IOSR Journal of Mobile Computing & Application (IOSR-JMCA)
e- ISSN: 2394-0050, P-ISSN: 2394-0042.Volume 9, Issue 2 (Mar. – Apr. 2022), PP 24-27
www.iosrjournals.org

Data LeakagePreventionfor Information Security in Hospitals

Cigdem Bakir
Yildiz Technical University, ComputerDepartment, 34015, Istanbul, Turkey

Abstract
Today, unauthorized access to data, propagation and modification of data bring many problems. Data leakage techniques are used to solve these problems. However, a model that will ensure data privacy by protecting the data of all patients in hospitals has not been fully developed. In our study, it is aimed to provide data confidentiality by labelling the patient's data. The patient's data are called EHD (Electronic Health Data) objects. Thus, each patient is provided with access to the information he/she authorizes. Each patient carries out the security management of their own health data.

Keys: *data leakageprevention, data access, authorization, data breach, privacy*

I. Introduction

Data leakage detection and prevention means data loss (DLP), data protection, information leakage prevention. Prevention of data leakage are techniques aimed at detecting data theft and protecting data by monitoring the access, use or transmission of data by unauthorized or unintentional persons. Briefly, it is the prevention of leakage of sensitive and valuable data from the transportation channels from the source to the target [1,2]. Thus, the movement of sensitive data on the network or in end-user systems is monitored and controlled [3,4].

Today, data breach, data propagation and data exposure pose a huge problem for many organizations. DLP techniques try to prevent attackers from breaching data. However, these methods cannot fully control the data traffic on the network. Data privacy, data integrity and a method that enables authorized users to access the system is required to control multiple nodes. Because organizations spend a lot of time and money to take security measures and to reduce risks. In addition, it is necessary to raise awareness of the users on this issue [5].

Each institution creates its own local security policies to prevent data leakage and data loss. However, it is very difficult for institutions to apply these policies to the system, to reduce the risk of data breaches, to improve compliance, to recognize malicious software, to optimize network bandwidth, to manage data, and to reduce time and costs. In particular, most security breaches are caused by intentional or unintentional behaviour by users within the organization. This necessitates the protection of personal information, that the data is not shared by unauthorized users, that it is not copied, and that the data are followed in communication paths. In addition, in case of loss of data, it must be securely backed up and stored.

II. Method

The intellectual property rights of companies and organizations, financial information, confidential information about patients in hospitals, information about diagnosis and treatment process, credit card information about customers in banks or other important information used in the industry constitute sensitive data. Leakage of this information to the outside by both people outside the organization and internal personnel brings some serious problems such as cost and time. For this reason, prevention of data leakage is of great importance in institutions and organizations. It is especially used in mobile devices, cloud computing, databases, and filing systems. Data leakage prevention techniques are shown in Table 1. [2].

Table 1: Data leakpreventiontechniques

Categories	UsedMethods
Defined DLP methods	Data in motion Data in use Data in rest
Access Control &Encryption	Device Control Encription Right Management Service
Advanced/Intelligent Security Metrics	Anomalydetection Activity basedverification
Standard Security Measures	Firewall Anti-viruses Intrusiondetectionsystems

1) Defined DLP methods: Techniques that prevent sensitive data from being sent, forwarded and copied to unauthorized persons, either intentionally or unintentionally. It shows that the objects (data in motion) on the broadcast node are in constant motion on the network. http, SMTP, P2P protocols, instant messaging, e-mail data protection are involved under this group [2]. The object used by the end user (data in use), means that the objects that are processed on the running node are in continuous use. The objects used are stored in the storage node (data in rest). Stored objects are stored in databases, file systems, and desktop computers as documents or files.

2) Access Control & Encryption: The text is encrypted with a key for unauthorized access to data. Data leakage can be prevented by decoding the encrypted text [3]. RMS (Right Management Systems) is used to protect sensitive file systems.

3) Advanced/Intelligent Security Metrics: Machine learning algorithms are used to detect abnormal behaviours in accessing data. Anomaly detection detects previously unseen attacks. It looks at events that are not considered normal. Users log into a system with their username and password. However, sometimes they choose passwords that are easily found or forget their passwords. In this case, users must be authenticated based on their behaviour and the actions they take. Users are authenticated with activity-based verification systems.

4)Standard Security Measures: Firewalls, intrusion detection systems and anti-viruses fall into this group. Firewall checks incoming and outgoing packets over the network, such as IP filtering, content filtering. Intrusion detection systems, on the other hand, examine the status of the system, detect an attack or data security problem, and work to eliminate this problem.

Application Example

Consider an example of keeping patient records in medical centers and sharing them securely: The goal here is to ensure data privacy. In hospital information management systems, information about patients is kept in objects called Electronic Health Record (EHR) [OC15]. The user includes patients, doctors, family physicians, pharmacists and all users who use and see the system in the medical center. Each actor has its own characteristics. For example; characteristics of the patient node, personal data such as name, surname, TR identity number, date of birth, place of birth, blood group, gender, phone, address and diagnosis, treatment process, past health findings, drugs used, laboratory reports, radiology reports, surgeries, chronic diseases, infectious diseases, pregnancy status etc. such as health-related data. These data are kept in the EHR object in the hospital information management system for each patient. Directional graph can be used to model this system. In Figure 1, G={v_1,v_2,v_3, v_4,v_5,v_6, v_7,v_8,v_9} with G (V, E) directional graphE={e_1,e_2,e_3, e_4,e_5,e_6, e_7,e_8,e_9, e_{10},e_{11}, e_{12}, e_{13}, e_{14}} show the interaction between the users. Interactions show the paths that EHR objects take. EHR object is labelled according to privacy, integrity and privacy policies. EHR objects with certain labels can be transferred to other users.

In medical centers, it is important to determine which users with which authorizations the health data will be given and their access rights. Access to health data of both internal personnel and external authorized/unauthorized users is subject to control. This control ensures that the patient's information can be accessed by the actors he has authorized. However, failure to complete this control causes problems such as unauthorized access/use or data spreading. It is necessary to provide a common control that can protect EHD objects. Data confidentiality is ensured with the labelling method. Thus, each patient performs the security management of their own health data.

For privacy, privacy restrictions are complied with when the object is transferred to the node (user) at the security level where it is located or to the higher level node.

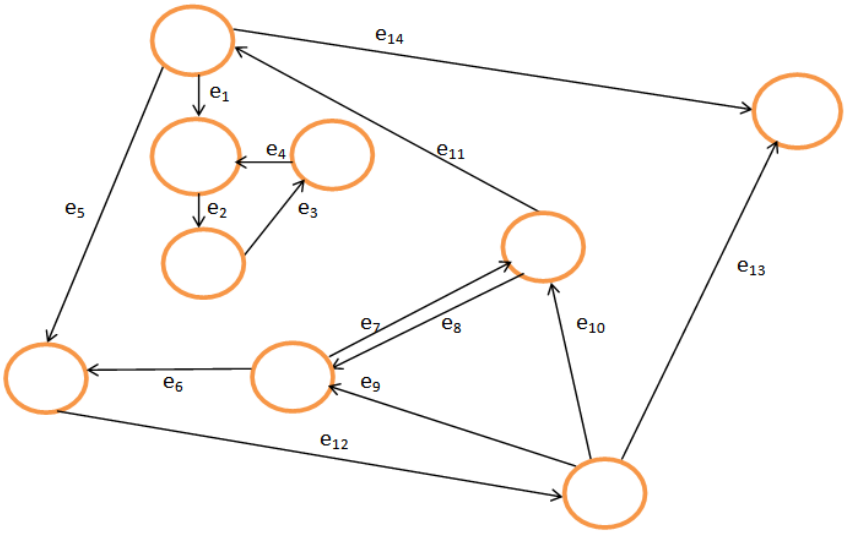

Figure1-The examplegraph

G(V,E) to be
V={Users}={v_1,v_2,v_3, v_4,v_5,v_6, v_7,v_8,v_9}
E={Places of EHRObjects}={e_1,e_2,e_3, e_4,e_5,e_6, e_7,e_8,e_9, e_{10},e_{11}, e_{12}, e_{13}, e_{14}}
Confidentialitylabels;
L={owner: readers}
//owner: userswhoowntheobjectlabeledowner
//readers: usersauthorizedbytheowner
Forconfidentiality, thelabelshowspatientsanddoctors.
Label= L ={ hastalar, doktorlar}
L_i=Label of patientnumber i in the EHR = {owner:v_i, readers:v_j}
L_1=1st patient= Displays thelabel of theobject of the v1 node.
Fortransmission of the EHR objectfromuser $v_1$touser v_5;
Confidentialitylabel of $v_1$user's EHR object L_1
Confidentialitylabel of $v_5$user's EHR object v_5
L_1= { v_1:v_5,v_9 } v_1 $ESK_{(1)}$ $v_5$patienttodoctor

v_1 $ESK_{(1)}$ $v_9$patienttodoctor

L_j=jstdoctor
L_5showsthelabel of the $v_5$doctornodeobject.
L_5={ v_1:v_5; v_5,v_8} v_1 $ESK_{(1)}$ $v_5$patienttodoctor

v_5 $ESK_{(1)}$ $v_8$doctortodoctor

//Inordertoensureconfidentiality, theruleL$_1$⊆L$_5$object is transferredtothesecuritylevelnode (user) orhigherlevelnode.
if $L_1 \subseteq L_5$
{
// uponauthorization
{patients: doctors} v_1;
{doctors} v_5;
// transferringtheEHRobjectfromthe$v_1$nodetothe$v_5$node;
$v_5 \leftarrow v_1$;
}
else
{
// When not authorized, encrypt it withlabel.
// transferringtheencryptedtexttothe $v_5$node.
$v_5 \leftarrow Encrip(ESK_1)$
}

III. Conclusion

Patient privacy, security and confidentiality of personal data is to prevent the patient's information from being viewed other than authorized persons. Our work aims to protect personal sensitive data by providing security and privacy.

Hospital Information Management Systems, i.e. patient data, are kept in the EHR. Patient data should be monitored, audited and recorded against cyber attacks. In short, it is necessary to ensure confidentiality, security, data integrity, traceability, control of data, access by authorized users. It is important to determine which users with which authorizations the health data will be given and their access rights. Access to confidential data should be prevented by both internal personnel and external users. Consent management allows the patient to access the information allowed by the authorized users. However, inadequate consent management creates many problems such as unauthorized access, dissemination and unauthorized use of data. Data transmission, sharing, access to, viewing, use of authorized users, protection against cyber attacks, ensuring confidentiality, integrity and confidentiality, and performing risk analysis are the most important problems. In our study, a common consent management was provided that could protect the data of each patient. With the labelling method, the patient determines their local policies for confidentiality and integrity. Thus, each patient performs his/her own consent management.

References

[1]. Prathaben K., "Data LossPrevention", SansInstituteInfosec Reading Room, 2008.
[2]. Asaf S., Yuval E. AdnLion R., "A Survey of Data LeakageDetectionandPrevention Solutions", 2012.
[3]. Jorge B., Julio C. andJuan E.T., "BypassingInfprmationLeakageProtectionwithtrustedapplications", Computer& Security, pp.557-568, 2012.
[4]. "Data LeakPrevention", Isaca White Paper, 2010.
[5]. PrathabenKanagasingham,"Data LossPrevention", SansInstituteInfoSec Reading Room, 2008.
[6]. Olca E., Can Ö., "Türkiye'de Elektronik Sağlık Kaydı Bağlamında Gizlilik ve Güvenlik Üzerine Teknolojiler", 3rd International Symposium on DigitalForensicsand Security", 2015.
[7]. Öğütçü G., Köybaşı S.C, "Elektronik Sağlık Kayıtlarının İçeriği, Hassasiyeti ve Erişim Kontrollerine Yönelik Farkındalık ve Beklentilerin Değerlendirilmesi", pp.88-97, 2015.
[8]. İzgi M.C., "Mahremiyet Kavramı Bağlamında Kişisel Sağlık Verileri", Türkiye Biyoetik Dergisi, vol.1, no.1, pp.25-37, 2014.
[9]. T.Pasquier, J.SinghandD.Eyers, "Information FlowAuditforPaaSclouds", IEEE International Conference on CloudEngineering (IC2E), 2016.
[10]. T.PasquierandD.Eyers, "Information FlowAuditTransparencyandCompliance in the Handling of Personal Data", In IC2E International Workshop on Legal Technical andScience, 2016.
[11]. Turgut N., Karaarslan E., Ergin A., Kılıç Ö., "Elektronik Sağlık Kayıtlarının Gizlilik ve Mahremiyeti", 2015.
[12]. Kişisel Verilerin Korunması Kanunu, 2016.