Semantic Interoperability, Privacy and Security Concerns in Electronic Health Records:Survery and Model Proposal

Arjmand Naveed
School of Electrical Engineering and Computer Science
University of Bradford
Bradford, UK
A.Naveed2@bradford.ac.uk

Mumtaz Kamala
School of Electrical Engineering and Computer Science
University of Bradford
Bradford, UK
M.A.Kamala@bradford.ac.uk

Tshiamo Sigwele
School of Electrical Engineering and Computer Science
University of Bradford
Bradford, UK
T.Sigwele1@bradford.ac.uk

Fun Hu
School of Electrical Engineering and Computer Science
University of Bradford
Bradford, UK
Y.F.Hu@bradford.ac.uk

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 lack of interoperability. Also, with the implementation of EHR system, there are security and privacy concerns during 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 the healthcare interoperability problem by enabling various healthcare standards from various healthcare entities (doctors, clinics, hospitals) 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 by utilizing data encryption and other technologies in the proposed framework to secure the communication for the EHR information while ensuring real time data availability.**

Keywords—Internet of Things(IoT); Semantic Interoperability; FHIR; HL7 standards,Semantic web,ontology;Security measures;

I. INTRODUCTION

Recently, healthcare organizations have gradually migrated paper-based patient medical records to digital electronic ones by the implementation of Electronic Health Records (EHR) systems which is a paradigm shift in the healthcare sector. Various EHR standards exists like IEEE DICOM, LOINC, SNOMED CT[1], HL7 and FHIR[2].

However, even with the introduction of EHR and its diver's standards, healthcare systems are still isolated from each other with no collaboration and interoperability between these systems and standards. Interoperability is the ability of two or more components, applications or systems to exchange and use information. Interoperability of EHR 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"**[2]**.** The data of EHR can be shared within different units of hospitals (intra-sharing) or between different units (inter-sharing), between different laboratories and external agencies such as insurance and other research units as shown in Fig. 1[3]. So, the major goal of interoperability in healthcare is to facilitate the seamless exchange of healthcare related data and an environment is needed which supports interoperability and secures transfer of data. Healthcare Interoperability has the following advantages: Easy access of patient's records; Reduction of medical errors hence less casualties; Healthcare cost reduction and reducing delays in medal healthcare systems. Some of the issues that require our attention to achieving complete interoperability of shareable 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;[3] Platforms for semantic interoperability; Ontology mapping;[4] Interpreting medical

terminologies[5]. In the context of interoperability, the key security issues are: whom to share; how to share; where to share that EHR data with such that no unauthorized access can be made to any data.[6] Another important challenge is assignment of authorization and access permission of required data to authorized person [7]. 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.[8] So, there is a need of proposing a framework that addresses both the interoperability and security issues in electronic health records.

This paper proposes a semantic interoperability framework for solving the healthcare interoperability problem by enabling various healthcare standards from various healthcare entities (doctors, clinics, hospitals) to exchange data and its semantics which 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 to secure the communication for the EHR information exchange while ensuring real time data availability. The main contributions of the paper are summarized as follows;

1. The critical review of the existing semantic interoperability approaches for data sharing between EHRs stakeholders.

2. The critical review of the Security measures in interoperability of EHRs.

3. Derivation of a secure semantic interoperability model which combines data interoperability for EHRs by removing conflicts between various medical data types, archetypes and the encryption techniques.

4. Definition of an EHR encryption and security model for filtering out malicious traffic from access the EHR data.

II. RELATED WORK

With the adoption of EHR, the main challenge is interoperability and security issues of data and these issues are getting important day by day. Many researchers have tried to addresses these two problems as summarized in this section but still there is room for further research and more robust solutions.

A. Interoperability

Authors in [7]explained that achieving semantic interoperability requires user intervention and thus limits the possibility of controlling and managing secured sharing of EHRs dynamically. Syntactic interoperability on the other hand has low-level technical issues like that of 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 [9], developed a model which is based on ontology for interoperability between heterogeneous systems. The authors focus on modelling, structuring, representing data along with its interoperability. There are various ways to model and represent data such as UMLF and SNOMED, however, they lack in providing full interoperability. The approaches such as knowledge base and ontology frameworks are widely adopted for providing full interoperability. The UntolUrgences is an ontology based framework for the emergency acts. Another ontology based framework is proposed to model medical decision support system to improve patient's lifestyle. Authors in [10] described that Electronic health record (EHR) solutions are complex, spanning multiple specialties and domains of expertise. These systems need to handle clinical concepts, temporal data, documents, and financial transactions, which leads to a large code base that is tightly coupled with data models and inherently hard to maintain. These difficulties can greatly increase the cost of developing EHR systems, result in a high failure rate of implementation, and threaten investments in this sector. Moreover, due to the wide variance in the level of detail across different settings, data exchange is becoming a serious problem, further increasing the cost of development and maintenance. Author in [11]stated that Semantic interoperability is of prime importance for healthcare systems to communicate with each other and provide better healthcare facilities to patients. Compatibility between heterogeneous healthcare standards for message schemas conversions requires ontology matching tools. The proposed system uses ontology matching tools to resolve the 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, in future main 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 Surface Oriented Architecture (SOA).

B. Security

Authors in [12] provided 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 which is cloud. The paper uses the "asymmetric public key cryptography" algorithm with key management to provide and ensure the authentication between client and service provider. By adopting this approach, less time is consumed because all the partitioned data is encrypted in parallel. This mechanism provides security to client data. The main challenge is the maintenance of patient privacy, when contents can be accessible from multiple devices like smart phones/tablets, PCs and iPod etc.

Authors in [13], utilized attributes based encryption to store and securely access the patient records on a public server. The proposed solution focuses 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 provides more access control over data as compared to the role based encryption. A framework of secure sharing of personal health records has been proposed in this paper. The future work is stated as to use homomorphism split key encryption to verify trustworthiness of system. Authors in[14],proposed a novel framework for sharing personal health records securely in cloud environment. They divide personal health records into multiple domains and describe multiple types of PHR owner scenarios to reduce the complexity of key management. The main idea behind their framework is to use attribute predicated encryption technique to encrypt personal health record file and access to the file is made available to the users. The paper provides a very abstract view of the proposed methodology. It is mentioned that the key distribution is managed by application logic server. However, it is very unclear, how the key is generated and shared among stakeholders. Additionally, it is required to use more encryption techniques and provide a comparison of the cost. Authors in [15],proposed a novel patient centric framework and a mechanism for data access control to PHRs stored in semi structured servers. This proposed scheme is more efficient than other methods since its cipher text size, public and private key size is smaller, easy to generate and cost effective. A scenario of trusted authorities who issue access policy over a set of attributes. Search methods used were Authorized private keyword searches (APKS), Hierarchical predicate encryption (HPE), Cipher text policy attribute based encryption (CP-ABE). Authors in[16], explained that privacy and security are the most important issues that healthcare industry is facing. These issues are mostly addressed by using access control and cryptographic techniques. Patient's privacy is the most considerable issues that EHR is facing. That's why various access models are introduced to solve privacy issue in healthcare.Review of literature on different access models shows that most of the work is done on extension of Role Based Access Control (RBAC) to achieve privacy and security in healthcare .So,trust between patient and EHR system can be improved by incorporating patient consent as an integral part of EHR component.To better address patient privacy and security concernsin cloud,authors proposed a hybrid patient centered access control model.For future research,authors planned to implement and develop an access control model for cloud based EHR system that addresses security requirements as well as patient privacy needs.

C. Summary of Interoperability Approaches

From the related work on interoperability in healthcare, the interoperability approaches can be summarized into four groups [7]. Each approach has its own merits and demerits with respect to interoperability and security concerns.

Approaches	Advantages	Disadvantages
Layered approach	It is based on the classification of inputs into syntax, object and semantic attributes. Decomposition of task gives ease in functionality and reduces complexity of execution. The functionality of each layer is independent of other.	A mapping is required between layers to generate a consolidated output or decision on the given input size. It is a viable approach in achieving interoperability but needs to address integrity issues while sharing EHR across multi-platform environments
Centralized approach	It manages and controls sharing of EHR in flexible client-server environment. Interoperability can be achieved well if the collaborating units are kept to minimum	With the increase in the number of units interoperability becomes highly complex and due to the flexible nature of the approach, sensitive health data becomes highly vulnerable to security breaches.
Decentralized approach	It exhibits high security because no direct access is permitted to each other databases. The organizations obtain the permit to share the data explicitly and only after gaining permission can access each other's data	Though, highly robust security parameter, decentralized approach falls low on interoperability as no EHR-system mutually integrates its functionality with other.
Similarity Based Approach	The approach Maintains a balance between interoperability and security of EHR while sharing between independent healthcare users.	Complexity increased in this approach.

Table 1: Summary of Interoperability Approaches[7]

D. Existing Interoperability Standards

There are some **Existing interoperability standards** which are currently used to enable interoperability in electronic health. These are:

A.IEEE:

The Institute of Electrical and Electronic Engineers is a technical professional organization. It is also a Technical Development Organization that focuses on electrical and electronic technical issues. The main IEEE standards relevant to digital health are IEEE 11073 Personal Health Device (PHD) standard. These enable communication between medical healthcare and wellness devices with external computer systems. These are developed to specifically address the interoperability of personal health devices (egg thermometer, blood pressure monitor) with an emphasis on Personal use and more simple communication model.[17] This family of standards ensures that the user of the data knows exactly what was measured, where and how and also the information is not lost when transported to /from the sensor to a gateway and then to EHR.The Personal Connected Health Alliance has made considerable progress towards aligning the 11073 standard to modern health services and provide certificate routes for adoption of this standard.

B.DICOM

DICOM stands for Digital Imaging and Communication in Medicine. It is a standard for handling,storing,printing and transmitting information in medical imaging.DICOM files can be exchanged between two entities that are capable of receiving image and patient data in DICOM format.The standard has been defined by National Electrical Manufactures Association(NEMA).[18].DICOM is known as NEMA standard PS3 and as ISO standard 12052:2006 "Health Informatics".DICOM include workflow and data management.DICOM enables the integration of scanners ,servers,workstations,printers and network hardware from multiple manufacturers into a picture archiving and communication system(PACS)[19].Devices come with DICOM conformance statements which clearly states the DICOM classes they support.DICOM has been widely adopted by hospitals and is making inroads in smaller healthcare facilities like dentists and doctors offices. It is a standard directed at addressing technical interoperability issues in medical imaging.[18]

C. LOINC

Logical Observation Identifiers Names and codes (LOINC) was organized to develop a common terminology for lab and clinical observation. It helps to support the growing trends of sending clinical data electronically. Most labs and clinical services use HL7 to send their results from their reporting system to their care system. However the tests in these messages are identified by means of their internal, idiosyncratic code values. As a result ,receding care system cannot fully understand and properly file the results unless they adopt they adopt the procedures tests codes or invest in work to map each result procedure code system to their internal code system.LOINC is a rich catalog of measurement including lab test, clinical measures like vital signs standardized survey and more.[3].It enable the exchange and aggregation of clinical results for care delivery, outcome management and research by providing a set of universal codes and structured names to unambiguously identify things that can be measured or observed.LOINC provides a common language for interoperable data exchange and it has been recognized as the preferred standard for coding ,testing and observation in HL7.

D.SNOMED CT

Systemized Nomenclature for Medicine Clinical Terms (SNOMED CT) is a systematically organized computer process able collection of medical terms providing codes, terms, synonyms and definitions used in clinical documentation and reporting.The primary purpose is to encode the meaning used in health information and to support the effective clinical recording of data with the aim of improving patient care. It provides the core general terminology and enables consistent process able representation of clinical content in EHRs. [1].It is a comprehensive clinical terminology having almost 300,000 concepts. Information is captured in electronic patient record using clinical phrases.SNOMED CT provides a dictionary for these clinical phrases. For example a patient sees a lot of clinicians to help manage her health condition. All these clinicians and the patient are thinking of the same thing but using different description. So we can say the concept is same but have different synonyms.[20] All concepts in SNOMED CT have a unique id(so computer can recognize it).So synonyms helps in better end user experience in understanding familiar terms and data quality for a statistical analysis.

E .FHIR:

Recently, HL7 is responsible for emerging standard Fast Healthcare Interoperability Resource.FHIR address around 80% of use cases with extensions covering the remainders and combines the features of the HL7 v2, HL7 v3 and CDA product lines. It is a standard for exchanging healthcare information electronically.FHIR defines as set of resources that represents granular clinical concepts.FHIR uses recourses like patients,Allergy,Order etc.[21] There are six categories of FHIR resources which are: Clinical resources for clinical use, Identification resources to track people, places and things, Workflow resources track care processes, Infrastructure supports the architectural framework, Conformance resources ensure interoperability and Financial Resources.FHIR is designed for web and is easy to implement[21].

E. HL7:

HL7 is used for global health data interoperability. In April 2013, HL7 has licensed its standard and other intellectual property free of charge.HL7 standards have been revised overtime. Variation in use between V2.0 and V3.0.System can cause complications if it is not clear which version of HL7 standard are being used as the interfaces can be significantly different.HL7 is one of the most widespread health based open messaging standard available[22].HL7 messaging standards are widely implemented by the healthcare industry and have been deployed internationally for decades. HL7 Version 2 ("v2") health information exchange standards are used mostly by local hospital for the exchange of healthcare information, including electronic medical record information. HL7 Version 3 ("v3") was designed to address the short comes of version 2. HL7 v3 has been heavily criticized by the industry as its documentation is too complex and expensive to implement in real world systems and has been accused of contributing towards many failed and stalled systems implementations[22].

III. PROPOSED INTEROPERABILITY FRAMEWORK

A. Detailed Framework Description

A framework that deals both with the security and semantic interoperability of EHR is proposed in this paper. As it is seen in the literature review that some frameworks deal with Security but not with semantic interoperability and some deal with interoperability but not with the security of EHR. That's why a framework is proposed that is the combination of Hierarchal based approach and Similarity based approach so that both issues can be resolved. Users of the proposed

framework can be physicians, nurses, radiologists, pharmacists, laboratory technicians, radiographers, students, researchers, administrative staff and patients. The framework is divided into 4 layers as shown in Figure 2.

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 sub categories such as clinical, personal, and financial and research related data into meaningful entities. Fast Healthcare Interoperability Resource (FHIR) 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 sub categories, 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 and domain level and top level ontology will be treated here.

For semantic interoperability this 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.

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.

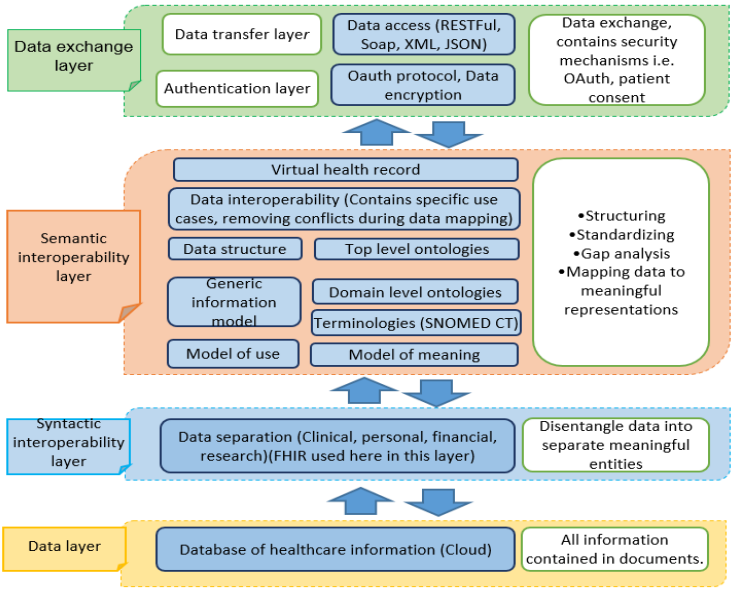

Figure 2: Proposed Interoperability Framework.

B. *Proposed Security Framework*

In proposed security framework Access control and Encryption techniques are used. For Access control, authentication is used like passwords and PIN numbers 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. AES is adopted as it is internationally recognized and can be easily used anywhere in the world and mostly used to encrypt sensitive data. 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 i.e. Network and Cloud Environment.

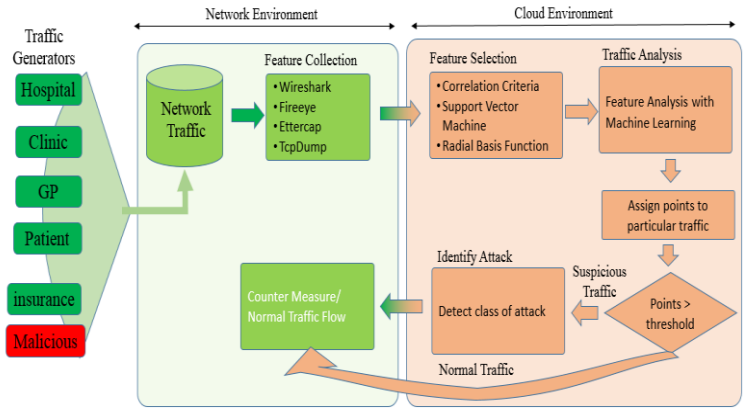

Figure 3: Security Model

1. Network Environment:

A comprehensive security framework is required 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 wireshark, Fireeye etc.

2. Cloud Environment:

This can be achieved by combining the capabilities of static and dynamic filtering. 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 above figure 4. The points are assigned based on benign or malicious traffic patterns and access to the resource is restricted if allotted points cross the threshold. The threshold is specified according to the availability of the resource accessed. This enables to create a pool which contains all the restricted nodes. The restricted nodes can be taken out from the pool and access is granted when desired resource is available. This technique allows a resource over the network to differentiate between legitimate and illegitimate users.

IV. CONCLUSION

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 and it's very difficult to achieve. It is observed that healthcare data is highly sensitive and required high level security and also it is observed that security varies from person to person and organization to organization. So there is a need of framework that will so solve both of these main issues.

So, we have proposed a framework that will solve both the issues in an effective way so that both of them donot effect each other. We are going to extend our framework to a prototype by simulation and by the help of protégé tool, we will build different healthcare systems, their ontology and also use RESTFUL API to integrate and transfer information between different systems. We will implement them with cloud environment and use machine learning and Artificial Intelligence techniques to make it more effective and progressive. As FHIR is the most popular standard used for interoperability now a days but even FHIR donot implement all the healthcare standards like SNOMED CT, DICOM etc.So in future we will extend FHIR so that the entire healthcare standards should be implemented in FHIR.

References

[1] N. H. S. C. F. Health, "Snomed Ct," *IEEE Journal of Biomedical and Healthcare Informatics*,vol. 19,issue 3, 2012.

[2] D.H.Interoperability,"DigitalHealthcareInteroperability," *www.novartisfoundation.org/sites/www...org/files/broadband-commission.pdf*, no. October, 2016.

[3] T. Sigwele, Y. F. Hu, M. Ali, J. Hou, M. Ali, and J. Hou, "An Intelligent Edge Computing based Semantic Gateway for Healthcare Systems Interoperability and Collaboration.",*IEEE Data Science and data Intensive System-2015*,pp.362-367

[4] 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.

[5] C. N. Mead, "Data interchange standards in healthcare IT--computable semantic interoperability: now possible but still difficult, do we really need a better mousetrap?," *J. Healthc. Inf. Manag.*, vol. 20, no. 1, pp. 71–78, 2006.

[6] S. Bhartiya, "Challenges to Sharing of Electronic Health Records in Interoperable Environments," *Procedia Comput. Sci.*, vol. 78, no. December 2015, pp. 192–198.

[7] 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.

[8] O. Iroju, A. Soriyan, I. Gambo, and J. Olaleke, "Interoperability in Healthcare: Benefits, Challenges and Resolutions," *Int. J. Innov. Appl. Stud.*, vol. 3, no. 1, pp. 262–270, 2013.

[9] Z. Bouanani-oukhaled *et al.*, "Ontological Model for EHR interoperability ,"*Conference on Informatics ,Management and Technology in Healthcare*, 2017.

[10] 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.

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

[12] A. Jha and M. C. Sunil, "Security considerations for Internet of Things."*http://pdf.semantic schloar.org/in security consideration of Internet of Things,L2T.Technology Service* ,2015.

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

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

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

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

[17] S. Schulz and C. Martínez-Costa, "How ontologies can improve semantic interoperability in health care," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8268 LNAI, pp. 1–10, 2013.

[18] A. Begoyan, "An overview of interopberability standards for electronic health records," *Soc. Des. Process Sci.*, pp. 1–8, 2007.

[19] Standards and Interoperability Framework, "Standards and Interoperability Framework: Query Health," 2014.

[20] K. R. Gøeg, R. Cornet, and S. K. Andersen, "Clustering clinical models from local electronic health records based on semantic similarity," *J. Biomed. Inform.*, vol. 54, pp. 294–304, 2015.

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

[22] D. Bender and K. Sartipi, "HL7 FHIR: An agile and RESTful approach to healthcare information exchange," *Proc. CBMS 2013 - 26th IEEE Int. Symp. Comput. Med. Syst.*, pp. 326–331, 2013.