Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 10, October 2014, pg.137 – 140

RESEARCH ARTICLE

A Novel Secure System for a Knowledge Sharing Environment

Harshitaa.B[1], G.Praveen Babu[2]

[1]Computer Networks and Information security, School of IT, JNTUH, India

[2]Department of CSE, School of IT, JNTUH, India

[1] hbhairavarasu@gmail.com; [2] pravbob@jntuh.ac.in

Abstract*— Knowledge is an essential part of an organization. Especially the knowledge about security context of an organization has become a primary necessity for the secure and healthy working of an organization. An organization like a huge hospital with many branches holds personal information by volume on both patients and staff. Much of this information constitutes 'sensitive personal data' and needs to be captured, managed, stored and disposed of securely. But the information is of no value unless readily accessible to clinicians and other staff tasked with providing healthcare. A knowledge framework for accessing information is introduced. Accessing information here means logging into IT systems which holds the organizational data, viewing it and processing it. It also helps in providing of secure access to the users and help with assuring the security for the data being accessed. The proposed system aims to provide for a secure accessing framework between knowledge sharing environments.

***Keywords*— information security, knowledge, accessing controls**

I. INTRODUCTION

Most enterprises agree that knowledge is an essential asset for survival and success in an increasingly competitive market; this awareness is one of the main reasons for the exponential growth of knowledge management in the past decade.

There is tension between user data protection and ease of accessibility. In the case of an organization holding personal and sensitive information of user's data information security is a critical factor. This information should be captured, managed, stored and modified securely based on the Data Protection Act 1998. But the information is of no value unless it is readily accessible by the authorized personnel to process and manage it. Hence there should be a balance between providing of security for the data reducing the risk context and a quick access for the staff to carry on about the business operations effectively.

Information security is to be considered the most important aspect in an organization. Considering the fact that information has been a critical asset for any organization or a business enterprise, information security has been less about being a technical aspect for the business and a more important for the sustainability of the business. Hence it requires a very descriptive model for effective security modeling. Information Security Model, which accumulates operational data and security experience, is formulated to assist the data collection process for risk analysis studies.

© 2014, IJCSMC All Rights Reserved

The exact role of information security is still not clearly defined in many organizations. While some still view information security as a cost center, it has been shown that effectively managed information security organizations can be instrumental in helping an enterprise meet its business goals by improving efficiency.

II. ACCESSING FRAMEWORK

- As mentioned above a robust accessing framework is required in a hospital organization which contains sensitive information to be managed, stored and processed. It should contain robust methodology in place to assess the business impact of access to information and apply the correct protection [e.g. to use technical controls combined with greater staff awareness]

- Acknowledgment that the ability to successfully apply responsibilities against individuals depends on the robustness of board policies[e.g. on how access permissions should be agreed and being clear on 'identity']

- Accessing here describes logging onto any IT systems which holds data as well as viewing or processing it in any way. Data in this context is used to describe the digital component parts (which may be just registration code, names, numbers) which when taken together form 'information' on an individual.

- A framework trying to strike a balance between the data protection and quick access is developed. It takes into consideration following factors.

  Authentication system **:** all access must have the proper credentials from all the users trying to log in.

  Data collection **:** Data collection is nothing but the data provided by the user's themselves.

  Clear identification **:** all access is from named individuals who are who they say they are.

  Appropriate authority **:** all access is authorised by a suitably qualified person.

  Legitimate relationship **:** all access is based on a legitimate relationship with the patient.

  Business need **:** all access is on a 'need to know' basis to provide healthcare and associated business.

  Time bound **:** all access is related to the period in which there is a relationship.

III. PROPOSED SYSTEM

As business has come to view information as a critical asset, and has increasingly come to depend on public networks to transport sensitive information, protecting information has become less about technology and more about sustainability of the enterprise itself. Hence it is really important to develop an accessing framework that provides a balance between facilitating quick business operations and at the same time providing a very secure system to protect the sensitive information.

Here a secure system is developed keeping in mind the knowledge sharing environment. The data to be shared and displayed with correct authentication. There are t two layers to maintain data, one layer is XML model and another layer is entity model (means relational data base). Here it allows developing an agreement system to implement such approach. In this application every user has to get authentication, then two users can setup agreement about exchanging of services in a digital format. It uses two a layer system, where in XML model is used for maintaining signature details, and in relational database model is for maintaining users information that who are establishing agreement.

This application takes care that the corresponding authority only is given permissions to allocate and register. The time bound cases are developed where one time used to allocate a doctor may not be used again. It finally provides an accessing framework that allows the correct authenticated person to check, modify data.

© 2014, IJCSMC All Rights Reserved

IV. STRUCTURAL MODEL

There are three entities considered which are the user uploading data, data itself and the user using the data. All the users are first authenticated and the data sets are loaded using the JDBC API's. The user is checked for right identity through random methodology and given a distribution based access. There is an authentication system that collects data from various entities of the organization. The other is the accessibility checking component that allows the authenticated users to use and share data.

This framework makes use of the MVC architecture which is a 3 tier structure constituting a client, server, model as elements. Model in the architecture means the databases which facilitates in collection of the huge information. The general structure of the application has factors like an authentication system, data collection, owner identification, sharing model, checking accessibility checking component and display context.

Main concept of this application is providing a new framework for accessing information. There are two layers to maintain data, one layer is XML model and another layer is entity model (means relational data base). It is used to develop an agreement system to implement this approach. In this application every user has to get authentication, then two users can setup agreement about exchanging of services in a digital format. In this agreement setup it is using a two layer system, where in XML model it is maintaining signature details, and in relational database model it is maintaining user's information that who are establishing agreement.

ALGORITHM

- Login page
- Connection with data sets established
- Check existence.
- Else stop accessibility
- Data collection by allowing to upload data set.
- Making distribution based accessibility for particular data.

Input: Let $U_I = U_i^n$ is a set of users data where U_i is i^{th} user
$i=1$

Let $D_{Ij} = \underset{i=0\ j=0}{d_{ij}^n}$ which is a set of data uploaded to server, where d_{ij} is j^{th} data uploaded by Ith user

Let $PK_{ijk} = \underset{i=0\ j=0\ k=0}{pk_{ijk}^{n\ m\ o}}$ which is a set of permission key to access data, where pk_{ijk} is key provided by i^{th} user, for k^{th} user to access j^{th} data.

Out:- Delivering data output.

Stp1:- Read $U_{(id)i}$ & $U_{(p\&w)i}$, where $U_{(id)p}$ is userid of i^{th} user and $U_{(P\&W)i}$ is password of the i^{th} from input form

Stp2:- Establish connection with data sets by using API.
Stp3:- Check Existence of pair of $U_{(id)i}$ and $U_{(p\&w)i}$ is available data sets.
3.1:- Let $U_{(ij)it}$ is available user id in data set.
3.2:- Let $U_{(p\&w)it}$ is available password in data set.
3.3:- If $U_{(id)i} == U_{(ij)it}$ and $U_{(p\&w)i} == U_{(p\&w)it}$
3.3.1:- Allow for data transactions
else
3.3.2:- stop accessibility
Stp4:- Data collection from U_i by allowing to upload image data set.
Stp5:- Making distribution based accessibility of a particular data.
5.1:- Let U_j is the user who are receiving D_k from user U_i
5.2:- Use random methodology to generate

Pk_{ijk},

© 2014, IJCSMC All Rights Reserved

Let Pk_{ijk}=0<r<rv where r is a number generated by random methodology, where rv is random

Stp6:- Let U_j is accessibility status of d_R which sent by U_i, representing
$d_{ijk}{}^E D_{IJK}$
Stp7:- Let $Pk_{(ik)j}$ is permission key specifying by user j
Stp8:- If Pk_{ijk} == $Pk_{(ik)j}$ then load data d_{ijk} for U_j,
Stp9:- else
display error message
Stp10:- stop.

V. CONCLUSION

All access permissions are replicated as far as possible by technical controls that prevent unauthorised access. It provides a methodology to guide the data collection process for risk assessment activity. Risk Assessment is nothing but providing a securable solutions to access information. This application designed an approach to access information with risk free nature taken prescription, and owner of prescription, patient details as an input, then checking whether the new doctor is accessible or editable etc type of risk assessment. To grant access permissions mean and whether access is 'read only' or gives the ability to modify or delete.

The above application has provided a methodology in place to assess the business impact of access to information and apply the correct protection. It strives for an updated security data specific to an organization could be obtained under the guidance of security knowledge maintained in the framework. The future enhancements would be 1.to test the concepts of applying ontology for the data integration mechanism and structured matching between the global schema and source schemas. 2. Enhancing with multiple distributed system by supporting cloud nature.

REFERENCES

[1] AnHai Doan, Pedro Domingos, and Alon Y. Levy. Learning source description for data integration. In WebDB (Informal Proceedings), pages 81--86, 2000.

[2] Kwok LF and Longley D. Security Modelling for Risk Analysis. Proc. 18th IFIP World Computer Con gress, IFIP 2004, 22-27 August 2004, Toulouse, France, pp29-45.

[3] Isabel F. Cruz and Huiyong Xiao. The Role of Ontologies in Data Integration. Journal of Engineering I ntelligent Systems: 13(4), December, 2005.

[4] A Business model for Information Security

[5] Java Server Programming - Apress

[6] Análysis & Design of InformationSystems – Senn

© 2014, IJCSMC All Rights Reserved