Blind Signatures Based Secured E-Healthcare System

Jayneel Vora [*], Parth Devmurari [†], Sudeep Tanwar [‡], Sudhanshu Tyagi, *Member, IEEE* [§],
Neeraj Kumar, *Senior Member, IEEE* [¶], and M. S. Obaidat, *Fellow of IEEE and Fellow of SCS*[‖]
[*†‡]Department of Computer Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat, India
[§¶]Thapar Institute of Engineering and Technology, Deemed to be University, Patiala, Punjab, India
[‖] King Abdullah II School of IT, University of Jordan, Jordan
Email: [*]15bce048@nirmauni.ac.in, [†]15bce029@nirmauni.ac.in, [‡]sudeep.tanwar@nirmauni.ac.in,
[§]sudhanshutyagi123@gmail.com, [¶]neeraj.kumar@thapar.edu, [‖]m.s.obaidat@ieee.org

***Abstract*—The E-Health cloud paradigm has evolved from the exchange and enhanced sharing of valuable information between various medical institutions, hospital systems and respective care providers. The aim of this system is to reduce the cost and making of efficient process. Preserving privacy of the health record and identity of a patient is one of the prominent concern of the cloud based paradigm. Major bottleneck for a wider reach to potential usages of the cloud is the fear of privacy loss. Patients may not trust the provider of the services and may hesitate to disclose their identities. One of the possible solution is to uphold their anonymity and securely clear their queries. Keeping the aforementioned points in to consideration, in this study, we propose an approach to preserve the identity. In addition to this, the proposed scheme holds the privacy of the patients using a flexible and adaptive approach in the paradigm through an authentication scheme that meets anonymity.**

***Index Terms*—Cloud Computing, e-health, Privacy, Anonymity, Securiy, Blind Signatures.**

I. Introduction

E-Healthcare is an emerging field that integrates the latest technologies with biomedical and medical infrastructure. This domain has included the regular monitoring and transfer of the health related issues from patient-centric environment to respective services providers. The process has involved Internet and other communication technologies, such as blue-tooth, zig bee, 5G etc. Nowadays, E-Healthcare is one of the prominent sector for the development of any country and ultimately for the entire society, due to which attaining the popularity globally. Implementing the E-healthcare system has several advantages like, online services for tele-consultation, e-prescription, e-referrals, tele-monitoring and tele-care systems. Key challenges of the system [1] are the requirements of high level of security and cost-effectiveness to maintain records and information of patients. There are lot of expectations from latest E-healthcare systems like needs and demands of patients, respective professionals, medical and research institutions on regular interval at very higher rate. Medications and consultations, e-prescriptions can be provided to the patients directly from the Internet itself that not only reduce the time, but also save the energy and effort traveling to hospital. Queries and comments of desiring agents can be directly handled by the domain experts (specialized doctors) with anywhere and anytime concept. Carrying and storage of hard copies of reports and prescriptions, records are no longer required. Respective records can be directly uploaded to the cloud, which can be retrieved wherever and whenever required. Cloud computing (CC) is one of the popular, demanding and evolving technologies in the world of automation technology. CC is an integration of hardware and software that stores and delivers several records and committed to provide different services on a large scale over a particular network. Usage of cloud enhances the level of security to some extent.

CC enables the stakeholders to process and utilize, store and retrieve various data and information related to the patients [4], [14]. This capability opens the doors to a wide pool of applications, which further improves the daily life to a new level. With the increase in the utilization of the applications by e-health users, a user requirement might follow a restricted access on the resources and anonymize the services provided. Medical Identity Theft is dangerous, due to the presence of inaccuracies in the permanent medical records and in turns affect the patients in career as well as private life, resulting in major losses in life and potential life threat. The concept of the anonymous authentication contradicts the paradigm itself. With the proof of a person's identity to be proved using the authentication scheme requires the identity to be revealed to be verified, and hence sabotaging the hypothesis. Several anonymity and authentication schemes have been proposed extensively researched and reviewed. One major consideration have been the definitions of the co-operative and centralized security schema for safeguarding the identities of the patient in the environment. One bottleneck has been providing the anonymity of the user as the key constituent. The objective of a cloud service provider is to ensure the safety of the identity and respect the privacy of a user. The aim of this study is to propose an authentication protocol that enhances the patient's anyonymity and safeguards the interests of all stakeholders.

A. Research Contributions

Following are our contributions of this paper:

- Proposed an architecture for the authentication of E-healthcare system by providing data abstraction using an anonymous credentials paradigm.
- Implementation of paradigm with the provision of blind signatures to the user.
- comparison of our approach with existing approaches to the most likely attacks.

B. Organization of the Paper

This paper begins with the introduction of various concepts related to the E-Health Paradigm. Section II describes the existing approaches in various health cloud security aspects and privacy issues in the e-health cloud paradigm. Our proposed approach is further described in Section III, followed by a description of preliminaries and model of threat. Section IV

978-1-5386-4599-4/18/$31.00 ©2018 IEEE

presents the overall description of the proposed authentication scheme with its Implementation. Finally, the paper is concluded with a discussion of the observations in Section V.

II. Existing Approaches

Using various advances in the field of telecommunication and medical monitoring devices, various efficient methods of remote patient monitoring have been discussed in the literature [1-2]. Health providers may use various sensors, communicate them via bluetooth and monitor the vital signs of a patient from oxygen levels to heart rates and breathing rates. Interesting aspect is that all these are provided in a very cost effective manner. Chronic as well as acute term patients are benefited from these paradigms owing to the possible prevention of a fatality, which may be sensed using the systems. Various E-health technologies have a potential to create a significant impact in the future of patient centric healthcare, especially by increasing citizen empowerment in terms of health maintenance and encouraging self care and related decisions. Service involving CC are normally provided by external vendors who own their resources and infrastructure that will be utilized for providing them for use. From a security perspective, an improvement is done using a centralized data center and an increase in security resources. Moreover, concerns grow over the loss of control over sensitive data. Various security challenges relating to privacy, leakage of data and protecting the identities prop up.

The major issue is with the users privacy in CC. The solution is to keep identity safe. Here anonymity is not a key component. A decentralized pseudonym method is to keep safe the identity of the patient in e-Health cloud [8-11]. All unimportant third parties and trusted authority issues certificates have been proposed to remove by the authors. They suggested a mechanism for interchange medical data sets and to keep the patients information safe. The privacy of the patient can be achieved by giving assurance of anonymity to the patient [11]. Most of the authors have used the trusted third party (TTP) scheme that has an information on the other parties to give approval. The cloud service is same to the TTP. So, the cloud service provider (CSP) must be honest for users privacy. The main goal is to apply anonymous authentication to e-Health application. In this e-Health cloud system, we have extended an innovative idea to propose an anonymous authentication scheme. This scheme must work efficiently while the patient is accessing the storage site where the sensitive information is stored.

A. E-Health Cloud

Currently CC based services have been used to increase the efficiency of the patient health monitoring. E-Health clouds can be categorized into three models: (1) Private cloud (internal creation), (2) Public cloud (outsourced), (3) Hybrid cloud (integration of internal creation and outsourced cloud).

The e-health paradigm [3] is the integration of various concepts including technology, commerce, health-related processes and vital information. The world health organization (WHO) has defined e-Health as the paradigm of information and various state of art technologies for health-related applications in a cost-effective manner. To handle a large amount of health-related data, the cloud paradigm provides a standard platform that gives standardized services. Among the major components used in this cloud paradigm [2] environment are:

- **Professionals with a background in health:** It refers to an expert (dentist, physician, pharmacists) who is delivering health services to the patient .
- **Healthcare Provider:** It refers to a group or an organization (hospitals) that provides services to the health professionals.
- **Personal Health Records (PHR):** Medical information in the sets of record and health-related data maintained by a patient.
- **Electronic Health Records (EHR):** Medical information in sets of record and health-related data maintained by various health professionals or organizations. They have been formed by number of personalized records and maintained by health providers/ hospital systems.

B. Privacy and Security

Nowadays, CC service is becoming popular because it offers on-demand and a large volume of storage, modules to provide different services based on health ecosystem. Most of the time patients have been worried due to privacy and feeling insecure as their personal data is taken care by third-party cloud provider. According to the Fujitsu Research Institute, around 88% of the users are concerned about their data privacy. They have to trust on service level agreement (SLA) and Cloud service provider (CSP). This creates the pressure on the healthcare service providers to protect the records of their patients.

Privacy is one of the right of an individual, as it has been universally declared in the ruling of human rights. The term privacy can be different in various countries, cultures, jurisdictions. It depends upon the nature of the information and user. This creates more attention of patients through various rights in the medical world. It should be concerned about patients physical condition and secret information. The users must have control over their data and authorization must not be overlooked [5]. Patients have rights to control healthcare data, how it is used, who is maintaining that data, etc. As per European commission, privacy is the most critical aspect of e-health record systems for both users (citizens and professionals) for all the countries [6], [7].

III. Proposed Approach

The services provided by CSP in the cloud and level of trust of the user are the major factors. Here, our aim is to utilize the cloud services without worrying about the level of trust. An overview of the proposed model using blind signatures is described in Fig. 1. The main goal is to achieve patients privacy by the anonymous authentication with access anonymously in the e-Health cloud. Some of the important components that are used in proposed model are defined as under:

Identity: It relates to the personal profile of a client of the cloud (user ID, pseudonym) or personally identifiable information (PII) system [11]. The identity contains information that distinguishes a person from the rest and utilized to locate the person, for examples range from the name, credit card number, house/ office address of a person or postal code of the region. The protection of PII from unauthorized access falls under the domain of the privacy protection of the user.

Privacy: In CC the clients have very less knowledge about tasks of the CSP system. It is the ability to keep safe PII from

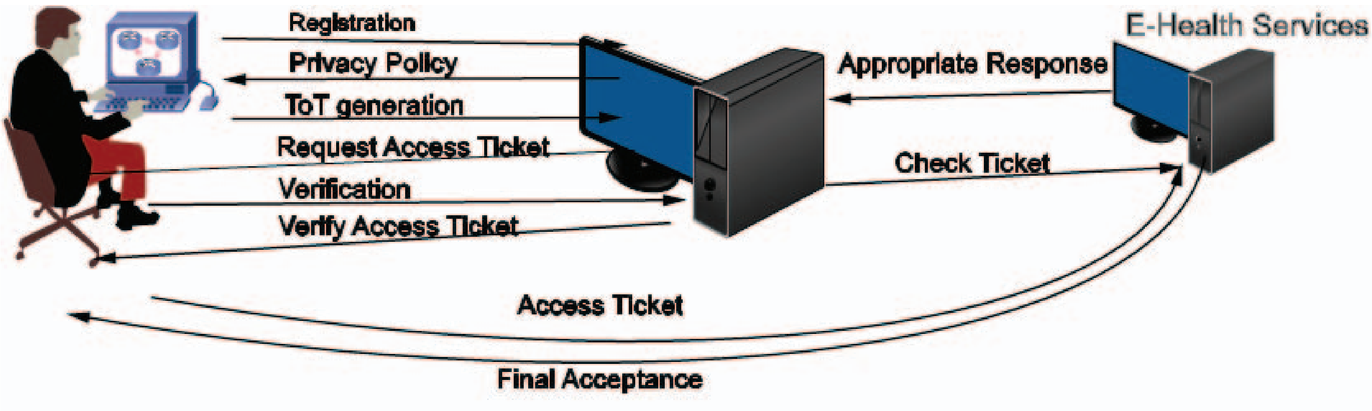


Fig. 1. An overview of the blind signature paradigm

unauthorized access [12]. Privacy is the discretion given to object to maintain its profile information, and providing/revoking access of the same to various Cloud service providers and stakeholders.

Anonymity: This is an event where the subject of importance or identification may not be recognizable. Various E-health records cannot be connected with a unique patient rather to a group of patients. Allowing the user to utilize a service or access a resource without revealing its identity or disclosing the PII [13].

Unlinkability: This is for the use of resources or interestingly the items without interlinking. The unauthorized entities must not be able to link the data. Here, multiple EHRs may not be linkable to a single owner. The importance of ensuring privacy of a user is of utmost concern. Various healthcare organizations may access the EHR by storing it on the cloud and the sensitive information on a private cloud.

Anonymous credentials (The case of blind signatures based on RSA): The blind signature is used to utilize various cloud services anonymously. The primary aim is to supply the anonymous tickets as credentials. This enables the client to create queries anonymously for using the services provided. A superficial way of putting the mechanism is when a part of the service issues credentials to the clients, which may be anonymously used for obtaining a cloud service [15]. Here, the issuing of the credentials is pursued by an entity of trust.

The RSA system creates the construction simple for a blind signature. Consider (a, b) two large prime numbers and $m = (a, b)$, two integers (p, q) satisfying equation 1. Where e and d are also integers satisfying the form: $e * d \equiv 1 \mod \psi(m)$.

$$\widetilde{k} = H(k) * t^e \mod m \quad (1)$$

$P_k = (m, p)$ is the signer's public key [16].
The owner of the document k has the knowledge of the key.
$S_k = (m, q)$ is the signer's private key.
The blind signature can be obtained from document k as follows:

- Firstly a random integer t will be selected by the owner of the document. Message is computed using Equation 2.

$$s = \widetilde{k}^d \mod m$$
$$\widetilde{k}^d = (H(k) * t^e)^d \equiv H(k^d r^{e^d}) \equiv H(k)^d \quad (2)$$

- The digital signature will be computed by the signer as per Equation 3:

TABLE I
ABBREVIATIONS TABLE

Abbreviation	Meaning
n	Counter to generate unique ToT
$PK+$	Public key for the access of a Patient P_i.
PK	Private key for the access of a Patient P_i.
$Ha(i)$	Hash function to secure a message
RTM	Manager for ToT generation and registration
$RTMK+$	Public key for the encryption process.
$RTMK-$	Private key for the encryption process
$RTMKS+$	Public key for applying to the signature
$RTMKS-$	Private key for applying to the signature
$RTMK+ = (N, e)$	Public key influenced by the RSA Blind Signature Technique.
$RTMK- = (N, d)$	Private key for applying to the signature
SM	Manager of the services
$SMK+$	Public key for encryption process having signature component
$SMK-$	Private key for encryption process having signature component
	All key pairs are validated by a certificate authority (CA).

$$s = H(k)^d$$
$$s^1 = s * t^{-1} \equiv H(k)^d \mod m \quad (3)$$

A. Model for Threat

Revealing the identity of any patient in the medical field is considered a violation of the privacy. In threat model, main parts of the threats against the privacy of the patient are:
Identity disclosure: Various users may be connected to the active databases depending on various quasi-identifiers. Abbreviations used in the paper are given in Table-I.
Sensitive information disclosure: The sensitive information are being related to individuals.
Inferential disclosure: Through data mining, sensitive information of the user can be inferred.
Control over the user location: This is related to location privacy of the user. In the threat model, the adversary considered being malicious may try to reveal the PII of the user in the scheme of the e-Health system, in the following ways:
The CSP itself assumed honest but may turn out dishonest, It may dump the data away or lose the data intentionally. Employees working as or for the CSP may use the information for benefit i.e. disconnected employee: an unauthorized service interruption, various types of social engineering attacks and unsecured APIs. The honesty of a cloud user is questionable in

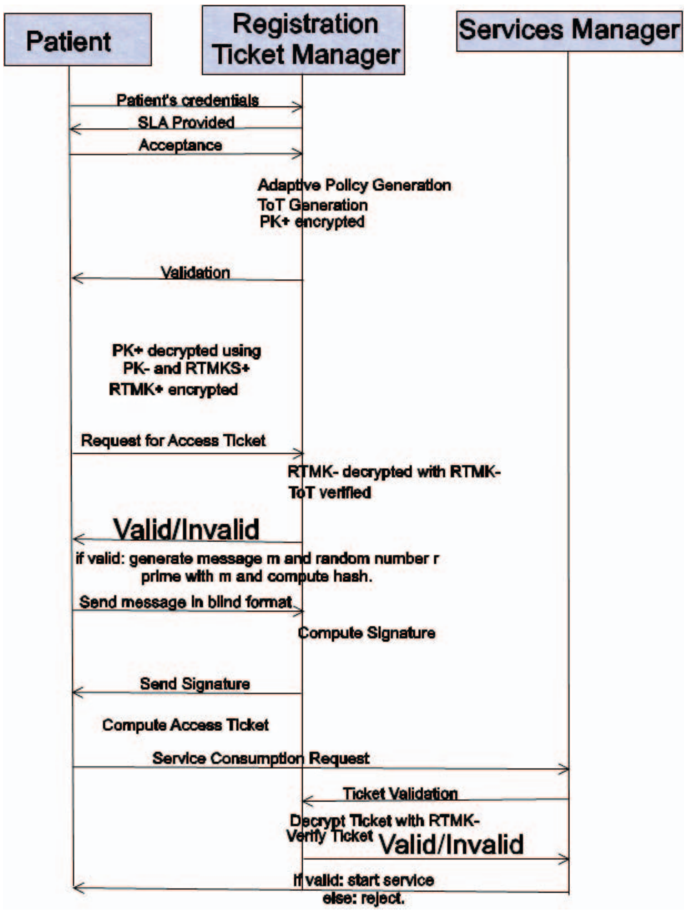
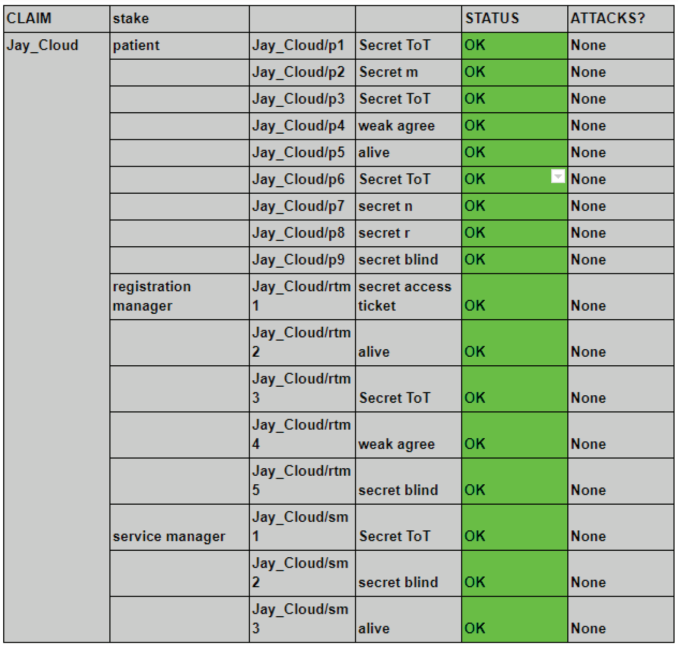


Fig. 2. A detailed model showcasing the working of the proposed authentication scheme between the RTM and SM during the conversation

certain scenarios without a background information. The user may perform a port scan on another genuine user and hence act maliciously. An external intruder is a malicious individual who is trying to reveal activity and information of the client of the cloud services. All above types are potentially supposed to be malicious. Through tracking the user in some situations privacy might be violated as clients anonymity is not taken as an important matter in the e-Health cloud system.

IV. Description and Implementation of Proposed Scheme

The anonymity of the patient is not considered frequently in e-Health systems. The absolute security does not exist in this kind of complex environment. Further, use of the existing application can be revealer of patients medical profile. A detailed ticket generation schema is described in Fig. 2, with two main actors in play- the Registration-Ticket Manager (RTM) and the SM. Here, the physical condition and illness is secret information of the patient. Our aim is to hide sensitive information from patients to keep them safe. To create an adaptive authentication scheme for a patient that allows them to access anonymously to their database or records, CSP will only see that patients request for a service. The aim is to give anonymous credentials when a patient requests to the cloud. Preservation of the privacy is the key element in systems architecture.



CLAIM	stake			STATUS	ATTACKS?
Jay_Cloud	patient	Jay_Cloud/p1	Secret ToT	OK	None
		Jay_Cloud/p2	Secret m	OK	None
		Jay_Cloud/p3	Secret ToT	OK	None
		Jay_Cloud/p4	weak agree	OK	None
		Jay_Cloud/p5	alive	OK	None
		Jay_Cloud/p6	Secret ToT	OK	None
		Jay_Cloud/p7	secret n	OK	None
		Jay_Cloud/p8	secret r	OK	None
		Jay_Cloud/p9	secret blind	OK	None
	registration manager	Jay_Cloud/rtm 1	secret access ticket	OK	None
		Jay_Cloud/rtm 2	alive	OK	None
		Jay_Cloud/rtm 3	Secret ToT	OK	None
		Jay_Cloud/rtm 4	weak agree	OK	None
		Jay_Cloud/rtm 5	secret blind	OK	None
	service manager	Jay_Cloud/sm 1	Secret ToT	OK	None
		Jay_Cloud/sm 2	secret blind	OK	None
		Jay_Cloud/sm 3	alive	OK	None

Fig. 3. Snapshot of SCYTHER tool: experimenting using various types of attacks

A. Authentication Scheme

The various steps in used for authentication of E-Health-based communication using blind signature scheme are:

*1) **Step1-Registration and users Adaptive privacy policy creation**:* In this step the SLA and privacy policy have been available to cloud user. It is for motivating users to join e-Health cloud system with being anonymous. The result generates the adaptive privacy policy by identifying the records of the particular patient. The starting ticket is also delivered with the name ToT which shows the proof of users registration and validates the same.

*2) **Step2-Obtaining an Access Ticket**:* Once the registration has been completed the user will get anonymous credentials(anonymous tickets) and can consume cloud service. This aim is to keep private patients sensitive information without revealing it to CSP.

*3) **Step3-Using access ticket, and gaining access to usual Services Obtained**:* The user uses the access ticket obtained in Step 2 to request the service, such as-EHR, applications, APIs etc. Here, the CSP will only know the user who requested the service.

B. Scheme Components

This scheme has various components and the brief description of each component is given below:

User: In this scheme, this is a kind of typical patients in e-Health applications. The operations that can be performed by patients are: (1) Registration, (2) An access ticket will be obtained by the patient to keep identity private, and (3) Begin anonymous use of services: Here, the various storage services for patients data and applications.

Cloud Service Provider: CC services are based on malicious provider. The cloud hosts handle various guest virtual machines that can be requested and may be communicated through a network connection on the cloud platform.

E- Health Registration-Ticket Manager (RTM): For registration of the new user this manager is responsible. It acts as a registration authority whose task is to give anonymous access ticket through blind signature to various patients that are registered.

E- Health Service Manager: This type of manager checks anonymous ticket of a patient with registration and RTM before allowing user to access the data of related to the patients.

C. Authentication Protocol

Fig 2. shows the various transitions of the patient to get anonymous access ticket or credentials. This scheme allows the patient to be unidentifiable. So, the e-Health provider will only know about patient request nothing else. This scheme can also be validated using the Scyther tool for automatic validation and verification. In our proposed scheme, the two session keys strengthen the environment for exchange while the access ticket is created by the RTM and while the service is used with the Service Manager(SM). There are two other important properties named weak agreement and vitality taht will also be checked.

D. Implementation

A scenario was created on Scyter GUI tool to experiment with various kinds of attacks to validate whether our proposed scheme may be able to defend against various attacks. The results have been displayed as a snapshot from the tool in Fig. 3.

V. Conclusion

Using CC to provide effective and low-cost healthcare services has resolved challenges of security and privacy for the data and mechanisms. The e-health cloud gives a potential opportunities to healthcare providers. In a scenario where two managers communicate regarding a patient's data, the traceability and identification of patients are hard to achieve. Patients get access using anonymous credentials without revealing any other identity or authentication credentials. To satisfy the aforementioned requirement, we have proposed an authentication scheme for e-Health users using anonymous, adaptive authentication services. Our proposed scheme has maintained a level of confidentiality of the data required by adding a layer of anonymity. This layer follows the simple principle that the presence of a health record implies the retrieval of healthcare services for a particular condition, which violates the privacy of patient instead of maintaining the confidentiality. Anonymous tickets work as the additional scheme of anonymity by offering consumption of the services, which allows the system not to depend on the 'trust'. The 'trust' concept demands a baseline of confidence for assuring the user's anonymity. The service provider, who may be physically able to access the machines and control the machines at any instant disclose and may hamper the patient's privacy. The tickets or other exchanges of data need to be well protected against any unauthorized third party access during the service consumption. Access control layer is used to guarantee a restriction on any unauthorized access to the health information, while fulfilling the tasks of providing a reasonable performance for security and privacy preservation. Our approach achieves a reliable efficiency in aspects of computations and space complexity with a reasonable overhead due to the communication paradigms.

Future works will include preserving the privacy by IP spoofing and controlling the visibility of the same and hence maintaining anonymity over the location of a person.

References

[1] J. Vora, S. Tanwar, S. Tyagi, N. Kumar and J. J. P. C. Rodrigues, "FAAL: Fog computing-based patient monitoring system for ambient assisted living," 2017 *IEEE* 19^{th} *International Conference on e-Health Networking, Applications and Services (Healthcom)*, Dalian, 2017, pp. 1-6.

[2] J. Vora, S. Tanwar, S. Tyagi, N. Kumar and J. J. P. C. Rodrigues, "Home-based exercise system for patients using IoT enabled smart speaker," 2017 *IEEE* 19^{th} *International Conference on e-Health Networking, Applications and Services (Healthcom)*, Dalian, 2017, pp. 1-6.

[3] S. Nabil, "Making use of cloud computing for healthcare provision: Opportunities and challenges" *International Journal of Information Management* vol 34, (2), pp. 177-184, 2014.

[4] Al Nuaimi, Al Shamsi, N. Mohamed and J. Al-Jaroodi, "e-Health cloud implementation issues and efforts," *International Conference on Industrial Engineering and Operations Management (IEOM)*, Dubai, 2015, pp. 1-10.

[5] Novitzky P, Smeaton AF, Chen C, Irving K, Jacquemard T, O Brolchin F, O Mathna D, Gordijn B. "A review of contemporary work on the ethics of ambient assisted living technologies for people with dementia." *Science and Engineering ethics* vol 21 (3), pp. 707-765, 2015.

[6] P. J. Soh, G. A. E. Vandenbosch, M. Mercuri and D. M. M. P. Schreurs, "Wearable Wireless Health Monitoring: Current Developments, Challenges, and Future Trends," in *IEEE Microwave Magazine*, vol. 16, no. 4, pp. 55-70, May 2015.

[7] Abbas A. Khan, Samee U. Khan, "e-Health Cloud: Privacy Concerns and Mitigation Strategies," *In Medical Data Privacy Handbook, Springer International Publishing*, pp. 389-421, 2015.

[8] A. Mazhar, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges" *Information sciences* vol 305, pp. 357-383, 2015.

[9] H. Wenlin and Y. Xiao "Privacy preservation for V2G networks in smart grid: A survey" *Computer Communications* vol 91, pp. 17-28, 2016.

[10] V. Pacheco and R. Puttini, "SaaS Anonymous Cloud Service Consumption Structure," 2012 32^{nd} *International Conference on Distributed Computing Systems Workshops*, Macau, 2012, pp. 491-499.

[11] A. Dubovitskaya, V. Urovi, M. Vasirani, K. Aberer and M. I. Schumacher, A Cloud-Based e-Health Architecture for Privacy Preserving Data Integration" *IFIP International Information Security Conference SEC 2015: ICT Systems Security and Privacy Protection*, 2015, pp. 585-598.

[12] Xu Liangyu, A. B. Cremers, and T. Wilken, "Pseudonymization for secondary use of cloud based electronic health record." *ASE BigData Social Informatics PASSAT BioMedCom Conference,* Harvard University, December 2014, pp. 14-16.

[13] Doel T., Shakir DI., Pratt R., Aertsen M., Moggridge J., Bellon E., David AL., Deprest J., Vercauteren T., Ourselin S. "GIFT-Cloud: A data sharing and collaboration platform for medical imaging research" *computer methods and programs in biomedicine* 139 (2017): pp. 181-190.

[14] Z. R. Li, E. C. Chang, K. H. Huang and F. Lai, "A secure electronic medical record sharing mechanism in the cloud computing platform," 2011*IEEE* 15^{th} *International Symposium on Consumer Electronics (ISCE)*, Singapore, 2011, pp. 98-103.

[15] N. Cao, C. Wang, M. Li, K. Ren and W. Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 1, pp. 222-233, Jan. 2014.

[16] Mohammad S. Obaidat and Noureddine Boudriga, Security of e-Systems and Computer Networks, *Cambridge University Press*, 2007.