ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 7, October 2015

Privacy and Security Issues in Big Data with Special Reference to Healthcare Sector

Abdul Mohisin[1], Mounika K[1], Rakesh Kumar[2]

Student V Semester, Dept. of MCA, AIMIT, St. Aloysius College (Autonomous), Mangalore, Karnataka, India

Assistant Professor, Dept. of MCA, AIMIT, St. Aloysius College (Autonomous), Mangalore, Karnataka, India

ABSTRACT: There is highly increasing cost for healthcare and increased health insurance premiums, we need a proactive healthcare and wellness. The new wave of digitizing medical records has seen a paradigm shift in the healthcare service industry. This resulted in health care industry witnessing an increase in high volume of data in terms of the complexity, diversity and timeliness. As healthcare experts look for every possible way to minimize the costs while improving the care process, delivery and management, big data emerges as a plausible solution with the promise saying that it will transform the healthcare industry. This standard shift from reactive to proactive healthcare can lead to an overall decrease in healthcare costs and also lead to the economic growth.In this paper, we have summarized the results of our survey related to the privacy and security issues of big data with reference to heath care sector.

KEYWORDS: Big data, Security, Medical services, Data privacy, Industries, Privacy, Real-time systems.

I. INTRODUCTION

The new change of digitizing medical records has seen a paradigm shift in the healthcare industry. As a result, healthcare industry is a witness for a huge increase in sheer volume of data in terms of complexity, diversity and timeliness. In healthcare, several factors provide the necessary drive to harness the power of big data.As the data size is very huge, it is difficult to use traditional database and software techniques to process it. In many organizations either the data is too large or it moves at extremely high-speed or it goes beyond existing processing capability.

A recent survey in the United States suggests that 75% of patients are concerned about health Web sites sharing information without their permission (Raman 2007). Possibly this is because medical data disclosure is the second highest reported break (Hasan and Yurcik 2006).

As the healthcare industry is a witness for the large volumes of data, the first step will involvegovernance and linking accurate and actionable data in real-time. In this age of connectivity, integrating health systems with huge amounts of clinical, financial, genomic, social and environmental data will be vital for real-timeanalytics and patient care.

II. LITERATURE SURVEY

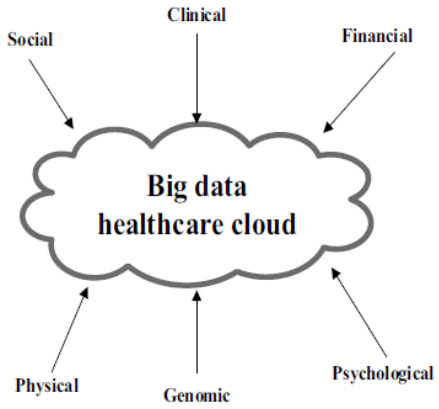
The first paper in the reference talks about the significant increase in security and patient privacy concerns. At the outset, patient's information is stored in data centres with varying levels of security. Moreover, the speak about the HIPAA (The Health Insurance Portability and Accountability Act of 1996)certification which most healthcare data centres have, but that certification does not guarantee patient record safety. The below figure portrays a big data healthcare cloud that hosts clinical, financial, social, genomic, physical and psychological data pertaining to patients.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 7, October 2015



Traditional security solutions cannot be directly applied to large and integrally diverse data sets. With the increase in popularity of healthcare cloud solutions, complexity in securing massive distributed Software as a Service (SaaS) solutions increases with difference in data sources and formats. Hence, big data governance is necessary before exposing data to analytics.

II.1Threats to privacy of information.

The second paper talks about the 2 big areas of information privacy, they categorized into two broad areas: (1) Organizational threats that arise from inappropriate access of patient data by either internal agents abusing their privileges or external agents exploiting vulnerability of information systems, such as an employee who accesses data without any legitimate need or an outside attacker (hacker) that infiltrates organization‘s information infrastructure to steal data or render it inoperable, and (2) Systemic threats that arise from an agent in the information flow chain exploiting the disclosed data beyond its intended use (NRC 1997).

II.2 Data Interoperability and Information Security

Some organizations store health information in different proprietary formats. Using some of the Data formats can lead as a major hurdle in sharing patient’s data among organizations as well as to medical and health policy research. Currently 33 states and one territory have developed plans to implement privacy and security policy solutions that enable seamless electronic exchange of health information. Most of these state plans recognize the need and call for development of a universal patient consent form that incorporates common information disclosure situations as well for specially protected information.

II.3 Information Security on Web Enabled Healthcare Provision

The emergence of internet has transformed the business model for customer oriented industries. The healthcare sector has also enabled itself to internet services and mobile technologies such as online consultation, remote health monitoring, e-clinical trials, and patient information access. Recent advances in web technology has enabled the “Banking on health” approach. If is a platform for storage and exchange of patient’s health records patterned after a personal banking system where consumers could deposit and withdraw information. Recent launches of “HealthVault” by Microsoft and “Google Health” by Google are examples of such health banking system. However such web enabled and mobile based services open up a whole gamut of security risks compounding the privacy problem. One such is, development of privacy preserving trust negotiation protocol for mobile healthcare systems (Dong and Dulay 2006) that facilitates trust between user devices in compliance with predefined access control and disclosure policies. Mobile devices, especially those possessed by patients, could be electronically tracked leading to unintended exposure of patient‘s location.

II.4 Information Security for Authorized Data Disclosure

In healthcare sector, it is necessary to share the data across the organizational boundaries to support the larger interests of multiple stakeholders as well as agencies involved with public health. However, the release of patient‘s data could cause personally identifying information as well sensitive information that may disrupt privacy as well cause

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 7, October 2015

socioeconomic consequences for patient. Advances in technology have led to consolidation of health records from multiple sources to a single research database which supports researchers engaged in improvement of public health, clinical methods and health services in general.

III. RELATED WORK

The data contains sensitive patient information which can have an impact on the patient's health and even on their life. It involve different health information management activities for different purposes and information security is important for all these functionalities. There are continuing discussions and developments in the area of consent mechanisms to ensure that the information security of patients has been kept safe.
As a result there needs to be a mechanism to address this efficiently to maintain patient privacy and fulfil the requirements of research. We try to ensure that information security should be studied extensively to make sure about patient safety by providing secure measures to healthcare providers, consumers, primary and secondary users of the patient's information.

IV. CONCLUSION

In this paper we discussed about the security and privacy issues in healthcare sector. It has been discussed that a well-planned security mechanism should be designed for the patient's data. We have found many important challenges in implementing a secure healthcare monitoring system (using medical sensors), with the fact that if the technology is safe, and then people will trust it.
At last we review some of the security and privacyissues in healthcare and predict a need for technologicalbreakthroughs in computational, storage and communicationcapabilities to meet the growing demand of securinghealthcare data. We hope that this survey will motivate future researchers to come up with more robust security mechanisms for real-time healthcare applications.

REFERENCES

[1] AjitAppari (Ajit.Appari@Tuck.Dartmouth.edu) andM. Eric Johnson (M.Eric.Johnson@Tuck.Dartmouth.edu) 'Information Security and Privacy in Healthcare Current State of Research1'Center for Digital Strategies Tuck School of Business Dartmouth College, Hanover NH
[2] Nanthealth Harsh KupwadePatil and Ravi SeshadriNanthealth Dallas, US 'Big data security and privacy issues in healthcare'
[3] Khin Than Win, 'A review of security of electronic health records'
[4] Pardeep Kumar and Hoon-Jae Lee 'Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey'