IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON SECURITY ANALYTICS AND INTELLIGENCE FOR CYBER PHYSICAL SYSTEMS

Received August 25, 2017, accepted October 11, 2017, date of publication October 30, 2017, date of current version February 14, 2018.

Digital Object Identifier 10.1109/ACCESS.2017.2767561

Privacy Preservation in e-Healthcare Environments: State of the Art and Future Directions

MUNEEB AHMED SAHI[1], HAIDER ABBAS[1,2], (Senior Member, IEEE), KASHIF SALEEM[2], XIAODONG YANG[3], (Senior Member, IEEE), ABDELOUAHID DERHAB[2], MEHMET A. ORGUN[4,5], (Senior Member, IEEE), WASEEM IQBAL[1], IMRAN RASHID[1], AND ASIF YASEEN[6]

[1]National University of Sciences and Technology, Islamabad 44000, Pakistan.
[2]Center of Excellence in Information Assurance, King Saud University, Riyadh 12372, Saudi Arabia.
[3]School of Electronic Engineering, Xidian University, Xi'an 710071, China.
[4]Department of Computing, Macquarie University, Sydney, NSW 2109, Australia.
[5]Faculty of Information Technology, Macau University of Science and Technology, Taipa 519020, Macau.
[6]The University of Queensland, Brisbane, QLD 4072, Australia.

Corresponding authors: Haider Abbas (hsiddiqui@ksu.edu.sa) and Xiaodong Yang (xdyang@xidian.edu.cn)

This work was supported in part by the Deanship of Scientific Research at King Saud University through the research group under Grant RG-1435-048 and in part by the National Natural Science Foundation of China under Grant 61671349.

ABSTRACT e-Healthcare promises to be the next big wave in healthcare. It offers all the advantages and benefits imaginable by both the patient and the user. However, current e-Healthcare systems are not yet fully developed and mature, and thus lack the degree of confidentiality, integrity, privacy, and user trust necessary to be widely implemented. Two primary aspects of any operational healthcare enterprise are the quality of healthcare services and patient trust over the healthcare enterprise. Trust is intertwined with issues like confidentiality, integrity, accountability, authenticity, identity, and data management, to name a few. Privacy remains one of the biggest obstacles to ensuring the success of e-Healthcare solutions in winning patient trust as it indirectly covers most security concerns. Addressing privacy concerns requires addressing security issues like access control, authentication, non-repudiation, and accountability, without which end-to-end privacy cannot be ensured. Achieving privacy from the point of data collection in wireless sensor networks, to incorporating the Internet of Things, to communication links, and to data storage and access, is a huge undertaking and requires extensive work. Privacy requirements are further compounded by the fact that the data handled in an enterprise are of an extremely personal and private nature, and its mismanagement, either intentionally or unintentionally, could seriously hurt both the patient and future prospects of an e-Healthcare enterprise. Research carried out in order to address privacy concerns is not homogenous in nature. It focuses on the failure of certain parts of the e-Healthcare enterprise to fully address all aspects of privacy. In the middle of this ongoing research and implementation, a gradual shift has occurred, moving e-Healthcare enterprise controls away from an organizational level toward the level of patients. This is intended to give patients more control and authority over decision making regarding their protected health information/electronic health record. A lot of works and efforts are necessary in order to better assess the feasibility of this major shift in e-Healthcare enterprises. Existing research can be naturally divided on the basis of techniques used. These include data anonymization/pseudonymization and access control mechanisms primarily for stored data privacy. This, however, results in giving a back seat to certain privacy requirements (accountability, integrity, non-repudiation, and identity management). This paper reviews research carried out in this regard and explores whether this research offers any possible solutions to either patient privacy requirements for e-Healthcare or possibilities for addressing the (technical as well as psychological) privacy concerns of the users.

INDEX TERMS e-Healthcare, privacy, anonymity, access control.

ABBREVIATIONS

HIPAA	Health3 Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health Act
PHI	Protected Health Information
PSN	Pseudonym
EHR	Electronic Health Record
EMR	Electronic Medical Record
ICT	Information and Communication Technology

RBAC	Role Based Access Control
ABAC	Attribute Based Access Control
IoT	Internet of Thnigs
WSN	Wireless Sensor Network
DES	Data Ecryption Standard
BAN	Body Area Network
AES	Advanced Encryption Standard

I. INTRODUCTION

Dating back to the start of 21st century, e-Healthcare is a relatively new concept in healthcare and medical sciences [1]. It envisions an ideal healthcare system that incorporates information and communication technology (ICT) in order to improve healthcare services by addressing the shortcomings of traditional healthcare approaches and improving efficiency [2], [3]. It also allows for remote patient assessment and makes it possible for patients to view their medical records at any given time and place. Ideally, e-Healthcare, while making an efficient use of ICT, allows for complete patient privacy as patients have the authority to allow or deny anyone to have access to their records. e-Healthcare dreams a healthcare enterprise that takes into account modern developments in technology as well as social limitations (i.e., the graying population, the need for 24/7 patient monitoring, the lack of healthcare personnel, and an increasing cost of healthcare/treatment).

There is a significant gap in existing e-Healthcare research because the existing studies usually focus upon their respective areas, rarely looking into other research areas. This results in proposed solutions which, while sufficient to address a particular problem/concern, fail to work overall as a part of the broader enterprise.

Recent advancements in ICT have made e-Healthcare an impending reality. However, there are certain issues that still need to be addressed [4], [5]. The preconditions of information security must be met in these systems, as they contain information of an extremely private nature for patients. Conditions of confidentiality, integrity, availability, accountability, non-repudiation, and others. must be met in these systems, as (end to end) total privacy cannot be ensured without them. Strong security measures and control mechanisms need to be set in place in e-Healthcare in order to gain patient trust. The use of wireless sensor networks (WSN) for patient monitoring by creating a body area network (BAN) is a relatively new phenomenon, which has been first mentioned at the start of 21st century, but not yet thoroughly addressed [4]. The contradictory requirements of less processing capability and high efficiency against high security need to be addressed in detail, and a careful balance needs to be struck between these [6].

The arrival of smart phones with more open operating systems (OS) may enhance trust in these systems, but they also present new threats and vulnerabilities associated with such operating systems due to their open nature. Smart phones and socializing applications are becoming an important part of e-Healthcare, and adoption of e-Healthcare monitoring and remote healthcare services have become a measure of an individual's prestige and social standing in the society [63]. Legislative regulations and personal risk benefit analysis, along with social norms, play an important role in one's perception towards adopting e-Healthcare solutions.

Introduction of cloud technology has brought advantages and as well as certain disadvantages to e-Healthcare [7]. According to Forbes, 83% of e-Healthcare service providers are using cloud technology in some capacity, and if this trend continues in the near future, almost all e-Healthcare businesses will employ cloud technology (public, private, and hybrid) as a core part of their enterprise. Therefor it is imperative to address security concerns originating from the incorporation of cloud technology in e-Healthcare, as it already is a core component of the e-Healthcare architecture. However, there is a lack of research and regulatory information regarding the incorporation of cloud technology in e-healthcare.

As is often the case with new enterprises, personnel training for e-Healthcare is lacking, along with an understanding by the users and patients of their associated rights and responsibilities in the context of privacy, confidentiality, integrity, and availability of patient healthcare information (PHI) and electronic health records (EHR) [69], [70]. Identity theft accounts for nearly half (46%) of all attacks targeting e-Healthcare enterprises [8]. Medical records and healthcare data now have more worth in the black market than credit card numbers, selling for an average of 40-50 USD per record [9]. As a result of the high value of the information they possess, e-Healthcare enterprises have been a frequent target for cyber attacks in the recent past. Several attacks, affecting more than a million users each, have occurred in the past five years. The biggest attack on an e-Healthcare enterprise resulted in the theft of the data of around 78 million people [10]. Of all medical data stolen in 2015, 72% was stolen from healthcare enterprises, and over 90% of industries have seen a PHI breach [11]. The high value of information, compounded with relatively weak security, has resulted in increased attacks on e-Healthcare enterprises every year. The fact that these attacks and data breaches occur, despite all attempts at preventing them, shows that existing policies and frameworks need to be re-evaluated. The failure of e-Healthcare enterprises to ensure the privacy and security of patient data has resulted in poor trust on the part of its users. Such incidents have seriously hindered the growth of e-Healthcare enterprises, not only because of security breaches, but also because of a lack of accountability and of corporations' inability to apprehend the culprits.

A gradual shift towards patient controlled access to and rights over healthcare information, coupled with an enhanced use of smart phones and devices, means that most e-Healthcare interaction will be taking place through a mobile (Andriod, IOS) application. The way in which these applications are designed, accessed, and secured is another area of concern for the e-Healthcare domain [68]. A comprehensive

study needs to be undertaken in order to evaluate the unique environment of e-Healthcare enterprises as well as the threats to it and its security requirements. Existing studies have tried to explain and highlight security and privacy requirements while also reviewing and analyzing current research, but there seems to be a gap in analysis, as there are not enough studies evaluating research on the basis of given e-Healthcare security and privacy requirements.

This study aims to review current research about privacy concerns and to assess whether this research is sufficient to handle the unique privacy and security environment of the e-Healthcare industry. In this way, it aims towards filling the gap between e-Healthcare security and privacy requirements at one end, while measuring and comparing existing e-Healthcare enterprises and ongoing research to these requirements on the other end. Finally, it is hoped that this study could help various stakeholders and participants involved in e-Healthcare enterprises in understanding the critical issues by examining the entire enterprise, rather than focusing on individual aspects. Now is the hour of need for all of these parties and stakeholders to come together in order to address these issues and design an e-Healthcare enterprises that are secure, efficient, and trusted by all of their users and the patients they serve.

This study is divided into following sections: Section two describes a general overview of the e-Healthcare architecture. Section three points out various issues pertaining to e-Healthcare enterprises while focusing on and highlighting privacy. Section four presents and reviews various privacy preserving techniques, and section five and six present a discussion, conclusions, and future work.

II. e-HEALTHCARE ARCHITECTURE OVERVIEW

An architectural understanding of e-Healthcare systems is necessary in order to better understand the e-Healthcare domain and the security considerations therein. Currently, there exist a number of operational e-Healthcare enterprises. However, there is not a singular set of standards or architectural design for e-Healthcare systems. Major differences exist in handling patient EHR. In some operational enterprises, EHR is patient controlled, while other enterprises have dedicated healthcare monitors for managing EHR [17]. Therefore, a broad architectural understanding of e-Healthcare enterprises is essential. To this end, a sample e-Healthcare system is presented in Figure 1. This diagram encompasses all the major components and can be taken as a generic overview applicable to all e-Healthcare systems. The major components (tiers) of any e-Healthcare system are [12]:

- a core network containing all the information and servers,
- a body area network (BAN) containing sensors and providing information about patient healthcare parameters,
- users of the e-Healthcare system, possibly located at a remote position with respect to the system's core network (physician, pharmacist, health insurance providers etc.), and;
- a communication link connecting each of these to form a single uniform system.

In some studies, these components are defined with respect to data (i.e., PHI/EHR) in order to better understand and address security and privacy concerns with respect to data. These are defined as: the user sphere (patient and their BAN), the joint sphere (cloud service provider and communication link), and the recipient sphere (physician, pharmacist, nurse etc.) [13]. These defining approaches address the same architectural and privacy concerns, but from a different perspective.

Security requirements for all tiers are already defined in detail and encompass both general healthcare as well as technical security requirements. Applying a single security mechanism over the entire enterprise is not feasible as each component is distinct from the others, with different requirements, and thus needs separate handling [14].

e-Healthcare systems need to be protected from threats at every point, from sensors to employing the internet of things (IoT) to the core network and everything in between. For instance, the BAN, and its communication link to mobile devices, has its own threat environment and security measures, which are unique to that particular section of the e-Healthcare enterprise. Mobile devices that are responsible for collecting sensor data, pre-processing it, and transmitting it to an e-Healthcare core network also have their own threats and vulnerabilities [15]. These vulnerabilities are compounded by the fact that a mobile device is a shared resource, used by the patient for their daily activities in addition to monitoring health data [16]. Research shows that the use of smart phones, along with dedicated applications, is on the rise and will soon become an essential part of e-Healthcare systems [59]. This is along with the introduction and use of popular social media applications for e-Healthcare social networking [65]. Communication links that transfer all this data from a mobile device to the core network, and connects all remote users to it, employ security measures best suited to themselves (encryption).

Once data securely arrives at the core network, its protection, privacy preservation, processing, and proper distribution comes into play. Prior to this stage, data confidentiality and privacy are somewhat similar, since hypothetically no one is supposed to see the data. Now however, access control, user anonymity, and other privacy preservation requirements need to be met. At this point, distinction is made between those who are allowed access to health records and those who are not. And perhaps more importantly, a distinction arises between who is allowed to see patient-centric information (name, ID number, etc.) and who is allowed to see healthcare-centric information (PHI).

e-Healthcare is already being deployed in various regions around the world. With certain note able exceptions, these enterprises have vulnerabilities and flaws that have been exploited in the past, compromising not only patient information but also putting mistrust among their users. A few successful e-Healthcare enterprises, however, do not address

privacy and security concerns in an end to end fashion but focus more upon access control of stored data. They do not look into accurate, timely collection and correct, efficient transmission of data to the healthcare database [69].

III. e-HEALTHCARE ISSUES

There are a number of challenges that arise due to the introduction of ICT, IoT, and cloud technology in the e-Healthcare environment. e-Healthcare enterprises must meet a lengthy list of requirements, including legal ones (e.g., HIPAA). Crucial among those are [18], [67], [73]:

- architecture security,
- device management (PDA or smart phone handling BAN),
- sensor security,
- data protection (confidentiality and integrity),
- incident response,
- identity management and access control (privacy preservation),
- identity proofing (authentication),
- legal issues,
- auditability of the enterprise, and
- privacy for entities other than patients in the e-Healthcare enterprise.

Although e-Healthcare systems are aimed at improving healthcare quality while reducing its cost, they also bring to light new issues concerning patients. These issues include IoT, communication link, cloud storage, and access control – both individually and when combined together to form the e-Healthcare enterprise. Patient data of an extremely confidential and private nature can be compromised at any point from sensors to cloud storage and mandates a vigilant security mechanism to protect it from all threats [19]. Security threats to e-Healthcare systems can originate at any level. These can be of varying nature: architectural (sensors, PDA, communication, cloud), managerial (weak policies and access control), or software (application). Each and every layer and component of an e-Healthcare system needs to be secured.

The first challenge in this regard is designing the hardware (i.e., WSN and communication link) connecting the patient to the hospital. Ensuring a secure and efficient transfer of data from a sensor's BAN to the core of an e-Healthcare system is crucial. Securing end to end communication from BAN to the core network has its own security threats and vulnerabilities. Their security objectives are similar to any other part of an e-Healthcare system (confidentiality, integrity, availability etc.), but threat perception and mitigation is IoT-centric and thus needs specific understanding and handling [20]. There is a serious lack of research being carried out on managerial and compliance aspects of WSN and IoT. A lack of standardization regarding this end of an e-Healthcare enterprise means serious inter-operability issues for e-Healthcare service providers.

The protection of data in transmission or storage is another crucial security concern. Strong data encryption techniques, along with rigorous authentication mechanisms, need to be integrated into e-Healthcare systems. Most patients want to use their existing mobile devices as a link between the BAN and the core e-Healthcare network, rather than using a dedicated mobile device (which is feasible, security-wise). However, the use of shared resources (smart phone, the Internet) makes the system inherently prone to threats and to the vulnerabilities of these resources (applications, OS, protocols) [21], [22]. Data storage, sharing, and access at a server are often a less discussed topic in e-Healthcare. Existing security measures at various operational enterprises and servers have been deemed sufficient for providing security, confidentiality, and other functions when deployed in e-Healthcare. However, further modifications are necessary to address the unique operational and compliance requirements of e-Healthcare enterprises. This requirement is further compounded by the adoption of cloud technology at the back end, which introduces issues pertaining to cloud technology into an already troubled e-Healthcare enterprise [66].

Privacy is perhaps the single largest hurdle preventing e-Healthcare service providers from gaining patient trust and implementing e-Healthcare systems in full capacity. An ordinary patient may perceive privacy to be the only portion of the e-Healthcare architecture that concerns them directly, although this may not be the case in reality. The trust deficit between the system and its users can be overcome by giving patients control of the rights to view and share their health records.

Aside from patient demands for security, another factor highlighting the need for privacy is that healthcare legislation in general, and surrounding e-Healthcare in particular, puts a strong emphasis on patients' privacy. Among existing e-Healthcare enterprises [23], the most widely used approaches regarding handling of PHI are user-oriented, meaning that the patient controls and manages their PHR. Conversely, in clinic-centered approaches, a caregiver is designated to manage PHR. The most desirable scenario in this regard is to enable the patient to control access to their medical information. It is control, rather than the ownership or possession over data, that defines privacy [17].

A rigorous privacy preservation mechanism is essential to ensure patient's privacy of identity, medical records, financial records, ongoing diagnosis, and treatments. Service providers' inability to come up with an efficient and effective privacy approach is the single biggest reason for patient discomfort with e-Healthcare. Many patients do not trust the service provider's security and privacy mechanisms.

HIPPA and HITECH are privacy requirements defined by the U.S. government for e-Healthcare service providers. These are meant to ensure that sufficient measures are in place by service providers in order to meet security criteria deemed significant for patient's information security [24], [25]. The definition and criteria set for privacy in healthcare are of a legal sort to which a technical answer is needed. The following definition explains privacy precisely:

"Health information privacy is an individual's right to control the acquisition, uses, or disclosures of his or her

identifiable health data. Confidentiality, which is closely related, refers to the obligations of those who receive information to respect the privacy interests of those to whom the data relate. Security is altogether different. It refers to physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure'' [26].

Privacy in e-Healthcare is a more challenging issue to address as compared to others because [60], [70]:

- the duration for which data is collected may span over days and weeks, which results in e-Healthcare systems learning a patient's everyday routine;
- data collected is not purely of a physiological nature but also of a habitual nature (i.e., patient diet or daily activities);
- data collected is often shared among various sections (i.e., health insurance and research); and
- the perception, preference, and requirements regarding privacy vary among individual users, genders, ethnic and cultural groups.

It has been noted that research regarding e-Healthcare in the recent past (2010-15) has focused on access control and data confidentiality while ignoring many critical aspects like privacy, anonymity, and auditability [62]. Recent research has also demonstrated the need for addressing security concerns for smart phone and PDA interfaces for patients and users. This calls for platform security and the development of security by design, which incorporates security in the planning and development phases [58], [62], [74].

Recent studies have shown that the lack of standardized security and privacy policy implementations have resulted in disruptions in e-Healthcare enterprises. An extended focus on theoretical requirements and implementations has resulted in unintended unavailability of information, workflow disruptions, and operational feasibility issues [64]. This, coupled with limited or no collaboration among various stakeholders and poor focus on the overall picture of e-Healthcare enterprises, has resulted in very limited progress towards an efficient, if not ideal, e-Healthcare industry [68], [76].

It must be noted that an emergency healthcare provision mechanism is needed as well for any e-Healthcare system to be viable. Emergency mechanisms in e-Healthcare will allow for bypassing rigorous security mechanisms in order to provide emergency healthcare. This also opens a potential window for exploitation, for example when the emergency mechanism is triggered by an attacker to bypass security. Thus, it is key to find a careful balance that provides security to an emergency mechanism to prevent misuse while also allowing for its invocation when needed [27].

IV. PRIVACY PRESERVATION IN e-HEALTHCARE ENVIRONMENT: A REVIEW OF TECHNIQUES

As patient requirements for information management in an e-Healthcare environment have become increasingly crucial, a number of protocols have been proposed to address this issue. These include the pseudonymization of patient's identity, encrypting patient data and information (attribute-based encryption being most recent suggestion), creation of public and private clouds to handle sensitive data along with sanitized data, privacy-preserving data publishing, privacy-centered access control and data outsourcing, and dynamic reconstruction of data [28]–[31]. It has been recognized that no technique can single handedly obtain the levels of privacy and security needed for a healthcare enterprise. Recently, hybrid protocols have been proposed as a way of addressing all the dimensions of privacy and security concerns. Hybrid protocols work by incorporating two or more previously proposed techniques in such a way that they reinforce each other with their strong points and their flaws are remedied by implementing them together. Some hybrid protocols include access control (hybrid access control), data and identity anonymization (de-identification plus statistical restructuring), and a combination of access control and anonymization techniques [28]. A number of recent works discuss and analyze such protocols [13], [46], [47], [51].

Overall, privacy preservation in any functional e-Healthcare enterprise requires access control and stored data security as well as an anonymization mechanism of some sort, particularly when data is shared for medical research and insurance outside the enterprise. The two most common strategies for secure data storage are pseudonymization and access control preservation. The rest of section four presents a review of all recent research immediately relevant to our proposed requirement of patient information privacy (identity as well as healthcare information). It takes into account requirements deemed crucial for privacy preservation and reviews articles relevant in this regard. Initial research is mainly focused on patient identity management through various techniques [32], [35]–[37] whereas recent research has seen and addressed the need for patient data management to ensure total privacy, as seen in figure 1 [13], [28].

A. PSEUDONYMIZATION

One of the earliest proposals with regards to user privacy preservation (personal and healthcare data) was data anonymization. The idea was to modify data so as to remove all information identifying a particular patient. This sanitization of patient information allows for patient trust in e-Healthcare enterprises while also allowing for healthcare record sharing for research without compromising privacy. Pseudonymization was one of the earlier approaches to address privacy issues related to a user's identity. For privacy preservation, the U.S. and EU demand the installation of strict measures for the use of such healthcare systems. Simply speaking, instead of using one's real identity for various tasks in the e-Healthcare system, a pseudo-identity is derived to replace a user's real identity and other unique attributes. This identity is used to perform all user tasks (i.e., sharing EHR with physicians and nurses and obtaining medicine from pharmacies). This identity cannot be traced back to the user unless all the information, along with the answer to a pre-programmed secret question and encryption information

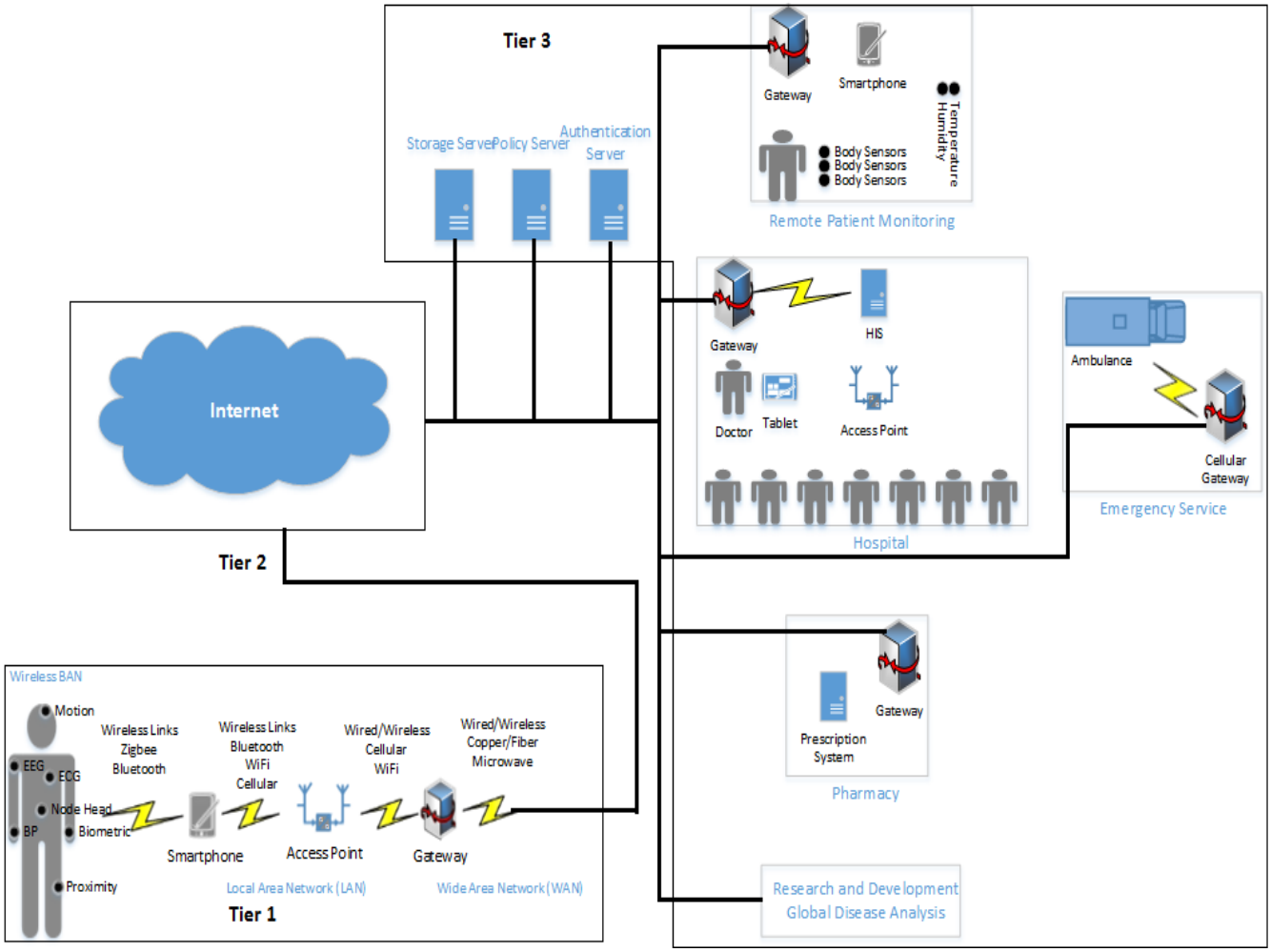


FIGURE 1. e-Healthcare architecture overview.

(key, algorithm) linking patient information to his/her pseudo identity, is available [32], [33]. The security of this algorithm lies both in the protocol's ability to deny any link between real and pseudo-identities and in the system's ability to securely store tabled entries of these identities. A crucial aspect in this approach is to categorize the patient's data into two sets: user-relevant data (for physicians and pharmacists) and personal, pseudonymized data. This approach is called depersonalization. The basic approach in deriving pseudonyms (PSN) is encryption or hashing. However, there are certain unique requirements when it comes to pseudonymization of PHI.

Pseudonymization of identities was the only privacy concern during the early stages of e-Healthcare enterprise development, and it was initially deemed sufficient for patient privacy preservation [34]. However, identity anonymization alone is now clearly not enough for patient privacy preservation. With the application of certain skills, it is possible to identify the patient by analyzing their healthcare attributes (PHI/EHR).

Certain issues regarding privacy breach have been identified, such as:

- the disclosure of sensitive personal information during transit or storage at cloud,
- unauthorized access to information due to a weak authentication scheme or poor access control, and
- the dynamic nature of cloud environments, which can cause aggregation in services.

Security and privacy requirements specific to the above mentioned privacy concerns have been defined as follows for e-Healthcare's patient identity management server.

- Support for cross system interaction due to various existing ID management systems (i.e. inter-operation and delegation).
- Systems must provide a vast range of security and privacy preserving properties such as one and two-factor authentication and attribute based encryption deployment.

Initially, pseudonymization centered on hiding an identity. This was due to the fact that information was not shared outside the hospital – a trusted environment. This allowed for a certain degree of patient trust towards the hospital. In this regard, the use of cryptographic hash functions

was proposed [35]. Although this allowed for privacy preservation of user identity, it did not provide any measures for when this data was shared with others. Aside from patients' identities, all user data was visible to others, which constituted a serious privacy breach. Earlier research revolving around the issue of data anonymity was very basic [35]. An important improvement over the traditional approach of using cryptography was that encryption and decryption were unnecessary. And more importantly, data could be readily processed with no decryption required. One obvious weakness in this older system was weaker data anonymization techniques (dividing data into chunks, each having incomplete patient information). Another security measure identified was the use of blank pseudo-identities, which increase security by decreasing the possibility of correlating PSNs to actual identity. Riedl *et al.* [32] propose a comprehensive solution in this regard. They recommend full patient control over who can access information and in what capacity.

One problem that arises from the prospect of assigning a new PSN to a patient every time, and for its multiple samples, is that it becomes very difficult to use patient information for improvement of e-Healthcare system components like medical research, improving and integrating bed and biology [36]. Another problem identified in this approach is the sheer volume of encryption requirements for PHI sets in the data base. The use of symmetric encryption creates additional processing requirements and causes performance issues. Slow processing overhead in this regard can be overcome with the use of newer, more efficient encryption techniques. Another possible solution is to replace symmetric block ciphers (Advanced Encryption Standard (AES), Data Encryption Standard (DES)) with nonlinear feedback shift registers, which have proved to be not only secure but also very efficient. Some researchers have pointed out the inability of this approach to correlate multiple PSNs to a single PHI, which eliminates the option of combining a single patient's information for better diagnosis and analysis [37]. Pommerening *et al.* [37] proposed a change in this regard. They introduced a new component to the system, which allowed correlation of multiple PSNs to a single PHI. In order to allow researchers to correlate multiple PHRs, each patient is also assigned an identity that can be used used for multiple PHR correlation.

It is critical to strike a balance between the anonymity of multiple patient records while maintaining access to detailed PHIs and all relevant information for better health care and research [39]. These somewhat contradictory requirements make it difficult to design an effective solution. The lack of correlation among multiple PSNs of any user was a major hurdle for medical research. Pseudonymization was introduced to help with sharing patient data for research purposes outside the trusted environment of the healthcare enterprise, but the inability to correlate multiple PSNs made it impractical. This was overcome by the introduction of multiple PSNs for a single user at different junctions of healthcare enterprise [40]. Further improvements could be to assign parent PSNs derived from the user identity, thus adding an additional layer of anonymity. All PSNs could be derived from this parent PSN, which would ennable more cogent anonymized records. This two-level pseudonymization would make it possible for researchers to distribute a single set of correlated PSNs, which would in turn be separated from the PIDs (Patients' ID) and accessible only to a pseudonymization authority. This makes it possible to correlate multiple PID's for a single patient, thus improving diagnostic and medical research while ensuring anonymity and privacy. A somewhat similar approach of having two PSNs was also introduced in other research [37], however this approach lacked the option of deriving multiple tier 2 PSNs from tier 1 PSNs. Thus PHI requestors would receive a full PHI, which violates the requirement to provide requestors with the least information required.

However, the approach of deriving multiple PSNs from a single EHR for treatment does not fully address patient privacy concerns. Patients must be given control over which PSNs from their EHR can be correlated and which are to be kept private, and it must be possible to override patient control over PHI/EHR in life threatening scenarios [41].

In another early article on pseudonymization, Jensen *et al.* [42] proposed issuing group identities instead of assigning an identity to each and every user. A group identity can be used by patients to share their PHI/EHR with healthcare providers. Service providers would know the group's identity and could use it to verify with the group that patient is a valid one. However, the provider cannot know the individual identity of any of the members in the group. Current privacy requirements do not even allow for cloud technology's ability to correlate users to a particular group, whereby, in determining the group, one could with some certainty guess the nature of its users EHRs. The approach defined by Jensen et al. covers non-interactive scenarios, but for an interactive scenario where cloud technology is expected to return an answer, it opts for a public recipient anonymous approach, where recipient would not be known at an individual level but will be known by his/her group identity. This approach has evident flaws, as these records could, with some skill, be correlated to their actual user by narrowing down defining attributes.

Current e-Healthcare systems are of isolated nature with differing architectures. This is a hurdle in the way of national healthcare program ambitions. An intermediary step in this regard is the ability to correlate different EHRs of a single patient at national level before their full incorporation into it. Alhaqbani and Fidge [41] have identified patient consent and authorization as crucial requirements for EHR linking within their privacy sphere. They have created a set of pseudo-identities, derived from primary identities, to be used independently from each other as electronic medical records (EMR) for treatment. Having once been part of a set of PSNs, these can be correlated. This approach ensures patient privacy by giving only the patient the authority to request correlation of their

multiple health records. However, the patient first has to identify all their EHRs, which is a difficult task completed over a longer time span. Data anonymization, de-identification and pseudonymization are all necessary to share an an EHR outside a patient's privacy and trust sphere. A ''search and replace'' of key identifiers has been used for this purpose, but it does not provide a desired level of anonymity [43]. Legal and corporate requirements for strong de-identification measures are meant to create greater user confidence in e-Healthcare systems, but current techniques in this regard are not up to the mark [44]. It is crucial for patients' privacy and PHI anonymity/de-identification that any healthcare data derived from primary health records is retained for a limited time and then either moved to a storage server not readily accessible or deleted. This is not the case for most existing primary healthcare records (PHR) [61], as is evident from comparing these articles and their propositions (see Table 1).

B. PRIVACY PRESERVING ACCESS CONTROL

Strict access control policies have long been considered to be the proper way to control access to information. A rigorous control of access to private information can help preserve privacy. However any single access control policy alone cannot preserve privacy for the entire e-Healthcare enterprise. Hybrid access control (i.e., the use of two or more access control policies to better create a secure and controlled access mechanism), is the solution in this regard. In order to ensure privacy, access control is essential, as it allows a user to define who has access to their information and to what extent others can use it. When combined with data anonymization, access control, in theory, solves the issue of privacy by hiding user's identity while also controlling the flow of their information. This has addressed all the major concerns of a patient with regard to PHI/EHR (i.e., preventing unauthorized access to PHI, storing and handling data in an anonymized manner, and sharing data with outside third parties without compromising patient privacy).

Narayanan and Güneş [45] discuss a number of access control schemes that are used by users worldwide for controlling access to information and resources. In reviewing their pros and cons, it becomes clear that no single mechanism is sufficient for our desired level of access control. They have implemented a role identity-based access control (RBAC) scheme. However it still has some limitations that need to be addressed. For example, a role defined as 'family' to allow family members to view patient EHR will allow every member the same level of access. But inner family members may need access to a patient's financial information, which is not possible in simple RBAC.

Younis and Merabti [46] also point out a number of issues in this access control approach. According to them, permissions in task-based authorization control (TBAC) are activated or deactivated according to the current task or process state. As there is no separation between roles and tasks, they use different factors such as users, information resources, roles, tasks, workflow, and business rules, to solve the separation problem and determine the access control mechanism. The scheme uses the workflow authorization model for synchronizing workflow with authorization flow. So, Younis et al. utilized tasks, which support active access control, and roles, which support passive access control.

Sun *et al.* [27] propose a new approach for e-Healthare patient monitoring. They propose a dedicated access control mechanism to give patients control over who accesses their PHI. Using an enabling security and patient centric access control (ESPAC), the patient assigns various categories of access to their PHI as desired. In contract-based e-Healthcare systems, where a patient signs an agreement with the medical center server regarding use of their PHI, this information is used to assign multiple access levels to elements of the system (doctors, insurance companies, etc.) regarding accessing PHI. The patients then approve access to their PHI when it is requested by someone without delegated access. (For example, the highest level entity doctor who is allowed to see PHI and pass recommendations will not be allowed to delegate this PHI to anybody until that delegatee's level is lowered to allow only viewing access). So, only a doctor can provide treatment, and anyone else who was delegated this PHI cannot initiate treatment aside offering an opinion to the doctor.

Sun *et al.* [47] have used a simple role-based access control scheme for their e-healthcare system to provide users with a defined EHR access policy. They have defined various roles in their system on the basis of activities performed by these entities (i.e., doctor, nurse, pharmacist). However, Sun et al. also have pointed out the limitations of using this approach. For example, not all doctors are supposed to have the same access to a patient's EHR. A more detailed access control policy needs to be defined and set in place to comprehensively handle access control in e-Healthcare environments, as flaws in traditional access control mechanisms render these mechanisms unsuitable for the e-Healthcare enterprise's specific requirements.

Requirements deemed necessary for successful access control mechanisms have been implemented successfully by Zhou *et al.* [48], along with a couple of new, and innovative techniques. Their approach intends to achieve both authentication and privacy with a single stroke – a great feat in an environment where overheads of security have become very cumbersome. With regard to privacy concerns, authors have proposed Authorized Accessible Privacy Model (AAPM). It not only efficiently resolves the access control requirements but also resolves the issue of managing physicians for a patient. In AAPM, access controls and privileges are defined by an access tree supporting flexible predicate thresholds. For new patients, it is difficult to find the right physician, so this approach allows patients to encrypt their PHI with an access policy. This allows only physicians meeting the criteria set by the access policy to decrypt that PHI. Despite its visible advantages in terms of being user friendly to the patient, it actually reduces the control a patient has over their information and access to it. Its automatic profile

TABLE 1. Pseudonymization techniques: A comparison.

Research Article	Proposition	Patient Anonymity Level	Correlating PHR for medical research	Anonymized data searching
Yang, Ji-Jiang, Jian-Qiang Li, and Yu Niu [13]	Vertical data partition and hybrid anonymized data searching	Strong (identity, data)	No	Yes
B. Riedl, T. Neubauer, G. Goluch, O. Boehm, G. Reinauer, and 1116 A. Krumboeck [32]	Assigning new PSN to a PHI for every session, preventing correlation of two PSNs originating from single PHI	Weak (identity)	No	No
J. Wang, Y. Zhao, S. Jiang, and J. Le [35]	Pioneering the idea of data anonymization with data partitioning; multiple tables with incomplete patient information	Weak (data)	No	No
B. Riedl, V. Grascher, S. Fenz, and T. Neubauer [38]	Assigning new PSN to a PHI for every session, preventing correlation of two PSNs originating from single PHI	Weak (identity)	No	Partial (researcher is assigned a new PSN to access PHI)
H.Aamot,C.D. Kohl,D.Richter,andP.Knaup-Gregori [36]	Identifies problems associated with pseudonymization approach introduced by Riedl et al. [32]	Weak (identity)	No	No
K.Pommerening,M.Reng,P. Debold,andS.Semler. [37]	2-tiered pseudonymization	Weak (identity)	Yes	No
R. Agrawal and C. Johnson [40]	Hippocratic data base for legal and ethical e-Healthcare compliance	Strong (identity, data)	No	Yes
B. Alhaqbani and C. Fidg [41]	EHR linking to individual EMRs	Weak (identity)	Yes	No

matching, which connects physicians to PHI's matching their skill profile, keeps patients from selecting a physician for themselves based on their own requirements and preferences. Also, a rogue physician could easily create, or be used to create, a profile to attract specific PHI's, thus compromising privacy.

We provide here the skeleton for a more comprehensive access control policy, along with its defining features, so as to further develop and refine it for implementation. We propose several features for a comprehensive hybrid access control policy:

- Roles defined as in the RBAC scheme.
- Graduated PHI privacy levels (i.e., a low privacy level for health information considered not so private, and a higher clearance level for critical and private health information).
- Patient profile containing categorized PHI as well as a list of users in e-healthcare environment who are allowed full access.
- A similar profile for doctors containing a list of patients to whose full PHI they have access.
- Patients can update their profile either to adjust their PHI sub levels or the list of users with access to their PHI.

Chen *et al.* [49] introduced a cloud-centered role-based access control mechanism called Cloud-based Privacy-aware Role Based Access Control (CPRBAC). This access control mechanism has been further enhanced by the introduction of an active auditing system (AAS). CPRBAC has certain features improving it over traditional RBAC, such as context-based access control, information sharing among different cloud servers, and authorization delegation [50]. It points out the weaknesses present in traditional RBAC schemes, which prompts the need for a tailored RBAC policy for e-Healthcare cloud environments [50]. Four new conditions, namely purpose, obligations, conditions, organizations have been defined in order to help easily and effectively define complex access control policies and rules. AAS is placed between CPRBAC and the backend data server in such a way that all data and communication has to take place through it, thus acting as an intermediary between the two. Its position allows it to monitor all processes between the server and CPRBAC, thus allowing for a real-time monitoring service. It keeps a check on all the activities and takes a prompt action in case a policy violation is detected. This prevents all attempts to have access to confidential information by bypassing the CPRBAC framework. It also generates alerts to notify relevant personnel about any misbehavior in the system. Chen et al.'s experimental results show that a combination of access control mechanisms, along with AAS, helps regulate the flow of information and prevents any unauthorized access, either deliberately or accidentally, against which traditional RBAC approaches fail [52].

Access control policies cannot be defined for all scenarios, and there are chances that a situation may arise that cannot be handled by the access control policy. Some sort of a fall back or initiation mechanism must be in place in order to normalize irregularities and assimilate them in the access control mechanism. It has been noted that in many proposed access control mechanisms, access control policies do not address data access or role changing if data is delegated to someone with less access to data than the one delegating it. Similarly, the use of third parties for handling several key and session management issues is again a potential cause for security or privacy violation [71], [75].

Deng *et al.* [53] have looked at the prospects of e-Healthcare system architectures with regard to privacy preservation. They have pointed out the advantages and challenges of using modern technology, primarily cloud services. Their research focuses on the privacy and confidentiality challenges brought up by the introduction of modern technology in a home-based healthcare system. It also looks at these challenges in the light of U.S. and EU legislation and explores the ongoing research on trustworthy clouds [54]. They also perform a critical analysis of cloud research methodologies, namely business-driven and architecture-driven. It has been pointed out that most of the research in this regard has been random and adhoc, failing to systematically address and analyze a particular problem. Coming back to their topic, they point out the challenges unique to home-based healthcare environments, namely semi-trusted cloud services, data-centric protection, efficiency, patient centric protection, control, and transparency. Regarding privacy preservation and patient-centric access control, authors have relied upon the use of attribute-based encryption (access control) and data encryption (privacy preservation), however no one has further elaborated on this.

Chen *et al.* [55] have proposed a protocol for secure data sharing among medical researchers and institutes without infringing upon the privacy and confidentiality concerns of patients [56]. The need for secure sharing among researchers to improve medical practices and services has been evident for a long time – since cloud technology's introduction into the e-Healthcare environment. Their protocol, dubbed PRECISE, intends to address this issue while ensuring privacy and other relevant concerns, both legal and technical. They have pointed out the limitations and flaws of existing techniques, which are centered around secure and anonymized data sharing among multiple healthcare service providers [57]. They have chosen homomorphic encryption and Yao's protocol of garbled circuits for their setup. Homomorphic encryption allows for data processing in an encrypted form, performing operations on encrypted data without having to reveal the information, thus ensuring the confidentiality and privacy of system users. Homomorphic encryption has been prescribed as a solution to e-Healthcare privacy concerns in other research articles as well, but it is a well established fact that homomorphic encryption at its current processing speed cannot be deployed in e-Healthcare enterprises, which already is constrained by the existing systems' processing powers [72]. PRECISE is intended to help healthcare service providers cooperate and share information in order to improve services and benefit from each other's experience. However, it has been mentioned that this approach is an experimental one and needs further development in order to make it suitable for industrial use. The work is being carried out in order to come up with more systems of such functionality, albeit with improved security footprint and efficiency.

V. DISCUSSION AND ANALYSIS

e-Healthcare offers a number of advantages over traditional healthcare approaches. However, its security and privacy concerns, particularly for patients, continue to hold it back from an implementation at the national level. Existing e-Healthcare enterprises have faced a number of attacks, undermining their efficiency and compromising patient trust. This article reviewed recent research concerning the privacy preservation of patient healthcare data during both its storage and usage.

Upon reviewing the work done in recent years regarding privacy preservation, it should be emphasized that privacy preservation using a single approach is not possible in an entire e-Healthcare enterprise. Privacy requirements and definitions may vary at different points in e-Healthcare systems. For example, anonymization and access control are both portrayed as a solution for privacy requirements in e-Healthcare. They both take care of certain privacy requirements, but also possess certain weaknesses and are thus unable to meet privacy requirements single handedly. Anonymization secures a patient's identity against PHI theft via correlation, but it does not address the access mechanism for this. Similarly, access control limits access to PHI/EHR but does not provide anonymity in the case of privilege escalation (access control failure).

Having studied recent research on privacy preservation in general, and for e-Healthcare in particular, this article suggests a hybrid approach. PSNs could be used to protect data stored and shared outside trusted e-Healthcare environments, while access control could be used to control data access and its flow within the trusted environment. Major privacy concerns in healthcare data privacy during storage and usage are unauthorized access to patient data and patient healthcare information sharing outside e-Healthcare environment prior to depersonalization. Most of the research carried out in this regard focuses on one or the other of these issues and fails to recognize the need to handle them simultaneously. This approach intends to address both simultaneously, which will ensure total privacy preservation for healthcare data stored in the cloud. In particular, it might address two primary concerns regarding privacy: patient-centric access control and hiding identity and information from exposure.

In the following, we suggest a solution for overcoming privacy preservation challenges in e-Healthcare.

- The Use of data anonymization (pseudonymization) during storage and transmission will ensure that patients' identity and personal information (name, address, social security number, contact information, etc.) are not revealed in case someone intercepts their PHI/EHR. Further analysis and research is needed in order to develop a suitable technique which is both efficient and secure in this regard.
- Patient-centric access control will allow patients to exercise control over who can have what level of access to their PHI/EHR. This not only meets privacy requirements but also allows the e-Healthcare system to gain patient trust – a vital component for e-Healthcare systems' success.
- Graduated PHI access levels will cater for different levels of access by patients and other users. Lower levels will only allow access to relevant data for the user (i.e., patient prescription requirements for a pharmacist). Physicians will have a higher level access, allowing them to see both the patient medical condition and diagnosis as well as treatment. This compartmentalized approach will allow for more secure and efficient management of the e-Healthcare system.
- PHI levels will be defined based on the user group information requirements. Healthcare insurance providers and government security agencies should not be concerned with the technical (medical) details of the patient but rather with their financial and general information, so a level allowing access to this particular information will be created. Similarly, there will be a level for the hospital staff revolving around the medical information of the patient.
- An alternate to this can be the use of multiple tickets for a single patient, each revolving around a certain aspect of patient's healthcare. Multiple tickets for hospital staff, healthcare insurance service providers, and medical researchers could be defined. This would reduce the overall complexity of the access control mechanism, but it may require the definition of more than one access control mechanism (Figure 2).
- As it has been noted that the use of traditional RBAC mechanisms for the PHI/EHR management is not feasible [47], [52], it is logical to divide healthcare information into sections based on usage, type, and privacy value. Figure 2 shows overall PHI divided into various components based on usage and type – patient insurance ticket (PIT) for health insurance management, patient profile (PP) for family and friends, hospital healthcare data (HHD) for hospital staff usage, and research data (RD) for sharing outside the e-Healthcare environment. Categorizing healthcare information in this way allows for separate policies and rules for categories of information, which in turn allows for better and more refined management and access control.
- We propose a two-tiered access control scheme somewhat similar to two-factor authentication, where both conditions must be met in order to be authenticated. This proposal uses RBAC on the upper level and identity/attribute-based access on certain lower levels (roles).
    - Physician, pharmacist, nurse, etc. are roles that are defined and possess a certain level of access. For example, a pharmacist needs read-only access, while a nurse checking body health parameters only needs write access in most cases. Meanwhile a physician needs both read and write access (see figure 3).

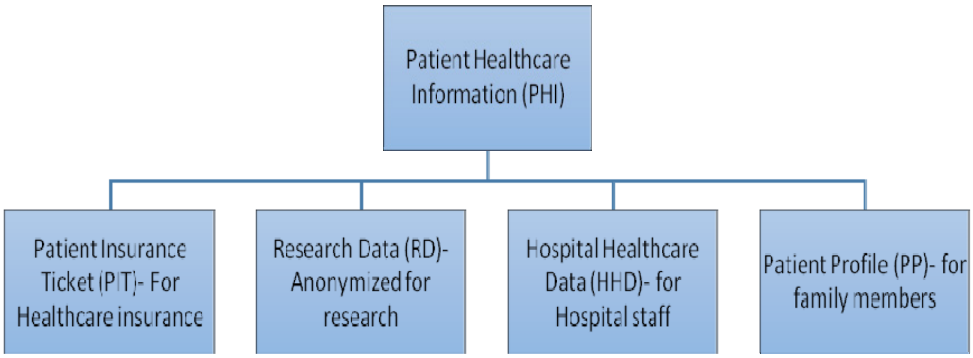


FIGURE 2. PHI compartmentalization for better control and security.

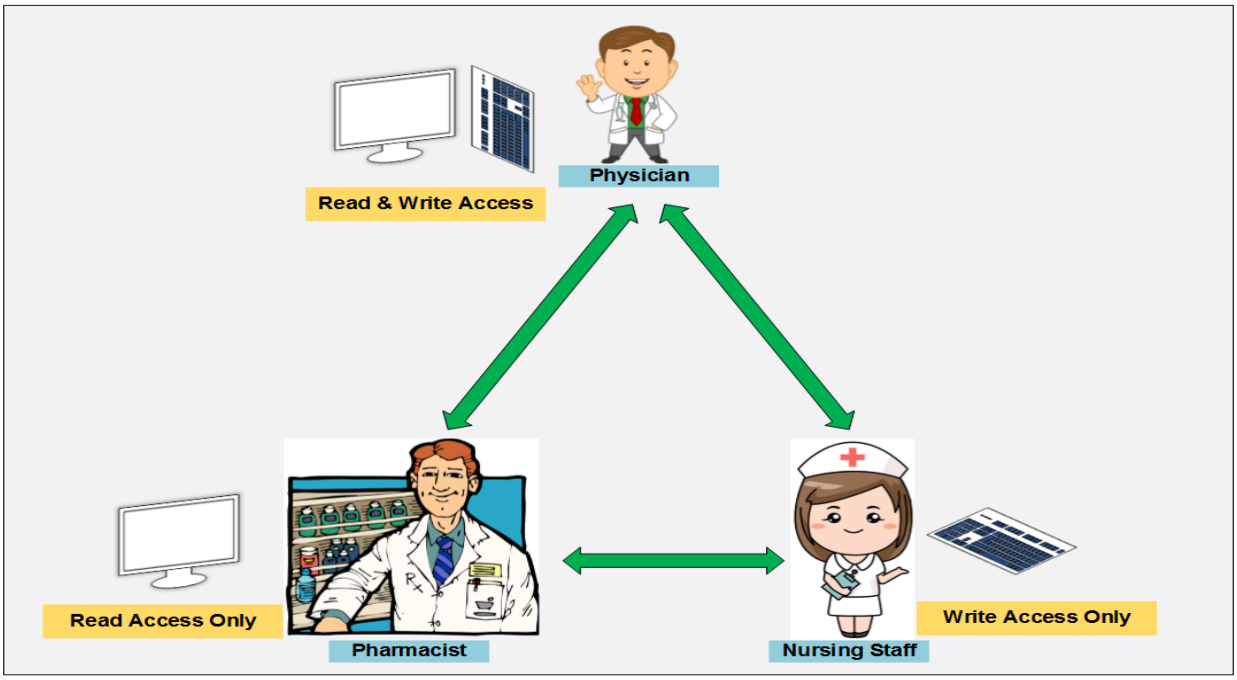


FIGURE 3. Hospital staff access control of PHI.

  - Since not all persons of a certain role are entitled to see PHI, identity/ attribute based access control comes into play.
- Computer security models delegate and enforce read and write bounds on upper and lower layers. This prevents people with lower level access from proliferating PHI. This also allows people with write access to PHI (physicians) to look for another opinion on healthcare matters from fellow physicians, but it does not give the consulted person authority to make any changes in PHI. That authority lies only with the authorized person (ex. a physician with write and read access).

On a broader scale, especially in the case of underdeveloped regions like parts of Africa and South Asia, the level of healthcare services provided may vary widely. Urban healthcare services tend to be more advanced and modern, while rural healthcare services center around more basic healthcare provisions. This heterogeneity can be employed to create a faster healthcare enterprise. Rural sections of the e-Healthcare enterprise, which tend to the medical needs of a greater section of society, are relatively simple, while more complex urban healthcare sections of the enterprise are handling fewer patients when compared to their rural counterparts. This allows them to be not only balanced out but also receive a maximum amount of benefit with relatively limited resources at the state's disposal [77].

Despite all this, it should be kept in mind that all these conditions and policies are not applicable in case of an emergency. An emergency healthcare provision requires immediate healthcare services, and traditional approaches cannot often be counted upon in such cases. Authentication and access control mechanism that are patient-dependent during normal operation of e-Healthcare do not work in the case of emergency. So, an alternate emergency response and processing mechanism must be devised and installed to allow for patient treatment without all these restrictions. However, it must not be possible to exploit the system – if emergency protocols are invoked unlawfully, unauthorized personnel might see a patient's PHI, thus resulting in a privacy breach.

VI. CONCLUSION

Having reviewed the latest research with regard to privacy preservation in e-Healthcare, it has been observed that use of any single technique is not sufficient, as it does not take care of all the privacy concerns. Understanding unique aspects of e-Healthcare is crucial for better privacy measures. Privacy needs to be defined in such a way that it takes into account the unique environment of e-Healthcare and its patients' situations. Time and again, in surveys conducted in various regions of the world, underlying issues in this regard have been the lack of precise definition and understanding of privacy, regulation, inter-agency cooperation, and conflicting goals among partners. Most importantly, privacy controls need to ensure patients that they are the ones with access control over their PHI/EHR. This article not only provides a review of research carried out in this regard but also presents a high-level sketch of a privacy preserving mechanism that addresses all major privacy concerns. The accompanying abstract architecture for privacy preservation in e-Healthcare works under the observation that individual protocols cannot ensure sufficient security and privacy for such a large and complicated enterprise. The solution is to divide patients' PHI/EHR into components based on privacy and access requirements. This compartmentalization allows for better management as different protocols can be adopted for different PHI/EHR sections. Lower-level components envisioned are patient profile (PP) for family members, patient health record (PHR) for hospital staff and treatment, patient insurance ticket (PIT) for healthcare insurance and financial management, and research data (RD) anonymized for healthcare research. In this way, a secure and privacy preserving e-Healthcare enterprise can be designed that allows for using multiple protocols at different components of PHI/EHR based on the security and privacy requirements of that information.

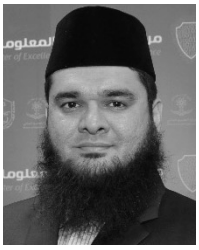
REFERENCES

[1] V. D. Mea, "What is e-health (2): The death of telemedicine?" *J. Med. Internet Res.*, vol. 3, no. 2, p. e22. 2001.
[2] C. R. Baker *et al.*, "Wireless sensor networks for home health care," in *Proc. 21st Int. Conf. Adv. Inf. Netw. Appl. Workshops (AINAW)*, vol. 2. May 2007, pp. 832–837.
[3] U. Varshney, "Pervasive healthcare and wireless health monitoring," *Mobile Netw. Appl.*, vol. 12, nos. 2–3, pp. 113–127, 2007.
[4] M. Al Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *J. Med. Syst.*, vol. 36, no. 1, pp. 93–101, 2012.
[5] T. Giannetsos, T. Dimitriou, and N. R. Prasad, "People-centric sensing in assistive healthcare: Privacy challenges and directions," *Secur. Commun. Netw.*, vol. 4, no. 11, pp. 1295–1307, 2011.
[6] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2688–2710, Oct. 2010.
[7] R. P. Nia, R. P. Mganga, "Enhancing information security in cloud computing services using SLA based metrics," Ph.D. dissertation, Dept. Comput. Sci., Blekinge Inst. Technol., Karlskrona, Sweden, 2011.
[8] *Verizone 2014 Data Breach Investigation Report, Figure 19;* Accessed: Aug. 27, 2016. [Online]. Available: http://www.verizonenterprise.com/resources/reports/rp_Verizon-DBIR-2014_en_xg.pdf
[9] Accessed: Jan. 4, 2016. [Online]. Available: http://www.nytimes.com/2015/02/06/business/experts-suspect-lax-security-left-anthem-vulnerable-to-hackers.html?_r=1
[10] Accessed: Jan. 4, 2016. [Online]. Available: http://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364
[11] *Verizone 2015 Protected Health Information Data Breach Report, Figure 7.* Accessed: Aug. 27, 2016. [Online]. Available: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf
[12] F. Miao, L. Jiang, Y. Li, and Y.-T. Zhang, "Biometrics based novel key distribution solution for body sensor networks," in. *Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*, Sep. 2009, pp. 2458–2461.
[13] J.-J. Yang, J.-Q. Li, and Y. Niu, "A hybrid solution for privacy preserving medical data sharing in the cloud environment," *Future Generat. Comput. Syst.*, vols. 43–44, pp. 74–86, Feb. 2015.
[14] W. B. Rouse, "Health care as a complex adaptive system: Implications for design and management," *Bridge-Washington-Nat. Acad. Eng.*, vol. 38, no. 1, p. 17, 2008. [Online]. Available: https://www.nae.edu/19582/Bridge/EngineeringandtheHealthCareDeliverySystem/HealthCareasaComplexAdaptiveSystemImplicationsforDesignand-Management.aspx
[15] V. Stanford, "Pervasive health care applications face tough security challenges," *IEEE Pervasive Comput.*, vol. 1, no. 2, pp. 8–12, Apr. 2002.
[16] P. Kulkarni, and Y. Öztürk, "Requirements and design spaces of mobile medical care," *ACM SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 11, no. 3, pp. 12–30, 2007.
[17] S. Avancha, A. Baxi, and D. Kotz, "Privacy in mobile technology for personal healthcare," *ACM Comput. Surv.*, vol. 45, no. 1, p. 3, 2012.
[18] T. J. Neela and N. Saravanan, "Privacy preserving approaches in cloud: A survey," *Indian J. Sci. Technol.*, vol. 6, no. 5, pp. 4531–4535, 2013.
[19] E. E. Egbogah and A. O. Fapojuwo, "A survey of system architecture requirements for health care-based wireless sensor networks," *Sensors*, vol. 11, no. 5, pp. 4875–4898, 2011.
[20] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," *Sensors*, vol. 12, no. 1, pp. 55–91, 2011.
[21] T. Dehling, F. Gao, S. Schneider, and A. Sunyaev, "Exploring the far side of mobile health: Information security and privacy of mobile health apps on iOS and Android," *JMIR mHealth uHealth*, vol. 3, no. 1, p. e8, 2015.
[22] D. He, M. Naveed, C. A. Gunter, and K. Nahrstedt, "Security concerns in Android mHealth apps," in *Proc. AMIA Annu. Symp. Amer. Med. Inf. Assoc.*, 2014, pp. 645–654.
[23] MHV. Microsoft. *The HealthVault Web-Based PHR*. Accessed: Jul. 9, 2016. [Online]. Available: http://www.healthvault.com
[24] (Dec. 24, 2015). [Online]. Available: http://www.legalarchiver.org/hipaa.htm
[25] (Dec. 24, 2015). [Online]. Available: http://www.whatishipaa.org/hitech-act.php
[26] S. P. Cohn. (2006). *Privacy and Confidentiality in the Nationwide Health Information Network*. [Online]. Available: http://www.ncvhs.hhs.gov/060622lt.htm
[27] J. Sun, Y. Fang, and X. Zhu, "Privacy and emergency response in e-healthcare leveraging wireless body sensor networks," *IEEE Wireless Commun.*, vol. 17, no. 1, pp. 66–73, Feb. 2010.
[28] J. L. Fernández-Alemán, I. C. Señor, P. Á. O. Lozoya, and A. Toval, "Security and privacy in electronic health records: A systematic literature review," *J. Biomed. Informat.*, vol. 46, no. 3, pp. 541–562, 2013.
[29] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," *J. Biomed. Informat.*, vol. 55, pp. 272–289, Jun. 2015.
[30] A. Abbas and S. U. Khan, "A review on the state-of-the-art privacy-preserving approaches in the e-health clouds," *IEEE J. Biomed. Health Informat.*, vol. 18, no. 4, pp. 1431–1441, Jul. 2014.
[31] C. C. Aggarwal and S. Y. Philip, *A General Survey of Privacy-Preserving Data Mining Models and Algorithms*. New York, NY, USA: Springer, 2008.
[32] B. Riedl, T. Neubauer, G. Goluch, O. Boehm, G. Reinauer, and A. Krumboeck, "A secure architecture for the pseudonymization of medical data," in *Proc. 2nd Int. Conf. IEEE Availability, Rel. Secur. (ARES)*, Apr. 2007, pp. 318–324.
[33] A. Pfitzmann and M. Hansen, "Anonymity, unlinkability, unobservability, pseudonymity, and identity management—A consolidated proposal for terminology," Tech. Rep., Dec. 2005. [Online]. Available: http://dud.inf.tu-dresden.de/Anon_Terminology.shtml Anon Terminology v0.25.pdf
[34] A. Lysyanskaya, "Pseudonym systems," in *Selected Areas in Cryptography*. Berlin, Germany: Springer, 1999.
[35] J. Wang, Y. Zhao, S. Jiang, and J. Le, "Providing privacy preserving in cloud computing," in *Proc. 3rd Conf. IEEE Hum. Syst. Interact. (HSI)*, May 2010, pp. 472–475.

[36] H. Aamot, C. D. Kohl, D. Richter, and P. Knaup-Gregori, "Pseudonymization of patient identifiers for translational research," *BMC Med. Informat. Decision Making*, vol. 13, no. 1, p. 75, 2013.
[37] K. Pommerening, M. Reng, P. Debold, and S. Semler, "Pseudonymization in medical research—The generic data protection concept of the TMF," *GMS Medizinische Informatik, Biometrie und Epidemiologie*, vol. 1, no. 3, pp. 2001–2005, 2005. [Online]. Available: http://www.egms.de/static/en/journals/mibe/2005-1/mibe000017.shtml
[38] B. Riedl, V. Grascher, S. Fenz, and T. Neubauer, "Pseudonymization for improving the privacy in e-health applications," in *Proc. 41st Annu. IEEE Hawaii Int. Conf. Syst. Sci.*, Jan. 2008, p. 255.
[39] J. Bickford and J. Nisker, "Tensions between anonymity and thick description when 'studying up' in genetics research," *Qualitative Health Res.*, vol. 25, no. 2, pp. 276–282, 2015.
[40] R. Agrawal and C. Johnson, "Securing electronic health records without impeding the flow of information," *Int. J. Med. Informat.*, vol. 76, no. 5, pp. 471–479, 2007.
[41] B. Alhaqbani and C. Fidge, "Privacy-preserving electronic health record linkage using pseudonym identifiers," in *Proc. 10th Int. Conf. Health Netw. Appl. Services (HealthCom)*, Jul. 2008, pp. 108–117.
[42] M. Jensen, S. Schäge, and J. Schwenk, "Towards an anonymous access control and accountability scheme for cloud computing," in *Proc. IEEE 3rd Int. Conf. Cloud Comput., Cloud*, Jul. 2010, pp. 540–541.
[43] L.-C. Huang, H.-C. Chu, C.-Y. Lien, C.-H. Hsiao, and T. Kao, "Privacy preservation and information security protection for patients' portable electronic health records," *Comput. Biol. Med.*, vol. 39, no. 9, pp. 743–750, 2009.
[44] B. S. Elger *et al.*, "Strategies for health data exchange for secondary, cross-institutional clinical research," *Comput. Methods Programs Biomed.*, vol. 99, no. 3, pp. 230–251, 2010.
[45] H. A. J. Narayanan and M. H. Güneş, "Ensuring access control in cloud provisioned healthcare systems," in *Proc. IEEE Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2011, pp. 247–251.
[46] Y. A. Younis and K. K. M. Merabti, "An access control model for cloud computing," *J. Inf. Secur. Appl.*, vol. 19, no. 1, pp. 45–60, 2014.
[47] J. Sun, Y. Fang, and X. Zhu, "Privacy and emergency response in e-healthcare leveraging wireless body sensor networks," *IEEE Wireless Commun.*, vol. 17, no. 1, pp. 66–73, Feb. 2010.
[48] J. Zhou, X. Lin, X. Dong, and Z. Cao, "PSMPA: Patient self-controllable and multi-level privacy-preserving cooperative authentication in distributedm-healthcare cloud computing system," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 6, pp. 1693–1703, Jun. 2015.
[49] L. Chen and D. B. Hoang, "Novel data protection model in healthcare cloud," in *Proc. IEEE 13th Int. Conf. High Perform. Comput. Commun. (HPCC)*, Sep. 2011, pp. 550–555.
[50] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," *Computer*, vol. 2, no. 2, pp. 38–47, 1996.
[51] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *Proc. IEEE Infocom*, Mar. 2010, pp. 1–9.
[52] L. Sainan, "Task-role-based access control model and its implementation," in *Proc. 2nd Int. Conf. Edu. Technol. Comput. (ICETC)*, vol. 3. Jun. 2010, pp. V3-293–V3-296.
[53] M. Deng, M. Petkovic, M. Nalin, and I. Baroni, "A home healthcare system in the cloud–addressing security and privacy challenges," in *Proc. IEEE Int. Conf. Cloud Comput. (CLOUD)*, Jul. 2011, pp. 549–556.
[54] *Trust Worthy Clouds (Tclouds)*. Accessed: Jun. 13, 2016. [Online]. Available: http://www.tclouds-project.eu
[55] F. Chen, S. Cheng, N. Mohammed, S. Wang, and X. Jiang, "PRECISE: PRivacy-preserving cloud-assisted quality improvement service in healthcare," in *Proc. 8th Int. Conf. IEEE Syst. Biol. (ISB)*, Oct. 2014, pp. 176–183.
[56] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography*. Berlin, Germany: Springer, 2006, pp. 265–284.
[57] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?" in *Proc. 3rd ACM Workshop Cloud Comput. Secur. Workshop*, 2011, pp. 113–124.
[58] M. Henze, L. Hermerschmidt, D. Kerpen, R. Häußling, B. Rumpe, and K. Wehrle, "A comprehensive approach to privacy in the cloud-based Internet of Things," *Future Generat. Comput. Syst.*, vol. 56, pp. 701–718, Mar. 2016.
[59] N. Lee and O. Kwon, "A privacy-aware feature selection method for solving the personalization-privacy paradox in mobile wellness healthcare services," *Expert Syst. Appl.*, vol. 42, no. 5, pp. 2764–2771, 2015.
[60] M. Anwar, J. Joshi, and J. Tan, "Anytime, anywhere access to secure, privacy-aware healthcare services: Issues, approaches and challenges," *Health Policy Technol.*, vol. 4, no. 4, pp. 299–311, 2015.
[61] B. Mounia and C. Habiba, "Big data privacy in healthcare Moroccan context," *Procedia Comput. Sci.*, vol. 63, pp. 575–580, 2015.
[62] A. Sajid and H. Abbas, "Data privacy in cloud-assisted healthcare systems: State of the art and future challenges," *J. Med. Syst.*, vol. 40, no. 6, pp. 1–16, 2016.
[63] H. Li, J. Wu, Y. Gao, and Y. Shi, "Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective," *Int. J. Med. Informat.*, vol. 88, pp. 8–17, Apr. 2016.
[64] R. Parks, H. Xu, C.-H. Chu, and P. B. Lowry, "Examining the intended and unintended consequences of organisational privacy safeguards enactment in healthcare: A grounded theory investigation," *Eur. J. Inf. Syst.*, vol. 26, no. 1, pp. 37–65, May 2016.
[65] M. N. K. Boulos, D. M. Giustini, and S. Wheeler, "Instagram and WhatsApp in health and healthcare: An overview," *Future Internet*, vol. 8, no. 3, p. 37, 2016.
[66] W. Wang, L. Chen, and Q. Zhang, "Outsourcing high-dimensional healthcare data to cloud with personalized privacy preservation," *Comput. Netw.*, vol. 88, pp. 136–148, Sep. 2015.
[67] H. Pussewalage, S. Gardiyawasam, and V. A. Oleshchuk, "Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions," *Int. J. Inf. Manage.*, vol. 36, no. 6, pp. 1161–1173, 2016.
[68] R. Pankomera and D. van Greunen, "Privacy and security issues for a patient-centric approach in public healthcare in a resource constrained setting," in *Proc. IST-Africa Week Conf. (IIMC)*, 2016, pp. 1–10.
[69] M. Puppala, "Data security and privacy management in healthcare applications and clinical data warehouse environment," in *Proc. IEEE-EMBS Int. Conf. Biomed. Health Informat. (BHI)*, Feb. 2016, pp. 5–8.
[70] M. M. Ama-Amadasun, "Patients and healthcare providers' perceptions towards privacy rights of patients: An investigation of listed Swiss participating hospitals," *Int. J. Sci. Eng. Res.*, vol. 7, no. 7, pp. 1189–1203, 2016.
[71] S. I. Fatima and S. Siddiqui, "Healthcare in cloud using multi-level privacy-preserving patient self-controllable algorithm," *Int. J. Adv. Sci. Res. Eng. Trends*, vol. 1, pp. 123–126, Aug. 2016.
[72] P. M. Lavanya and P. Valarmathie, "Big data in healthcare using cloud database with enhanced privacy," *Int. J. Adv. Res. Comput. Eng., Technol.*, vol. 5, no. 5, pp. 1696–1701, 2016.
[73] E. Mehraeen, M. Ghazisaeedi, J. Farzi, and S. Mirshekari, "Security challenges in healthcare cloud computing: A systematic review," *Global J. Health Sci.*, vol. 9, no. 3, p. 157, 2016.
[74] N. H. Hassan and Z. Ismail, "Information security culture in healthcare informatics: A preliminary investigation," *J. Theor. Appl. Inf. Technol.*, vol. 88, no. 2, p. 202, 2016.
[75] N. S. Shaikh and S. Y. Raut, "International journal of engineering sciences & research technology PSMPV: Patient self-controllable and multi-level privacy-protecting cooperative validation in distributed M-Healthcare cloud computing," *Int. J. Eng. Sci. Res. Technol.*, vol. 5, no. 7, pp. 909–916, 2016.
[76] V. Kumar. *Tata Elxsi's Solution Suite for Tackling the Challenges for Wireless Technology in Healthcare*. Accessed: Sep. 15, 2016. [Online]. Available: http://www.tataelxsi.com/Perspectives/WhitePapers/IoTbasedsolutionsforhealthcareapplications.pdf
[77] P. Deshmukh, "Design of cloud security in the EHR for Indian healthcare services," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 29, no. 3, pp. 281–287, 2017.

MUNEEB AHMED SAHI received the B.S. and M.S. degrees from the National University of Sciences and Technology, Pakistan. His research interests include information security governance, management, network communication and security, and IoT.

HAIDER ABBAS (SM'15) received the M.S. degree in engineering and management of information systems and the Ph.D. degree in information security from the KTH-Royal Institute of Technology, Stockholm, Sweden, in 2006 and 2010, respectively. His professional career consists of activities ranging from research and development, and industry consultations (government and private), through multi-national research projects, research fellowships, doctoral studies advisory services, international journal editorships, conferences/workshops chair, invited/keynote speaker, technical program committee member, and reviewer for several international journals and conferences. He is a Cyber Security Professional, Academician, Researcher, and Industry Consultant who took professional trainings and certifications from the Massachusetts Institute of Technology, USA; Stockholm University, Sweden; Stockholm School of Entrepreneurship, Sweden; IBM, USA; and EC-Council. He is also an Adjunct Faculty and a Doctoral Studies Advisor with the Florida Institute of Technology, USA. In recognition of his services to the international research community and excellence in professional standing, he has been awarded one of the youngest Fellows of The Institution of Engineering and Technology U.K.; Fellow of The British Computer Society, U.K.; and Fellow of The Institute of Science and Technology, U.K.



KASHIF SALEEM received the M.E. and Ph.D. degrees in electrical engineering from University Technology Malaysia in 2007 and 2011, respectively. He was an Associate Editor and a Guest Editor of journals, the Chair, a TPC Member, an Invited Speaker, and a reviewer for several conferences and workshops. He took professional training and certifications from the Massachusetts Institute of Technology, IBM, Microsoft, and Cisco. He has been an Assistant Professor with the Center of Excellence in Information Assurance, King Saud University, since 2012. He has authored several research publications that are presented and published in renowned conferences, books, and journals. Dr. Saleem acquired research funding and is running several scientific research projects at KSA, EU, and the other parts of the world. His research interests include telecommunications, computer security, wireless communication, wireless security, artificial intelligence, and bioinformatics.

XIAODONG YANG (SM'17) has authored more than 30 peer-reviewed journal papers in highly ranked journals. His research interests include body area networks (BANs) and information security. He is on the Editorial Board of several prestigious journals. He has a global collaborative research network in the field of information security, BANs, and health informatics.

ABDELOUAHID DERHAB received the Engineering, master's, and Ph.D. degrees in computer science from the University of Sciences and Technology Houari Boummediene, Algiers, in 2001, 2003, and 2007, respectively. He was a Computer Science Engineer and a full-time Researcher with the CERIST Research Center, Algeria, from 2002 to 2012. He is currently an Assistant Professor with the Center of Excellence in Information Assurance, King Saud University. His research interests include mobile ad hoc networks, wireless sensor networks, Internet of Things, network security, malware detection, and mobile security.

MEHMET A. ORGUN (SM'96) received the B.Sc. and M.Sc. degrees in computer science and engineering from Hacettepe University, Ankara, Turkey, in 1982 and 1985, respectively, and the Ph.D. degree in computer science from the University of Victoria, Canada, in 1991. He is currently a Professor with the Department of Computing, Macquarie University, Sydney. His current research interests include knowledge discovery, multiagent systems, and trusted and secure systems. His professional service includes editorial and review board memberships of several leading journals and program committee and senior program committee memberships of numerous national and international conferences. He was the Program Co-Chair of the 14th Pacific-Rim International Conference on Artificial Intelligence in 2010; and the Conference Co-Chair of the Seventh and Eighth International Conferences on Security of Information and Networks (SIN 2014 and SIN 2015).

WASEEM IQBAL received the bachelor's degree in computer sciences from the Department of Computer Science, University of Peshawar, in 2008. He completed the master's degree in information security from the Military College of Signals-NUST in 2012. He did his master's thesis in wireless personal area networks. He was a Lecturer with the Department of Information Security, Military College of Signals-NUST, in 2012, and was promoted to Assistant Professor in 2015. He has authored several conference and journal research publications. His research areas include wireless network security, digital forensics, information security management, network security, cloud computing security, and IoT security. Prof. Iqbal was a recipient of the University Best Teacher Award for year 2014-2015. He achieved merit-based scholarship throughout his bachelor's degree.

IMRAN RASHID received the B.E. degree in electrical (telecomm) engineering from the National University of Sciences and Technology, Pakistan, in 1999, the M.Sc. degree in telecomm engineering (optical communication) from D.T.U. Denmark in 2004, and the Ph.D. degree in mobile communication from the University of Manchester, U.K., in 2011. He has been qualified for four EC-Council certifications, i.e., Certified Ethical Hacker, Computer Hacking Forensic Investigator, EC-Council Certified Security Analyst, and EC-Council Certified Incident Handler. He is also a Certified EC-Council Instructor and has conducted numerous trainings. He is currently the Head of the Electrical Engineering Department, National University of Sciences and Technology, Pakistan. His research interests are in mobile and wireless communication, MIMO systems, compressed sensing for MIMO OFDM systems, massive MIMO systems, M2M for mobile systems, cognitive radio networks, cyber security, and information assurance.

ASIF YASEEN received the Ph.D. degree in agribusiness (entrepreneurship) from the University of Queensland, Australia, in 2015, and the M.Sc. degree in ICT Entrepreneurship from the KTH-Royal Institute of Technology, Stockholm, in 2008. He is a Post-Doctoral Research Fellow with the ARC-Industry Transformation Training Centre, University of Queensland, Australia. His research addresses marketing and technology entrepreneurship in Agrifood chains and understanding the use of 'E' technologies in developing Smart Agrifood chains.