www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242

Volume 3 Issue 10, October 2014 Page No. 8502-8509

Decision Support System for Information Security in the Semantics of Bio- Medical Documents

Tadi Bhanu Venkata Pradeep
2 M.tech, cse, griet.
G. N. Beena Bethel,Assoc. Professor, CSE Dept., GRIET,
Hyderabad.

Abstract

Technology and it's requirement comes in various ways, considering one of the aspect as the building tool to next level journey of security as Information Security with the Theme behind to make the Bio-Medical efficiently in the context of Technology , i.e. how it plays the role in making and controlling the decision system. Making a prejudice statement on the support system is lead to nest level of insecurity. But In this paper we try to give a best perdition based on information where we consider as security to the information system. Time and Technology may play the complementary aspect in the decision support based on information security, at now we can give the best to mingle of various technology where security and its related decision are most important to these days software revolution, which we call it as most important and high risky to main component if IT market for Bio- Medical. The purpose of the security plan is to provide an overview of the security requirements of the system and describe the controls that are in place or those controls that are planned for meeting the security requirements. The system security plan also delineates responsibilities and expected behavior of all the individuals who access the system. The security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for the system. It should reflect input from the various managers who are responsible for the system. This includes the information owners, the system operators, the system security manager, and the system administrators.

Keywords: Bio-Medical Cluster Document, Security, Data Semantics.

1. Introduction

In general, **security** is "the quality or state of being secure to be free from danger. "In other words, protection against adversaries from those who would do harm, intentionally or otherwise is the objective. National security, for example, is a multilayered system that protects the sovereignty of a state, its assets, its resources, and its people. Achieving the appropriate level of security for an organization also depends on a multifaceted system.

Different Security Mechanism are Present to monitor the software decision system which in turn we call as an automated processing for Decision support system, which we see as the most achieving technology in tomorrow global market.

- **Physical security**, to protect physical items, objects, or areas from unauthorized access and misuse.
- **Personal securities**, to protect the individual or group of individuals who are authorize to access the organization

  and its operations.
- **Ope rations security**, to protect the details of a particular operation or series of activities.
- **Communications security**, to protect communications media, technology, and content.
- **Network security**, to protect networking components, connections, and contents.
- **Information security**, to protect information assets.

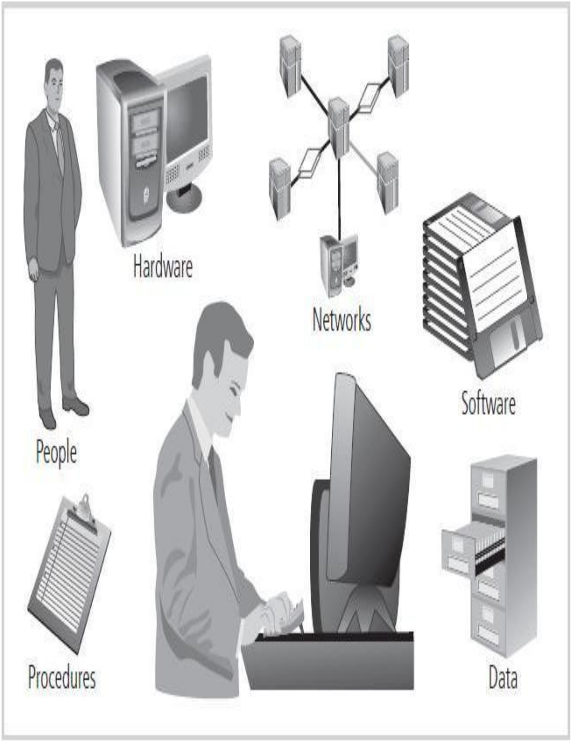

Fig.1.1 Components of Information System.

Information security (InfoSec), as defined by the standards published by the Committee on National Security Systems (CNSS), formerly the National Security Telecommunications and Information Systems Security Committee (NSTISSC), is the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information.

2. Related Work

Technology and its related work which has done in the past give to next level of research. The value of information comes from the characteristics it possesses. If we consider characteristic which in turn we call as part of information getting changed, the real value of that information gets impact to global value of data either in the search engine of Google or some other, or decreases. In the aspect, some characteristics information may affect information’s value to users more than others do with regard to search value which used as most important factor information security. It may be context oriented; for example, timeliness of information can be a critical factor, as of information loses much or all of its value as process goes on making decision and controlling the flow of decision giving rise to though information security professionals and end users share an understanding of the characteristics of information, the need to secure the information from threats conflicts with the end users’ need for unhindered access to the information with regardless of high end ethical hackers who can penetrate the system with the very best use of their algorithmic approach. Let us consider the example of; end users may perceive a tenth-of-a-second delay in the computation of data to be an unnecessary annoyance lead to high level data insecurity. Information security professionals, however, may perceive that tenth-of-a-second as a minor delay that enables the accomplishment of an important task, like data encryption. Hence the mechanism cryptography, we need to explore to next level of cryptographic technology where information is most important.

Each Character comes under the following criteria of triangle of point which is shown in the fig.2.1.

- ❖ Availability
- ❖ Accuracy
- ❖ Authenticity
- ❖ Confidentiality
- ❖ Integrity
- ❖ Utility
- ❖ Possession

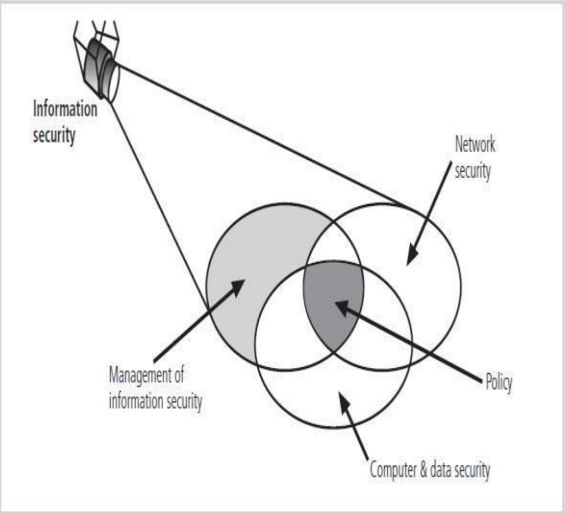

Fig. 2.1 Triangle Face of related Components Required in Decisions Support System.

If we look forward the level of complexity in today's information systems, the implementation of information security has often been described as a combination of art and science. In the modern age, System technologists, especially those with a gift for managing and operating computers and computer-based systems, have long been suspected of using more than a little magic to keep the systems running and functioning as expected with some additional moral values which lead to next research. In information security such technologists are sometimes called *security artisans*. The people who studied computer systems can appreciate the anxiety most people feel when faced with complex technology with the determination of next level of innovation in the context of level of journey to Information Security. Let us Consider the inner workings of the computer: with the mind-boggling functions of the transistors in a CPU, the interaction of the various digital devices, and the memory storage units on the circuit boards, it's a miracle these things work at all lead to more impacted in various field s i.e. one of them is Information Security and also next to lead with Information Security to journey of AI to Decision Support System.

3. Methodology

In the Modern age of Technology , Methodology and it's concern take to effect with the very best solution which we would like to reflect in the SDLC phases , which we believe to very best extend to make the Industry sure that to9 follow of each and every process to regulate in the very proper and optimal to give the best solution to the client which needs security analysis on information system to make the very best critical and typical solution on decision to management level and to the high level design and architecture level. Let me go with the step which we follow the solution of classical water flow model where each and every phase to be intimate to next level of analysis is as follows and we explained by taking the fig.3.1.to explain it to clarity manner which we implemented in our next level architectural diagram.

3.1 System Identification

Following are sub system which is reflected in the system analysis to make the decision in the optimal and strategic way.

- System Name/Title
- Responsible Organization
- Information Contact(s)
- Assignment of Security Responsibility
- System Operational Status
- General Description/Purpose
- System Environment
- System Interconnection/Information Sharing
- Applicable Laws or Regulations Affecting the System
- General Description of Information Sensitivity.

The process may be initiated in response to` specific conditions or combinations of conditions. The impetus to begin any project may be event-driven that we lead to take into analysis of strategic plan and the way of implementation to the global market of investment and others involved in that one. In this aspect, we maintain the level layer of data and logic in very best coupled way so as next changes should be consistent to ensure data integrity.

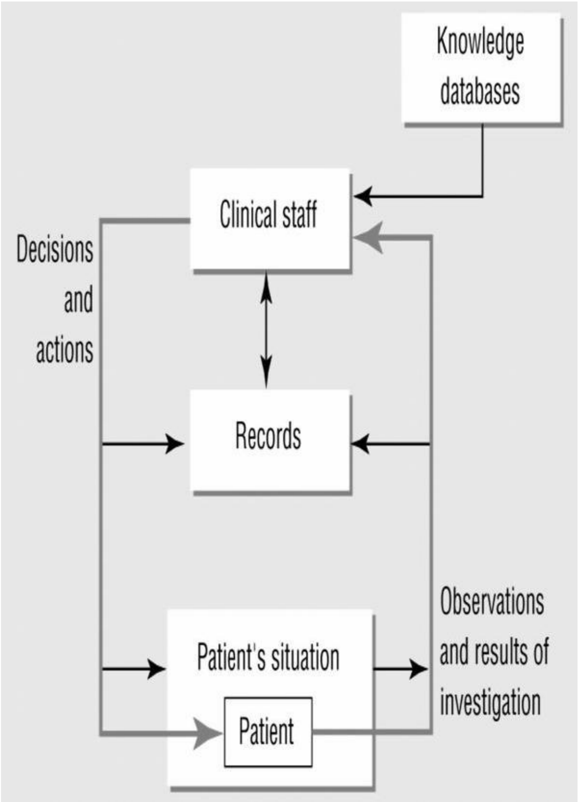

Fig.3.1.1 Mining Process Based on Information Security

Maintenance and change Repeat Investigation Analysis Logical design Physical design Implementation. Once the need for information security is recognized, the SDLC methodology ensures that development proceeds in an orderly, comprehensive fashion. In each phase comes a structured review or reality check, to maintain the very phase level analysis ensuring if the project should be continued, discontinued, outsourced, or postponed, depending on the need for additional expertise, organizational knowledge, or resources. The process begins with an investigation of the problem facing the organization, continues with an analysis of current organizational practices considered in the context of the investigation, and then proceeds to the logical and physical design phases. During the design phases, potential solutions are identified and are associated with evaluation criteria. In the implementation phase, solutions are evaluated, selected, and acquired through a make-or-buy process. These solutions, whether made or bought, are tested, installed, and tested again. Users of systems are trained and documentation developed.

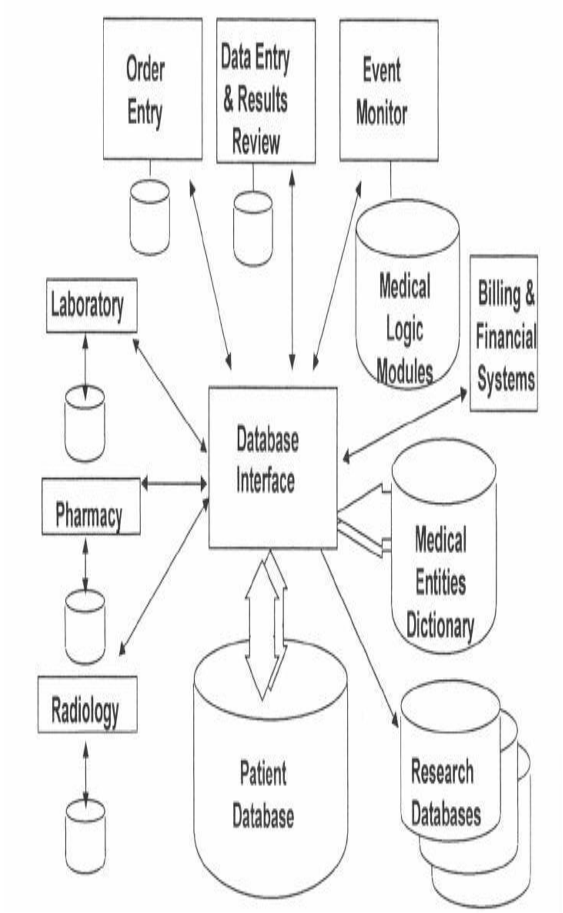

Fig.3.1.2 Architecture Diagram Showing the Components Involved in the Process.

Finally, the system becomes mature and is maintained (and modified) over the remainder of its operational life. Any information systems implementation may have multiple iterations, as the cycle is repeated over time. The information security follows many expectations due of which provides the best of way the information can maintain the decision system. The following sections describe the activities of each phase of the traditional SDLC.

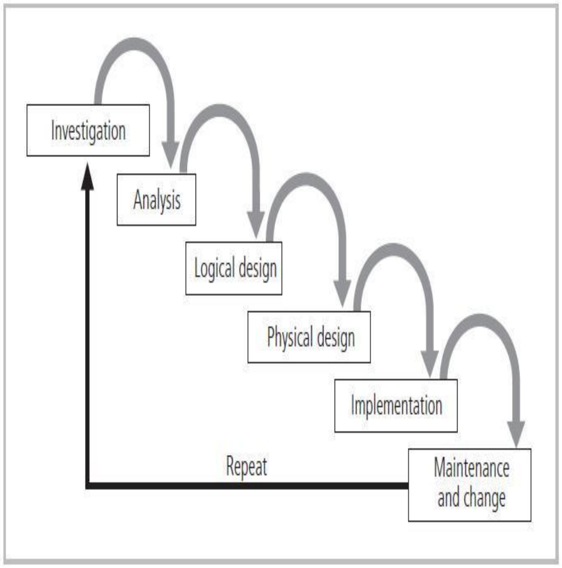

Fig. 3.1.3 Logical Steps Involved In Decision Support System Based On Information Security.

In the logical design phase, the information gained from the analysis phase is used to begin creating a systems solution for a business problem. In any systems solution, it is imperative that the first and driving factor is the business need. Then, based on the business need, applications are selected to provide needed services. Based on the applications needed, data support and structures capable of providing the needed inputs are then chosen. Finally, based on all of the above, specific technologies to implement the physical solution are delineated. The logical design is, therefore, the blueprint for the desired solution. The logical design is implementation independent, meaning that it contains no reference to specific technologies, vendors, or products. It addresses, instead, how the proposed system will solve the problem at hand. In this stage, analysts generate a number of alternative solutions, each with corresponding strengths and weaknesses, and costs and benefits, allowing for a general comparison of available options. At the end of this phase, another feasibility analysis is performed.

3.2 Architecture and Strategic of Decision Support System

The phase and cycle in quantitative research internal validity refers to the degree to which the findings describe reality, external validity is shown by the ability to generalize findings in different environments, reliability is shown by the degree to which measurements remain the same when the experiment is repeated and objectivity is shown by quantitative measures which are value-free. In this approach we have considered the very best to analysis each component in to consideration which makes the best value to data rather the solution we are providing. By taking OOPS concept, which makes us reusability and other stuffs to next level of journey to programming concept make the software maintenance and enhancement easier as compared to classical language.

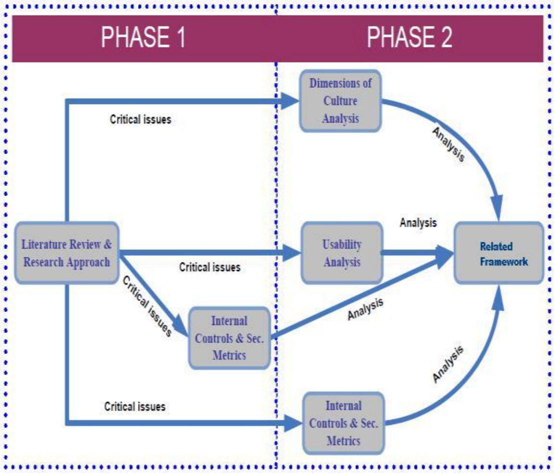

Fig. 3.2.1 Architecture of decision Support and Logical Flow.

In the above flow level, we consider the strategic level in the optimal and the throughput level of the high level supercomputing on stress testing and boundary value analysis, whether IBM based high computing engine can able do the performance in the very best way. In the fig.3.2 , we have the two axis or level approach where issue and analysis are in phase 1 and phase 2 respectively in ordered to analysis the business data in very best and providing the best coupling which call lose coupling in the software engineering field.

This architecture describes the very best solution in a very high level abstraction providing the data, business layer in phases and differing from refactoring to nest level of changes. Keeping an eye, of those factors as data and business is always a changing, it will help to modify and making changes easier. Considering the above parameters we would like to describe the framework; is a support structure or extensible structure for describing a set of concepts, methods, technologies, and cultural changes necessary for a complete product design and manufacturing process. Key components of this framework are three assurance aspects, namely: system life cycle, non-technical assurance factors and technical assurance factors. Fig. 3.2 shows issues to consider prior to identifying assurance methods. The selection of assurance methods depends on the life cycle stage and whether one wants to deal with non-technical or technical issues.

The output of a strategically designed and well- managed organization-wide can be used to maintain a system's authorization to operate and keep required system information and data (i.e., System Security Plan together with Risk Assessment Report, Security Assessment Report) up to date on an ongoing basis. Security management and reporting tools may provide functionality to automate updates to key evidence needed for ongoing authorization decisions. It also facilitates risk-based decision making regarding the ongoing authorization to operate information systems and security authorization for common controls by providing evolving threat activity or vulnerability information on demand. A security control assessment and risk determination process, otherwise static between authorizations, is thus transformed into a dynamic process that supports timely risk response actions and cost-effective, ongoing authorizations. Continuous monitoring of threats, vulnerabilities, and security control effectiveness provides situational awareness for risk-based support of ongoing authorization decisions. An appropriately designed strategy and program supports ongoing authorization of type authorizations, as well as single, joint, and leveraged authorizations.

4. Conclusion

Our research was mainly qualitative as its aims were to understand the technical and nontechnical aspects of information systems security assurance to Bio-Medical. In this endeavor we chose to conduct a socio-technical analysis including the aspects of security culture, usability testing, specification of security requirements and re-use of such requirements, and the establishment and measuring of internal security controls. The Common Criteria was extensively used, either directly or secondarily for this work. They were used to analyses systems security requirements including examining the possibilities of their re-use, and developing heuristics for performing the usability evaluation. They were also together with Systems Security Engineering Capability Maturity Model a large part of background information for the analyses of internal controls and security metrics. For the cultural studies, the GLOBE culture dimensions together with the Common Criteria were used as a starting point to examine the national, organizational and security culture through questionnaires in biomedical science..

5. Reference

[1]. F.P. Lees. Loss Prevention in Chemical Process Industries. Butterworth, London, 2nd edition, 1996.
[2] http://www.ncbi.nlm.nih.gov/omim
[3] http://lucene.apache.org/java/docs/

[4] R. Baeza-Yates and B. Ribeiro-Neto,

Modern Information Retrieval. Reading, MA: Addison-Wesley, 1999.

[5] M. Lee, W. Wang, and H. Yu,

"Exploring supervised and unsupervised methods to detect topics in biomedical text,"

BMC Bioinformat., vol. 7,no. 1, p. 140, Mar. 2006.

[6] G. Salton and M. McGill, *Introduction to Modern Information Retrieval*. New York: McGraw-Hill, 1983.

[7] J. Lin and W. Wilbur, "PubMed related articles: A probabilistic topicbased model for content similarity," *BMC Bioinformat.*, vol. 8, no. 1,p. 423, Oct. 2007.

[8] T. Theodosiou, N. Darzentas, L. Angelis, and C. Ouzounis, "PuReDMCL: A graph-based PubMed document clustering methodology," *Bioinformatics*, vol. 24, no. 17, pp. 1935–1941, Sep. 2008.

[9] S. J. Nelson, M. Schopen, A. G. Savage, J. L. Schulman, and N. Arluk, "The MeSH translation maintenance system: Structure, interface design, and implementation," in

Proc. MEDINFO, 2004, pp. 67–69.

[10] I. Yoo, X. Hu, and I.-Y. Song,

"Biomedical ontology improves biomedical literature clustering performance: A comparison study," *Int. J. Bioinformat. Res.*

Appl., vol. 3, no. 3, pp. 414–428, Sep. 2007.

[11] X. Zhang, L. Jing, X. Hu, M. Ng, and

X. Zhou, "A comparative study of ontology based term similarity measures on PubMed document clustering," in *Proc. DASFAA (LNCS 4443)*, 2007, pp. 115–126.

[12] S. Zhu, J. Zeng, and H. Mamitsuka,

"Enhancing MEDLINE document clustering by incorporating mesh semantic similarity,"

Bioinformatics, vol. 25, no. 15, pp. 1944– 1951, Aug. 2009.

[13] D. Hanisch, A. Zien, R. Zimmer, and T.

Lengauer, "Coclustering of biological networks and gene expression data,"

Bioinformatics, vol. 18, no. S1, pp. 145– 154, Jul. 2002.

[14] W. Pan, "Incorporating gene functions as priors in model-based clustering of microarray gene expression data,"

Bioinformatics, vol. 22, no. 7, pp. 795–801, Apr. 2006.