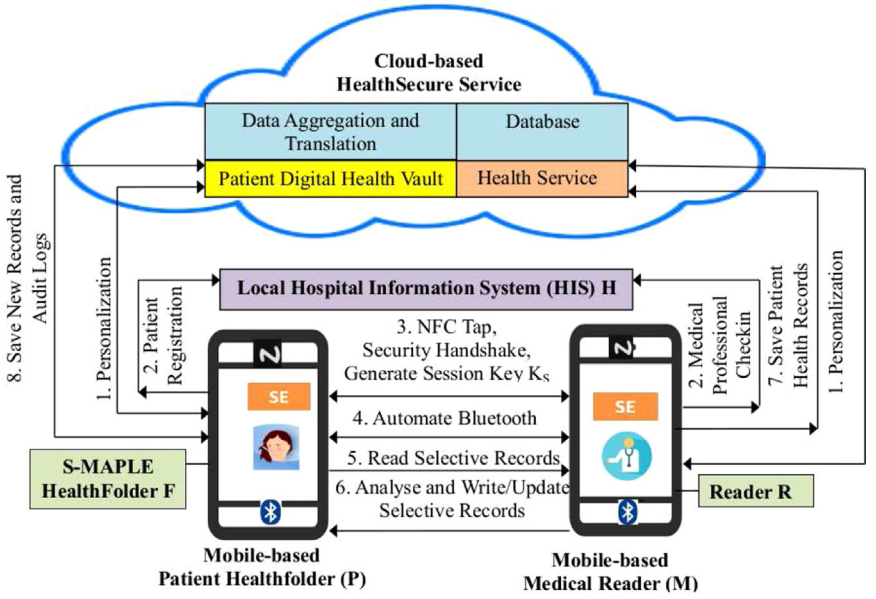

Fig. 1. System Model for Smart Health Record Management System.

cryptographic computations. Fig. 1 demonstrates the flow of the interaction between the components and the steps are listed below:

1. The HealthSecure service assists in the personalisation of SEs of valid users to store the credentials and identity on their mobile devices.
2. The patient and the medical professional register and check-in respectively for an OPD session in the hospital.
3. During an OPD session the patient and medical professional tap their devices close for initiating a security handshake with an end-to-end *NFC SE-based Mutual Authentication and Attestation (NSE-AA) protocol* (Sethia et al., 2018a) previously proposed by us to verify that only valid and trustful devices interact. It sets up a unique session key which encrypts all further communication.
4. The HCE tap further automates Bluetooth pairing over HCE to provide higher throughput for the exchange of large data such as medical images. The mobile devices without NFC can alternatively use secure QR-Code to automate Bluetooth pairing using inbuilt cameras (Vazquez-Briseno et al., 2012).
5. The reader application interfaces with the card application using bidirectional HCE or Bluetooth interface to selectively read old dispersed health records for the last few years and a summary of older health records.
6. The medical practitioner analyses the health records, and updates the new observations, diagnosis and prescription as a new health record and writes it on the health folder over the HCE interface using the HL7 format. Hence the health folder is up to date and satisfies requirement *R2*.
7. The reader device uses existing translation services on the HealthSecure service to translate the HL7 format to the local health format of the HIS to store them locally.
8. The health folder stores the health records as well as the audit logs on the secure digital vault for future reference.

2.1.3. System architecture

We describe the various software components for the system architecture which is illustrated in Fig. 2.

- **Patient/Medical professional mobile devices** The patient mobile device retains a card application on the mobile processor to emulate an HCE-based contactless card. The encrypted S-MAPLE health folder resides in an insecure region such as the internal memory or a microSD card. We use a special microSD card with insecure storage and a secure embedded tamper-resistant Secure Element (SE).
  The medical professional's mobile device retains an HCE reader application on the mobile processor. It can access the S-MAPLE health folder using NFC-based HCE bidirectional library and Bluetooth.
  The SE contains Java Card applets to (1)Retain identity, certificates and decryption keys (2)Perform cryptographic computations for the end-to-end NSE-AA protocol over HCE (Sethia et al., 2018a).
- **HealthSecure Service** It is a cloud-based service which provides the following services for the secure portable health system:

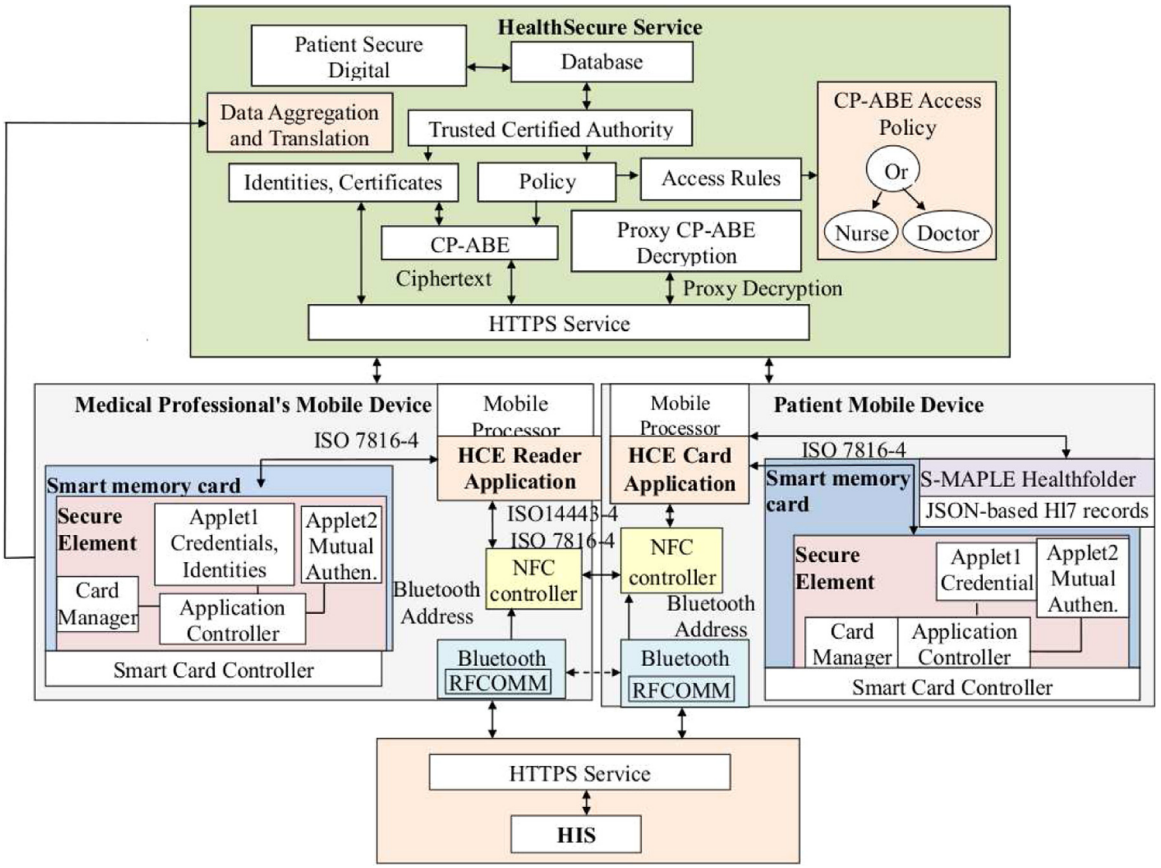

Fig. 2. System Architecture.

1. *Data aggregation and translation:* Both the card and reader devices exchange health records using the HL7 format. The HealthSecure service uses existing tools such as Mirth Connect (Mirth, 2018) to help translate health records so that the physician can store them on the HIS also in the local health format.
2. *Trusted Certified Authority (TCA):* The TCA administers cryptographic credentials and identities of registered patients and medical professionals. The Healthsecure service or the owner may define the access policy for the SPIRC scheme (Sethia et al., 2018b) and allocate decryption keys to the stakeholders. Due to the computational overheads of bilinear pairing, the S-MAPLE framework outsources the SPIRC encryption to the HealthSecure service. The TCA also provides a trusted proxy server to support partial decryption for the SPIRC scheme for managing a revocation list and providing the proxy components over HTTPS to assist decryption on the mobile devices.
3. *Secure Digital Vault:* The medical professional data syncs all new records on the secure digital vault. It can be used to refurbish the health folder in the case of loss or theft of the device and to access old records that are not available in the health folder.

- **Health Information System(HIS)** It maintains the EHRs locally on the hospitals such as the openMRS (OpenMRS, 2018) system using translations tools from the HealthSecure service.

2.1.4. Bidirectional HCE communication

Typically the payment applications use bidirectional HCE communication (Alattar & Achemlal, 2014). The application of HCE for a mobile-based health wallet presented in this paper for patient mobility across hospitals does not exist to the best of our knowledge. The HCE-based cards can be designed with the proprietary Application Protocol Data Unit (APDU) (Java Card, 2018) packets to enhance data security and trust. However, the APDU command and response packets can carry data limited to 255 bytes (Android,) on currently available Android-based devices. We have developed an HCE library for the exchange of large-sized data between the card and reader for reading and writing data which is larger than 255 bytes. Both card and reader devices can send and receive data to each other. A sender device fragments large data and sends the fragments in multiple packets. The receiver device further reassembles them. The HCE-based communication comprises of a bidirectional protocol with error control for reading and writing to the health folder.

The bidirectional HCE tap is used to (1) Identify mobile devices and ensure their trustful states using the NSE-AA protocol (Sethia et al., 2018a) (2) Automate Bluetooth pairing for higher throughput (3) Exchange of data for reading and writing.

Traditionally Peer-to-peer NFC mode is used to automate Bluetooth pairing without manual intervention. We use the HCE mode to exchange the Bluetooth address and establish a connection over Radio frequency communication(RFCOMM) sockets without any manual intervention. The NSE-AA protocol and proof-of-locality wth NFC assure that the Bluetooth pairing is between the two devices in proximity.

The HCE library has a Reader Mode and a Writer Mode. Both the reader and card devices open their separate applications to initiate the communication. The reader device taps and selects the card AID (Application Identifier) and sends the read or write command to the card. The sender sets the *More Fragment Packet (mfp) flag* to 1 if more fragments are pending and 0 if there are no more fragments. The receiver reassembles all packets when it receives a packet with *mfp* as 0. When the devices lose contact, the interface terminates.

3. Security requirements and solutions

The S-MAPLE health folder has a strong security framework to satisfy requirement *R7*. Due to the limitation of space in this paper, we present the security requirements and their solutions in brief. We have identified the following security requirements:

- **SR1: Confidentiality** The health folder must be encrypted and be accessible to authorized users.
- **SR2: Integrity** An intruder must not be able to alter the health information.
- **SR3: Mutual Authentication and Trust** A valid patient and authorized medical professional must have unique identities and must be able to authenticate each other for a trustful session. The mobile devices may have malware that can risk the health card and reader applications. The two devices must prove their trustful states to each other before the exchange of any data.
- **SR4: Privacy** It must retain the privacy for the patient's identity when stored on the devices as well as when used during communication.
- **SR5: User Anonymity** Each device must have a unique virtual identity which is known only to the user. It may be generated using a password known to the user and credentials on the SE. The adversary must not be able to use it for replay attacks or to find the actual identity.
- **SR6: Proof-of-locality** The devices must initiate communication only when they are close and can assure proof-of-locality. The requirement for the proximity of devices must make MITM attack and eavesdropping difficult.
- **SR7: Secure Storage** Since mobile devices are prone to threats, there must be secure storage on the mobile device to store health records and cryptographic credentials.
- **SR8: Selective Access** Since the health folder may have a collection of different types of health information, they must be accessed using selective RBAC by medical professionals based on their role.
- **SR9: Revocation** The health folder must revoke malicious users such as a patient submitting wrong medical bills or an intruder impersonating as a doctor or involved in medical identity theft. However, it must allow uninterrupted access to the non-revoked users without requiring re-encryption of re-distribution of keys.
- **SR10: Delegation** Patients must be able to temporarily delegate a decryption key to a family or friend to collect a report or medication on their behalf.
- **SR11: Emergency** A patient must be able to share the emergency information with the emergency personnel to indicate the right treatment needed. The security framework must support special access to the health folder using the Break the Glass (BTG) key (Gardner et al., 2009; Sethia et al., 2016).
- **SR12: Theft of device** In the case of theft or loss of the device, there must be a provision to revoke old credentials and refurbish the health records on a new patient mobile device.
- **SR13: Audit Logs** All events of reading and writing to the health folder must be recorded in the cloud along with a backup of the transaction for reference in the case of improper access.

The framework must also protect the contactless health folder from the threats that affect smart cards such as Yang, Ma, & Jiang (2012):

- **TR1: Dos attack** An Intruder can try to access the portable health folder on a contactless card with attempts to initiate the authentication which fail and hence make it useless for an actual user.
- **TR2: Replay attack** An Intruder can attempt to replay some of the messages to access the S-MAPLE health folder.
- **TR3: Collusion attack** A host *H* can use another host *V's* information to access the unauthorized information.
- **TR4: Parallel session attack** An Intruder can eavesdrop and gather the messages and replay them to cause a parallel session attack.
- **TR5: Forgery attack** An Intruder can use a registered stakeholder's identification and access the S-MAPLE health folder.
- **TR6: Platform impersonation attack** A malicious server can replace the actual server for the TCA services.
- **TR7: Man-in-the-middle (MITM) attack** An unregistered user can eavesdrop, spoof, decrypt and relay a message.
- **TR8: Insider attack** An intruder who is an insider can impersonate the credentials of a user such as a medical professional and try to seek health information of a patient during an OPD session.

- **TR9: Relay attack** In a relay attack, the attacker which is a proxy reader can masquerade itself as a valid reader by relaying the information received from the actual card to a proxy card over Bluetooth or remote access. The proxy card can further communicate it to the actual reader and similarly relay back the response to the actual card (Sethia et al., 2018a). It can cause theft of identities and health information or writing wrong prescription and medication by a malicious reader to harm the patient.

Proposed security solutions: In our previous work, we have presented novel protocols for a CP-ABE-based SPIRC scheme (Sethia et al., 2018b) for confidentiality, selective RBAC and scalable revocation; an end-to-end mutual authentication protocol between the SEs of the devices over HCE with the NFC-AA protocol (Sethia et al., 2018a) to ensure valid devices can interact with each other. Both protocols are compared with the related protocols and improve the security with acceptable performance results for computation and communication overheads. These protocols can also provide secure access to the S-MAPLE health folder. We propose the following security solutions to fulfil the security and threat requirements that have been identified.

1. **S1: Secure Element** The SE provides tamper-resistant storage and secure computations for the NSE-AA protocol (Sethia et al., 2018a).
2. **S2: CP-ABE** We encrypt all health records with a variation of Bethencourt et al.'s CP-ABE scheme, called SPIRC (Sethia et al., 2018b). It provides scalable user revocation without the requirement of re-encryption and re-distribution of the key to the unrevoked users. A proxy server maintains a revocation list and assists in partial decryption. Whenever a user accesses the ciphertext and must decrypt it, it contacts the proxy server to seek proxy components over HTTPS. The proxy server modifies the proxy components only for the malicious users so that decryption fails and allows uninterrupted access to the other non-revoked users. We present a detailed security analysis and comparison with related schemes for the SPIRC scheme in our previous paper (Sethia et al., 2018b). It is Collusion resistant, satisfies forward secrecy and is CPA (Chosen Plaintext Attacks) secure.
3. **S3: Mutual Authentication and Attestation** In our previous work we have proposed NFC SE-based Mutual Authentication and Attestation (NSE-AA) protocol (Sethia et al., 2018a). It provides proof-of-locality with NFC, end-to-end anonymous mutual authentication between the SEs using limited lightweight symmetric encryption and also associates it with a remote attestation phase to ensure trustful states of the devices. We present a detailed security analysis with formal and informal security proof using the ROR model (Abdalla, Fouque, & Pointcheval, 2005). It is robust and has less computation and communication overheads as compared the existing schemes. A simulation of the protocol on Automated Validation of Internet Security Protocols and Applications (AVISPA) tool (Armando et al., 2005) proves that it is safe.
4. **S4: NFC** It ensures that the two devices in proximity are only interacting and makes eavesdropping and MITM attack difficult.
5. **S5: Digital vault** It provides a secure backup of the patient health records and helps to store the audit logs and to refurbish the health folder in the case of theft or loss of the device.

Tables 3 and 4 illustrate how the security solutions S1-S5 fulfil the security and threat requirements respectively for the secure S-MAPLE health folder access.

Table 3
Fullfillment of security requirements.

Solution	S1:SE	S2:CP-ABE	S3:Mut Auth	S4:NFC	S5:Dig. Vault
SR1:Confidentiality	y	y	y	y	y
SR2:Integrity	y	y	y	y	y
SR3:Mutual Auth and Trust	y	–	y	–	–
SR4:Privacy	y	y	y	–	y
SR5:User Anonymity	y	–	y	–	y
SR6:Proof-of-locality	–	–	y	y	–
SR7:Secure Storage	y	–	–	–	y
SR8:Selective Access	–	y	–	–	–
SR9:Revocation	–	y	–	–	–
SR10:Delegation	–	y	–	–	–
SR11:Emergency	y	y	–	–	–
SR12:Theft of device	y	y	–	–	y
SR13:Audit Logs	y	y	–	–	y

4. Implementation and performance analysis

We have practically implemented the HCE card and reader applications on the mid-range priced Android 4.4 devices such as Sony Xperia M2 Dual and use the HCE-based bidirectional library for communication. We choose the SE form factor of a microSD card from GoTrust (GO-Trust, 2018) for ease of deployment. Special mobile applications compiled with libraries provided by GoTrust can access the SE internally The Java card applets use Java Card version 2.2.2 to store cryptographic credentials and assist in the end-to-end NSE-AA protocol between the SEs over the HCE interface (Sethia et al., 2018a).

The mobile-based health wallet retains the S-MAPLE health folder as a JSON file as discussed in Section 4.3. The HCE reader application helps to read and write over the S-MAPLE health folder. The prototype encrypts the health folder with the SPIRC scheme (Sethia et al., 2018b) and validates the devices with the end-to-end NSE-AA protocol between the SEs over HCE (Sethia et al., 2018a).

The performance results for accessing an S-MAPLE health folder with 10 text-based health records (size 57 KB) are as follows:

- t_E: Time for Encryption on server: 4197 ms (Sethia et al., 2018b)
- t_N: NFC transactions: 207 ms
- t_{MAA}: HCE Mutual Authentication: 3551 ms (Sethia et al., 2016)
- t_B: Transfer over Bluetooth: 5119 ms
- t_{DP}: Proxy decryption support: 450 ms (Sethia et al., 2018b)
- t_{DD}: Device decryption: 2143 ms (Sethia et al., 2018b)
- t_D: Net decryption time: $t_{DP} + t_{DD}$: 2593 ms
- t_{NR}: $t_N + t_{MAA} + t_B + t_D$: 11,470 ms $\approx$ 12 s

The total time to read the card over HCE comprises of the NFC transaction, Bluetooth pairing, HCE mutual authentication, transfer over Bluetooth followed by decryption on the remote device, which is around 12 s. According to a smart card health system proposed by Kardas and Tunali (2006), it takes around 9 s to start a user session once the card is inserted into the reader device. Hence, the overheads of around 12 s seem acceptable since it provides easy access over the NFC tap along with a robust security handshake. We did not find performance for access time in the other related schemes. Fig. 3 illustrates the effect of access time on the number of health records. We observe that with the increase in the number of records, the encryption and decryption timings are not affected and the read time increases significantly due to the overheads of communication. The details for the prototype and a demo are available in our technical report (Portable, 2018) and a Patent application (Sethia et al., 2016).

Table 4
Fullfillment of threat requirements.

Solution	S1:SE	S2:CP-ABE	S3:Mut Auth	S4:NFC	S5:Dig. Vault
TR1:Dos	y	–	y	–	–
TR2:Replay	y	–	y	–	–
TR3:Collusion	y	y	y	–	–
TR4:Parallel session	y	y	y	–	–
TR5:Forgery	y	–	y	–	–
TR6:Platform impers.	y	–	y	–	–
TR7:MITM	y	–	y	–	–
TR8:Insider	y	–	y	–	–
TR9:Relay	y	–	y	–	–

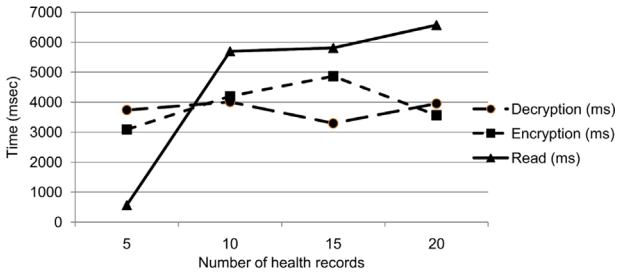

Fig. 3. Testing results (Sethia et al., 2016).

5. Related work

Portable devices: MyHealthAvatar (Spanakis et al., 2014) is a portable device which only provides backup of health records from the different sources. MyCareCard (Rybynok et al., 2011) is a USB-based device which is up to date but is used only for offline access. A Poket Doktor System (Hall et al., 2003) is a large spaced Bluetooth-enabled smart card with Radio Frequency Identification (RFID) interface to automate Bluetooth for sharing health records with a medical professional. It is a system nearest to our work to provide ease of access through device proximity and availability of health records. However, it lacks aggregation of health data from different sources and selective RBAC. None of the portable health systems looks into the requirement for usability across different hospitals.

Mobile devices: Most research work store the primary health records in the cloud and use the mobile devices only for backup and offline access. Hence, the health data on mobile devices is not up to date, especially in disconnected networks. Akinyele et al. (2011) presented an iPhone-based application to store and backup health records which are encrypted using Bethencourt et al.'s CP-ABE (Bethencourt et al., 2007) scheme for selective access. However, the scheme is not suitable for a portable device to support scalable user revocation (Sethia et al., 2018b). Doukas et al. (2010) proposed an Android-based mobile-based application to access the medical images from the cloud and does not store them. Dmitrienko et al. (2010) proposed a TruWallet application for a Nokia device. It uses a security kernel, trusted hardware for application isolation and credential storage with a virtual machine environment for securing health records. However, this scheme is difficult to implement on non-rooted mobile devices since it requires kernel access.

RFID and NFC: Radio Frequency Identification (RFID) has been used for ease of access with proximity and improving healthcare applications (Amendola et al., 2014; Catarinucci et al., 2015).

NFC is a low energy wireless technology operating at 13.56 MHz frequency, with few centimetres of access distance and a maximum throughput of 424 kbit/s for simple access of a device to communicate with another device or an NFC, Radio Frequency Identification (RFID) and smart card tag. An NFC-enabled mobile device can operate in different modes: (i) Reader mode for accessing tags. (ii) Peer to Peer (P2P) mode to communicate with another device (iii) Card emulation mode to emulate a contactless card on a Secure Element (SE) (iv) Host Card Emulation (HCE) mode (Alattar and Achemlal, 2014; Secure, 2018) to emulate a software-based contactless card. HCE has several advantages as compared to the other NFC modes, such as support for bidirectional communication, higher computing capability, larger storage, lower development complexity and cost, independence of the service provider for deployment and direct accessibility by another mobile device (Java, 2018). Table 5 illustrates the comparison between the different modes.

An SE is a secure smart card microchip which communicates with the NFC controller of a mobile device. It provides tamper-resistant storage and support for hardware card emulation. It uses the ISO 7816-4 standard for communication with APDU command and response packets (Java card, 2018). An SE can be accessed internally through applications compiled with special libraries on the processor. It has various form factors such as embedded SE (e.g. iPhoneSE), Universal Integrated Circuit Card (UICC) (e.g. Subscriber Identification Module (SIM) card) and a Secure Memory Card (e.g., microSD card GO-Trust, 2018). It utilises Java Card version 2.2.2 (Java card, 2018) which supports execution of Java-based applets on smart cards.

NFC has been used for improving healthcare applications such as identification of patients for an improved public healthcare (Marcus et al., 2009), reducing medical errors with NFC (Lahtela et al., 2008), prescription of drugs (Vergara et al., 2010) and to provide a secure medicine anti-counterfeiting system (Wazid et al., 2017). In our previous work (Sethia et al., 2014) we have proposed a mobile-based health card which uses NFC modes other than the HCE mode but does not support selective access. The S-MAPLE health folder is robust since it uses HCE which has several advantages of the other NFC modes, has better storage and support for bidirectional communication for a robust security handshake. We use the HCE for the first time for a next-generation contactless health card that can provide a mobile-based health wallet and patient mobility across hospitals.

CP-ABE (Bethencourt et al., 2007) It is a variation of Attribute-based Encryption, which associates the access policy with the ciphertext and the attributes with the decryption key. The users can have different decryption keys with a different set of attributes as per their roles. A decryption key can decrypt the ciphertext only if its attributes satisfy the access policy of the ciphertext. Hence CP-ABE can provide selective Role-based Access Control (RBAC) for reading and writing to the shared data such as the health records.

Table 5
Comparison of NFC modes (Secure, 2018; Roland & Langer, 2013; Alattar & Achemlal, 2014).

Mode	Reader-Write	Peer to Peer	Card Emulation	HCE
Security	poor	medium	high	high with SE
Storage	few bytes	large	few Kbytes	large
Speed	low	fast	medium	fastest
Communication	unidir	bidir	bidir	bidir
Open dev.	yes	no	yes	yes
Mobile-based reader	yes	yes	no	yes

Table 6
Comparison of the portable health record management systems.

Requirements	Spanakis et al. (2014)	Rybynok et al. (2011)	Hall et al. (2003)	Akinyele et al. (2011)	Doukas et al. (2010)	Sethia et al. (2014)	S-MAPLE
R1:Aggregation	Y	N	N	N	N	N	Y
R2:Up to date	N	Y	N	N	N	Y	Y
R3:Usability across hospitals	N	N	N	N	N	N	Y
R4:Availability	Y	Y	Y	Y	Y	Y	Y
R5:Easy Accessibility	N	N	Y	Y	N	Y	Y
R6:Selective Access	N	N	N	Y	N	N	Y
R7:Security and Privacy	N	N	N	N	N	N	Y

In our previous work, we have also proposed Proxy-based Immediate Revocation of Attribute-based Encryption (PIRATTE) which is a variation of CP-ABE scheme (Sethia et al., 2016). However, it can revoke only limited users at a time. The SPIRC scheme used in the S-MAPLE healthfolder improves the PIRATTE scheme with scalable revocation so that it is accessible uninterruptedly to all non-revoked stakeholders and also improves the performance for encryption and decryption. It can further provide delegation of keys and revocation to help refurbish lost or corrupted health folder on a mobile device.

Table 6 illustrates the comparison of the S-MAPLE health folder with the other related schemes. For comparison for requirement *R7*, we consider the solutions S1-S5 Secure Element, CP-ABE, Mutual Authentication and Attestation, NFC, Digital Vault respectively in Section 2.6. None of the prior schemes satisfies all the requirements *R1-R7* which are essential to provide patient mobility across different hospitals. Only the S-MAPLE health folder offers a robust security framework with all security solutions S1-S5.

6. Conclusion and future work

In this paper we propose a next-generation portable smart health record management system with health records on an S-MAPLE health folder on a secure NFC-enabled mobile device and credentials on an SE. The novelty of this work is to provide a mobile-based health wallet using NFC-based HCE mode for the first time that can be accessed directly by the medical professional's mobile device. NFC provides ease of access and allows a secure next-generation future mobile-based health wallet to be accessed for direct read and write by various medical professionals across different hospitals. It assures that a medical professional can access the data only through proximity to the portable health device, with proof-of-locality and a security handshake. It fulfils all requirements *R1-R7* to support patient mobility across hospitals and up to date aggregated health history. We also present the security and threat requirements and their solutions *S1-S5* in brief. The SPIRC scheme (Sethia et al., 2018b) provides confidentiality, selective RBAC and scalable revocation. The end-to-end NSE-AA protocol (Sethia et al., 2018a) between the SEs of the devices ensures that only valid devices interact. The performance evaluation of the prototype on mid-range priced Android-based mobile devices indicates acceptable delays for accessing the S-MAPLE health folder.

Limitations and future work: The S-MAPLE healthfolder has some limitations which we can improve in the future. Currently, for requirement *R1* the S-MAPLE folder only aggregates the health data. There are open challenges of semantic interoperability of health records due to lack of common standards across different countries. Various techniques such as Ontology, and cloud-based services (Hammami, Bellaaj, & Kacem, 2014) can address them in the future. Health standard such as Fast Healthcare Interoperability Resources (FHIR) (FHIR, 2018) can provide semantic interoperability across different health systems. Recently there is a trend of Patient Generated Health Data (PGHD) [5] from personal observations, health monitoring and fitness devices. We can further enhance the S-MAPLE health folder by aggregating the PGHD along with heterogeneous EHRs. It is also essential to reduce the burden of digital entry for medical professionals from the mobile reader application in the future since they are more at ease to write than type. There must be a provision to scan hand-written health records and translate to standard digital health formats such as HL7, especially to translate paper-based health records on the S-MAPLE health folder. The current S-MAPLE health folder uses SEs with slow processing capabilities which leads to increased time in end-to-end mutual authentication between the SEs. High-speed SEs and extended APDUs with HCE can help in the access time between the health card and reader devices.

References

Abbas, A., & Khan, S. U. (2014). A review on the state-of-the-art privacy-preserving approaches in the e-health clouds. *IEEE Journal of Biomedical and Health Informatics*, *18*(4), 894–906.

Abdalla, M., Fouque, P.-A., & Pointcheval, D. (2005). Password-Based Authenticated Key Exchange in the Three-Party Setting. In *Proceedings of the International workshop. Public Key Cryptography*, pp. 65–84.

Akinyele, J.A., Pagano, M.W., & Green, M.D. (2011). Securing electronic medical records using attribute-based encryption on mobile devices. In *Proceedings of the ACM international conference on security and privacy in smartphones and mobile devices*, pp. 75–86.
Alattar, M., & Achemlal, M. (2014). Host-based Card Emulation: development, security, and ecosystem impact analysis. In *Proceedings of the IEEE international conference on high performance computing and communications*.
Ambrosin, M., Cont, M., & Dargahi, T. (2015). On the Feasibility of Attribute-Based Encryption on Smartphone Devices. In *Proceedings of the ACM international conference on IoT challenges in mobile and industrial systems*, pp. 49–54.
Amendola, S., et al. (2014). RFID technology for IoT-based personal healthcare in smart spaces. *IEEE Internet of Things Journal*, *1*(2), 144–152.
Android developer IsoDep. URL ⟨https://developer.android.com/reference/android/nfc/tech/IsoDep⟩.
Armando, A. et al. (2005). The AVISPA Tool for the Automated Validation of Internet Security protocols and Applications. In *Proceedings of the international conference on computer aided verification*, pp. 281–285.
Bahga, A., & Madisetti, V. K. (2013). A cloud-based approach for interoperable Electronic Health Records (EHRs). *IEEE Journal of Biomedical and Health Informatics*, *17*(5), 894–906.
Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-policy attribute-based encryption. In *Proceedings IEEE international conference symposium on security and privacy* (SP), pp. 321–334.
Catarinucci, L., et al. (2015). An IoT-aware architecture for smart healthcare systems. *IEEE Internet of Things Journal*, *2*(6), 515–526.
Chen, W., et al. (2010). Developing electronic health records in Taiwan. *IEEE IT Professional*, 17–25.
Coskun, V., Ozdenizci, B., & Ok, K. (2013). A survey on Near Field Communication (NFC) technology. *Springer Wireless Personal Communications*, *71*(3), 2259–2294.
Dmitrienko, A. et al. (2010). Securing the Access to Electronic Health Records on Mobile Phones, In *Proceedings of the international conference biomedical engineering systems and technologies of the series communications in computer and information science*, 273, pp. 365–379.
Doukas, C., Pliakas, T., & Maglogiannis, I. (2010). Mobile healthcare information management utilizing Cloud Computing and Android OS. In *Proceedings of the IEEE international conference engineering in medicine and biology society*.
Fernandez-Aleman, J. L., et al. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics*, *46*(3), 541–562.
Overview - FHIR v1.0.2 - HL7.org, Last accessed Oct. 2018. URL ⟨https://www.hl7.org/fhir/overview.html⟩.
Gardner, R.W. et al. (2009). Securing medical records on smart phones. In *ACM Proceedings of the international workshop on security and privacy in medical and home-care systems*, pp. 31–40.
GO-Trust Secure microSD Java, Last accessed October 2018. URL ⟨http://www.go-trust.com/products/⟩.
Haasa, S., et al. (2011). Aspects of privacy for electronic health records. *International Journal of Medical Informatics*, *80*(2), 26–31.
Hall, E., et al. (2003). Enabling remote access to personal electronic medical records. *IEEE Engineering in Medicine and Biology Magazine*, *22*(3), 133–139.
Hammami, R., Bellaaj, H., & Kacem, A. H. (2014). Interoperability for medical information systems: An overview. *Health and Technology*, *4*(3), 261–272.
Hapi, The Free, Open, and Best HL7 Parser and Library for Java, last Accessed October 2018. URL ⟨https://hapifhir.github.io/hapi-hl7v2/⟩.
Java card platform security, Last accessed October 2018. URL ⟨http://www.oracle.com/technetwork/java/javacard/⟩.
Java Card 3 Platform Programming Notes - Extended APDU Nominal Cases, Last accessed October 2018. URL ⟨https://docs.oracle.com/javacard/3.0.5/prog notes/extended_apdu_nominal_cases.htm#JCPCL168⟩.
Kardas, G., & Tunali, E. T. (2006). Design and implementation of a smart card based healthcare information system. *Computer Methods and Programs in Biomedicine*, *81*(1), 66–78.
Kotz, D., et al. (2016). Privacy and security in mobile health: A research agenda. *IEEE Computer*, *49*(6), 22–30.
Lahtela, A., Hassinen, M., & Jylha, V. (2008). Using NFC-enabled Mobile Phones for Public health in developing countries. In *Proceedings IEEE international conference on pervasive computing technologies for healthcare*.
Marcus, A. et al. (2009). Using NFC-enabled Mobile Phones for Public Health in Developing Countries. In *Proceedings of the ACM international workshop on Near Field Communication*, pp. 30–35.
Mirth Connect, Last accessed October 2018. URL ⟨http://www.mirth.com⟩.
NHS Digital Systems and services, Last accessed on October 2018. URL ⟨https://digital.nhs.uk/article/196/Systems-and-services⟩.
OpenMRS, Last accessed October 2018. URL ⟨http://www.openmrs.org/⟩.
Portable mobile based secure healthcard, ⟨https://sites.google.com/site/divyashikhasethia/home/portable-mobile-based-secure-healthcard⟩, Last accessed October 2018.
Roland, M., & Langer, J. (2013). Comparison of the usability and security of NFCs different operating modes in mobile devices. *Elektrotechnik und Informationstechnik*, *130*(7), 201–206.
Rybynok, V. O., Kyriacou, P. A., Binnersley, J., & Woodcock, A. (2011). MyCare Card Development: Portable GUI framework for the personal electronic health record device. *IEEE Transactions on Information Technology in Biomedicine*, *15*(1), 66–73.
Secure Element Deployment and Host Card Emulation v10, last Accessed October 2018. URL ⟨http://simalliance.org/wp-content/uploads/2015/03/Secure-Element-Deployment-Host-Card-Emulation-v1.0.pdf⟩.
Sethia, D., Gupta, D., & Saran, H. (2018a). NFC secure element-based mutual authentication and attestation for IoT access. *IEEE Transactions on Consumer Electronics*, *14*(8). https://ieeexplore.ieee.org/document/8477059.
Sethia, D. et al. (2014). NFC based secure mobile healthcare system. In *Proceedings of the IEEE international conference communication systems and networks*, pp. 749–760.
Sethia, D., et al. (2016). Mutual authentication protocol for secure NFC based mobile healthcard. *IADIS International Journal on Computer Science and Information Systems*, *11*(2), 195–202.
Sethia, D. et al. Portable computing device based secure medical records management, patent Office India: Application number: 1313/DEL/2015 A (Nov. 2016). URL ⟨http://www.ipindia.nic.in/writereaddata/Portal/IPOJournal/1_410_1/Part1.pdf⟩.
Sethia, D., Gupta, D., & Saran, H. (2016). Security framework for portable NFC mobile based health record system. In *IEEE Proceedings of the international conference wireless and mobile computing, networking and communications*.
Sethia, D., Saran, H., & Gupta, D. (2018b). CP-ABE for selective access with scalable revocation: A case study for Mobile-based Healthfolder. *Journal of Network System*, *20*(4), 689–701.
Spanakis, E. G., et al. (2014) MyHealthAvatar Personalized and empowerment health services through Internet of Things technologies. In IEEE Proceedings of the international conference wireless mobile communication and healthcare.
The new EU Regulation on the protection of personal data: what does it mean for patients?, Last accessed Oct. 2018. URL ⟨http://www.eu-patient.eu/globalassets/policy/data-protection/data-protection-guide-for-patients-organisations.pdf⟩.
Vazquez-Briseno, M., et al. (2012). Using RFID/NFC and QR-Code in mobile phones to link the physical and the digital world. *Journal Interactive Multimedia*, 219–242.
Vergara, M. et al. (2010) Mobile prescription: An NFC-based proposal for AAL. In *Proceedings of second international workshop on Near Field Communication*.
Wazid, M., et al. (2017). Secure authentication scheme for medicine anti-counterfeiting system in IoT environment. *IEEE Internet of Things Journal*, *4*(5), 1634–1646.
Wuyts, K., Scandariato, G. V. R., Joosen, W., & Dumortier, J. (2012). What electronic health records don't know just yet. A privacy analysis for patient communities and health records interaction. *Springer Health and Technology*, *2*(3), 159–183.
Yang, L., Ma, J.-F., & Jiang, Q. (2012). Mutual authentication scheme with SmartCards and password under trusted computing. *International Journal of Network Security*, *14*(3), 155–162.