Addressing Semantic Interoperability, Privacy and Security Concerns in Electronic Health Records

Arjmand Naveed[1*], Tshiamo Sigwele[2], Yim Fun Hu[1], Mumtaz Kamala[1], Misfa Susanto[3]

[1]*Faculty of Engineering and Informatics, University of Bradford, BD7 1DP, United Kingdom*
[2]*Department of Computing and Informatics, Faculty of Science, BIUST University, Private Bag 16, Palapye, Botswana*
[3]*Department of Electrical Engineering, Faculty of Engineering, University of Lampung, Jl. Prof. SumantriBrojonegoro No. 1, Bandar Lampung 35145, Indonesia*

[*]*Email: a.naveed2@bradford.ac.uk*

Article Information:

Received:
10 March 2020

Received in revised form:
2 May 2020

Accepted:
5 May 2020

Volume 2, Issue 1, June 2020
pp. 31 – 38

http://dx.doi.org/
10.23960/jesr.v2i1.40

Abstract

The use of Electronic Health Records (EHR) in healthcare has the potential of reducing medical errors, minimizing healthcare cost and significantly improving the healthcare service quality. However, there is a barrier in healthcare data and information exchange between various healthcare systems due to the lack of interoperability. Also, with the implementation of EHR system, there are security and privacy concerns in the storage and transferring data entities. The healthcare interoperability problem remains an issue of further research and this paper proposes a semantic interoperability framework for solving this problem by allowing healthcare stakeholders and organizations (doctors, clinics, hospitals)using various healthcare standards to exchange data and its semantics, which can be understood by both machines and humans. Moreover, the proposed framework takes into consideration the security aspects in the semantic interoperability framework by utilizing data encryption and other technologies to secure the communication for the EHR information while ensuring real time data availability.

Keywords:. *Semantic interoperability; Interoperability standards; Electronic Health records(EHR);Artifical Intelligence Techniques; Natural Language Processing (NLP), Word2Vec, skip gram, CBOW*

I. INTRODUCTION

Recently, there is a gradual paradigm shift in the healthcare sector to gradually migrated paper-based patient medical records to digital electronic ones through the implementation of Electronic Health Records (EHR) systems [1]. Various EHR standards exists like IEEE [2], DICOM [3], LOINC, SNOMED CT [4], HL7 [5] and FHIR [6].However, even with the introduction of EHR and its diver's standards, healthcare systems are still isolated from each other without much collaboration and interoperability between them [7]. Interoperability of EHR is defined in Health Information Management System Society (HIMSS) as "the ability of two or more applications being able to communicate in an effective manner without compromising the contents of transmitted EHR" [6]. The data of EHR can be shared within different units of hospitals, between different laboratories and external agencies such as insurance and other research units [2]. A major goal of interoperability in healthcare is to facilitate the exchange of healthcare related data generated by different platforms. As such, an environment is needed to support interoperability, secure the transfer of data, enable easy access of patient's records and reduce medical errors hence less casualties; thereby reduce healthcare cost and delays in healthcare service provision [2].

Some of the issues that require attention to achieving complete interoperability of EHR systems are as follow: [1]

- Partial mapping from multiple sources.
- Need of user intervention.
- Setting of standards/Guidelines.
- Addressing contextual constraints.
- Existence of semantic differences in attributes.
- Platforms for semantic interoperability.
- Ontology mapping; interpreting medical terminologies.

In the context of interoperability, the key security issues are with whom to share; how to share and where to share that EHR data with such that no unauthorized access can be made to any data [8][9][10].Another important challenge is control the access of required

data to only authorized person [11]. Moreover, ensuring confidentiality and privacy of patient's sensitive health data shared within the departments of one hospital as well as between different hospitals is another challenge to be addressed. Hence, there is a need to define a framework that addresses both the interoperability and security issues in electronic health records [12].In this paper, a semantic interoperability framework for solving the healthcare interoperability problem is proposed. The framework allows different healthcare organizations and users (doctors, clinics, hospitals) to exchange data and its semantics that can be understood by both machines and humans. In addition, the proposed framework takes into consideration the security aspects of the semantic interoperability framework by utilizing data encryption and other technologies framework to secure the communication for the EHR information exchange while ensuring real time data availability. The paper is structured as follows, Section 2 describes the related work in terms of Healthcare interoperability and the security measures in EHR. Sections 3 describe the proposed Interoperability framework including the encryption algorithm together with malicious traffic filtering model. Finally, Section 4 gives the concluding remarks.

II. MATERIALS AND METHODS

A. Related Work:

1 Interoperability:

Authors in [11]explained that achieving semantic interoperability required user intervention, thus limiting the possibility of controlling and managing secured sharing of EHRs dynamically. Syntactic interoperability on the other hand has low-level technical issues such as formats, schema and protocols that can be resolved using various techniques and approaches. Semantic interoperability requires different levels of integration in inter as well as intra organizations and is difficult to obtain. Also, it is observed that healthcare domain exhibits data having high sensitivity in terms of required security. Moreover, the need of EHR security differs from person to person or case to case. Hence, a dynamic and robust technique or approach must be appropriately selected for permitting secured sharing of sensitive health data in disparate interoperable healthcare domain. Authors in [13][14], developed a model based on ontology for interoperability between heterogeneous systems, focusing on modelling, structuring, representing data along with interoperability. There are various ways to model and represent data, however, they lack in providing full interoperability. Authors in [15]argued that EHR solutions were complex, spanning multiple specialties and domains of expertise. Furthermore, these systems required to handle clinical concepts, temporal data, documents, and financial transactions, which would lead to a large code base being tightly coupled with data models and inherently hard to maintain. These difficulties can greatly increase the cost of developing EHR systems, resulting in a high failure rate of implementation, and threatening investments in this sector. Moreover, due to the wide variance in the level of details across different settings, data exchange is becoming a serious problem, further increasing the cost of development and maintenance. Authors in [16][17]stated that Semantic interoperability is of prime importance for healthcare systems to communicate with each other and provide better healthcare facilities to patients. Ontology matching tools were proposed to resolve data level heterogeneities between different healthcare standards and achieve message schema level conversion. Services based on ontology matching helps healthcare systems to communicate with any other system. Therefore, focus will be on working towards establishing more accurate mapping services and more detail level interaction study of existing healthcare Standards mapping services based on Service Oriented Architecture (SOA).Authors in [18] presented an architectural model with an agent–based middleware to enhance collaborative virtual environments with interaction interoperability facilities. The heterogeneity of user interfaces was handled through an interface standardization performed at a middleware level, so each user is able to choose his favorite coupling of input device and interaction technique to perform an interaction task.

2 Security:

Authors in [19] proposed a new way to provide data security, privacy and authentication on different cloud models, especially in public cloud model by placing a new layer between client and service provider. The paper used the asymmetric public key cryptography algorithm with key management to provide and ensure the authentication between client and service provider as well as data encryption. However, this did not resolve the challenge of maintaining patient privacy, when contents can be accessible from multiple devices like smart phones/tablets, PCs and iPod etc. Authors in [20], utilized attributes based encryption to store and securely access the patient records on a public server. The proposed solution focused on enhancing privacy, enabling scalability of key management, flexible access of data to data owners and public users, policy updates and revocation of users. The authors argued that

attributes-based encryption would provide more access control over data as compared to the role-based encryption and proposed using homomorphism split key encryption to verify trustworthiness of system in the future. Authors in [21] proposed a novel framework for sharing personal health records securely in cloud environment. They divided personal health records into multiple domains and described multiple types of Personal Health Records (PHR) owner scenarios to reduce the complexity of key management. The main idea behind their framework was to use attribute predicated encryption technique to encrypt personal health record file and access to the file is made available to the users. Although the paper mentioned that the key distribution would be managed by an application logic server, it is very unclear, how keys would be generated and shared among stakeholders. Authors in [22] proposed a novel patient centric framework and a mechanism for data access control to PHRs stored in semi-structured servers. The authors claimed that the proposed scheme was more efficient than other methods since its cipher text size, public and private key size was smaller, easier to generate and more cost effective. The authors proposed to combine other privacy-enhancing techniques with cryptographic techniques to enhance the efficiency to address the security and privacy issue of PHR systems. Authors in [23] reviewed different access models which were designed to resolve patients' privacy issues facing the EHR systems and showed that most of the work being done was based on the extension of Role Based Access Control (RBAC) to achieve privacy and security in healthcare. To improve trust between patient and EHR system, patient consent was incorporated as an integral part of EHR component. Authors in [24] presented continuous and transparent access control framework consisting of three core components: adaptive authentication, risk analysis, and data transparency mapped with Role Based Access Control. The adaptive authentication component validates the user through behavior profiling; risk analysis measures the amount of risk in user data access and data transparency allows patients and administrators to monitor data consumption and detect deviation from patient consent. Authors in [25] proposed a framework that mitigated both security and privacy risks in healthcare which in turn increased the confidentiality and integrity of patient's information and also access to health information. The framework took into consideration the security of health-related information during syntactic and semantic interoperability. In addition, the framework incorporated an audit trail system to monitor the activities and transactions in the system. In [26] and [27] the Health Insurance Portability and Accountability Act (HIPAA) and international standards published by the International Organization for Standardization (ISO) were compared. HIPAA is an integrated act to provide confidentiality, integrity and accessibility of EHR in the US, whereas ISO standards such as ISO 20000,ISO 27001 have been used for security of EHR.In parallel with widespread use of information technology, electronic attacks may affect the important terms of EHR; these attacks may change personal information without permission. Privacy of EHR is very important but since they include health information from different systems and organizations, there is a risk of security of personal records and system fails to provide security. ISO20000 and ISO27001 are used to provide information security in health sector and relevant laws and by laws are referred for sanction. HIPAA laws can be given international standard form like ISO standards and establishing integrated laws like HIPAA will provide maximum security for EHR.

B. Proposed Interoperability Framework

In view of the deficiencies of the different interoperability mechanisms reviewed above, a framework that deals both with the security and semantic interoperability of EHR is proposed in this paper. The proposed framework combine a Hierarchal based approach and a Similarity based approach so that both issues can be resolved. Users of the proposed framework can be patients. The framework is divided into 4 layers as shown in **Figure**1 below.

Layer 1- Data layer: The first layer manages data in the cloud. This layer contains repositories to store data related to EHR from hospitals. All information in documents like patient information, EHR's and other system of records located on cloud will be stored here. On this layer, MySQL database is used to store data.

Layer 2- Syntactic Interoperability Layer*:* This layer will define all the archetypes related to the different kinds of data such as blood pressure and Syntactic separation of the EHR data. This means that data is extracted from the database from first layer and separated into various subcategories such as clinical, personal, and financial and research related data into meaningful entities. Fast Healthcare Interoperability Resource (FHIR) [28] is used here.

Layer 3- Semantic Interoperability Layer: This layer will define all the repositories to store archetypes and is responsible for semantic interoperability of the EHR dataset. This layer is divided into two subcategories, model of use and model of meaning. Model of use include generic information model and data structure of healthcare data. Model of meaning include different

health terminologies and for this we will use SNOMED CT standard [29] and domain level and top-level ontology will be treated here. For semantic interoperability, the similarity analyzer is very important and is placed with the cloud based EHR. Similarity analyzer performs various functions such as data structuring, data mapping, data modeling and conflict removal. Data is structured into various archetypes which provide specific information about an object such as blood pressure. Different types of conflicts are removed from the data to model data into common types which can be interpreted by different stakeholders. The similarity analyzer is fully explained in the part B of this section.

Layer 4: Data Exchange Layer:

This layer defines how the data will be transferred to different stakeholders. Archetypes specify the design of the clinical data that a Health Care Professional needs to store in a computer system. Archetypes enable the formal definition of clinical content by domain experts without the need for technical understanding. These conserve the meaning of data by maintaining explicitly specified and well-structured clinical content for semantic interoperability. These can safely evolve and thus deal with ever-changing health knowledge using a two-level approach.

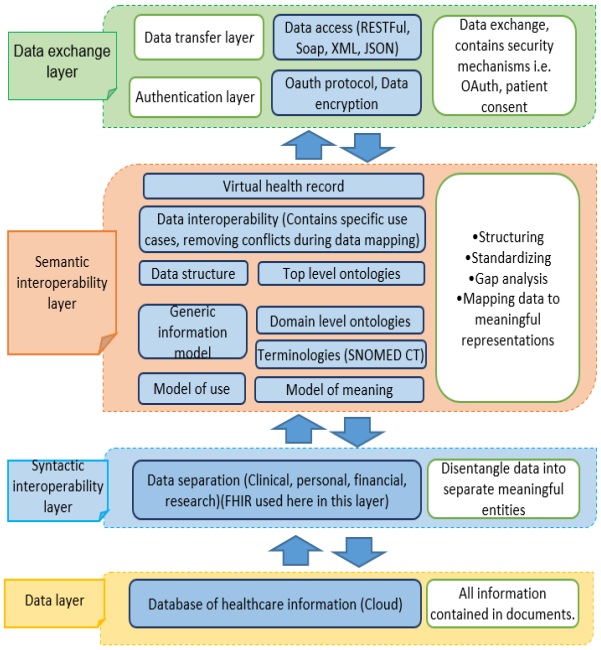

Figure 1. Proposed Interoperability Framework.

C. Similarity Analyser for Semantic Interoperability:

Data interoperability goal is achieved when heterogeneous systems problems are resolved through ontology matching and through accurate mapping file generation and it helps in clinical message conversion from one standard to another. Healthcare standards play an important role in achieving interoperability between EHR systems [30]. Each healthcare system has its own goals and objectives. These include:

- **HL7**: Related to messaging.
- **SNOMED CT**: Related to terminologies [31].
- **Open EHR and HL7 CDA**: Clinical information and patient records.
- **DICOM**: Digital imaging and communication in medicine that is related to imaging and communication in medicine [32].

Two organizations are interoperable, if they are complaint with the same standards. Problem arises when different healthcare system uses different standards e.g. Open EHR complaint system cannot directly communicate with HL7 complaint system.
For this problem one solution is ontology mapping which is the process of eliminating the terminological and conceptual conflicts and discovering similarities and for this purpose similarity analyzer is introduced in our proposed framework and AI mapping techniques are used in similarity analyzer. So, by using AI mapping, we can standardize clinical data records quickly and efficiently.

Working of Similarity Analyser Using AI:

Similarity analyzer performs various functions such as data structuring, data mapping, data modeling and conflict removal. Data is structured into various archetypes which provide specific information about an object such as blood pressure. Different types of conflicts are removed from the data to model data into common types which can be interpreted by different stakeholders in healthcare. So, the main task of similarity analyzer is that it takes the query from one hospital, analyze the standard or variation and then convert it into a standard format and reply back the required information in the desired standard.

For this purpose, the EHR data is classify into following types.

- Numeric Data.
- Textual Data.
- Images.

Numeric Data:

For numeric data variations, we use Rule Based technique to convert the numeric data from one format to another. A simple example is that one hospital can use the patient's date of birth format like D/M/Y and the other hospital use the format like M/D/Y, so for this problem, Rule Based technique is used which work according to the query and convert the numeric data into desired format.

Textual Data:

For Textual data, we classify data into two main components. One is **unstructured data** like physical examination reports, clinical laboratory reports, doctor's notes, summaries and other one is **medical terminologies**.

For unstructured data, Natural Language Processing (NLP) technique is used. NLP extract information from unstructured data and converts it into supplement and enriched structured medical data. NLP technique target at unstructured textual data and convert it into machine readable structured data by using Machine Learning (ML) techniques.

An NLP pipeline comprises of two main components. (1) Text processing and (2) classification. Through text processing, the NLP identifies the series of disease relevant keywords in the clinical notes, clinical laboratory notes based on patient's history database and then further analysis can be done on the reports and then these relevant keywords then enter and enrich the structured data and help in clinical decision making.

For Medical Terminologies, proposed similarity analyzer will use the Word2Vec AI technique.Word2Vec technique embed the words .Machine learning and deep learning cannot access text directly ,so we need some sort of numeric representation so that the algorithm ca process the data. In simple machine learning techniques, relationship between words cannot be reserved, so Word2Vec technique is used to embed the words. Word2Vec is used to generate word embedding in a given text corpus. Word embedding means mapping of word in a vector space. So, it preserves the relationship between words and deals with addition of new words in a vocabulary. The main objective is to cause the words that occur in similar context to have similar embedding. Two algorithms CBOW and Skip gram are used to generate vectors from words. CBOW predicts the target words from context and Skip gram algorithm is used to predict the context words from target. So, to improve the accuracy, we have to increase the training datasets, vector dimensions and window size but the drawback is that it increases the time duration.

Images:

For images processing, our proposed similarity analyzer use auto encoder technique which is a deep learning technique in which we add the images of different disease and then if there is a query arrived then it can predict the similarity in an unsupervised manner.

D. Proposed Security Framework:

Our proposed security framework utilizes simple access control techniques such as passwords and PIN to limit access to patient information to authorized individuals, for example the patient's doctors or nurses. For encryption, the symmetric block chain cipher Advanced *Encryption Standard (AES)* is used to protect classified EHR data from various health entities with different standards before storing data into the cloud repository as shown in **Figure** 2.

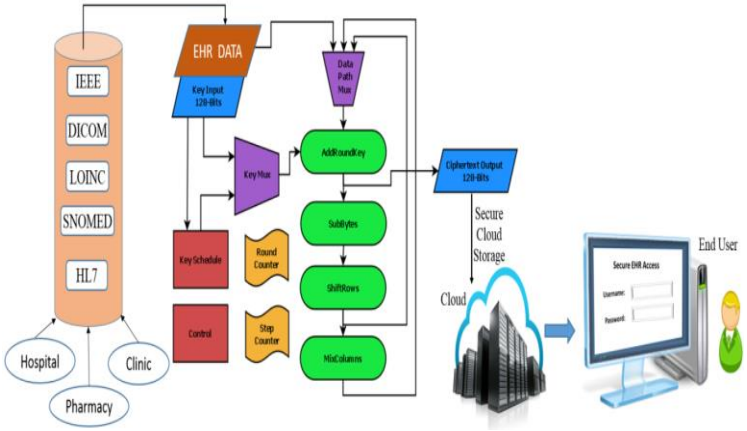

Figure 2. Adopting AES as a security measures in proposed interoperability Framework.

In addition to data encryption, a model is proposed for filtering out malicious traffic from accessing the EHR data. The proposed security model is shown in **Figure** 3**.** The proposed security model has two main environments: Network Environment and Cloud Environment.

Network Environment is a comprehensive security framework to assess the network traffic which contain healthcare traffic having health related data and allow only legitimate users and deny others. Data can be collected by using different simulators and software like wire shark, Fire eye etc.

Cloud Environment combines both static and dynamic filtering capabilities. The process involves examining the behavior of the traffic in the cloud environment based on the originating sources and assigning them the entry points as illustrated in below **Figure** 3. The points are assigned based on or malicious traffic patterns and access to the resource is restricted if allotted points cross the threshold, which is specified according to the availability of the resource accessed. This enables the creation of a pool of all the restricted nodes. The restricted nodes can be taken out from the pool and access is granted when the desired resource becomes available. This technique allows a resource over the

network to differentiate between legitimate and illegitimate users.

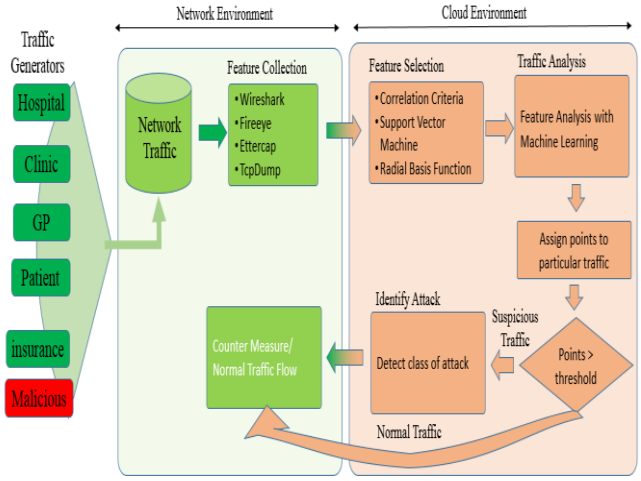

Figure 3. Proposed Security Model for filtering malicious traffic from accessing EHR data.

III. Results and Discussions

In this section, we provide experiments using our similarity algorithm based on Word2Vec AI technique. The experiment is performed in python language .In our initial experiment, the dataset of diseases with their symptoms is used and we used Euclidean distance algorithm, with Word2Vec two algorithms CBOW and Skip gram to find out the semantic similarity for the word disease "pneumonia". Results are shown in the Table 1. We concluded that as we added the symptoms, the accuracy improves and it is shown in the table that skip gram provides high accuracy and there are more chances to predict the similar words related to the given disease.

Table 1 Word2Vec word similarity for the word pneumonia

Similar Word	CBOW Accuracy	Skip Gram Accuracy
decreased translucency	0.98	0.99
Cough	0.86	0.97
Infection	0.81	0.87
Lung-nodule	0.79	0.80
Bronchitis	0.75	0.79

IV. Conclusions

In healthcare, semantic interoperability has prime importance and achieving semantic interoperability needs user intervention, therefore, the possibility of controlling and managing secured sharing of EHR is limited. Semantic interoperability requires different levels of interaction within the organization as well as outside the organization, which is very difficult to achieve. In addition, healthcare data is highly sensitive and required high level security, which may vary from person to person and from organization to organization. Our proposed a framework aims to resolve both issues Our proposed similarity analyzer help in overcome the issue of semantic interoperability during the exchange of the electronic health records between organizations using AI techniques. We proposed that the semantic interoperability is required in terms of numerical, textual, and images-based information. We provide detailed assessment of two Word2Vec algorithm CBOW and Skip Gram to find the semantic similarity of the numerical and textual based disease dataset and show their accuracy. The future work includes the implementing of the semantic interoperability in our proposed framework based on the images in the electronic health records.

References

[1] C. Park, J. Lim, and S. Park, "ISO / IEEE 11073 PHD Standardization of Legacy Healthcare Devices for Home Healthcare Services" in IEEE International Conference on Consumer Electronics(ICCE), pp. 547–548, 2011.

[2] I. S. O. I. Standards, "Design and Development of a Ubiquitous Healthcare Monitoring System Based on Android Platform and,",in IEEE International Conference on Consumer Electronics (ICCE), no. 61302033, pp. 1165–1168, 2016.

[3] R. D. Sriram, S. Member, and B. Lide, "The Role of Standards in Healthcare Automation",in IEEE International Conference on Automation Science and Engineering, pp. 79–82, 2009.

[4] S. Paraiso-medina, D. Perez-rey, A. Bucur, B. Claerhout, and R. Alonso-calvo, "Semantic Normalization and Query Abstraction Based on SNOMED-CT and HL7 : Supporting Multicentric Clinical Trials,"in IEEE Jouranal of Biomedical and Health Informatics , vol. 19, no. 3, pp. 1061–1067, 2015.

[5] T. M. Alenazi and A. A. Alhamed, "A Middleware to Support HL7 Standards for the Integration between Healthcare Applications,",in IEEE international Conference on Healthcare Informatics, 2015.

[6] D. H. Interoperability, "Digital Healthcare Interoperability,",in www.novartisfoundation.org/sites, October, 2016.

[7]. Y. Yang, X. Liu, and R. H. Deng, "Lightweight break-glass access control system for healthcare internet-of-things," IEEE Trans. Ind. Informatics, vol. 14, no. 8, pp. 3610–3617, 2018.

[8] C. Techapanupreeda and R. Chokngamwong, "Accountability for Electronic-Health Systems,"in IEEE Region 10 Conference(TENCON), 2016.

[9] N. K. Jha, "Smart healthcare," 2018 IEEE International Conference on Consumer Electronics., p. 1, 2018.

[10] A. Abbas, S. U. Khan, and S. Member, "A Review on the State-of-the-Art Privacy-Preserving Approaches in the e-Health Clouds,"in IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 4, pp. 1431–1441, 2014.

[11] S. Bhartiya, D. Mehrotra, and A. Girdhar, "Issues in Achieving Complete Interoperability while Sharing Electronic Health Records," Procedia - Procedia Comput. Sci., vol. 78, no. December 2015, pp. 192–198, 2016.

[12] Y. Zhang, D. Zheng, and R. H. Deng, "Security and Privacy in Smart Health : Efficient Access Control,"in IEEE Internet of Things Journal, vol. 5, no. 3, pp. 2130–2145, 2018.

[13] Z. Bouanani-oukhaled et al., "Ontological Model for EHR interoperability To cite this version : HAL Id : hal-01457845 Ontological Model for EHR interoperability,"in Conference on Informatics,Management and Technology in Healthcare, 2017.

[14] R. R. Rao, "Ontology based semantic representation for Public Health data integration,"in IEEE International conference on Healthcare Informatics ,pp. 357–362, 2014.

[15] S. S. El-Atawy and M. E. Khalefa, "Building an Ontology-Based Electronic Health Record System," Proc. 2nd Africa Middle East Conf. Softw. Eng. - AMECSE '16, no. May 2016, pp. 40–45, 2016.

[16] W. A. Khan and S. Lee, "Achieving Interoperability among Healthcare Standards : Building Semantic Mappings at Models Level," Icuimc, 2012.

[17] J. Li, "A Service-Oriented Approach to Interoperable and Secure Personal Health Record Systems,"in IEEE Symposium on Service -Oriented System Engineering(SOSE), pp. 38–46, 2017.

[18] M. Ciampi, L. Gallo, A. Coronato, and G. De Pietro, "Middleware Mechanisms for Interaction Interoperability in Collaborative Virtual Environment,2010.

[19] A. Jha and M. C. Sunil, "Security considerations for Internet of Things."in http://pdfc,Semantic Schloar.org/ in Secirity Considerations of Internet of Things,Technology Service,2015.

[20] M. Chase, "Multi-authority Attribute Based Encryption," Proc. 4th Conf. Theory Cryptography., vol. 4392, pp. 515–534, 2007.

[21] A. S. Azeemuddin and A. Majeed, "Achieving Secure Personal Health Records Using Encryption in Cloud Abstract ", in International Journal of Professional Engineering Studies, vol. IV, pp. 134–137,2014..

[22] V. Mini and J. A. Celin, "A Homomorphic Encryption Technique for Scalable and Secure Sharing of Personal Health Record in Cloud Computing,"in International Journal of Computer Applications, vol. 67, no. 11, pp. 40–44, 2013.

[23] M. Ehsan Rana, M. Kubbo, and M. Jayabalan, "Privacy and Security Challenges Towards Cloud Based Access Control in Electronic Health Records."in Asian Journal of Information Technology, 2017.

[24] M. Jayabalan and T. O. Daniel, "Continuous and Transparent Access Control Framework for Electronic Health Records : A Preliminary Study,"in 2nd International Conference on Information Technology,Information System and Electrical Engineering(ICITISEE), pp. 165–170, 2017.

[25] M. Habiba, S. Workforce, M. Injamamul, and I. Kashem, "A Framework for Providing Security to Personal Healthcare Records,"in International Conferenceon Networking System and Security(NSysS), 2017.

[26] O. E. Par and E. Soysal, "Security Standards for Electronic Health Records," 2012 IEEE/ACM Int. Conf. Adv. Soc. Networks Anal. Min., pp. 815–817, 2012.

[27] J. Li, "Privacy Preserving Data Analysis in Mental Health Research,"in IEEE International Conference on Big Data , 2015.

[28] M. L. Braunstein, "Patient - Physician collaboration on FHIR (Fast Healthcare Interoperability Resources)," 2015 Int. Conf. Collab. Technol. Syst. CTS 2015, pp. 501–503, 2015.

[29] C. Martinez-Costa, M. C. Legaz-Garcia, S. Schulz, and J. T. Fernandez-Breis, "Ontology-based infrastructure for a meaningful EHR representation and use," 2014 IEEE-EMBS Int. Conf. Biomed. Heal. Informatics, BHI 2014, pp. 535–538, 2014.

[30] B. Silverajan and J. Jiménez, "Implementation Experiences of Semantic Interoperability for RESTful Gateway Management,"in IoT Semantic Interoperability Workshop, pp. 1–4, 2016.

[31] K. Rosenbeck and M. Hummeluhr, "An Empirical Approach to Enhancing Terminology Binding – An HL7 FHIR,"in www.ncbi.nlm.gov/pubmed/2967952, 2018.

[32] A. Rajkomar et al., "Scalable and accurate deep learning with electronic health records," npj Digit. Med., no. March, pp. 1–10,in http://arxiv.org>cs, 2018.