Future Generation Computer Systems 68 (2017) 1–13

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

Research issues for privacy and security of electronic health services

Buket Yüksel, Alptekin Küpçü, Öznur Özkasap *

Department of Computer Engineering, Koç University, İstanbul, Turkey

HIGHLIGHTS

- We present a survey of state-of-the-art electronic health services (EHS) research focusing on the security, privacy, and integrity aspects.
- We categorize state-of-the-art studies according to their architecture, access control, emergency cases, sharing, search, and anonymity techniques.
- We consider components, characteristics, and challenges of e-health services.
- We systematically analyze and evaluate the systems with a method-based approach, and lay out a comprehensive survey of cryptographic approaches of EHS.
- We identify relevant open problems and provide future research directions for enhancing security and privacy of EHS.

ARTICLE INFO

Article history:
Received 4 March 2016
Received in revised form
9 August 2016
Accepted 16 August 2016
Available online 1 September 2016

Keywords:
Electronic health services
Privacy
Security
Cryptography
E-health

ABSTRACT

With the prevalence of information and communication technologies, Electronic Health Services (EHS) are commonly used by patients, doctors, and other healthcare professionals to decrease healthcare costs and provide efficient healthcare processes. However, using EHS increases the concerns regarding security, privacy, and integrity of healthcare data. Several solutions have been proposed to address these issues in EHS. In this survey, we categorize and evaluate state-of-the-art electronic health system research based on their architecture, as well as services including access control, emergency access, sharing, searching, and anonymity methods by considering their cryptographic approaches. Our survey differs from previous EHS related surveys in being method-based such that the proposed services are classified based on their methods and compared with other solutions. We provide performance comparisons and state commonly used methods for each category. We also identify relevant open problems and provide future research directions.

1. Introduction

Electronic Health Services (EHS) are increasingly used by patients, providers, employers, doctors, policy makers, and other healthcare workers. EHS have several **advantages** such as **decreasing healthcare costs** and **providing faster and more efficient processing**. However, using EHS increases the **concerns** of **security**, **privacy**, and **integrity** of healthcare data. These concerns affect patients' willingness to disclose their healthcare data and can cause life-threatening consequences. For example, United States Department of Health and Human Services estimated that about *two million* Americans suffering from mental illnesses did not seek treatment because of privacy concerns [1].

We present a combination of proposed EHS functions in Fig. 1. Although there is no such existing system that includes all the EHS functions; the elements and functions illustrated in Fig. 1 provide a general view of our survey content. Patients, healthcare professionals, and data storages are the basic elements of EHS. Patients can share their health data among each other or with healthcare professionals. Furthermore, patients can delegate or revoke authorization on their health data. In privacy preserving EHS, patients encrypt their health data and store them at hospitals and cloud storage servers. When patients need their health data, they first get the encrypted data and decrypt with their keys. Access control techniques are used to limit access to health data based on the properties and requirements of the EHS. They also prevent unauthorized parties to reach the data. In addition, healthcare professionals may need to search for certain health data. While searching, healthcare professionals first retrieve encrypted search results and then they decrypt with their keys. Finally, in an emergency situation, health data may not be used by the patient himself, therefore patients' authorization for emergency

* Corresponding author.
E-mail addresses: byuksel13@ku.edu.tr (B. Yüksel), akupcu@ku.edu.tr (A. Küpçü), oozkasap@ku.edu.tr (Ö. Özkasap).

http://dx.doi.org/10.1016/j.future.2016.08.011
0167-739X/

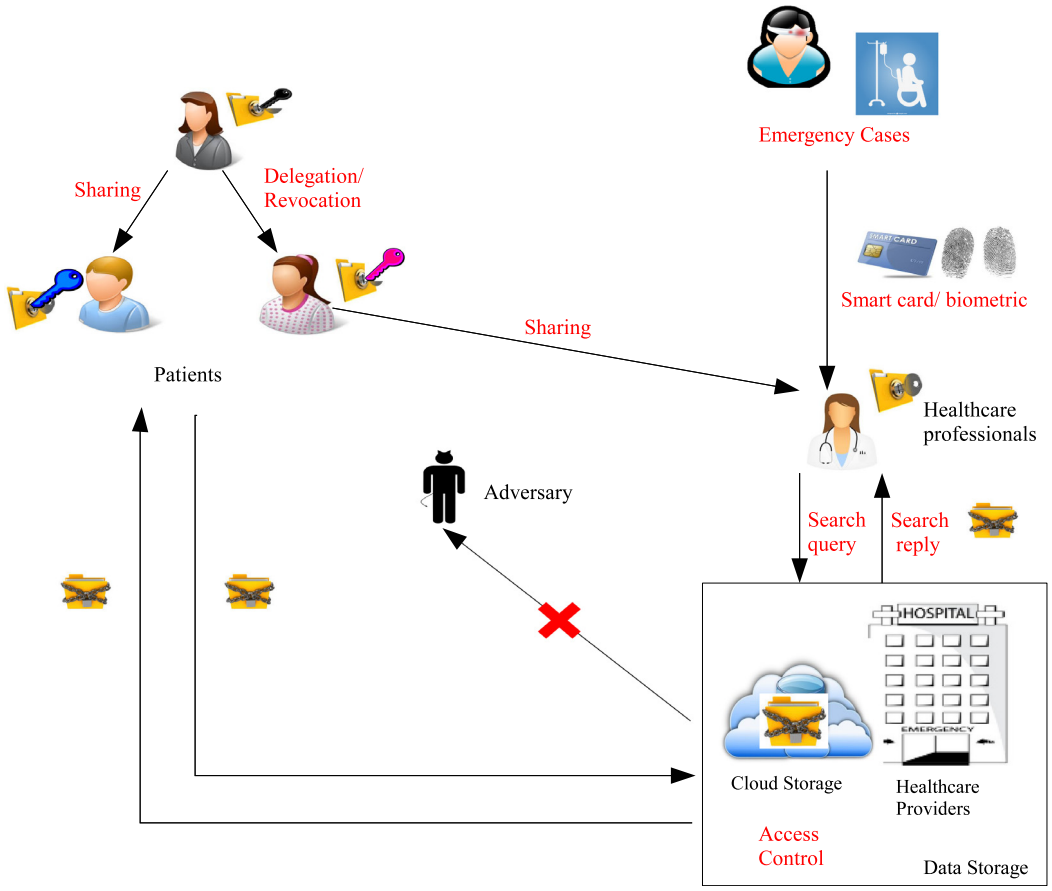

Fig. 1. Electronic health services overview.

cases must be addressed in EHS via mechanisms such as smart cards, biometrics, or trusted parties.

Our focus in this survey is to provide a novel method-based classification of state-of-the-art solutions regarding privacy and security of EHS. Our approach is named as *method-based*, because we first identify commonly used cryptographic methods for EHS, and then group the solutions in the literature according to these specified methods. As shown in Fig. 2, we identify and propose six general service categories to investigate the existing solutions.

- **Architecture** is one of the most important design issues of the proposed healthcare services. Since patients' health data are distributed to multiple entities such as hospitals, healthcare centers, and cloud servers, centralized solutions would not be convenient. Considering the nature of health data, we categorize EHS architectures into two groups, namely *distributed* and *cloud*. Distributed architecture requires methods for providing trust management. We present two solutions commonly used for trust management in distributed systems, namely Hierarchical Identity-Based Public Key Infrastructure (HIB-PKI) and credential-based access control. We also describe cloud architecture types, which are public, private, hybrid, and community. Moreover, we state three types of servers used in cloud architecture, which are trusted, semi-trusted, and untrusted.
- **Access control** encompasses techniques that provide selective restrictions to the data. We identify *role-based, attribute-based*, and *identity-based* access control techniques as commonly used solutions in the proposed healthcare systems. In the role-based access control technique, users are assigned certain roles to access sensitive health data. In addition to the traditional role-based systems, time-bounded functionalities are used to increase privacy and security of EHS. For attribute-based access control, there exist cryptographic and non-cryptographic approaches. Cryptographic approaches are Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and Key-Policy Attribute-Based Encryption (KP-ABE). Besides, we consider a non-cryptographic approach, which refers to the systems having a trusted third party that holds the private keys and gives the keys to the authorized users when necessary. The third access control method is Identity-Based Access Control (IBAC). In this method, identity-based encryption (IBE) is used, which employs users' identity information for encryption.
- **Emergency** characteristics of EHS focus on the consent exceptions when patients are unable to control their health data. In an emergency situation, legal actions must be taken, privacy protection must be provided, and consent exceptions must be given with a fine-grained approach. We identify *private-key storage, smart card usage, emergency responder*, and *break-glass approach* as the methods proposed for privacy-concerned EHS, when a patient has an emergency situation.
- **Sharing** is one of the most important characteristics of healthcare systems. Data can be shared among healthcare providers, hospitals or health organizations. Besides, patients can share their health information and treatment of their illnesses in social environments. Similarly, some social environments let doctors share their suggestions about specific illnesses related to their professional area. Sharing in EHS involves complex authentication and access control techniques. We present some important sharing characteristics of the proposed healthcare services, which are *source verifiability*, *total sharing*, *selective sharing*, and *social sharing*.
- **Search** is another significant function of EHS. *Proxy encryption* and *public-key encryption* are some of the encryption techniques

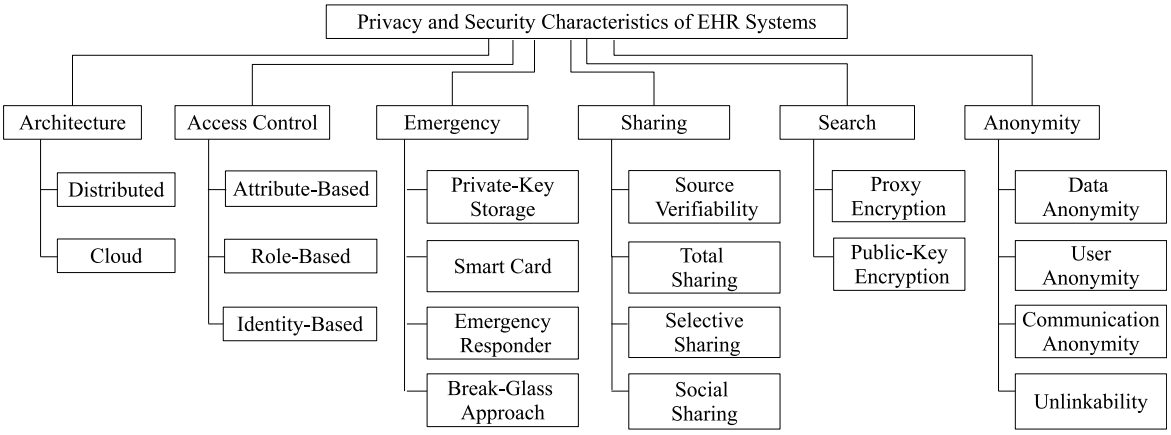

Fig. 2. Classification of privacy and security characteristics in proposed EHS.

Table 1
Comparisons with the other EHS related surveys.

Reference	Cryptographic approach	Business approach	Access control	Sharing	Search	Anonymity	Emergency	Open problems
[2]	+		+	+				
[3]	+	+	+	+		+	+	
[4]		+		+				
[5]		+	+	+		+		+
[6]	+	+	+	+		+	+	+
[7]		+		+				
[8]	+	+	+	+		+	+	
Our survey	+		+	+	+	+	+	+

used for searching specific data securely. These encryption techniques enable the server to return answers of the queries in encrypted format. If users have the corresponding key, they can decrypt the specific data.

- **Anonymity** methods can be used in EHS to keep the identity of users, contents of health data, and information about communication secret from unauthorized third parties. We identify four types of anonymity: *data anonymity*, *user anonymity*, *communication anonymity*, and *unlinkability*.

1.1. Related work

There exist prior studies providing survey of e-healthcare services with a focus on security, privacy, and integrity features. In prior work, as shown in Table 1, different aspects are considered regarding techniques used in healthcare systems. Some of the surveys focus on cryptographic approaches (e.g. cryptographic access control techniques, sharing health data, or anonymization of health data) [2,3,5,6,8]. Another group of studies considers business approaches (e.g. HIPAA rules, adoption and attitudes of healthcare providers, patients' opinions about EHS) of existing systems [4,7]. On the other hand, most of the related surveys present access control and sharing techniques of healthcare systems without going into details of cryptographic issues [2–6,8]. Some prior studies review healthcare systems that use anonymity techniques [5,6,8]. Furthermore, there exist few studies that consider emergency scenarios [3,6,8] and some of them discuss open research problems [5,6].

In contrast to prior work, we categorize and evaluate state-of-the-art electronic health services considering their cryptographic approaches. Our survey differs from previous studies in being method-based and covering all privacy and security approaches proposed for EHS. We first identify categories as architecture, access control, emergency cases, sharing, search, and anonymity methods, and then for each category we explain existing methods and the research based on these methods. To the best of our knowledge, no prior survey has considered search methods in the context of privacy and security. Different from the recent EHS related surveys [6–8], our study systematically covers all aspects and methods of privacy and security in EHS. Although a recent survey focuses only on mobile healthcare technologies [6], our work considers general healthcare services *including* mobile healthcare technologies. While we categorize all privacy and security related issues with a method-based approach in detail, [8] explains in an article-based approach, does not state details of the methods, and does not cover search techniques in healthcare systems and open problems. On the other hand, while [7] considers business approach of EHS, our survey addresses cryptographic approaches of EHS.

1.2. Our contributions

As the main contributions of this paper, we:

- present state-of-the-art approaches regarding security, privacy, and integrity aspects of EHS.
- Systematically analyze and evaluate the systems with a **method-based** approach, and lay out a comprehensive survey of **cryptographic** approaches of EHS.
- Consider components, characteristics, and challenges of e-health services.
- Categorize state-of-the-art studies according to their architecture, access control, emergency cases, sharing, search, and anonymity techniques.
- Discuss open problems and provide future directions for enhancing security and privacy of EHS.

The remainder of the article is structured as follows. Section 2 presents the review of the **architectural** aspects of EHS. Section 3 describes the **access control** techniques proposed for healthcare systems. Section 4 presents the proposed methods for EHS to preserve privacy of the users when an **emergency** situation happens. Section 5 presents **sharing** functionality and provides

comparisons for the proposed sharing methods. Section 6 presents **search** techniques that can be suitable for the application of EHS. Section 7 describes the **anonymization** approaches of EHS. Finally, Section 8 presents the **open research problems** about e-health services related to privacy, security, and integrity of the health data, followed by concluding remarks in Section 9.

2. Architecture

We present two types of architectures used in EHS, which are distributed and cloud. We do not specifically discuss centralized architecture because privacy and security research issues are prevalent in decentralized settings and the techniques for providing privacy and security can be easily applied to a centralized setting. Furthermore, decentralized architecture is the most common and practical one among the proposed e-health services. As a centralized architecture example, Microsoft developed HealthVault, using which patients can search and share their health data or allow healthcare professionals to track their data while data privacy and security are provided [9].

2.1. Distributed

Distributed architecture refers to a collection of independent computers that each has a role in information processing, but it appears as a single, integrated system to the users. In EHS, distributed architecture is commonly used due to the distributed nature of healthcare data. Since patients' EHS data is stored by multiple institutions, a distributed EHS architecture becomes a realistic approach.

In some distributed EHS proposals, the architecture consists of two levels. Local hospitals are located at the first level. Patients go to the nearest local hospitals and store their EHS data. These local hospitals are responsible for storing patients' data securely and do not depend on each other. In the second level, there is a main server. The main server does not store all the data of local hospitals. However, when a patient visits another hospital to get treatment from a different doctor, patient's relevant EHS data is sent to the main server. An important issue is that EHS data must be securely sent to the main server, and SSL/TLS can be used for this purpose. Then, other local hospitals can access the patient's data after logging in to the main server. This approach is shown to reduce the security and privacy concerns [10].

When distributed architectures of EHS are considered, trust management is one of the most important issues for the patients' sensitive data. **Trust management** is an approach to establish the trust between parties so that these parties can interact with each other. As a sub-part of trust management, **trust negotiation** method enables an entity to gain access to the local resource of another entity, through the use of credentials. We present two different methods that are used to apply trust management in distributed EHS systems.

The first solution is to use **Hierarchical Identity-Based Public Key Infrastructure (HIB-PKI)**. In this method, there is a hierarchy for the domains. A department called Health and Human Services is located at level 0, health information organizations are located at level 1, hospitals are located at level 2, and doctors are located at level 3 in the hierarchy. When healthcare providers would like to share health information with another provider, authentication must be performed until the top level in the hierarchy [11].

The second solution is establishing the trust management between domains according to **credential-based access control** [12]. In credential-based access control, there exists a trusted authority that issues the users' credentials and there is a hierarchy like HIB-PKI. In EHS, a central service that stores the patients' identities is located at the top level, a health service is located at the second level, and hospitals are located at the third level. When a patient is unable to direct his EHS information (e.g. while in coma) and his doctor accepts to assign one of the patient's relatives as his agent on the health service, first the patient's relative sends a request to the hospital. Then, the hospital sends a request to patient's health service and the health service requests the hospital's health organization credential. After these credential confirmations, the health service sends agent credential to conclude that the hospital delegated the patient's relative as the patient's agent. When the emergency situation ends and the patient wants to handle his own data, his doctor can deactivate the relative's role and activate the patient's role again [12].

Table 2
Server types in cloud architecture.

Reference	Trusted	Semi-trusted	Untrusted
[17]	+		
[18]	+	+	
[24] [25] [33] [19] [28] [31] [34] [22] [29] [23] [30] [20] [32] [21]		+	
[26] [27]		+	+

2.2. Cloud

Cloud architecture consists of a set of remote servers that allows data storage and online access to data. There are four types of cloud architectures, namely *public, private, hybrid,* and *community*. In the **public cloud** model, all servers in the cloud infrastructure are publicly available to use. A **private cloud** is a cloud model that only a specific organization can use. A **hybrid cloud** allows to use private and public clouds together, and a **community cloud** is a cloud model that only a specific group of organizations can use [13–16].

Cloud environment is an appropriate platform to store and share EHS data due to its advantages such as cost effective services, providing scalability, easy implementation, and reaching and handling the data easily. However, privacy protection of EHS data in the cloud architecture is a major security issue.

Several studies use cloud environment in their EHS frameworks, however their assumptions about servers and architectural privacy-related issues differ in the proposed solutions. In addition, although most of the prior work do not specifically state the cloud type, we infer that they mostly assume *public* clouds.

As shown in Table 2, we consider three types of servers in the cloud architecture: trusted, semi-trusted (honest-but-curious), and untrusted. **Trusted server** refers to a server that is fully trusted, and while applying the specified protocol, the server is assumed to never get any information about the stored data [17,18]. **Semi-trusted (honest-but curious) server** means that the server does exactly what the protocol says, but at the same time it may want to learn additional information from the protocol [19–25]. **Untrusted server** means that the server is not trusted, and without access control techniques and privacy protection; it would not be suitable

Table 3
Access control techniques in proposed EHS.

Reference	Role-based	Attribute-based		Identity-based
		Cryptographic	Non-cryptographic	
[36] [12] [37] [38] [39]	+			
[40]	+			+
[41] [24] [17] [26] [33] [28] [42] [43] [23] [21]		+		
[44]			+	
[11] [18]				+

to store the plaintext data, and hence proper encryption methods should be employed [26,27].

Some EHS are based on both private cloud and public cloud, assuming that private cloud server is considered to be totally trusted, whereas public cloud servers are considered to be honest-but-curious. In these systems, users outsource data processing tasks to private cloud and store the processed data on the public cloud [18]. On the other hand, another group of systems are based on public cloud services (e.g. Amazon EC2 servers) with the assumption that the servers are honest-but-curious [18,26–34]. Outsourcing health data to public cloud services includes more security and privacy concerns as compared to private cloud services. However, public cloud services (e.g. Amazon, Microsoft) spend more budget to provide a secure storage compared to most of the hospitals which may have limited budget and infrastructure to provide privacy for the health records. Therefore, it could be more convenient to use public cloud services for especially small hospitals and clinics [35].

3. Access control

Access control is a way of preventing or limiting access to a resource according to properties and requirements of the system. The purpose of access control techniques is that only authorized parties should contact the system and decrypt the data. Since EHS are dealing with patients' data, which is very sensitive, access control methods play a significant role. As shown in Table 3, we classify access control techniques for EHS into three categories, namely *role-based* access control, *attribute-based* access control, and *identity-based* access control.

Role-Based Access Control (RBAC) is an access control technique that restricts system access to unauthorized users according to their preassigned roles. In RBAC, members of the organization are assigned particular roles according to their qualifications and based on these roles, the system grants or denies access to each member. In healthcare organizations, roles are assigned according to jobs and responsibilities (e.g. physician or nurse). Access privileges of EHS data are given according to these roles. RBAC is considered to be well-suited in the systems where access control is provided according to qualification of users. Since permission is given according to roles, access control becomes easy to manage in the EHS. It is also easy to exclude, include, and delegate roles in RBAC rather than using traditional access control lists [45]. Therefore, RBAC is considered to be well-suited for EHS because of its **simplicity**, **efficiency**, and **scalability** properties [12,36–38,40].

In RBAC, users are assigned to functional roles (e.g. doctors, patients). A user can have many roles (i.e. a doctor can be a patient at the same time) and roles are assigned to healthcare operations. A doctor has permission to enter or update patients' information or the description of medical treatment [46]. Moreover, a doctor can send a patient's information to another doctor to provide different treatment. The disclosure decision of the healthcare data is made by considering the roles and the authorization policies in EHS [12,38,47,48].

In addition to traditional RBAC, time-bounded functionalities can be added to the EHS to increase privacy and security of the health data access. A role-based and time-bounded access control method where each role has a limited time to access the specific data is proposed in [39]. Since patients are the most important entities to decide over the roles for accessing their data, they are placed at the root of the hierarchy. Then, physician-in-charge is at the second level, and other physicians and nurses are at the lower levels according to their roles. Time parameters are added in the process of key generation, and the doctors in the higher hierarchy derive the key for the doctors in the lower hierarchy. Therefore, each doctor can access specific patient's data for a limited time. This hierarchy allows aggregation through the hierarchy and it is very suitable for EHS.

The second access control method is **Attribute-Based Access Control (ABAC)** where users can only access the system if they have the attributes that are desired by the system. In EHS, an *attribute* generally refers to property of an owner and the owner's EHS data, such as "illness", "age", and "gender" space [21]. We group ABAC into two types, which are *cryptographic* and *non-cryptographic*. In **cryptographic ABAC**, **Attribute-Based Encryption (ABE)** is used [16,17,21,23–26,28,33,41–44,49,50]. There exist two types of ABE: *ciphertext-policy* attribute-based encryption and *key-policy* attribute-based encryption.

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) [51] allows a user to encrypt a value using specific attributes, such that only users who own those attributes can decrypt the ciphertext and obtain the original value. Users' keys correspond to attributes, and the ciphertext corresponds to an access structure, which may be encrypted by a Boolean or threshold combination of those attributes (e.g. only those who have "doctor" and "researcher"

attributes can decrypt). In CP-ABE, there must exist a trusted authority who keeps a master secret key that can decrypt any ciphertext. The users obtain their attributes from the authority by proving their attributes (via a separate channel). Some CP-ABE schemes distribute this trust to multiple authorities [52]. When applied to the health context, attributes may correspond to proficiencies of the medical personnel, or the illnesses. For example, only cancer researchers may be able to decrypt a ciphertext that requires a "cancer" attribute. Several EHS use CP-ABE to realize efficient access control on healthcare data [17,23,41,53].

Key-Policy Attribute-Based Encryption (KP-ABE) [54] is another type of ABE. As opposed to CP-ABE, in KP-ABE, ciphertexts correspond to attributes and user's keys correspond to access structure. A ciphertext can only be decrypted by a key whose attribute set matches the private key's access policy. For example, if the access structure of a doctor's private key corresponds to "heart diseases" or "vascular diseases", the doctor can only access to the patients' data that has heart disease or vascular disease attribute. We can specify the **difference between CP-ABE and KP-ABE** as follows: in CP-ABE, there is an access tree for the ciphertext, whereas in KP-ABE, there is an access tree for the private key. KP-ABE also requires a trusted authority to manage users' key.

In **non-cryptographic ABAC**, there exist a trusted third party, which holds the private keys. When a doctor wants to view a patient's EHS data, he first needs to get authorization from the trusted third party, gets the key, and decrypts the data rather than satisfying attribute set of the patient's encrypted data [44].

The third access control method is **Identity-Based Access Control (IBAC)**. In the IBAC approach, users' identity information (e.g. name, e-mail address) is used for encryption via **identity-based encryption (IBE)**. When a person wants to send an e-mail to another person, the sender first encrypts the message with the receiver's identity (i.e. e-mail address). When the e-mail is received, the receiver gets authorization (i.e. decryption key) from the third party and then decrypts the message [55,56]. In EHS, doctors or patients can encrypt the data with the patient's identity information. When the patient wants to decrypt the data, he can similarly obtain his private key from the third party and can decrypt the EHS data. Some EHS studies use this approach [11,18,40].

The access control methods that we described above are mostly application specific and can exhibit varying performance depending on the infrastructure and requirements of EHS. However, there exist some common issues related to the usage of access control methods. First of all, if the EHS includes too many roles, it can be difficult to apply RBAC as an access control method as it causes low performance. Because the access control list will be overloaded and difficult to handle after some time [57]. In addition, whenever a role changes in EHS, access control specification needs to change as well. In IBAC, there is a third party holding all the private keys, which is needed to provide extra security. In addition, the third party must be always available to provide private keys to the users [58]. Therefore ABAC, even though still requires a trusted party, might be a better access control method, and usually shows better performance compared to other access control methods because of its simplistic control over data.

4. Emergency cases and consent exceptions

In addition to regular access control, emergency cases and how to consent the usage of EHS data in these cases are crucial concerns in EHS. Patients may not be able to handle their EHS data in an **emergency situation**; the patient can be in a coma or physically or mentally incapable. There can be smart card or biometric failure issues or patients can forget their user names/passwords when they do not use EHS for a long time [59]. Privacy and security of EHS data must still be protected in an emergency situation. Healthcare professionals must access only the necessary data rather than the patients' complete health information. Furthermore, when the emergency situation ends, all consent exceptions must be revoked and nobody should access the sensitive data.

Consent exceptions can have different meanings in EHS. The patient can be a minor (who needs his parents or legal guardians to access and manage his EHS data), have mental illnesses, or have an emergency situation such that he cannot handle his own data. However, data needs to be disclosed to healthcare professionals in order to do the necessary treatment. Therefore, the patient needs someone else to access and manage his data. These situations are called consent exceptions [60].

In emergency situations, consent exceptions should be given carefully when the patient cannot control his EHS data [40]. As shown in Table 4, there exist different approaches proposed to handle the emergency cases and consent exceptions without abolishing the confidentiality of the data. We classify the proposed methods into four groups, namely *private-key storage*, *smart card*, *emergency responder*, and *break-glass*.

The first approach is to use a **private-key storage**. In this approach, all private keys of the patients in the EHS are stored in a trusted server and EHS data can be decrypted in an emergency case, similar to a key escrow system. In the proposed systems, to encrypt and decrypt the EHS data, patients should first obtain a key from a healthcare certification authority. If the patient is in a coma while all EHS data is encrypted or if doctors make treatment without knowing the allergic history or illness history of the patient, it can cause a great risk. In order to reduce such risks, key management of EHS data and recovering the key become important concerns. To recover the key in an emergency situation, the proposed system includes a healthcare certification authority (or a key escrow agent) and a server of healthcare provider. When an emergency situation happens, the certification authority recovers the patient's key and enables access to the necessary data [17,25,28,31,48,60–63].

The second approach is to use **smart cards** [48,60,61]. Smart cards are small and functional devices that are used to identify a user in a system. Smart cards are generally used with additional information which has a functionality to enable the smart card. The card user is the only one that knows the additional information. Therefore, even if the card is stolen, nobody can provide the additional information. In order to provide secure and privacy-concerned EHS, using smart cards is one of the possible solutions where the patients can use smart cards to access their EHS data. However, accessing data in an emergency situation can be a problem. Because, the patient needs to provide additional information in order to activate the smart card and that may not be possible in an emergency situation. Therefore, there must be key recovery processes and necessary information should be revealed to the healthcare professionals in the emergency cases [60].

In some real world EHS applications, smart cards are used with an identification number (PIN). While using smart card in EHS, a patient needs to provide three personal pieces of information that only he knows (e.g. password, PIN), a smart card belongs to the patient himself, and biometric data [65] (e.g. fingerprint, iris) of the patient. Smart cards also have capability to apply access decisions of patients [66].

The third approach is to use **emergency responder**. Since patients cannot manage their own data in an emergency case, a trusted person (namely emergency responder) is allowed to manage their EHS data. In this approach, there is a trusted responsible person in the hospital who provides patients' necessary EHS data for the treatment in an emergency situation. Emergency responder must only be active for a limited duration of time in order to protect patients' privacy [40,44].

The fourth approach is to use the **break-glass** method in the emergency situations. Basically, break-glass solution is used to

Table 4
Emergency case methods in proposed EHS.

Reference	Private-key storage	Smart card	Emergency responder	Break-glass
[62]				
[63]				
[17]				
[25]	+			
[28]				
[31]				
[48]				
[60]	+	+		
[61]				
[44]				
[40]			+	
[24]				
[26]				
[64]				+
[23]				

break access controls not only in emergency cases but also in other unexpected situations such as when the patients forget their user name/password to enter the EHS or there can be problems on their smart cards or biometric information [59]. In the proposed approaches, at the beginning of the EHS data creation, the patient enters *emergency attributes* to the system and with these attributes the patient also creates a *break-glass key* and sends this key to the emergency department.

When an emergency case happens, the emergency department sends the patient's key to the medical staff and they can reach the patient's data temporarily. During the break-glass period, patient's data is audited. When the emergency situation ends, the patient can cancel other people's access to his data [23,24,26,64]. In some real world EHS applications, there exist a break-glass button for healthcare professionals. When the doctor presses the break-glass button for a specific patient, they can access all of the patient's sensitive data. The system and actions are monitored and audited in order to control data access.

Access control in emergency cases must always be carefully handled with one of the methods discussed above. However, there exist some drawbacks for each of these methods. Server/biometric system failures, account problems, forgotten smart card information, losing smart cards, and security concerns can always be an issue for the patients. Although break-glass approach can also have some problems, it is more commonly used, and it mostly shows better performance compared to other methods. Because in an emergency situation, break-glass solution can become available quickly without any latency. However, it is important that patients' data must be audited and view-only so that in an emergency situation each action of medical staff is recorded and no one can change the original health information [59].

5. Sharing

Patients, doctors, and other healthcare workers electronically **share EHS data** among each other. The important concern is EHS data sharing must be done by considering security and privacy issues. One may think of emergency as a special case of sharing. In modern EHS, patients are able to share their information with several healthcare professionals including doctors, research institutes, and insurance companies using various system settings (including social EHS). Hospitals, research institutes, and healthcare workers may also need to share patients' data with other parties.

We divide sharing characteristics of EHS into four categories, namely *source verifiability*, *selective data sharing*, *total data sharing*, and *social sharing*, as shown in Table 5.

The first characteristic, **source verifiability**, is related to the patients' attributes and verification of the patients' health information by an authority in the system. There exist two approaches for source verification. The first approach is *verification of the patients' attributes* (which we can call *attribute verification*) [42], and the second approach is the *verification of the patients' health information* [44]. In these systems, there exist a central authority, which decides and verifies the patients' attributes (e.g. name, age) or health information (e.g. illnesses) in terms of correctness, reliability, and validity.

We present two different approaches related to sharing type, which are selective data sharing and total data sharing. **Selective data sharing** means sharing a desired part of the data with authorized users [34,62]. As an example in this category, selective sharing with the help of Patient Controlled Encryption (PCE) is proposed [62]. In PCE approach, each patient has a root secret key and generates multiple subkeys from this root key. The patient encrypts his different EHS data portions using different subkeys (e.g. dental records employ a different key from optometry records). When the specific portion of the data should be decrypted, the corresponding subkey is used. PCE provides patients the ability to *selectively share* their EHS data [62]. There exist some methods that use selective sharing approach in their EHS [11,62].

On the other hand, in **total data sharing**, the patient can share his whole data with a healthcare professional but the patient cannot select a specific data portion. In other words, total data sharing is an atomic approach, where the patient either shares the whole data or shares nothing with other users [21,23,32,37,42–44,64].

Another sharing approach, namely **social sharing**, refers to the scenario where patients or doctors share their health data or professional experiences in health-specific social environments. In social environments, patients share information about their illnesses and doctors can help patients online according to their professional area [32,43]. In some cases, patients and doctors see each other's profile based on their common attributes. If two patients do not have common attributes, they cannot communicate with each other and share their data. The social network server first calculates the attribute intersection value between patients (the attributes are patients' symptoms in this case). Then, if the attribute intersection value is higher than some predefined threshold, patients can reach each other's data [21]. Likewise, a scheme where each user has a trust score in the social EHS environment is proposed [32]. There are some metrics for patients (e.g. availability, popularity, participation of the user in the social environment). A trust score is calculated as a weighted sum of these metric values (where weights are assigned by the user between 0.1 and 0.9). The user whose trust score is low can trust a

Table 5
Main characteristics of proposed EHS sharing.

Reference	Source verifiability	Selective data sharing	Total data sharing	Social sharing
[44]				
[42]	+		+	
[62]				
[34]		+	+	
[37]				
[64]			+	
[43]				
[32]			+	+
[21]				

user who has a higher trust score in the social EHS. Trust score helps patients to determine with whom they share their health data [32].

When we consider the nature of health data, selective sharing and source verifiability are two commonly used sharing characteristics. Sharing the desired part of the health data is obviously a more convenient and privacy-concerned action compared to sharing the entire health data. Therefore, an EHS having a selective sharing option is preferred over the EHS which does not let patients share the desired part of the data. Likewise, EHS having source verifiability characteristics is preferred as opposed to those without this option. Lastly, although social sharing is a great opportunity for many patients and doctors to share health information, it is very important to provide secure and privacy-concerned social environments.

6. Search

Whenever data is shared, naturally, it is also searched. **Searching data** in the server is one of the important functions of EHS. Patients' data is encrypted and stored in a server. When patients, doctors, or researchers need to search the data, the server should return not more than the queried data and ideally should not learn anything about the query [19]. A basic EHS search scenario is shown in Fig. 3.

We can divide search scenarios into two parts: *searching in the plaintext* form of data and *searching in the encrypted form of data*. Searching techniques in the plaintext are well-studied, and are not in the scope of this study. However, in order to search in the encrypted data, several cryptographic schemes are proposed. As shown in Table 6, we present approaches and methods that support search over the encrypted data.

In the first approach, the clients encrypt the data before uploading it to an untrusted server and **when a search is requested, the client retrieves the entire encrypted data from the server, decrypts it**, and gets the specific data needed. Communication security between user and the server is provided by SSL/TLS. This approach is secure against attacks on the server side. The server cannot extract anything from the stored data. However, it is very inefficient because for a specific portion of the data, the client needs to get *all* the data. In some studies, secret sharing methods are used to prevent cloud providers from accessing the stored data. Since each cloud provider has different data shares, they cannot access the whole data [67]. This approach is also inefficient when search is needed. Because in order to search data, we need to first combine the data shares from cloud providers, and then search for a specific data. Since an EHS server includes several patients' data, it would not be logical to apply this method for searching multi-patient EHS records when the privacy and efficiency issues are considered.

Searchable symmetric encryption (SSE) allows users to encrypt their document with an additional data structure, called index, and store in the server. Users can search over the encrypted data by selecting some keywords and generating corresponding search tokens via a secret key. The server searches over encrypted index and returns the specific data that includes the user's keyword [68]. However, **SSE is not preferred as a search method in EHS**. The most important reason is the **key management issue**. Since SSE is a *symmetric* system (if someone can encrypt the data with a key, they can also decrypt it with the same key), when a doctor wants to store a patient's health data in a server, the patient has to give the encryption/decryption key to the doctor. Therefore, the doctor can see patient's entire data with this key [62].

Table 6
Search methods in proposed EHS.

Reference	PEKS	Proxy encryption
[62]		
[17]		
[11]	+	
[40]		
[70]		
[71]		+

The second approach is using **public key encryption with keyword search (PEKS)**. It is used to find out if a document includes specific keywords or not without identifying the content of the document. PEKS was firstly used in the e-mail services in order to determine if an e-mail includes a given keyword or not without revealing any information about the content of the encrypted e-mail [11,69]. In EHS, a doctor encrypts the patient's EHS data with the patient's public key and stores it in the server. Then, when a search is needed, the server replies if encrypted document includes the specified keyword or not without learning anything more about the content of the data. This approach is used for searching in encrypted format of EHS data and it guarantees minimum necessary data access [40]. In addition, PEKS algorithms are combined with hierarchical IBE [11,62] or ABE [17] to search over encrypted EHS data (see Section 3). PEKS is combined with hierarchical IBE in [62] where hierarchical IBE enables patients to share their data selectively in the EHS. Different types of illness categories are encrypted and shown in a hierarchy. The person who is given access to specific data portion is also eligible to search in it using PEKS. Likewise, the approach in [11] uses hierarchical IBE for encryption and PEKS for the keyword search in health data. On the other hand, work of [17] uses ABE to provide encryption using attributes of the users and uses PEKS for keyword search in EHS data.

The third approach is **proxy encryption**. In a proxy encryption scheme, there exist a proxy function that transforms a ciphertext to another ciphertext that is encrypted with a different key. Proxy functions change the ciphertext without revealing any information [72]. In the context of EHS, if a patient wants his relatives to access his data, he can use a proxy function to change the ciphertext to one that can now be decrypted with another private key, and sends this modified ciphertext to his relative.

Fig. 3. Searching data in proposed EHS.

By using the proxy function, the patient can prevent his relatives from learning his own private key. However, proxy encryption is not collusion-safe [70,71]. Collusion-safe means that if two or more users combine their keys, they cannot decrypt the data. In a proxy encryption scheme, it is possible to collude with the server, combine keys, and decrypt the data [71].

Some other access control techniques can be combined with the proxy encryption scheme. There exist systems that combine proxy encryption scheme with ABE [73,74]. In the proposed systems, users have some attributes and store their data in a cloud environment. When they want to share their EHS data with someone, they use proxy encryption scheme. However, when the user wants to revoke the access rights, revoked user still has the previously assigned key. If the user does not re-encrypt the ciphertext immediately, revoked users can still access the data after revocation time. Therefore, in order to reduce the workload of the user, cloud service provider does all the necessary tasks. When the user wants to revoke someone's access rights on the data, he sends proxy re-encryption key to the cloud service provider. Then, the cloud service provider re-encrypts the ciphertext. The drawback of this approach is that the user has to be online to send proxy re-encryption key to the cloud service provider in order to end the access time of the other user. To address this problem, [53] presents a time-based proxy encryption scheme to revoke the access time of the sensitive data automatically. Data is stored using ABE and all the users have an access time attribute in addition to their own attributes (e.g. doctor, nurse). Since the data owner declares the allowed access time of the other user at the beginning, the workload of user is reduced and the user does not have to be online all the time. A patient can decide the access time of his doctor at the beginning and use time-based proxy encryption scheme to end the doctor's access to the health data automatically. This approach can be used as an efficient solution for EHS.

As mentioned above, SSE is not commonly used in EHS because of the key management issues. However, PEKS and time-based proxy encryption systems show better performance in terms of security, privacy, and access times. PEKS approach guarantees minimum data access and provides keyword search in encrypted format [40]. Time-based proxy encryption scheme provides a system where users do not have to be online all the time to revoke someone's access/search rights on the data. Therefore, PEKS and time-based proxy encryption schemes are commonly used in EHS that supports search functionality.

7. Anonymity

In addition to protect the data, users may want to remain anonymous in an electronic healthcare system. **Anonymity** means that the identity of a user is unknown in the system [75]. In EHS, anonymization is necessary for many reasons. As shown in Fig. 4, it can be used to provide statistics about medical data without revealing the identities of the patients, and it also helps to hide the identity of the patients from some institutions (e.g. insurance companies). In addition, unauthorized third parties should not learn the communication between the patient and the EHS.

When patients enroll in local hospitals, they are asked to submit their personal preferences about data privacy, and declare their preferences about usage of health data such as whether they want to share personal health data with governmental organizations, research institutes, or not. In addition, they can prefer to share their data with academic organizations for research purposes but not with medical companies. However, sometimes hospitals' data privacy policy may include sharing health data with governmental organizations for legal cases or to prove patient's disability (if it exists). Therefore, hospitals must declare this policy content to the patients and get their permission to before sharing health data to governmental organizations when required [76].

EHS data usage can be classified based on their primary usage and secondary usage. **Primary usage** of EHS data is for patients' individual care and treatment. **Secondary usage** of EHS is for the medical research or actions that can improve the quality of healthcare. For example, a patient goes to a hospital and gets treatment about a specific illness (e.g. cancer). Patient's physician stores the EHS data and medicines that the patient used. This is a primary usage of EHS data. On the other hand, data of groups of cancer patients in a specific geographic region can be used by the physicians to conduct a statistical research. This is an example of secondary usage of EHS data. Especially for the secondary usage of EHS data, it is crucial to provide anonymization [77].

As shown in Table 7, we present four approaches of anonymization for the proposed EHS: *data anonymity*, *user anonymity*, *communication anonymity*, and *unlinkability*.

The first approach is **data anonymity** which is provided if nobody can establish a relationship between a user and the user's specific data in EHS [78]. For example, in some EHS (especially in social EHS), instead of using their own identity, patients or doctors use *pseudonyms* to interact with each other. In these systems, nobody should be able to establish a relationship between attributes and the identity of the patients or doctors. However, patients and doctors must prove that they actually have those diseases or they are doctors in real life [42], respectively. *Zero-knowledge proofs* are used to provide data anonymity. With these methods, it is possible to prove that a statement is true without giving any additional information [42,79].

The second approach is **user anonymity** which is provided if a user's messages do not reveal any information about his/her identity [78]. In EHS, patients' identity should be protected. For example, there can be some research about the statistics of cancer patients. While gathering these statistics, patients' identity must be anonymous. Some solutions use *pseudo anonymity*. In this technique, there is a trusted third party that accesses the patient's data and replaces his/her identifier with a value, which cannot be traced to find patient's identity [42,67,80–85]. For example, the value that is given to the patient can be the symmetric encryption of the patient's identifier. If the key is kept secret, it is impossible to invert the pseudonym to the patient's identifier [86]. In some solutions, identifier hash is used to create pseudo-identifiers of the patients [83,84].

In addition, PIPE (Pseudonymization of Information for Privacy in E-health) [88] provides user anonymity for secondary usage

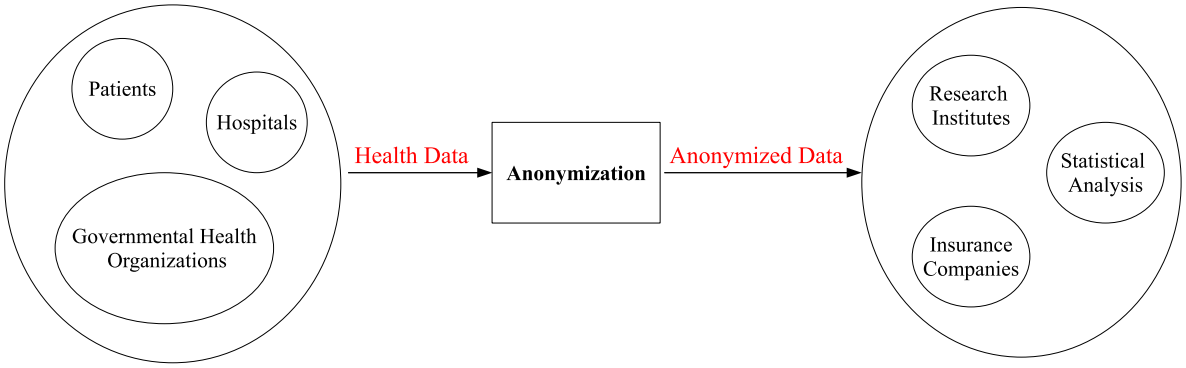

Fig. 4. Anonymization in proposed EHS.

Table 7
Anonymization methods in EHS.

Reference	Data anonymity	User anonymity	Communication anonymity	Unlinkability
[79]	+			
[85] [80] [82] [83] [81] [84]		+		
[42]	+	+	+	+
[87] [67]		+		+

of EHS data. This method hides the link between EHS data and patient's identity. When EHS data is stored, it is divided into two parts, which are patient's personal data and pseudonymized EHS data. The patient controls his EHS data and he has full access on his data. PIPE includes three layers. In the outer and the middle level, there exist some asymmetric key pairs used for authenticated users to decrypt the data. Third level (concealed level) includes pseudonyms. Pseudonyms are assigned to the patient's data for the secondary usage in order to hide the link between personal information and the EHS data [89].

The third approach is **communication anonymity**. Communication anonymity provides privacy by hiding the link between the user and the system [78]. In some solutions, collision-resistant pseudonyms are used to provide anonymous communication similar to the user anonymity [42]. Onion routing is one of the popular techniques that provides anonymous communication. In onion routing, a message is encrypted many times and sent over the network. Data passes through several onion routers until it reaches the destination. Each onion router decrypts the message, determines where to send next, and sends the data to the next onion router until it reaches the destination [90]. Each router only knows the next one, an no one knows the whole communication path; in particular, the sender and the receiver cannot be linked by any single participant. Although onion routing provides anonymity when a message is sent, the information about how much anonymity is provided cannot be known unless a model that records network traffic through the connection exist [91]. Tor is a state-of-the-art onion-routing system that can be used in practice [92]. To the best of our knowledge, there is no EHS that uses onion routing for communication anonymity.

Providing unlinkability is one of the most important properties in anonymous systems. **Unlinkability** means that an adversary who tracks the data transaction between some senders and a receiver cannot establish a relationship between any data and sender [86,93,94]. There are different methods to provide unlinkability in systems. [42] presents a system such that healthcare professionals use different pseudonyms and different commitments for attributes at each communication. Therefore, an attacker who observes the communication between healthcare professionals cannot determine which attribute belongs to which identity. In some studies, a cryptographic hash function is calculated on the concatenation of internal identifiers such as patient-id, health center-id, and share-id. Since hash functions are hard to invert, it is hard to find a patient's identity by an attacker or a cloud provider [67,87]. However, such schemes may be vulnerable to dictionary attacks on patient and healthcare provider identifiers. If the authentication method does not provide anonymity, the attacker can easily link the pseudonym to the holder of the pseudonym.

In addition to the aforementioned techniques, **differential privacy** may be used in EHS. Differential privacy aims to provide privacy by adding noise to the data. In this manner, anonymity of the person is provided but still some statistics can be extracted from the data [95,96]. For example, if there is a research about the people who have heart disease, the researcher should not learn anything about the patients' identity, but is allowed to learn some statistical results from the data, such as the patients' average age. Since adding noise to EHS data makes the research error-prone, other anonymity techniques are used rather than differential privacy in EHS [96,97].

All types of anonymity techniques are profoundly important for EHS. Patient identity, content of health data, and communication among patients must be anonymous to provide privacy in the system. As we stated before, application of differential privacy requires adding noise to the data and this method is difficult to apply on the health data. However, PIPE, which shows good performance on hiding the link between EHS data and patient's identity is commonly used [88].

8. Open issues and guidelines

In this section, we present several research questions about privacy, security, and integrity considering our categories in EHS.

Architecture is an important design aspect of EHS. Since it is mostly difficult to store healthcare data in a centralized way, there exist two different architectures that are used in EHS: distributed and cloud architecture. We identified two major research questions regarding the **architecture** related issues:

1. In a distributed health data architecture, how does the EHS efficiently inform the patients about who is using their data and why?

2. In a cloud environment, how can patients be sure that their privacy is protected by cloud providers? Which data is allowed to be disclosed for statistical analysis by cloud providers?

Access control is an important aspect of privacy-preserving EHS. We presented state-of-the-art proposed methods of access control, mainly based on roles, attributes, and identities. Open research questions inspired by **access control** features are:

1. Which access control methods are the most efficient for the EHS?

2. Which access control method is more efficient for the emergency situations?

Since EHS records contain very sensitive data, sharing is a very important concern for patients and healthcare professionals. When an emergency situation happens, EHS' functionalities are also crucial. Since sharing and emergency situations are related to each other, here we state open research questions inspired by both **sharing** and **emergency** features:

1. In an emergency case, when selective sharing is used in the system, how can the system decide which data should be disclosed to the responsible healthcare professionals?

2. In an emergency situation, how can patients allow the healthcare personnel to reach their health information?

3. Without assuming a healthcare trusted authority exists, how can it be possible to use smart cards in emergency situations?

4. How can biometrics be used by patients in an emergency situation?

5. How can we create an EHS that satisfies both source verifiability and selective sharing properties?

Search is another important aspect of EHS. There exist different methods that provide search in healthcare data. Based on these methods, we identified three major open research problems regarding the **search** mechanisms:

1. Can it be possible to create a privacy-concerned search method different than the proxy encryption and PEKS methods?

2. Is it possible to create collusion-safe proxy encryption scheme?

3. Is it possible to develop a proxy encryption scheme that uses semi-trusted or untrusted servers?

We also presented anonymization methods used in EHS. In order to provide privacy-preserving EHS, anonymity is an essential property. For instance, while making medical statistics about patients and illnesses, the system should not reveal patients' identities. When we consider **anonymization** methods, we identify the following open problems:

1. How can we provide unlinkability for patients' attributes in EHS?

2. Is it worth the cost to use onion routing algorithms to provide communication anonymity in EHS?

3. How can differential privacy techniques be applied to EHS, while obtaining meaningful results?

We categorized and evaluated research aspects of privacy and security in EHS, and discussed about the open issues based on their architecture and services including access control, emergency access, sharing, searching, and anonymity methods by considering their cryptographic approaches. Among these categories, some of them are more important and critical than the others. Access control is the most important functionality in any EHS. A system without secure and privacy concerned access control techniques cannot be used for sensitive health data. Privacy concerned emergency access methods and anonymity methods are also profoundly important for an EHS. However, sharing and search can be thought as optional functions and their absence does not cause privacy and security problems unlike access control function; they are complementary features increasing efficiency and usability of the EHS. Therefore, while sharing and search are the optional functionalities; access control, emergency access, and anonymity are crucial functions of EHS.

9. Conclusion

Electronic health services are increasingly used by patients, doctors, and other healthcare professionals. Although using EHS has several advantages, it brings several privacy, security, and integrity problems together. In this article, our key contribution is to present state-of-the-art approaches regarding security, privacy, and integrity aspects of EHS by considering the components and challenges of e-health services. We systematically evaluated the studies with a method-based approach, and provided a comprehensive survey of cryptographic approaches of EHS. Our major contribution is to categorize state-of-the-art EHS studies into different aspects, namely architecture, access control, emergency cases, sharing, search, and anonymity. In addition, we identified the open research problems of each category by stating different approaches, advantages, and disadvantages providing directions for future studies.

References

[1] D.C. Peel, Electronic health records vs. patient privacy: Who will win? 2012. http://www2.idexpertscorp.com/blog/single/electronic-health-records-vs.-patient-privacy-who-will-win.

[2] R.C. Barrows, P.D. Clayton, Privacy, confidentiality, and electronic medical records, J. Amer. Med. Inform. Assoc. 3 (2) (1996) 139–148.

[3] P. Ray, J. Wimalasiri, The need for technical solutions for maintaining the privacy of EHR, in: Engineering in Medicine and Biology Society, EMBS'06, 28th Annual International Conference of the IEEE, 2006, pp. 4686–4689.

[4] D.C. Kaelber, A.K. Jha, D. Johnston, B. Middleton, D.W. Bates, A research agenda for personal health records (PHRs), J. Amer. Med. Inform. Assoc. 15 (6) (2008) 729–736.

[5] A. Appari, M.E. Johnson, Information security and privacy in healthcare: current state of research, Int. J. Internet Enterprise Manage. 6 (4) (2010) 279–314.

[6] S. Avancha, A. Baxi, D. Kotz, Privacy in mobile technology for personal healthcare, ACM Comput. Surv. (CSUR) 45 (1) (2012) 3.

[7] S.P. Ahuja, S. Mani, J. Zambrano, A survey of the state of cloud computing in healthcare, Netw. Commun. Technol. 1 (2) (2012) p12.

[8] J.L.F. Alemán, I.C. Señor, P.Á.O. Lozoya, A. Toval, Security and privacy in electronic health records: A systematic literature review, J. Biomed. Inform. 46 (3) (2013) 541–562.

[9] A. Sunyaev, D. Chornyi, C. Mauro, H. Krcmar, Evaluation framework for personal health records: Microsoft HealthVault vs. Google Health, in: System Sciences (HICSS), 2010 43rd Hawaii International Conference on, IEEE, 2010, pp. 1–10.

[10] D. Patra, S. Ray, J. Mukhopadhyay, B. Majumdar, A. Majumdar, Achieving e-Health care in a distributed EHR system, in: e-Health Networking, Applications and Services, Healthcom, 11th International Conference on, IEEE, 2009, pp. 101–107.

[11] J. Sun, Y. Fang, Cross-Domain data sharing in distributed electronic health record systems, IEEE Trans. Parallel Distrib. Syst. 21 (6) (2010) 754–764.

[12] M.Y. Becker, P. Sewell, Cassandra: Flexible trust management, applied to electronic health records, in: Computer Security Foundations Workshop, 17th IEEE, 2004, pp. 139–154.

[13] S. Rajasudhan, R. Nallusamy, A study on cryptographic methods in cloud storage, Int. J. Commun. Comput. Technol. 2 (2) (2014) 1–5.

[14] P. Mell, T. Grance, The NIST definition of cloud computing, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg, 2011.

[15] Y.S. Lee, N. Bruce, T. Non, E. Alasaarela, H. Lee, Hybrid cloud service based healthcare solutions, in: Advanced Information Networking and Applications Workshops (WAINA), 2015 IEEE 29th International Conference on, IEEE, 2015, pp. 25–30.

[16] B. Balamurugan, P.V. Krishna, N.S. Kumar, G. Rajyalakshmi, An efficient framework for health system based on hybrid cloud with ABE-outsourced decryption, in: Artificial Intelligence and Evolutionary Algorithms in Engineering Systems, Springer, 2015, pp. 41–49.

[17] S. Narayan, M. Gagné, R. Safavi-Naini, Privacy preserving EHR system using attribute-based infrastructure, in: Proceedings of the 2010 ACM workshop on Cloud computing security workshop, ACM, 2010, pp. 47–52.
[18] Y. Tong, J. Sun, S.S. Chow, P. Li, Towards auditable cloud-assisted access of encrypted health data, in: Communications and Network Security, CNS, 2013 IEEE Conference on, IEEE, 2013, pp. 514–519.
[19] M. Li, S. Yu, N. Cao, W. Lou, Authorized private keyword search over encrypted data in cloud computing, in: Distributed Computing Systems, ICDCS, 2011 31st International Conference on, IEEE, 2011, pp. 383–392.
[20] K. Yang, X. Jia, K. Ren, B. Zhang, DAC-MACS: Effective data access control for multi-authority cloud storage systems, IEEE Trans. Inf. Forensics Secur. 8 (11) (2013) 1790–1801.
[21] F. Xhafa, J. Li, G. Zhao, J. Li, X. Chen, D.S. Wong, Designing cloud-based electronic health record system with attribute-based encryption, Multimedia Tools Appl. 74 (10) (2015) 3441–3458.
[22] M.R. Asghar, M. Ion, G. Russello, B. Crispo, ESPOON: Enforcing encrypted security policies in outsourced environments, in: Availability, Reliability and Security, ARES, 2011 Sixth International Conference on, IEEE, 2011, pp. 99–108.
[23] M. Li, S. Yu, Y. Zheng, K. Ren, W. Lou, Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption, IEEE Trans. Parallel Distrib. Syst. 24 (1) (2013) 131–143.
[24] M. Li, S. Yu, K. Ren, W. Lou, Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings, in: International Conference on Security and Privacy in Communication Systems, 2010, pp. 89–106.
[25] M. Deng, M. Petkovic, M. Nalin, I. Baroni, A home healthcare system in the cloud–addressing security and privacy challenges, in: Cloud Computing, CLOUD, 2011 IEEE International Conference, pp. 549–556.
[26] J.A. Akinyele, M.W. Pagano, M.D. Green, C.U. Lehmann, Z.N. Peterson, A.D. Rubin, Securing electronic medical records using attribute-based encryption on mobile devices, in: Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, ACM, 2011, pp. 75–86.
[27] H. Wang, Q. Wu, B. Qin, J. Domingo-Ferrer, FRR: Fair Remote Retrieval of outsourced private medical records in electronic health networks, J. Biomed. Inform. 50 (2014) 226–233.
[28] S. Alshehri, S.P. Radziszowski, R.K. Raj, Secure access for healthcare data in the cloud using ciphertext-policy attribute-based encryption, in: Data Engineering Workshops, ICDEW, 2012 IEEE 28th International Conference on, IEEE, 2012, pp. 143–146.
[29] Y.-C. Chen, G. Horng, Y.-J. Lin, K.-C. Chen, Privacy preserving index for encrypted electronic medical records, J. Medical Systems 37 (6) (2013).
[30] J. Li, Y. Bai, N. Zaman, A fuzzy modeling approach for risk-based access control in eHealth cloud, in: 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, 2013, pp. 17–23.
[31] T.-S. Chen, C.-H. Liu, T.-L. Chen, C.-S. Chen, J.-G. Bau, T.-C. Lin, Secure dynamic access control scheme of PHR in cloud computing, J. Medical Systems 36 (6) (2012) 4005–4020.
[32] Y. Bai, L. Dai, S. Chung, D.D. Devaraj, Access control for cloud-based eHealth social networking: design and evaluation, Secur. Commun. Netw. 7 (3) (2014) 574–587.
[33] M. Green, S. Hohenberger, B. Waters, Outsourcing the decryption of ABE ciphertexts, in: USENIX Security Symposium, 2011.
[34] R. Wu, G.-J. Ahn, H. Hu, Secure sharing of electronic health records in clouds, in: Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2012 8th International Conference on, 2012, pp. 711–718.
[35] H.A.J. Narayanan, M.H. Güneş, Ensuring access control in cloud provisioned healthcare systems, in: Consumer Communications and Networking Conference, CCNC, IEEE, 2011, pp. 247–251.
[36] R.S. Sandhu, E.J. Coyne, H.L. Feinstein, C.E. Youman, Role-based access control models, Computer 29 (2) (1996) 38–47.
[37] J. Hu, A.C. Weaver, A dynamic, context-aware security infrastructure for distributed healthcare applications, in: Proceedings of the First Workshop on Pervasive Privacy Security, Privacy, and Trust, 2004.
[38] D.M. Eyers, J. Bacon, K. Moody, OASIS role-based access control for electronic health records, IEEE Proc.-Softw. 153 (1) (2006) 16–23.
[39] R. Zhang, L. Liu, R. Xue, Role-based and time-bound access and management of EHR data, Secur. Commun. Netw. 7 (6) (2014) 994–1015.
[40] J. Sun, X. Zhu, C. Zhang, Y. Fang, HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare, in: ICDCS, IEEE Computer Society, 2011, pp. 373–382.
[41] L. Ibraimi, M. Asim, M. Petković, Secure management of personal health records by applying attribute-based encryption, in: Wearable Micro and Nano Technologies for Personalized Health (pHealth), 2009 6th International Workshop on, IEEE, 2009, pp. 71–74.
[42] L. Guo, C. Zhang, J. Sun, Y. Fang, PAAS: A privacy-preserving attribute-based authentication system for ehealth networks, in: Distributed Computing Systems, ICDCS, IEEE 32nd International Conference, 2012, pp. 224–233.
[43] X. Liang, M. Barua, R. Lu, X. Lin, X.S. Shen, Healthshare: achieving secure and privacy-preserving health information sharing through health social networks, Comput. Commun. 35 (15) (2012) 1910–1920.
[44] A. Mohan, D. Bauer, D.M. Blough, M. Ahamad, B. Bamba, R. Krishnan, L. Liu, D. Mashima, B. Palanisamy, A patient-centric, attribute-based, source-verifiable framework for health record sharing, 2009, Georgia Institute of Technology.
[45] J. Reid, I. Cheong, M. Henricksen, J. Smit, A novel use of RBAC to protect privacy in distributed health care information systems, in: Information Security and Privacy, Springer, 2003, pp. 403–415.
[46] D.F. Ferraiolo, D.R. Kuhn, Role-based access controls, in: 15th National Computer Security Conference, 1992.
[47] A. Al-Faresi, D. Wijesekera, K. Moidu, A comprehensive privacy-aware authorization framework founded on HIPAA privacy rules, in: Proceedings of the 1st ACM International Health Informatics Symposium, 2010, pp. 637–646.
[48] J. Bacon, K. Moody, W. Yao, A model of OASIS role-based access control and its support for active security, ACM Trans. Inf. Syst. Secur. 5 (4) (2001) 492–540.
[49] Z. Liu, J. Weng, J. Li, J. Yang, C. Fu, C. Jia, Cloud-based electronic health record system supporting fuzzy keyword search, Soft Comput. (2015) 1–13.
[50] G. Ramu, B.E. Reddy, Secure architecture to manage EHR's in cloud using SSE and ABE, Health Technol. 5 (3–4) (2015) 195–205.
[51] J. Bethencourt, A. Sahai, B. Waters, Ciphertext-policy attribute-based encryption, in: Security and Privacy, SP'07, IEEE Symposium, 2007, pp. 321–334.
[52] M. Chase, Multi-authority attribute based encryption, in: Theory of Cryptography, Springer, 2007, pp. 515–534.
[53] Q. Liu, G. Wang, J. Wu, Time-based proxy re-encryption scheme for secure data sharing in a cloud environment, Inform. Sci. 258 (2014) 355–370.
[54] V. Goyal, O. Pandey, A. Sahai, B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, in: Proceedings of the 13th ACM Conference on Computer and Communications Security, ACM, 2006, pp. 89–98.
[55] A. Shamir, Identity-based cryptosystems and signature schemes, in: Workshop on the Theory and Application of Cryptographic Techniques, Springer, 1984, pp. 47–53.
[56] D. Boneh, M. Franklin, Identity-based encryption from the Weil pairing, in: Advances in Cryptology-CRYPTO 2001, Springer, 2001, pp. 213–229.
[57] A. Cavoukian, M. Chibba, G. Williamson, A. Ferguson, The importance of ABAC: Attribute-based access control to big data: Privacy and context, 2015, Privacy and Big Data Institute, Ryerson University, Toronto, Canada.
[58] C. Youngblood, An introduction to identity-based cryptography, 2005, CSEP 590TU.
[59] J.N. Security, P.C. (SPC), Break-glass- an approach to granting emergency access to healthcare systems, Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC) Paper, 2004. http://www.medicalimaging.org/wp-content/uploads/2011/02/Break-Glass_-_Emergency_Access_to_Healthcare_Systems.pdf.
[60] W.-B. Lee, C.-D. Lee, A cryptographic key management solution for HIPAA privacy/security regulations, IEEE Trans. Inf. Technol. Biomed. 12 (1) (2008) 34–41.
[61] L.-C. Huang, H.-C. Chu, C.-Y. Lien, C.-H. Hsiao, T. Kao, Privacy preservation and information security protection for patients' portable electronic health records, Comput. Biol. Med. 39 (9) (2009) 743–750.
[62] J. Benaloh, M. Chase, E. Horvitz, K. Lauter, Patient controlled encryption: ensuring privacy of electronic medical records, in: CCSW, 2009, pp. 103–114.
[63] J. Hu, H.-H. Chen, T.-W. Hou, A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations, Comput. Stand. Interfaces 32 (5) (2010) 274–280.
[64] J. Jin, G.-J. Ahn, H. Hu, M.J. Covington, X. Zhang, Patient-centric authorization framework for electronic healthcare services, Comput. Secur. 30 (2) (2011) 116–127.
[65] A. Omotosho, O. Adegbola, B. Adelakin, A. Adelakun, J. Emuoyibofarhe, Exploiting multimodal biometrics in e-privacy scheme for electronic health records, J. Biol., Agricult. Healthcare 4 (2015) 22–33.
[66] S.C. Alliance, Smart card technology in us healthcare: Frequently asked questions, Smart Card Alliance, Estados Unidos, 2012.
[67] B. Fabian, T. Ermakova, P. Junghanns, Collaborative and secure sharing of healthcare data in multi-clouds, Inf. Syst. 48 (2015) 132–150.
[68] R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky, Searchable symmetric encryption: improved definitions and efficient constructions, in: Proceedings of the 13th ACM conference on computer and communications security, ACM, 2006, pp. 79–88.
[69] D. Boneh, G. Di Crescenzo, R. Ostrovsky, G. Persiano, Public key encryption with keyword search, in: Advances in Cryptology-Eurocrypt 2004, Springer, 2004, pp. 506–522.
[70] L. Ibraimi, Q. Tang, P. Hartel, W. Jonker, A type-and-identity-based proxy re-encryption scheme and its application in healthcare, in: Secure Data Management, Springer, 2008, pp. 185–198.
[71] C. Dong, G. Russello, N. Dulay, Shared and searchable encrypted data for untrusted servers, J. Comput. Secur. 19 (3) (2011) 367–397.
[72] M. Blaze, G. Bleumer, M. Strauss, Divertible protocols and atomic proxy cryptography, in: International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 1998, pp. 127–144.
[73] G. Wang, Q. Liu, J. Wu, M. Guo, Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers, Comput. Secur. 30 (5) (2011) 320–331.
[74] S. Yu, C. Wang, K. Ren, W. Lou, Achieving secure, scalable, and fine-grained data access control in cloud computing, in: INFOCOM, 2010 Proceedings IEEE, 2010, pp. 1–9.
[75] Y. Deng, C. Palamidessi, J. Pang, Weak probabilistic anonymity, Electron. Notes Theor. Comput. Sci. 180 (1) (2007) 55–76.
[76] R. Agrawal, C. Johnson, Securing electronic health records without impeding the flow of information, Int. J. Med. Inform. 76 (5) (2007) 471–479.
[77] P. Wilson, M. Sundgren, P. Singleton, Primary and secondary use of EHR systems, 2007, http://www.eurorec.org/files/filesPublic/ehrworkshop/2007/EHR%20workshop%20Recommendations%20-%20Interaction%20Model%20Stream.doc.

[78] D. Slamanig, C. Stingl, The degree of privacy in web-based electronic health records, in: 4th European Conference of the International Federation for Medical and Biological Engineering, Springer, 2009, pp. 974–977.
[79] M. Louk, H. Lim, H.J. Lee, Security system in cloud computing for medical data usage, in: Advanced Science and Technology Letters, vol. 38, 2013, pp. 27–31. http://dx.doi.org/10.14257/astl.2013.38.06.
[80] B.S. Alhaqbani, C.J. Fidge, Privacy-preserving electronic health record linkage using pseudonym identifiers, in: 10th International Conference on e-health Networking, Applications and Services, HealthCom, IEEE, 2008, pp. 108–117.
[81] T. Neubauer, J. Heurix, A methodology for the pseudonymization of medical data, I. J. Med. Inform. 80 (3) (2011) 190–204.
[82] B.S. Elger, J. Iavindrasana, L. Lo Iacono, H. Müller, N. Roduit, P. Summers, J. Wright, Strategies for health data exchange for secondary, cross-institutional clinical research, Comput. Methods Programs Biomed. 99 (3) (2010) 230–251.
[83] R. Zhang, L. Liu, Security Models and Requirements for Healthcare Application Clouds, IEEE, 2010, pp. 268–275.
[84] C. Quantin, D.-O. Jaquet-Chiffelle, G. Coatrieux, E. Benzenine, F.-A. Allaert, Medical record search engines, using pseudonymised patient identity: An alternative to centralised medical records, I. J. Med. Inform. 80 (2) (2011) e6–e11.
[85] B. Riedl, T. Neubauer, G. Goluch, O. Boehm, G. Reinauer, A. Krumboeck, A secure architecture for the pseudonymization of medical data, in: ARES, 2007, pp. 318–324.
[86] S. Mohammed, Ubiquitous Health and Medical Informatics: The Ubiquity 2.0 Trend and Beyond, IGI Global, 2010.
[87] T. Ermakova, B. Fabian, Secret sharing for health data in multi-provider clouds, in: Business Informatics, CBI, 2013 IEEE 15th Conference, pp. 93–100.
[88] T. Neubauer, M. Kolb, S.B. Austria, A legal evaluation of pseudonymization approaches, Int. J. Adv. Secur. 2 (2&3) (2009).
[89] T. Neubauer, M. Kolb, An evaluation of technologies for the pseudonymization of medical data, in: Computer and Information Science, Springer, 2009, pp. 47–60.
[90] M.G. Reed, P.F. Syverson, D.M. Goldschlag, Anonymous connections and onion routing, IEEE J. Sel. Areas Commun. 16 (4) (1998) 482–494.
[91] J. Camenisch, A. Lysyanskaya, A formal treatment of onion routing, in: Advances in Cryptology–CRYPTO, Springer, 2005, pp. 169–187.
[92] R. Dingledine, N. Mathewson, P. Syverson, Tor: The Second-generation Onion Router, Tech. Rep., DTIC Document (2004).
[93] A. Pfitzmann, M. Hansen, Anonymity, unlinkability, unobservability, pseudonymity, and identity management-a consolidated proposal for terminology, Citeseer (2005).
[94] S. Haas, S. Wohlgemuth, I. Echizen, N. Sonehara, G. Müller, Aspects of privacy for electronic health records, Int. J. Med. Inform. 80 (2) (2011) e26–e31.
[95] C. Dwork, A. Roth, The algorithmic foundations of differential privacy, Found. Trends Theor. Comput. Sci. 9 (3–4) (2014) 211–407.
[96] F.K. Dankar, K. El Emam, The application of differential privacy to health data, in: Proceedings of the 2012 Joint EDBT/ICDT Workshops, ACM, 2012, pp. 158–166.
[97] F. Dankar, K. El Emam, Practicing differential privacy in health care: a review, Trans. Data Privacy 6 (1) (2013) 35–67.

Buket Yüksel is a Ph.D Candidate in the Department of Computer Engineering at Koç University. She received the Bachelor's degree in Computer Engineering from Yasar University, Turkey in 2013. Her research interests are privacy and security.

Alptekin Küpçü received his Ph.D. degree from Brown University Computer Science Department in 2010. Since then, he has been working as an Assistant Professor at Koç University, and leading the Cryptography, Security & Privacy Research Group he founded. His research mainly focuses on applied cryptography, and its intersection with cloud security, privacy, peer-to-peer networks, and game theory and mechanism design. He has also led the development of the Cashlib cryptographic library, which is available as open source online. Dr. Küpçü has various accomplishments including 3 patents granted, 8 funded research projects (for 6 of which he was the principal investigator), 2 European Union COST Action management committee memberships, a Royal Society Newton Advanced Fellowship, and Koç University Teaching Innovation Grant. https://crypto.ku.edu.tr.

Öznur Özkasap received the M.S. and Ph.D. degrees in Computer Engineering from Ege University, Izmir, Turkey, in 1994 and 2000, respectively. From 1997 to 1999, she was a Graduate Research Assistant with the Department of Computer Science, Cornell University, Ithaca, NY, USA, where she completed her Ph.D. dissertation. She is currently an Associate Professor with the Department of Computer Engineering, Koç University, Istanbul, Turkey, which she joined in 2000. Her research interests include distributed systems, multicast protocols, peer-to-peer systems, bioinspired distributed algorithms, mobile ad hoc networks, energy efficiency, cloud computing, and computer networks. She serves as an Area Editor of the Future Generation Computer Systems journal, Elsevier Science. She also served as an Area Editor of the Computer Networks journal, Elsevier Science, and as a Management Committee Member of the European COST Action IC0804: Energy efficiency in large-scale distributed systems.