Real Time Security Compliance Monitoring In Big Data Environment

#1S.Thirumal#2A.Manikandan,#3Dr.D.venkatasubramanian
Department of Computer Science and Engineering VISTAS. Pallavaram, Chennai.
Department of Computer Science and Engineering.Velammal Institute of Technology
#1thirumal.se@velsuniv.ac.in #2mani.se@velsuniv.ac.in,#3bostonvenkat@yahoo.com.

Abstract

In the computer oriented environment data plays a vital role for which we need to provide a security .There were traditional mechanisms available to improve the security for data, but the data have taken its own evolution and migration to the Big Data environment. As the data taken different dimensions the security issues also grown along with it. The traditional mechanism cannot be applied for the current real time data and we have set of security compliances to adhere it. This paper provides a survey about the various security compliances mechanisms available. It also provide the study of the compliance mechanism evolution and their application on the data available in the Big Data environment and compares the different mechanisms. It also differentiate the mechanisms from each other according to the type of the data and after the comparisons this work allows us to choose the exact mechanism for the appropriate data.

Keywords: security compliance, Health record, Critical data, Big Data.

Introduction

It is believed that in traditional systems data was hacked only by the hacker who is outside the trusted environment and it is proved that the data theft was happened most of the time by the insiders only, it was also convinced that encrypting and firewalls will provide data security but over the period of time these are proved to bypassed. There were mechanisms available to overcome the security issues in the traditional systems. At present we live in Big data environment which as lot differences with traditional data in terms of variety, volume and velocity. Over the decade the data generated by the communities like finance, Health, scientific and social media was huge. In order to ensure the security and privacy we have the various security compliances available which defines the policy schemes.

In this paper we first discuss about the Big data characteristics, followed by security issues present in Big Data environment, then we discuss about the available security compliances and their comparisons.

2. Big Data Definition and characteristics

Big data is a collection of heterogeneous large complex data, which difficult to process when compared to the traditional system. The Big Data is new age technology that has 4Vs. ie., variety -different types of unstructured data, velocity- the speed of the data, volume- as the term Big data itself defines the size of the data is huge and value refers to the social values of the particular data [4]. The challenges we face kind of data are in capturing, storing, sharing and transferring [1]. This Big data is not only a data but also an information and as it become an information, that has to follow information regulation policy standards. We have various information security compliance mechanisms for handling Big Data, but the problem we face here was to opt which kind of polices. This paper will gives you an outline of various security compliance available and their advantages and disadvantages which will help us to choose the required compliance based on the data [2]. Let’s look in detail about the generic functionality of the security compliances. The security standards are defined by international regulatory bodies to ensure safety for the data lets discuss few of the standards in detail and also discuss the pro and eons each security compliances [3].

3. Security compliance mechanisms

The security compliance mechanisms will provide us set of framework to ensure a security to the data in the Big Data environment [5]. Before discussing the various security compliance mechanisms available

4. Health insurance portability and Accountability Act (HIPPA)

This is one of the well-known security compliance in the health care, and this was one of the landmark law that was enacted by the US government in the year 1996 as the government takes care of the health insurance it was done with more care. In the developing as well as developed countries a person working in a company and insurance companies [7].

In this scheme the employee may be well -benefited but how far the privacy to his medical record was ensured, and it was done by this security compliance standard [6]. This as two parts, the first part takes care of the portability -if a person change organizations the policy schemes from the current working company should have to suit the other company to which the employee moves. The second part ensures security and confidentiality to his medical record. Prior to this law an individual's record may be shared without the concern of the individuals. In the recent times all the records are converted to digital format which will be stored in cloud, where we need to restrict the access to the personal health records (PHR)[9][10][11]. The cloud service provider (CSP) stores the PHR in the encrypted format, also there are meaningful usage of the medical records which has two stages. The stage-1 capturing the health information in the structured format and tool support to take decision on some medical management record, and the second stage takes care of exchanging the information in the structured format. The security rules of HIPAA defines how the access to record by the authorized personal, it also have audit mechanisms to monitor, integrity control to avoid alteration and security mechanisms to transfer data electronically, by this security and privacy to PHR is ensured[8].

5. Sarbanes- Oxely Act

In the previous compliance standard it is discussed about the personal health record information and now we look at another standard that takes care of financial data [12]. This enable the management of financial data of the public accounting companies by the security and Exchange commission (SEC) [13]. This act provides a security to the investors and it contains two main sections 302 & 404. The section says that the Chief Executive officer and Chief Financial Officer should personal assessment to certify the financial reports, and the second stresses that the company assess the internal report and control which is submitted to SEC. This was also supported by the Control Objective for information related Technology (COBIT) and Information Technology Governance Institute (ITGI). The aim of COBIT is to have an authoritative internationally accepted set of information technology control objective for IT and assurance professionals, and ITGI is a governing body to ensure the business goals are met. The control objectives can also subdivided into following 1)Security policy, 2)Security standards, 3)Access and Authentications, 4)Network security, 5)Monitoring, 6)Segregation of duties, 7)Physical Security, with these security compliance the security for the financial data was ensured.

6 .Federal Information security Modernization Act (FISMA)

This is a security compliance mechanism that ensures security for the country's critical information [14]. This was led to some main important contributions in risk based information programs. It also made the security organizations to develop an organization wide security programs which should adhere to the security configuration standards [15][16]. This taken some new forms in recent times where behaviour based anomaly detections to find the deviations in the regular activities [17]. We vendors who provide a comprehensive policy engine have threat indicators to alert the agencies. This promotes the standard for minimum baselines in controls. Refine controls for using a risk assessment, documenting the controls of system security plan, Implement security controls in required information systems, assessing the effectiveness of the security controls after the implementations, Determining risk at the agency level, Authorization of the Information system for processing. Monitoring the security continuously. Hence by this mechanisms the security for the national critical information was ensured.

7. Family Educational Rights and Privacy Act (FERPA)

This is one of the compliance standard that ensures security to the educational records of the students[18]. The records should be known to the student and the corresponding parents, over the period the rights of the parents would shift to the student [19]. Parents and the students have the right to ask or request the record if it is believed to be wrong at the same time they can also inspect the records. The records may not be shared to anyone but in few cases it can be done, the school may have written consent from the parent to share the information. There are also few cases where the schools may have the right to share the without the consent also, those conditions are 1) when the student is transferred 2) to the specific officials for audits 3) Financial Aids concerns related to students studies 4) To the officials in the cases of medical and other emergencies 5) when it comply with judiciary norms[[20]]. This system also have a dictionary information system, with some basic demographic information but it may change for the current student and the alumni. This also have the classifications namely 1) biographic data, 2) application data, 3) Matriculation data. In addition to the above mechanisms to have the student's information this also have the mechanism to discard the inactive records.

8.References

[1] “Data security Challenges” https://www.docs.oracle.com . Date accessed:23.02.2017

[2] “Information Security Compliance: Which regulations relate to me?” www.urinnov.com. Date accessed: 23.02.2017

[3] “7 Biggest IT compliance Headached and how CIOs can cure them” http://www.eio.com. Date accessed: 23.02.2017

[4] “Big Data” https://en.wikipedia.org/. Date accessed: 23.02.2017

[5] Matthew Scholl & Andrew Regenscheid “safeguarding Data Using Encryption” computer security division, ITL, NIST,US department of Commerce

[6] “why is the HIPAA privacy Rule needed?” https://www.hhs.gov. Date accessed: 23.02.2017

[7] “Hipaa Background” http://hipaa.bsd.uchicago.edu. Date accessed: 23.02.2017

[8] “HIPPA definition” http://searchdatamanagement.techtarget.com/. Date accessed: 23.02.2017

[9] “Security Assessment Tool” https://www.healthit.gov. Date accessed: 23.02.2017

[10] “HIPAA encryption best practices” https://www.sookasa.com/. Date accessed: 23.02.2017

[11] “Transmission Security encryption: What to do and How to Do it” https://www.hipaa.com. Date accessed: 23.02.2017

[12] “Sarbanes-OxleAct” https://en.wikipedia.org/wiki/. Date accessed: 23.02.2017

[13] Greg Stults” An Overview of Sarbanes- Oxley for the Information security Professional” part of GIAC repository, SANS Institute 2004.

[14] “Federal Information security Management Act of 2002” https://en.wikipedia.org/wiki. Date accessed: 23.02.2017

[15] “Federal Information Security Management Act “ http://www.securonix.com/. Date accessed: 23.02.2017

[16] “Federal /information Security Modernization Act (Fisma) Implementation http://csrc.unist.gov. Date accessed: 23.02.2017

[17] “Federal Information Security Management Act” http://searchsecurity.techtarget.com/. Date accessed: 23.02.2017

[18] “Family Educational Rights and Privacy Act (FERPA)” https://www.2.ed.gov/. Date accessed: 23.02.2017

[19] “Guidelines and Regulations for Implementation of the family Educational rights and Privacy Act of 1974” https://cam.illinois.edu/ “.Date accessed: 23.02.2017

[20] “Guidelines for the Implementation Of The Student Records Access Policy And The Federal Family Educational Rights And Privacy Act (Ferpa)” Office of the General Counsel February 2009.