International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

# A Survey on Security Challenges of Healthcare Analysis Over Cloud

Jaishree Jain[1]
Research Scholar,
Department of CSE,
Uttarakhand Technical University,
Dehradun[1]

Dr. Ajit Singh[2]
Associate Professor,
BTKIT, Dwarahat[2]

***Abstract*-The evolution of cloud computing in healthcare has revolutionized how the computing is abstracted and utilized on remote third party infrastructure. Introducing the cloud services in the health sector not only facilitates the exchange of electronic medical records among the hospitals and clinics, but also enables the cloud to act as a medical record storage center. Moreover, shifting to the cloud environment relieves the healthcare organizations of the tedious tasks of infrastructure management and also minimizes development and maintenance costs. Because of probable disclosure of medical records stored and exchanged in the cloud, the patients' privacy concerns should essentially be considered when designing the security and privacy mechanisms. Security strength defines the success of any network service. This survey paper aims to discuss, analyze security challenges and available solutions in cloud computing. Various approaches have been used to preserve the security of the health information in the cloud environment.**

***Keywords: Security Challenges, Electronic Healthcare Record, Cloud Computing.***

## I. INTRODUCTION

The cloud computing is an internet based environment allows us to use software, data and services over the internet from any location on any web enabled device [1]. By combining a set of existing and new techniques from research areas and Virtualization, cloud computing is seen as a computing paradigm where data resources are stored over at the platonic world of Internet. Cloud computing provides consumers a new way to share data resources and services that belong to various organizations or sites. Current developments in remote healthcare system, has been influenced by the development of IT industry and it will provide health services everywhere and in an easy way. These systems provide a platform for sharing medical information systems, infrastructure and applications in a format with the ability to provide automatic subscription. Since cloud computing shares distributed resources via the network in the open environment, thus security problems are important issues to address by developing application programs which will secure to work best for medical purposes [2]. In cloud computing performance, availability and security are main research topics. Among them cloud computing security is one of the important research topic. Cloud computing deploy resources and monitors the usage of resources all at times. Cloud computing collects the information, resources and also provides services to millions of users simultaneously. Data security is the major problem in cloud computing. For security, different attribute based encryption schemes are used for encryption before outsourcing data to cloud server. Personal Health Record (PHR) service is an emerging model for health information exchange. It allows patients to create, update and manage personal and medical information. Also they can control and share their medical information with other users as well as health care providers [3]. Security and privacy are considered as a critical issue in a cloud computing environment due to the sensitive and important information stored in the cloud for customers[4].

In general, cloud computer security identifies following main objectives:

1) Availability: The goal of availability for Cloud Computing systems is to ensure that data and services are always available for its users at any time, at any place.

2) Confidentiality: The goal of confidentiality is to keep users data secret in the Cloud systems by making it available only to eligible entities and no unauthorized access to data can be obtained.

3) Integrity: The goal of Data integrity in the Cloud system is to assure that data has not been altered in any way while it is stored or while its transport over the network.

4) Authentication: The goal of authentication is to assure the identity of the entity involved in the communication.

5) Accountability: The goal of accountability is to assure that no entity can deny its participation in a data transfer between them.

The main problems cloud computing faces are conserve confidentiality and integrity of data in aiding data security. The initial solution for these problems is encryption. Still encryption of data also raises new problems like Trust, Legal Issues & Confidentiality. Here is an analysis of some of the major problems faced by cloud systems and some respective solutions.

*a) Trust*

Today the major issue is Trust between the Service provider and the customer in the cloud computing. There is abstaining for the customer to be sure whether the management of the Service is trustworthy, and whether there is any risk of internal attacks. The only legal document between the user and service provider is the Service Level Agreement (SLA). This document consists of all the agreements between the user and the service provider.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

*b) Legal Issues*

There are several regulatory requirements, privacy laws and data security laws that cloud systems need to be adhere. One of the major problems with adhering to the laws is that laws alter from country to country, and users have no control over where their data is physically located.

*c) Confidentiality*

Confidentiality is preventing the abnormal disclosure of information. Preserving confidentiality is one of the major issues faced by cloud systems, since the information is stored at a remote location that the Service Provider has full access to it. Therefore, there has been some method required to achieve it.

These security objectives require the employment of certain security mechanisms and services to be implemented. A security mechanism can be defined as a process, or a device, which aimed to detect, or prevent, or recover from a security attack. The rest of this article is organized as follows. Section 2 gives a brief review of some security related definitions and concepts. Section 3 provides comparison of security approaches. Section 4 concludes the review article.

## II. REVIEW OF SOME SECURITY RELATED DEFINITIONS & CONCEPTS

Security considerations relate to risk areas like external knowledge storage, dependency on the "public" web, lack of management, multi-tenancy and integration with internal security. Compared to ancient technologies, the cloud has several specific options, like its massive scale and therefore the incontrovertible fact that resources happiness to cloud suppliers is fully distributed, heterogeneous and all virtualized. Ancient security mechanisms like identity, authentication, and authorization are not any longer enough for clouds in their current type. Security controls in Cloud Computing are completely different than security controls in any IT surroundings. However, as a result of the cloud service models used the operational models and therefore the technologies accustomed modify cloud services [5].

Prof. D. G. Vyawahare used key policy advanced encryption standard associated with user authorization period (KP-AESAP) allows user to decrypt data only within predefine authorization period [6]. To achieve fine-grained access control, attribute based encryption (ABE) is used to encrypt data before storing them. The cipher text (encrypted data) can be decrypted by any user if his secret key satisfies the access policy. To tackle the first challenge of ABE integration, both symmetric cryptography and ABE are used. Mostly, each file is encrypted with a randomly generated symmetric key (RSK) and RSK is again encrypted with ABE. Both the encrypted file and the encrypted RSK are sent to the cloud for storage to allow fine grained access[7]. Waleed, 2016 [8] demonstrated an innovation for user privacy and security in cloud computing open source software. This research paper focused on the user privacy and security in cloud computing and the solutions to improve privacy and security of cloud computing. The study employs UEC (Ubuntu Enterprise Cloud) Eucalyptus for simulation, which is the accepted open source cloud computing software as a solution. In this paper, simulation of some of the potential attacks to users' metadata and data stored in Eucalyptus database files is used in order to supply the necessary information on the consequences of abuse of cloud users' information privacy. Based on the research, RSA is secure but once the number of bits is beyond 3223 bits, it takes a long time to factor until it reaches appoint that the hardware cannot factor it out. Christian Esposito [9] used the seven phases of a key management process & breach identification module to monitor the data exchanged and stored within clouds when a given manufacturing process is performed, checked the correct flow of data within the overall infrastructure. Despite all of the preventive measures put in place by a company, a data breach can still occur. Breach identification remains an open research issue, and lacks a substantial body of literature. SAJID et. al.[10] highlighted some important facts about industrial SCADA (Supervisory control & data acquisition) systems with an emphasis on threats, vulnerabilities, and management. In such environments, the nature of data is such that it must be stored on server/s for backup or sharing purposes, and these server/s are mostly managed by a third party. This third party management means that these servers are likely to contain large numbers of clients and their confidential servers cannot information. The result is that the privacy of data on these clouds be guaranteed, as the data may or may not be shared with other clients. Deshmukh 2016 [11] proposed a frame work for storing the health records and accessing them by patients and physicians as authorized by key-control scheme. The scenarios we have considered here are of rural and urban health care centers and hence more appropriate for Indian health care services. The proposed scheme has double data security by introducing isolation between encryption schemes of transmitted data and stored data. The main concern of EHR system is to have simple structure of passwords and thus, attribute based or predicate based cryptographic algorithms are more suitable. Premarathne 2016 [12] addressed how to securely store and manage big EHR data, and how to ensure secure access to this data. To manage EHRs efficiently and securely, the author proposed a design based on steganography, which we use to hide confidential EHR data inside the ECG host data. Robust key exchange management between various parties is not involved in this paper. Marwan 2016 [13] addressed the security and privacy issues in medical image seems to allow a better and more secure deployment of cloud throughout the health sector. The key encryption management, access control policies are still obstacles that need to be overcome. Kumarage et al. 2016 [14] described how fully homomorphic encryption with efficient data processing models can help achieve data security and privacy in cloud-based data analytics systems. They proposed a distributed anomaly-detection model based on fuzzy data modeling as uniquely suitable for implementing secure cloud-based analytics as a service complemented with FHE (Fully Homomorphic Encryption). At any given instance only the data of a particular person will be subject to the clustering and anomaly-detection procedure.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

Mehraeen 2017 [15] investigated the security challenges in cloud computing. Review of articles showed that for ensuring healthcare data security, it is important to provide authentication, authorization and access control within cloud's virtualized network. Chouhan 2016 [16] discussed Denial of Service (DoS) attacks, Cloud Malware Injection Attack, Side Channel Attacks, Authentication Attacks and Man-In-The-Middle Cryptographic Attacks of cloud computing and also provided some possible solutions. The concepts discussed in this paper will help to build a strong architecture for security in the field of cloud computation. Alzoubaidi 2016 [17] proposed a national cloud computing data centers architecture solution to host healthcare system services computing resources components, proposing building a national e-health cloud environment to overcome many of the challenges confronting the success of Hakeem the core of the National e-Health System (NHS) for the provision of e-Health as a Service. Rani 2016 [18] proposed an Integrated Secure Authentication (ISA) in e-health Care application using cloud environment to use spatial information of Received Signal Strength (RSS), a physical property associated with each node, that is difficult to modify, and not based on cryptography. Similarly, Tri Mode Algorithm is introduced that can secure the data storage and fully authenticated data sharing from the use of Trusted Third Party (TTP). The algorithm can be implemented on three stages SetUP, CheckUP and LockUP. A simulated and analytical result highlights the security, efficiency and simplicity of our proposed scheme is better than the existing approach. Kaur 2016 [19] compared important techniques with each other in terms of encryption comparative study between two such widely used encryption algorithms( AES) and (RSA) and Congestion control mechanisms. Barthelus 2016 [20] applied an evidence-based research methodology that consists of a systematic review of primary literature and a thematic synthesis of findings. The findings indicate that the primary reasons for resistance to cloud adoption within the healthcare industry are security and privacy risks to sensitive patient data, integration challenges, and a firms' potential to lose control of data to cloud providers. However, incorporating analytical tools and safeguards into the decision process can mitigate these challenges. This study deepens knowledge of innovation resistance, which has been limited to innovation research thus far, and presents a conceptual model of how resistance affects each stage of the innovation decision process. This study proposes the cloud adoption toolkit to healthcare decision makers as a practical solution to address the challenges of cloud adoption. Noufal 2016 [21] defined the design and execution of e-health monitoring system. The system architecture consists of smart devices and wireless sensors for real time analysis and storage of medical parameters of patients. The system aims at creating a universalaccess to retrive and analyse the medications taken by the patient by using RFID module. The system is designed to monitor the physical status of the patient. While monitoring, the acquired data is updated automatically and is saved in the cloud, so that it can be retrieved whenever required. The privacy is maintained by providing the patients with a unique ID, where the patients can update their records after each medication. Raval 2016 [22] achieved data confidentiality and identity privacy with high efficiency and efficiently realized access control of patient's personal health information by resisting various kinds of malicious attacks and far out performed previous schemes in terms of storage, computational and communication overhead. Tewari 2016 [23] focused on various limitations and their possible solutions available within WBANs in order to provide secure and private information management to its dependents and users. Desai 2016 [24] discussed the cloud computing evolution, how can the health care industries use the cloud computing and improves the service to patient in India, challenges of cloud in health care and benefits of cloud techniques in health care industries. Zriqat 2016 [25] proposed a novel Context-aware Access Control Security Model (CARE) to capture the scenario of data interoperability and support the security fundamentals of healthcare systems along with the capability of providing fine-grained access control. Sangeetha et. al.[26] defined a public-private key pair for each attribute. For each user' secret key, there is a combination of user's ID and the attribute's secret key, thereby ensuring that each attribute presents a different key to each user. Data files are encrypted by public key components and access matrices converted from the access structure; user secret keys are defined to reflect their access privileges so that a user can only decrypt a cipher text if they have the matched attributes to satisfy the cipher text. To resolve the challenging issues of collusion resistance, this scheme provides users with a public key fitted to their secret keys; this paper used user's ID to "tie" together the attributes belonging to this user so that they cannot be successfully combined with another's user's attributes. Hanen 2016 [27] proposed solution shows that the MCMAS (Multi Cloud Multi Agent system) has a commanding capability to cope with the problem of traditional application. The performance of the MCMAS is compared with the traditional system in polyclinic ESSALEMA which showed that this prototype yields better recital than using usual application.

Rao 2015 [28] discussed data security challenges and solutions are provided for these challenges to overcome the risk involved in cloud computing. However, proper key management techniques can be used to distribute the key to the cloud users such that only authorized persons can access the data. Griebel et. al. 2015 [29] discussed on the status of cloud-computing in healthcare and to identify areas of interest beyond typical "OMICS" topics. They found that especially resource intensive (e.g. medical imaging) and communication intensive areas such as various kinds of tele-applications are predestined for cloud computing use. Rezaeibagha 2015 [30] investigated crucial technical security and privacy requirements of EHR systems based on a comparison of a systematic review of the literature with ISO/IEC 27002:2013 and ISO/IEC 29100:2011 standards. It demonstrated, regardless of the enormous effort required, well defined access control policies should be mandated in order to provide patient privacy by limiting the access rights to patient data with

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

proper access control policy languages and standards. Dubovitskaya 2015 [31] proposed an architecture of a secure and scalable privacy preserving eHealth cloud system that allows to store and efficiently search over patient data used for the treatment and an algorithm that allows to build a database with patients' data for the research purposes. With the proposed algorithm we only preserve the utility of the *RSDB( Non –Redundant representative sequence)*. However, to improve utility of the data from *RSDB*, the possibility to de-generalize the data from *RSDB* without violation of patients' privacy during bounded time interval need to be considered. Bhati 2015 [4] focused on the issues related to the data security aspect of cloud computing know are reactive security measure. Rathi 2015 [32] proposed to protect the healthcare data in the cloud. This system had a double layer protection in which the EHRs are stored in the cloud. However, Encryption/ Decryption can be done in one layer and in the other layer; Splitting/ Merging of the cipher text can be done. Thus, data security can be improved in cloud computing. Zhou [33] proposed a secure and efficient privacy-preserving dynamic medical text mining and image feature extraction scheme PPDM (Privacy-Preserving Protocol for Cloud-Assisted e-Healthcare Systems) in cloud-assisted e-healthcare systems. Elmogazy 2015 [34] proposed homomorphism cryptography with Attribute Based Encryption. In this scenario, we suggest that EHR is stored as a Hierarchical record; each part of patient record (i.e. Personally Identifiable Information and Healthcare data) is encrypted separately using different keys. Sedem 2015 [35] measured the ICT awareness of stakeholders in healthcare while also providing an evidence of the possibility of cloud implementation by Ghana Health Services (GHS) in relation to the ICT awareness of stakeholders. It also provides a framework for a cloud based E-Health adoption by the GHS. Sengupta 2015 [36] proposed hybrid RSA encryption technique provides higher level of security than only RSA algorithm. Encryption of data for IaaS will secure the data from confidentiality but to maintain integrity of data in cloud, secure protocol (like FTP with SSL, HTTPS, Secure Copy Program) transactions are required.[20] Boyinbode 2015 [37] proposed and implemented a cloud-based electronic medical record (CloudeMR) system to improve the delivery of healthcare system in the rural communities of Nigeria. In this paper, a complete, robust and efficient cloud-based EMR system has been designed and implemented. Fabian 2015[38] presented a novel architecture and its implementation for inter-organizational data sharing, which provides a high level of security and privacy for patient data in semi-trusted cloud computing environments. This architecture features attribute-based encryption for selective access authorization and cryptographic secret sharing in order to disperse data across multiple clouds, reducing the adversarial capabilities of curious cloud providers. An implementation and evaluation by several experiments demonstrate the practical feasibility and good performance of our approach.

Donald 2014 [39] analyzed the importance of the data security in the cloud. Reason for choosing symmetric encryption algorithms are effective to handle encryption for large amount of data, and effective speed of storing data in the cloud. Only security and privacy for protecting the data in cloud storage is included. Youssef 2014 [40] proposed a framework for secure Health Information Systems (HISs) based on big data analytics in mobile cloud computing environment. The framework provides a high level of integration, interoperability, and sharing of EHRs among healthcare providers, patients and practitioners. The cloud permits a fast Internet access, sharing, and provision of EHRs by authenticated users. Big data analytics helps analyze patient data to provide right intervention to the right patient at the right time. The proposed framework applies a set of security constraints and access control that guarantee integrity, confidentiality, and privacy of medical data. Zafar 2014 [41] presents a cloud driven healthcare service model, and explores different services of cloud for health industry. Paper also shed light on the constraints associated with cloud adoption for healthcare. Paper concludes that healthcare stakeholders can take advantage of cloud services to offer novel patient care applications, reduce costs and management, and ultimately provide quality healthcare services. Tebaa 2014 [42] presented the security limitations in the single Cloud and the usefulness of adopting rather Multi-Clouds strategy to reduce security risks, through the use of DepSky which is a virtual storage system that ensures better availability and high confidentiality of data. The homomorphic encryption applied to single cloud allows operations on encrypted data without decrypting. The swot analysis of the different security mechanisms used in the multi-clouds allows to cloud providers to know what is the mechanism to use to provide better security (Confidentiality, Integrity and Availability) of data stored in their data centers, and the client can understand the limitations of single cloud and the benefits of multi-clouds, DepSky is the most reliable mechanism. The use of multi-clouds computing is not restricted to data storage, but also performing operations on data. Plachkinova [43] proposed a framework focusing on the security issues related to implementing EHR systems on the cloud. The framework targets evaluators from healthcare practitioners and is designed to be a comprehensive tool for improving decision making.

Sultana 2014 [44] proposed an Information Integration and Informatics framework. The proposed framework allows: (1) Data Integration – integrating data from scattered and different sources into a same nomenclature and establishing effective use of clinical data combined from diverse EHRs, (2) Data Access – querying and getting healthcare data stored in the cloud, (3) Data Analytics – efficient data analysis of big healthcare data collected in cloud, (4) Data Storage – healthcare data storage and lifecycle management. The importance of the proposed work obtained from the using and developing of technologies for clinical data tools, integration and techniques for explicate healthcare data effectively, which strengthen the benefits and economics of present cloud computing environments already in or entering the use in other domains. Nagaty

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

2014 [45] presented a secure mobile health application which is based on hybrid cloud architecture combined with cryptographic techniques to protect privacy, integrity and security of patients and health care givers data and with role based access control to authenticate and authorize users. Hybrid cloud platform combines the advantages of both the private cloud which guarantees privacy and safety of data and the public cloud which provides a platform for reduced services costs. Integrating cryptography and role based access control with hybrid cloud computing ensures the safety of patients' medical records and enable user authentication and authorization for access control. This integrated technology can provide the mobile health care the required safety and privacy to flourish. Gurav 2014 [46] proposed novel patient-centric framework and suite of mechanism for data access control to PHR's stored in semi trusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR file. Data owner update the personal data into third party cloud data centers. Multiple data owners can access the same data values. Our scheme supports efficient on-demand user/attribute revocation. Thilakanathan 2014 [47] discussed why data sharing in the Cloud is important and the traditional approach to data sharing in the Cloud and also discussed key management in the Cloud and how proper key management leads to more secure and confidential data which can aid secure and private sharing of data in the Cloud. The different techniques, namely ABE and PRE that are currently used to enable secure data sharing in the cloud are also discussed. Scholar 2014 [3] enabled dynamic modification of access policies or file attributes, support efficient on demand user/attribute revocation. However some practical limitations are in building PHR system. The data access right could be given based on user's identities rather than their attributes, while ABE does not handle that efficiently. For solving this problem in this paper proposed PHR system, based on Attribute Based Broadcast Encryption (ABBE). Madarkar 2014 [48] proposed TSFS algorithm which very lightweight efficient encryption algorithm. It helps to maintain confidentiality of healthcare data and also discussed about security of E-hospital management in cloud computing and image conversion model. Now days healthcare is important topic in cloud computing but it is very defend less toward security. Louk et.al. [2] proposed the constructive idea of Healthcare data via cloud computing and the security accessing data by authorized individuals. This paper also described security elements like monitoring, recording, tracking and notification. For the purpose of encryption-decryption, AES-256/SHA is used. Re-encryption "tag" and "mark" for data access system is only be functional for every legal user. It suggests that the cloud computing based on encryption and decryption services. Encrypted medical data could be accessed and decrypted from anywhere and whomever with particular authentication. Ribeiro 2014 [49] presented a software proxy that enables the outsourcing of XDS (Cross-enterprise document sharing**)** architectural parts while preserving the interoperability, confidentiality, and searchability of clinical information. A key component in our architecture is a new searchable encryption (SE) scheme—Posterior Playfair Searchable Encryption (PPSE)—which, besides keeping the same confidentiality levels of the stored data, hides the search patterns to the adversary, bringing improvements when compared to the remaining practical state-of-the-art SE schemes. [44]described the design of an Information Integration and Informatics framework that allows storing, integrating and analyzing healthcare data in the cloud. The Information Integration and Informatics framework allow the development of advanced healthcare application with data integrated in difference database. Application developers can quickly develop healthcare applications by not thinking about the data management in cloud and cloud infrastructure management deployment configuration which are taken care by the Information Integration and Informatics framework. Ikuomola 2014 [50] proposed a system that ensure the security of electronic health records stored in the cloud using Homomorphic Encryption to secure patients medical records and Bilayer Access Control to gives access right to the records. Khan et. al. 2014 [51] presented a secure cloud-based mobile healthcare framework using wireless body area networks (WBANs). The research work presented here is twofold: first, it attempts to secure the inter-sensor communication by multi-biometric based key generation scheme in WBANs; and secondly, the electronic medical records (EMRs) are securely stored in the hospital community cloud and privacy of the patients' data is preserved. The evaluation and analysis shows that the proposed multi-biometric based mechanism provides significant security measures due to its highly efficient key generation mechanism.

## III. COMPARISON OF THE SECURITY APPROACHES

### *3.1 Research Aim*

The aim of this study was to investigate the security challenges in cloud computing related to healthcare. So, this paper introduces a detailed review of the healthcare cloud computing security issues and explores the main challenges focusing on the compliance concerns and ensuring trust data security with a systematic review of 51 articles.

### *3.2 Research Questions*

Q1.How Confidentiality concerns in the healthcare cloud computing?
Q2. How can we ensure access control in cloud computing infrastructures?
Q3. How privacy is protected in healthcare cloud computing?
Q4.How data integrity can be ensured?
Q5.How can we ensure availability of data?

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

Table: 5.1 Summary of final studied articles and their relevance to the research questions

| S. No. | Work | Researcher | Year | Problem Characteristics | Related Results | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | Q1 | Q2 | Q3 | Q4 | Q5 |
| 1 | [15] | Mehraeen et.al. | 2017 | Security Challenges in Healthcare Cloud Computing: A Systematic Review | Y | Y | Y | N | N |
| 2 | [8] | Waleed et. al. | 2016 | User Privacy and Security in Cloud Computing | Y | N | Y | N | N |
| 3 | [9] | Christian Esposito et. al. | 2016 | Cloud Manufacturing: Security, Privacy, and Forensic Concerns | Y | N | Y | N | N |
| 4 | [10] | Sajid et.al. | 2016 | Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges | Y | N | Y | Y | Y |
| 5 | [11] | Deshmukh | 2016 | Design of cloud security in the EHR for Indian healthcare services | Y | N | N | N | N |
| 6 | [12] | Premarathne et.al. | 2016 | Hybrid Cryptographic Access Control for Cloud- Based EHR Systems | Y | Y | N | N | N |
| 7 | [13] | Marwan et. al. | 2016 | Cloud-Based Medical Image Issues | Y | Y | N | N | N |
| 8 | [14] | Kumarage et al. | 2016 | Secure Data Analytics for Cloud-Integrated Internet of Things Applications | Y | N | Y | N | N |
| 9 | [20] | Barthelus et.al. | 2016 | Adopting cloud computing within the healthcare industry: opportunity or risk? | Y | N | N | N | Y |
| 10 | [16] | Chouhan et. al. | 2016 | Security Attacks on Cloud Computing With Possible Solution | Y | N | N | N | Y |
| 11 | [17] | Alzoubaidi et. al. | 2016 | Cloud Computing National e-health services: Data Center Solution Architecture | N | N | N | N | Y |
| 12 | [18] | Rani et. al. | 2016 | An efficient secure authentication on cloud based e-health care system in WBAN. | Y | Y | Y | N | Y |
| 13 | [19] | Kaur et. al. | 2016 | Data Privacy In Healthcare Networks With Secure Key Exchange Mechanism | Y | Y | Y | Y | N |
| 14 | [21] | Noufal et.al. | 2016 | Smart e-Health Monitoring and Maintenance Using Cloud | Y | N | N | N | N |
| 15 | [22] | Raval et. al. | 2016 | Cloud based Information Security and Privacy in Healthcare | Y | Y | Y | N | N |
| 16 | [23] | Tewari et.al. | 2016 | Security and Privacy in E-Healthcare Monitoring with WBAN: A Critical Review | Y | N | Y | N | N |
| 17 | [24] | Desai et.al. | 2016 | Opportunity and Implementation of Cloud Computing in Indian Health Sector | Y | N | N | N | Y |
| 18 | [25] | Zriqat et.al. | 2016 | Security and Privacy Issues in E healthcare Systems: Towards Trusted Services | N | Y | Y | N | N |
| 19 | [26] | Sangeetha et. al. | 2016 | Analysis Of An Effective, Scalable And Secured Data Sharing Service In Cloud Computing | Y | N | Y | N | N |
| 20 | [27] | Hanen et.al. | 2016 | An enhanced healthcare system in mobile cloud computing environment | Y | N | N | Y | Y |
| 21 | [1] | N.H. Hussein | 2016 | A survey of Cloud Computing Security challenges and solutions | Y | N | Y | Y | N |
| 22 | [5] | R. Kumar | 2016 | A Survey on Security Issues in Cloud Computing | Y | Y | N | Y | Y |
| 23 | [6] | P. D. G. Vyawahare et.al. | 2016 | A Survey on Security Challenges and Solutions in Cloud Computing | Y | N | Y | Y | N |
| 24 | [28] | Rao et.al. | 2015 | Data Security Challenges and Its Solutions in Cloud Computing | Y | N | N | N | Y |
| 25 | [29] | Griebel et. al. | 2015 | A scoping review of cloud computing in healthcare | Y | Y | N | N | N |
| 26 | [30] | Rezaeibagha et. al. | 2015 | A systematic literature review on security and privacy of electronic health record systems: technical perspectives | Y | N | Y | N | N |
| 27 | [31] | Dubovitskaya et. al. | 2015 | A Cloud-Based eHealth Architecture for Privacy Preserving Data Integration | N | Y | Y | Y | N |
| 28 | [4] | Bhati et.al. | 2015 | Review of Passive Security Measure on Trusted Cloud Computing | Y | Y | Y | N | N |
| 29 | [32] | Rathi et.al. | 2015 | Healthcare Data Security in Cloud Computing | Y | Y | N | N | N |
| 30 | [33] | Zhou et. al. | 2015 | PPDM: A Privacy-Preserving Protocol for Cloud-Assisted e-Healthcare Systems | | | | | |
| 31 | [34] | Elmogazy et. al. | 2015 | Towards Healthcare Data Security in Cloud Computing | Y | Y | Y | N | N |
| 32 | [36] | Sengupta et.al. | 2015 | Designing of Hybrid RSA Encryption Algorithm for Cloud Security | Y | N | N | N | N |
| 33 | [35] | Sedem et. al. | 2015 | Cloud Computing Framework for E-Health in Ghana: Adoption Issues and Strategies: Case Study Of Ghana Health Service | N | N | N | N | Y |

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 34 | [37] | Boyinbode et. al. | 2015 | CloudeMR: A Cloud Based Electronic Medical Record System | N | N | N | N | Y |
| 35 | [43] | Plachkinova et. al. | 2015 | Health Records on the Cloud: A Security Framework | N | N | N | Y | Y |
| 36 | [38] | Fabian et.al. | 2015 | Collaborative and secure sharing of healthcare data in multi-clouds | Y | N | Y | N | N |
| 37 | [39] | Donald et.al. | 2014 | A Comparative Analysis of Encryption Techniques and Data Security Issues in Cloud Computing | Y | N | N | N | N |
| 38 | [40] | Ahmed E. Youssef | 2014 | A Framework For Secure Healthcare Systems Based On Big Data Analytics In Mobile Cloud Computing Environments | Y | Y | N | N | Y |
| 39 | [41] | Zafar 2014 | 2014 | Cloud Computing Services for the Healthcare Industry | Y | N | Y | N | N |
| 40 | [42] | M. Tebaa and S. E. L. Hajji | 2014 | From Single to Multi-Clouds Computing Privacy and Fault Tolerance | Y | N | N | Y | Y |
| 41 | [44] | Sultana et.al. | 2014 | Cloud-Based Development Of Smart And Connected Data In Healthcare Application | N | N | N | Y | N |
| 42 | [45] | Nagaty et.al. | 2014 | Mobile Health Care on a Secured Hybrid Cloud | Y | Y | Y | Y | N |
| 43 | [46] | Y. B. Gurav et. al. | 2014 | Scalable and Secure Sharing of Personal Health records in Cloud Computing Using Attribute Based Encryption | Y | Y | Y | N | N |
| 44 | [47] | Thilakanathan et.al. | 2014 | Secure Data Sharing in the Cloud | Y | N | Y | N | N |
| 45 | [3] | Raseena et.al. | 2014 | Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Broadcast Encryption | Y | Y | Y | N | N |
| 46 | [48] | Jitendra Madarkar.et.al. | 2014 | Security issues of Patient Health Records in E-Hospital Management in Cloud | Y | N | Y | N | N |
| 47 | [2] | Maya Louket et.al. | 2014 | Security System for Healthcare Data in Cloud Computing | Y | Y | N | N | N |
| 48 | [49] | Lu´ıs S. Ribeiroet.al. | 2014 | XDS-I Outsourcing Proxy: Ensuring Confidentiality While Preserving Interoperability | Y | N | Y | N | N |
| 49 | [50] | Ikuomola et. al. | 2014 | Securing Patient Privacy in E-Health Cloud Using Homomorphic Encryption and Access Control | Y | Y | N | N | N |
| 50 | [51] | Khan et.al. | 2014 | A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks | Y | Y | Y | Y | Y |
| 51 | [7] | Freire et.al. | 2014 | Security issues in cloud environments : a survey | Y | Y | N | Y | N |

*Y* yes, *N* no

## IV. CONCLUSION

This literature survey is based on security challenges in healthcare analysis over cloud. Articles of Journals from 2014 to 2017 have been taken for the purpose of literature survey (Table 5.1). One among various security challenges in cloud computing is worry about sensitive data which is communicated over cloud. With the references of studied articles; we have found that there is much insecurity. The research has not been completed to secure these problems i.e.

1. Data Security: The major issues in cloud computing is data security and it has many aspects like confidentiality, Integrity, reliability, availability, backup and recovery. The potential research direction would be to find the ways to store and process data in a way that does not breach the privacy and security.
2. Access Control: The owner create the set of access control rules on his data and send the data along with the access control policy. In this way, any member of his panel can only use the data by the access control policy given by the owner. If the member tries to access the data, the access control policy should "lock" without the permission of owner. This is a challenge in access control.
3. Protection from Malicious Code: Malicious Code affects on theft of data and loss the data. Malicious code is created by the hackers to change the information. These issues have provided a barrier to the worldwide adoption of the Cloud. The health cloud environment may reveal sensitive information to the unauthorized individuals by monitoring the sequence of the events. Therefore, it is highly desirable that the mechanisms should be developed to deploy efficient auditing and accountability mechanisms that anonymously monitor the utilization of health records.

The security challenges research issues analyzed here provide good understanding that leads to future research.

## REFERENCES

[1] N. H. Hussein, "A survey of Cloud Computing Security challenges and solutions II- Infrastructure as Services," vol. 14, no. 1, pp. 52–56, 2016.
[2] M. Louk, H. Lim, and H. J. Lee, "Security System for Healthcare Data in Cloud Computing," vol. 8, no. 3, pp. 241–248, 2014.
[3] P. G. Scholar, "Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Broadcast Encryption," vol. 102, no. 16, pp. 13–19, 2014.
[4] M. Bhati and P. Rani, "Review of Passive Security Measure on Trusted Cloud Computing," no. 3, 2015.
[5] R. Kumar and A. Pandey, "A Survey on Security Issues in Cloud Computing," vol. 3, no. 3, pp. 506–517, 2016.
[6] P. D. G. Vyawahare, R. B. Bende, D. N. Bhajipale, R. D. Bharsakle, and A. G. Salve, "A Survey on Security Challenges and Solutions in Cloud Computing," pp. 4069–4073, 2016.
[7] M. M. Freire and P. R. M. Inácio, "Security issues in cloud environments : a survey," pp. 113–170, 2014.
[8] A. Waleed and L. Chunlin, "User Privacy and Security in Cloud Computing," vol. 10, no. 2, pp. 341–352, 2016.
[9] C. Esposito, A. Castiglione, B. Martini, and K. K. R. Choo, "Cloud Manufacturing: Security, Privacy, and Forensic Concerns," IEEE Cloud Comput., vol. 3, no. 4, pp. 16–22, 2016.
[10] A. Sajid, H. Abbas, and K. Saleem, "Cloud-Assisted IoT-Based SCADA Systems Security : A Review of the State of the Art and Future Challenges," vol. 4, 2016.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

[11] P. Deshmukh, "Design of cloud security in the EHR for Indian healthcare services," J. KING SAUD Univ. - Comput. Inf. Sci., pp. 1–7, 2016.
[12] U. Premarathne, A. Abuadbba, and A. Alabdulatif, "Hybrid Cryptographic Access Control for Cloud- Based EHR Systems," 2016.
[13] M. Marwan, A. Kartit, H. Ouahmane, A. Jabran, K. Jabran, and B. P. El, "Cloud-Based Medical Image Issues," vol. 11, no. 5, pp. 3713–3719, 2016.
[14] H. Kumarage, I. Khalil, and A. Alabdulatif, "Secure Data Analytics for Cloud- Integrated Internet of Things Applications," 2016.
[15] E. Mehraeen, M. Ghazisaeedi, J. Farzi, and S. Mirshekari, "Security Challenges in Healthcare Cloud Computing : A Systematic Review," vol. 9, no. 3, pp. 511–517, 2017.
[16] P. Chouhan and R. Singh, "International Journal of Advanced Research in Security Attacks on Cloud Computing With Possible Solution," vol. 6, no. 1, pp. 92–96, 2016.
[17] A. R. Alzoubaidi, "Cloud Computing National e-health services: Data Center Solution Architecture," Int. J. Comput. Sci. Netw. Secur., vol. 16, no. 9, pp. 1–6, 2016.
[18] A. A. V. Rani and E. Baburaj, "An efficient secure authentication on cloud based e-health care system in," pp. 53–59, 2016.
[19] E. R. A. Kaur, "Data Privacy In Healthcare Networks With Secure Key Exchange Mechanism," pp. 2449–2451, 2016.
[20] L. Barthelus, "Adopting cloud computing within the healthcare industry: opportunity or risk?," Online J. Appl. Knowl. Manag., vol. 4, no. 1, pp. 1–16, 2016.
[21] M. M. Noufal, "Smart e-Health Monitoring and Maintenance Using Cloud," no. 3, pp. 61–65, 2016.
[22] D. Raval, "Cloud based Information Security and Privacy in Healthcare," vol. 150, no. 4, pp. 11–15, 2016.
[23] A. Tewari, "Security and Privacy in E-Healthcare Monitoring with WBAN : A Critical Review," Int. J. Comput. Appl., vol. 136, no. 11, pp. 37–42, 2016.
[24] V. L. Desai, "Opportunity and Implementation of Cloud Computing in Indian Health Sector," no. July, pp. 333–338, 2016.
[25] A. Zriqat, "Security and Privacy Issues in Ehealthcare Systems : Towards Trusted Services," vol. 7, no. 9, pp. 229–236, 2016.
[26] Sangeetha, ANALYSIS OF AN EFFECTIVE , SCALABLE AND SECURED DATA," pp. 135–141, 2016.
[27] J. Hanen, Z. Kechaou, and M. Ben Ayed, "An enhanced healthcare system in mobile cloud computing environment," Vietnam J. Comput. Sci., vol. 3, no. 4, pp. 267–277, 2016.
[28] R. V. Rao and K. Selvamani, "Data Security Challenges and Its Solutions in Cloud Computing," Procedia - Procedia Comput. Sci., vol. 48, no. Iccc, pp. 204–209, 2015.
[29] L. Griebel et al., "A scoping review of cloud computing in healthcare," pp. 1–16, 2015.
[30] F. Rezaeibagha, K. T. Win, and W. Susilo, "A systematic literature review on security and privacy of electronic health record systems : technical perspectives," vol. 44, no. 3, 2015.
[31] A. Dubovitskaya, V. Urovi, M. Vasirani, K. Aberer, and M. I. Schumacher, "A Cloud-Based eHealth Architecture for Privacy Preserving Data Integration," vol. 2, pp. 585–598, 2015.
[32] G. Rathi, M. Abinaya, and D. M. K. T, "Healthcare Data Security in Cloud Computing," pp. 1807–1815, 2015.
[33] C. Systems et al., "PPDM : A Privacy-Preserving Protocol for," vol. 9, no. 7, pp. 1332–1344, 2015.
[34] H. Elmogazy and O. Bamasak, "Towards Healthcare Data Security inCloud Computing," no. 3, pp. 356–361, 2009.
[35] A. A. Sedem and J. K. Panford, "Cloud Computing Framework for E-Health in Ghana : Adoption Issues and Strategies : Case Study Of Ghana Health Service," Int. J. Comput. Appl., vol. 118, no. 17, pp. 13–17, 2015.
[36] N. Sengupta, "Designing of Hybrid RSA Encryption Algorithm for Cloud Security," pp. 4146–4152, 2015.
[37] O. Boyinbode and G. Toriola, "CloudeMR : A Cloud Based Electronic Medical Record System," Int. J. Hybrid Inf. Technol., vol. 8, no. 4, pp. 201–212, 2015.
[38] B. Fabian, T. Ermakova, and P. Junghanns, "Collaborative and secure sharing of healthcare data in multi-clouds," Inf. Syst., vol. 48, pp. 132–150, 2015.
[39] A. C. Donald, M. P. Scholar, M. P. Scholar, and A. C. Donald, "A Comparative Analysis of Encryption Techniques and Data Security Issues in Cloud Computing" no. November, 2014.
[40] A. E. Youssef, "A F RAMEWORK FOR SECURE HEALTHCARE SYSTEMS BASED ON BIG DATA ANALYTICS IN MOBILE CLOUD," vol. 2, no. 2, pp. 1–11, 2014.
[41] Z. Zafar, S. Islam, M. S. Aslam, and M. Sohaib, "Cloud Computing Services for the Healthcare Industry," pp. 25–29, 2014.
[42] M. Tebaa and S. E. L. Hajji, "From Single to Multi-Clouds Computing Privacy and Fault Tolerance," IERI Procedia, vol. 10, pp. 112–118, 2014.
[43] M. Plachkinova, A. Alluhaidan, and S. Chatterjee, "Health Records on the Cloud : A Security Framework," pp. 152–158.
[44] S. N. Sultana, G. Ramu, and P. B. E. Reddy,"CLOUD-BASED DEVELOPMENT OF SMART AND CONNECTED DATA IN HEALTH CARE APPLICATION," vol. 5, no. 6, pp. 1–11, 2014.
[45] K. A. Nagaty, "Mobile Health Care on a Secured Hybrid Cloud," vol. 4, no. 2, 2014.
[46] Y. B. Gurav and M. Deshmukh, "Scalable and Secure Sharing of Personal Health records in Cloud Computing Using Attribute Based Encryption," vol. 3, no. 7, pp. 2012–2014, 2014.
[47] D. Thilakanathan, S. Chen, and R. A. Calvo, "Secure Data Sharing in the Cloud," pp. 45–73, 2014.
[48] J. Madarkar, "Security issues of Patient Health Records in E-Hospital Management in Cloud," vol. 9359, no. 6, pp. 46–51, 2014.
[49] S. Ribeiro, C. Viana-ferreira, and C. Costa, "XDS-I Outsourcing Proxy : Ensuring Confidentiality While Preserving Interoperability," vol. 18, no. 4, pp. 1404–1412, 2014.
[50] A. J. Ikuomola and O. O. Arowolo, "Securing Patient Privacy in E-Health Cloud Using Homomorphic Encryption and Access Control," Int. J. Comput. Networks Commun. Secur., vol. 2, no. 1, pp. 15–21, 2014.
[51] F. A. Khan, A. Ali, H. Abbas, and N. A. H. Haldar, "A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks," Procedia Comput. Sci., vol. 34, pp. 511–517, 2014.