Centralized Access Distribution Security System a Solution to Data Breach Security Problem

Syed Ehsen Mustafa[1], Irfan Anjum Manarvi[2]

GJCST Classification (FOR)
H.2.7, C.2.0

***Abstract*- The focus of this paper is to identify critical data security problems after analyzing the data breach incidents reported during the years 2006 to 2009, in order to provide an effective and efficient solution by proposing a security system that would provide protection against data beaches. In this Paper the analysis of databases for security breach incidents provides a good review for type of businesses that are affected by the data breaches, the type of data targeted for data breach attacks, frequency for type of breaches and attacks that are used to compromise the data security. After the identification of higher frequency threats and ways in which data is compromised, a solution has been provided using the problem solving techniques. The proposed Centralized Access Distribution (CAD) Security System is an efficient and effective solution based on the nine components essential to provide a solution to the identified problems of data breaches. CAD focuses on providing a configurable security system that would provide data confidentiality, data integrity, intrusion detection and prevention, automation of security procedures while monitoring the states of objects and subjects available in access control lists and features of data logging for threat analysis, thus providing a complete solution to data breaches on the rise.**

Keywords- Data breach, Information security, Centralized Access distribution, RBAC model, Network Security.

I. Introduction

This paper attempts to provide a solution for the problems identified after the detailed analysis of the records (i.e. Data breach incidents reported) available at [12]. In this paper the analysis has been done on the records for year 2006 to 2009 in order to identify the data breach problems being faced by the different business types including Private Businesses, Government Organizations, Educational Institutions and Medical Institutions.In order to solve the problems of security breach and data breach most of the security systems are based on Access control models. Two commonly known access control models are Discretionary Access control (DAC) and Mandatory Access Control (MAC). DAC [1, 2, 4, 13] provides basic security on information flows and is useful in development of commercial security systems, but the problem with DAC is that it is vulnerable to the attacks of unauthorized access, for example it does not provide protection against attacks like Trojans. In comparison to DAC, MAC [1, 2, 4] does provide the functionality of unauthorized access, for example it does not provide protection against attacks like Trojans. In comparison to DAC, MAC [1, 2, 4, 14] does provide the functionality of preventing unauthorized user access, but the limitation of MAC is that due to the level of security achieved by MAC and the complexity of its implementation, it is mainly used for military security systems.Role Based Access Control Model (RBAC) was proposed in early 1990‘s by American National Standards and Technology Research Institute. RBAC model [1, 2, 3, 4, 5, 15] has been powerful in controlling information flows as compared to the functionalities provided by the traditional DAC and MAC models. RBAC model has proved to be a generic model that could be extended to develop new security models and security systems where the data security criteria of data confidentiality, data integrity, intrusion detection and prevention are fulfilled.In this paper study of different extensions of RBAC model have been done, where each extension solves a problem of data security for different working environments. The solution provided in this paper as a Centralized Access Distribution is based on the combination of features presented in different RBAC model extensions discussed below.In [1] a feature of task based permission management has been added to existing RBAC model. This feature is helpful in managing the access control of users on multiple devices on the network. Addition of this feature ensures the authentication and authorization of users on the network at abstraction layer and controlling dependencies of subjects and objects involved in the network management system.Adding the functionality of automated prevention and monitoring to existing RBAC model by using State Transfer Based Dynamic policy would result in development of an effective and efficient access control system [2]. The concept of this policy is to assign access priorities to systems on network and monitor the states of the system that are active on the network. The state of the system can change dynamically based on the policy defined for the active systems. The state based transfer controls the unauthorized requests of active systems and grant access to system of high priority, thus integrating user authentication and access control to achieve better security [16]. Combination of object oriented approach with RBAC model results in controlling information flows and providing intrusion prevention functions [4]. The concept of Access control List (ACL) is used to control information leakage and unauthorized access to databases of data under protection.As Business environments are targeted for compromising the data confidentiality and information leakage, [6] provides concept of combined Network security and data security that

About[1]- Syed Ehsen Mustafa is MSc Engineering Management Student at CASE, Centre of Advanced Studies in Engineering, Islamabad Pakistan ehsen67@yahoo.com.

About[2]- Irfan Anjum Manarvi is Associate Professor at Iqra University Islamabad Campus, Islamabad Pakistan. irfanmanarvi@yahoo.com.

would be effective in securing the business environments. The key is to group the data and processes (that are available in a Business information networks) in to authorized access level Sets. Once the access levels are defined a function would be implemented that would assign the access rights to each group according to their access level [17]. Such a controlled implementation would control unauthorized access within the network and prevent any external unauthorized access. Implementing ACL in security systems could help in improving Network security [18]. An access control approach of using encryption techniques can be used to prevent an unauthorized access of data [7, 8]. The policy of hiding data from unauthorized user such that only legitimate users can see and access the information can be used as a feature addition to the existing RBAC model for enhanced security. This feature ensures secure information exchange between different processes running on a network.Information leakage is a major threat for any social networking environment. The solution provided in [9] not only considers the logical access of the system but also the physical access in order to ensure security of data on network. [19] Introduces the feature of automated monitoring for detecting intrusions by controlling the states of all components on the network under protection.For the development of a security system it is essential to follow a formal security model, where a model can be extended to achieve desired level of security [10].It is also important that a security system should be configurable, in order to update the security processes against newly identified threats [11], just like the Preventive Information security management system providing strong intrusion prevention capabilities. But in addition to intrusion prevention features [20] discusses about the control of authorized user in order to avoid insider malicious activities, as a network without insider security is still vulnerable even if it is protected for outside security threats.In this paper Section II describes the methodology used for data analysis for identification of problems and the techniques used for solving the problems identified. Sections III to XIII are about the analysis of data breach incidents. Section XIV explains CAD system in detail. Section XV is presents the summary of all the finding of analysis and finally section XVI discusses conclusions.

II. Methodology

In this paper a detailed analysis of security breach incidents has been done. In order to analyze the real time data breach incidents a database of data breach records was downloaded from [12] for a period of four years 2006 to 2009. The data acquired from this website was used to analyze the data breach incidents. The variables used for analysis are four business domains targeted for data breach attacks, eleven breach types used for attacks, three different data types that were targeted for data breach attacks, total number of people affected by these attacks, four different sources of attacks and variable for data recovery after data breach attacks. In general tools used for analysis were bar plots, time series plot, doughnut plots, pie charts and pivot tables.First it was analyzed that how many people were affected due to data breach incidents during years 2006 to 2009. A pie chart was drawn showing the yearly percentages of people getting affected by data breach attacks, where the year 2009 was observed to be the year where maximum people were affected in comparison to other years.Then a variable of business types was analyzed by drawing a pie chart of percentages showing that private businesses are the most affected by these incidents. A pivot table of business domains versus total affected was created in order to analyze the frequency for number of people getting affected in each business domain. A bar plot was also drawn to graphically observe the relation of total affected versus business domains.After identifying the variable of business domains, the variable of breach types was analyzed by creating a pivot table and a bar plot showing the frequency of breach type being used most of the time to launch data breach attacks. The fact that the total number of people getting affected by each breach method was also analyzed by drawing a pie chat of percentages for total affected versus breach type.After analyzing the most critical breach types, analysis of different data types was done in order to evaluate how different breach methods affect different data types and to identify the data type being targeted maximum number of time during these years. For this purpose pivot tables and bar plots were drawn, with a time series plot also drawn for analyzing the trend of data types being affected during years 2006 to 2009 such that the facts gathered will be helpful while developing a new security systems. Comparison of data type versus business type was also done by drawing pivot table and bar plots to analyze the type of data getting affected corresponding to each business domain mentioned in records. Next the analysis of total affected versus data types was done in order to analyze that how many are affected with respect to each data type mentioned in records.The variable of Attack types was also analyzed by in order to identify the sources of these data breach incidents. Again this variable was analyzed by using pivot tables and bar plots. Time series plot was also drawn in order to identify the trend of attacks being launched during last four years. Finally the variable of data recovery was also analyzed by drawing a doughnut plot showing the percentages of data recovered and the data that was unable to get recovered.After analyzing the and identifying the high frequency threats, a solution was proposed that would result in an security system providing solution to all identified high frequency threats.In order to propose a solution study of different security models was done. As the goal was to present a security system, it very important to select a traditional model on which the proposed security system should be developed. So the studied security models were then evaluated on the criteria identified after analysis of data breach incidents. The different alternatives were first rated using Thomas Saaty‘s Matrix and then selection was done by using SFF matrix.

III. Analysis of total affected by data breach incidents

It is important to analyze that the total number of people affected by the data breach incidents during years 2006 to 2009 in order to evaluate the depth of this problem that is affecting millions. Following Figure-1 shows the percentages of total number of people affected by data breach incidents every year.

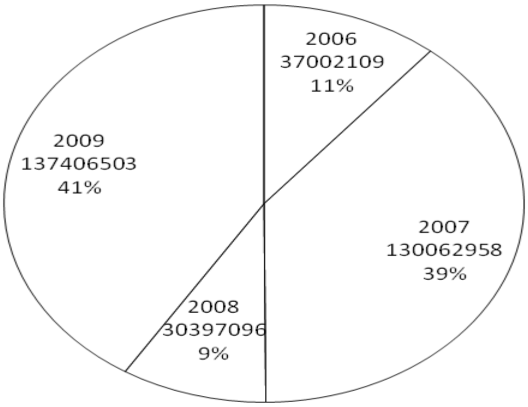


Fig.1. Percentages of Total affected by Data Breaches

Inferences drawn from the above figure are as follows:

(1) A total of 334868666 have been affected by the data breach incidents during years 2006 to 2009.

(2) About 41% got affected during year 2009 being the highest number of people affected in comparison to years 2006 to 2008.

(3) It shows that there is an increase in number of people getting affected by data reach incidents in 2009

Next it‘s required to analyze domains/businesses that have been affected, the methods that been use used to affect 334868666 people and the type of data that has been targeted for data breach.

IV. Analysis of different Business types affected by data breach incidents

The variable Business Types in the records represents four different types of business domains that are affected by the data breach security problems. The data breach incidents are reported for the following business domains:-

1) Private businesses (Biz), that includes corporate offices, IT firms, Banks, Leisure and Food Industry.
2) Educational Institutions (Edu).
3) Government Organizations (Gov).
4) Medical Institutions (Med).

Following Figure-2 shows a pie chart for the percentages of above mentioned business domains affected by the data breach incidents during years 2006 to 2009.

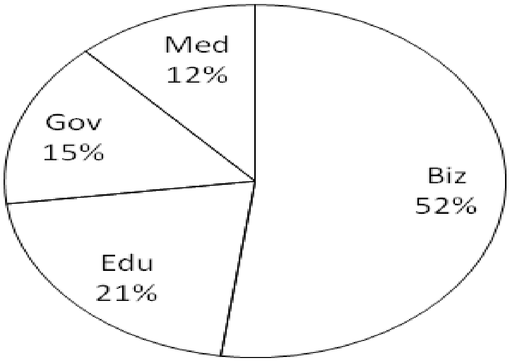


Fig.2. Percentages of Types of Business domains affected

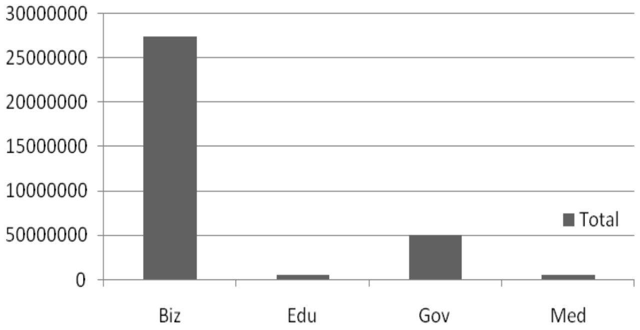


Fig.3. Total Affected Vs Business Types

Business Types	Sum of Total Affected
Biz	274500860
Edu	5287712
Gov	50513093
Med	4567001
Grand Total	334868666

Table 6.Pivot Table for Sum Total Affected Vs Business Types

Inferences drawn from the above figures are as follows:

1) Private businesses are the most affected by data breach incidents with 52% as the highest percentage of incidents being reported from this domain.
2) Second highest domain affected by the data breach incidents is Educational institutions with a percentage of 21%.
3) According to Table-1 274500860 affected are related to Private business domains. It shows that Private business domains are more vulnerable to data breach attacks as compared to other business domains.
4) As inferred that Private businesses are the most affected can be verified by observing the histogram in Figure-3 and Table-1 that significant amount of people affected are from Private business domains.

As private businesses are the most affected type, it‘s required to analyze different breach methods used to attack different business domains.

V. Analysis of Breach Types Reported in Records

The variable Breach Type represents the methods used for attempting data breach in different business domains. Following are different breach types reported:-

(1) Data breach using web based attacks.
(2) Data breach based on fraud or scam (usually insider-related), social engineering.
(3) Data breach using hacking techniques. Computer-based intrusion including data that should not be exposed publically.
(4) Data breach because of exposure to personal information via virus or Trojan (i.e. keystroke logger, possibly classified as hacking).
(5) Data breach by snail mail. Scenario can be of personal information in "snail mail" getting exposed to unintended third party.
(6) Data breach because of disposal document i.e. information disclosure because of documents not being disposed of properly.
(7) Data breach because of information disclosure due to lost or stolen document.
(8) Data breach via stolen laptops or stolen computers.

Table-1 is a pivot table showing the sum of different breach types during years 2006 to 2009, Figure-2 is the depiction of Table-1 in terms of highest numbers of method used to compromise the data.

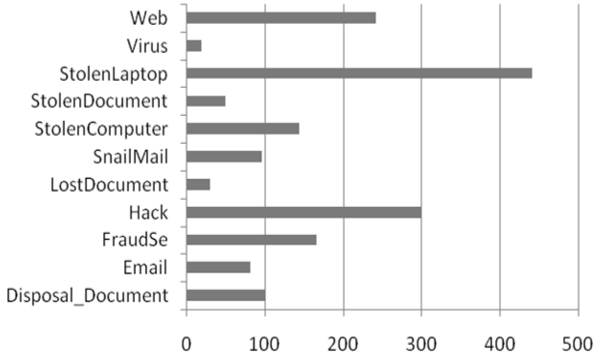


Fig.4. Bar plot showing sum of all Breach Types

Row Labels	Count of Breach Type	Sum of Total Affected
Disposal_Document	101	454740
Email	81	166279
FraudSe	165	23827397
Hack	299	254990453
LostDocument	30	1143278
SnailMail	95	7808681
StolenComputer	143	31292269
StolenDocument	49	351954
StolenLaptop	441	12420046
Virus	18	56230
Web	241	2357339
Grand Total	1663	334868666

Table 7.Pivot Table for Sum of Breach Types

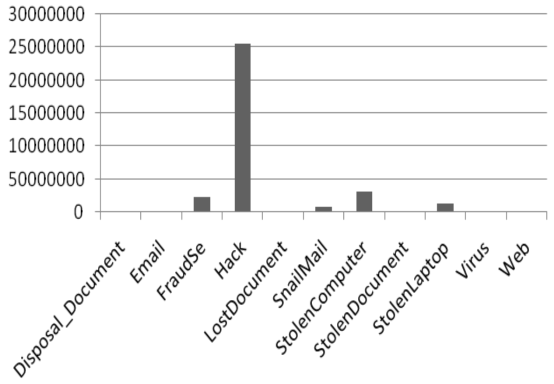


Fig.5. Frequency of Total Affected Vs Breach Types

Inferences drawn from the above pivot table and figures are as follows:

1) Data breach due to stolen laptops has the highest count of 441, showing that most of the times a major reason of data being compromised is due to storage of confidential data on laptops.
2) Second highest methods used for data breach are hacking and web based attacks as the reported incidents for hacking are 299 and web based attacks are 241.
3) Viewing the bar plot we can see that most of the data is compromised or leaked because of unprotected data available on stolen laptops, computers, documents or lost documents.
4) According to the pivot table, method of Hacking has affected about 255499053 as the highest number in comparison to other methods. Histogram in Figure-5 is the depiction of pivot table-2 for total affected versus breach types and it verifies the inference that data breach due method of hacking has affected the significant amount of people.
5) Observation shows that the lack of features for protected data availability, and data confidentiality in a security system could lead to data breach incidents on stolen laptops and computers. A security system must ensure that the data being used by the authenticated employees must be protected and remain confidential after their use.
6) Hacking as observed to be the second most method used for data breaches but the number of people it has affected is greater than any other method discussed in this analysis. This shows that a security system should have control over malicious and ambiguous events occurring within the network.
7) After analyzing different methods used for data breaches, different data types that are vulnerable to data breach needs to be analyzed in order to

classify data types targeted using the methods discussed in above inferences.

VI. Analysis of Data types Affected

The variable Data Types represents different types of data that are under attack of data breaches. Following is the description of different types for data, reported to have been compromised:-

1) Financial Information (FIN) including Credit Card numbers, Bank Account information etc.
2) Data related to Social Security Numbers (SSN).
3) Medical data (MED) including patient history, employee Medical History available in HR records etc.).
4) Mixed data including both financial data and social security numbers.
5) Mixed data including both financial and medical data.

Following Figure shows the sum of different data types being targeted for data breach attacks.

	Data Types					
Years	FIN Data	MED Data	MED and FIN Data	SSN and FIN Data	SSN Data	Grand Total
2006	60	20	2	51	247	380
2007	67	22	1	59	215	364
2008	116	48	5	72	296	537
2009	98	58	5	65	156	382
Grand Total	341	148	13	247	914	1663

Table 8.Pivot Table for Data Types

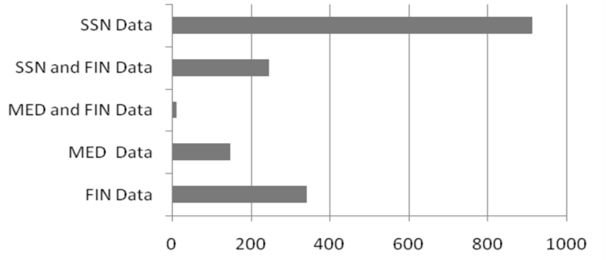


Fig.6. Bar Plot showing sum of all Data Types

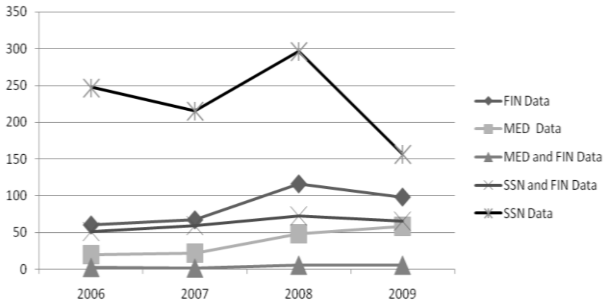


Fig.7. Time Series plot for Data Types

Inferences drawn from the above pivot table and figures are as follows:

1) Figure-6 shows different frequencies of data types presenting the fact that during years 2006 to 2009 most of the data breach attacks targeted Social Security Numbers data.
2) Out of 1663 incidents reported 914 were related to Social Security Numbers, which is about 55% in total.
3) Figure 7 representing a time series plot for different data types also shows that every year from 2006 to 2009 attacks on Social Security Numbers were the high frequency reported incidents.
4) According to Figure 7 and pivot table 3 highest numbers of incidents were recorded in year 2008 and after analyzing Pivot Table-3 it can be observed that total numbers of incidents dropped by 28% in year 2009. But still incidents related to Social Security Numbers were the highest according to the observations in Figure 7.

VII. Comparison of Business type Vs Data type

Table-4 shows the comparison of two variables from the data breach incidents recorded.Figure-8 is the depiction of pivot table-4.

	Data Types					
Business Domains	FIN Data	MED Data	MED and FIN Data	SSN and FIN Data	SSN Data	Grand Total
Biz	295	21	8	199	345	868
Edu	10	24		15	296	345
Gov	25	16	1	24	187	253
Med	11	87	4	9	86	197
Grand Total	341	148	13	247	914	1663

Table 4.Sum of Data Types Vs Business Domains

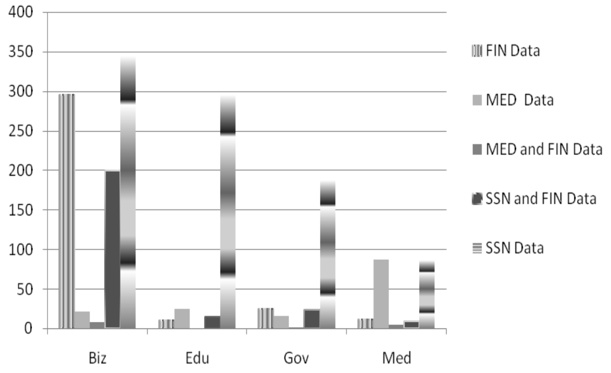


Fig.8. Comparison of Business Type vs. Data Type

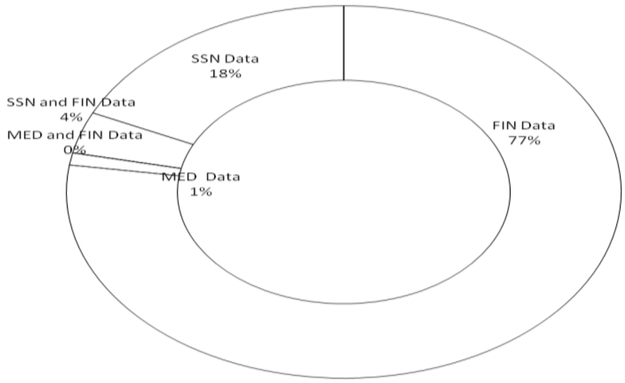


Fig.9. Percentages of Total Affected Vs Data Type

Inferences drawn from the above pivot table and figure are as follows:

1) Figure-8 shows that data breach attacks on Private businesses targeted Social Security Numbers data and financial data with recorded 345 and 295 frequencies of incidents respectively. These records are the highest in comparison to other businesses.
2) In Educational Institutions and Government Organizations frequency of attacks on Social Security Numbers data is recorded as the highest in number (i.e. 296 and 197).
3) According to the above inferences information leakages of Social Security Numbers data is on the rise during years 2006 to 2009.It shows that the features of data hiding and data confidentiality should be supported by security systems in order to protect this large amount of data.
4) Although a large number of incidents reported were related to attacks on Social Security Numbers data but according to Figure-9 doughnut plot most of the people are affected by attacks on financial data. Doughnut plot in Figure-9 shows that 77% of 334 million people are affected by attacks on financial data.

I. Comparison of Breach Type Vs Data Type

Figure-10 represents the frequencies of data type against the two highly recorded breach types in order to analyze how different breach types target different types of data.

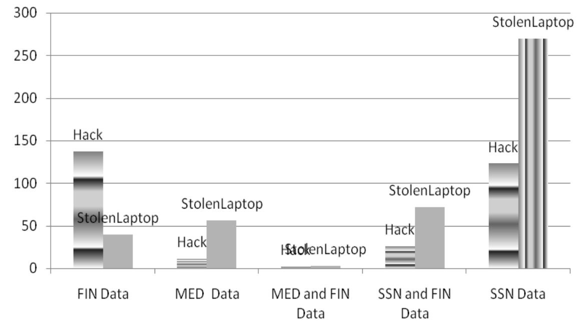


Fig.10. Comparison of Breach Type Vs Data Type

Inferences drawn from the above pivot table and figure are as follows:

(4) Figure-10 shows that data breach from stolen laptops and hacking affects Social Security Numbers databases, where SSN data breach incidents due to stolen laptops is above 250 and due to hacking are above 100.
(5) Incidents where financial data type is compromised are below 50 in case of stolen laptops and above 140 in case of hacking as a method of data breach attack.
(6) The method of hacking and information leakage due to stolen laptops has also affected medical related data but the amounts of incidents recorded are less in comparison to other data types.

In the next section analysis of attack type needs to be done in order to identify the security measures that are needed to be implemented for prevention of data breach attacks.

II. Analysis of Attack Types

The analysis of variable Attack type will help to identify the security procedures that need to be taken to prevent the data breach attacks. Following is the description of different categories of attacks as per records:-

1) Outside attacks (hacking, malware, viruses)
2) Inside Malicious attacks (Intruder attacks, Fraud, scams).
3) Inside Accidental attacks (Due to untrained employees, careless management of data, documents).

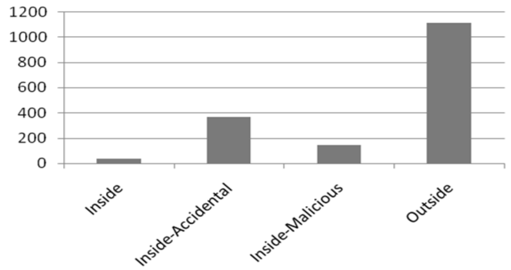


Fig.11. Frequency of Attacks Types

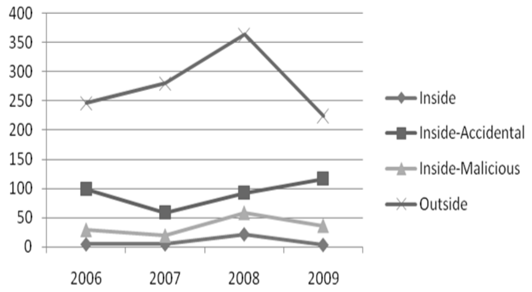


Fig.12. Time series plot for Type of attacks 2006 to 2009

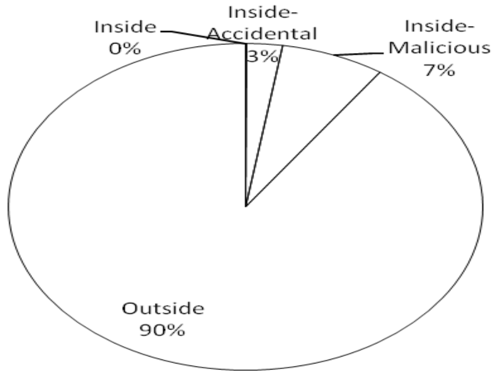


Fig.13. Percentages of Total Affected Vs Attack Type

Inferences drawn from the above pivot table and figure are as follows:

1) Figure-11 shows that maximum of data breach attacks are from the category of outside attacks, with a frequency of 1113 incidents recorded as outside attacks. This shows that Automation of monitoring and data breach prevention techniques needs to be present in a security system in order to take care of outsider attack threats.
2) Second highest number (i.e. 368 out of 1663) of incidents recorded are related to insider malicious attacks category, which shows that accidental exposure of confidential data is also a case of data breach. Such a problem requires automated monitoring to prevent accidents and development of security training policies.
3) Figure-12 shows the time series plot verifying that outsider attacks are highest during years 2006 to 2009 where Figure-13 shows that outsider attacks has affected 90% of 334 million people. So outsider attacks are a major problem for data security and have been affecting millions of people during years 2006 to 2009.
4) As inferred that from Figure-12 that frequency of insider accidental attacks is the highest but according to Figure-13 pie chart insider malicious attacks (7%) has affected 4% more people then insider accidental attacks (3%).So it more critical to solve problem of insider malicious attacks then insider accidental attacks.

X. Comparison of Attack Type Vs Data Type

Following comparison helps in analyzing how different attack types have affected different data types during years 2006 to 2009.

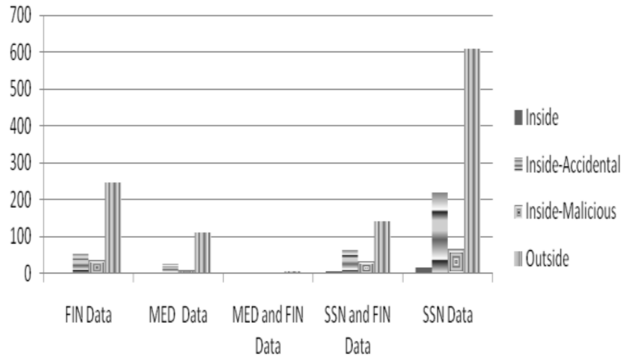


Fig.14. Comparison of Attack Type Vs Data Type

Inferences drawn from the above pivot table and figure are as follows:

1) As from the previous inferences we already know that SSN data is the most targeted data for data breach attacks, observation on Table-6 shows that 600 plus records of incidents as the highest in number are related to the category of outside attacks used to compromise SSN data.
2) Figure-14 shows that inside accidental attacks and outside attacks both are a major source of attacks used to compromise SSN data.
3) By observation inside accidental attacks and outside attacks again are the major source attack types for financial data recorded as the second highest data type under data breach attacks.

XI. Comparison of Attack Type Vs Business Type

Following comparison helps in analyzing the high frequency breach methods used to perform data breach attacks.

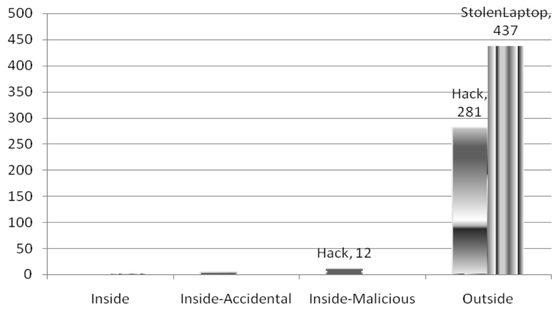


Fig.15. Comparison of Attack Type Vs Business Type

Inferences drawn from the above figure are as follows:

1) Figure-15 shows that outside attacks have affected all four types of business domains with a maximum amount of incidents recorded as outside attacks, where above 590 incidents as the maximum number of attacks have been reported for private businesses.
2) Figure-15 also verifies the previous inferences that the category of inside accidental attacks as the

second highest in number has also affected all four business domains.

XII. Comparison of Attack Type Vs Breach Type

Following comparison helps in analyzing the high frequency breach methods used to perform data breach attacks.

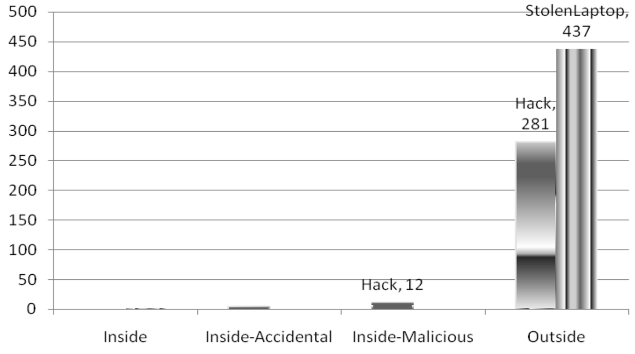


Fig.16. Frequency of Attack Type Vs Breach Type

Inferences drawn from the above figure are as follows:

1) Figure-16 shows that outside attacks with maximum number of 437 incidents recorded used stolen laptop breach method (i.e. previously inferred to be the most commonly used breach method).
2) Figure-16 shows that outside attacks with frequency of 281 out of 1663 records used hacking as a breach method (i.e. previously inferred to have affected maximum number of 25 million people).

a) Analysis of Data Recovered

The variable of data recovered shows the statistics for data recovery out of all the incidents reported. The facts drawn from the following figure will help in identifying the need of integrating data backup and data logging features in a security system.

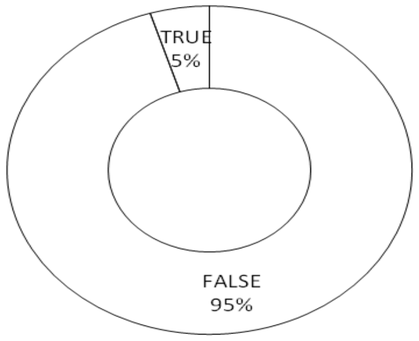


Fig.17. Doughnut plot showing percentages of Data Recovered

Inferences drawn from the above figure are as follows:

1) Figure-17 doughnut plot showing the percentages for data recovered in reported incidents where in 95% of the recoded data breach incidents data was not recovered which shows that the features of data logging and feedback are missing from most security systems.
2) It means that this 95% of data that was lost shows the scale of information leakage problem that is related to 334 million people (according to the above discussed statistics) needs one generic solution against the threats of hacking, network intrusion, and accidental information exposure.

XIV. Centralized Access Distribution System

The detailed analysis of data breach incidents in the above discussions shows that in current business environments following critical problems are observed.

1) Problem of data confidentiality (mostly observed in private business domains).
2) Controlling unauthorized access in to the networks (as maximum numbers of incidents recorded are outside attacks i.e. outside network intrusion).
3) Prevention of breach methods like hacking.
4) Data logging and feedback mechanisms.
5) Training policies to avoid accidental exposure of confidential data.

The goal of this newly proposed Centralized Access Distribution (CAD) system is to provide solution for the above identified problems. In order to develop a security system it is essential that a security system should be developed based on some traditional authorized security model where basic elements of providing security are available. The importance of security model compliance is that it provides a structured base one can use and enhance for achieving desired security.So for the proposal of CAD security system, first a traditional security model should be selected. As discussed in the Introduction section there are three commonly known traditional data security models being used for development of security systems and can be extended for proposal of new security model to be used for specific environments.In this paper three models that are selected for evaluation are Discretionary Access model (DAC), Mandatory Access Model (MAC) and Role Based Access Control (RBAC) Model. Evaluation of these selected models is done on the defined criteria using Thomas Saaty‘s Matrix. The following criteria are the basic requirement of proposed CAD model:-

1) Does the model Provide data confidentiality features?
2) Does it provide data Integrity?
3) Does it provide protection against unauthorized intrusion?

Alternatives	DAC	MAC	RBAC	SUM	RANK
DAC		0	0	0	3rd
MAC	1		0	1	2nd
RBAC	1	1		2	1st

Table 5.Thomas Saaty's Matrix for Model evaluation

RBAC model stands at first position as it fulfills the criteria required for developing basic structure of proposed CAD model, where as DAC and MAC models do support data security but they have their own limitation as discussed and mentioned in the Introduction section of this paper.For the selection of best alternative SFF Matrix is used. Criteria for SFF are as follows:

1. *Criteria for suitability*

Does this model provide data security mechanisms for secure access control over the network and data sources?

2. *Criteria for Feasibility*

Implementation complexity of the Model (Is it easily implementable and generic to be used commercially).

3. *Criteria for Flexibility*

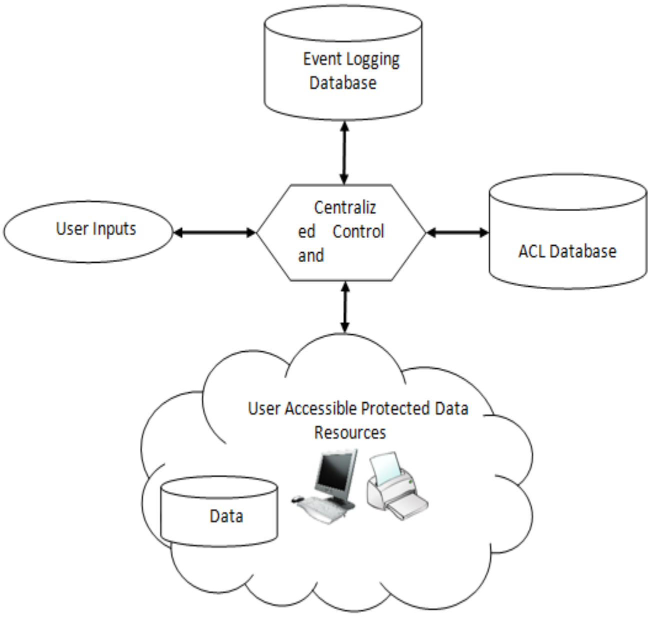
Is it easily extendable for achieving desired security (i.e. addition of new features)?Now the selected Alternatives (i.e. security models) will be awarded points from 1 – 3 with 1 being the lowest point and 3 being the highest in SFF Matrix below.

Alternatives	Suitability	Feasibility	Flexibility	Total
DAC	1	1	1	3
MAC	2	1	1	4
RBAC	2	2	2	6

Table 6. SFF Matrix for selection of Security Model

On the basis of results obtained from SFF Matrix, RBAC model has a higher total of 6. In comparison to the results of Thomas Saaty's Matrix RBAC model was ranked at first position and here at SFF Matrix also RBAC has proved to be the best alternative, so RBAC model will be used for the development of Centralized Access Distribution system.After the analysis and identification of core problems from the data breach incident database, the proposed CAD system is defined based on nine components that would serve as the features of the CAD system. Each of these nine components provides a solution to the real time industrial problems identified after analysis. Figure 18 shows the architecture of CAD security system proposed as a solution to Identified problems

Fig.18. Architecture of CAD Security Syste



CAD Security System consists of three types of Access control Lists (ACL):-

1) Access control list for Users registered into the security system with a tag representing active and inactive users.
2) Access control list for roles and permissions associated with each user to access resources.
3) Access control list for resources that are under observation and available on the network.

As shown in Figure-18 a database for access control lists is available and a list a database of event logging is also available. One centralized module functions to control the user inputs (for accessing the network resources) and monitor the activities going on the user accessible protected data resources. Whenever there is a request from the user to access a protected resource, the central monitoring module verifies user registration from user ACL and then verifies the request such that the user is authorized to access the protected resource. Once the authorization process is complete user is allowed to access the desired resource.

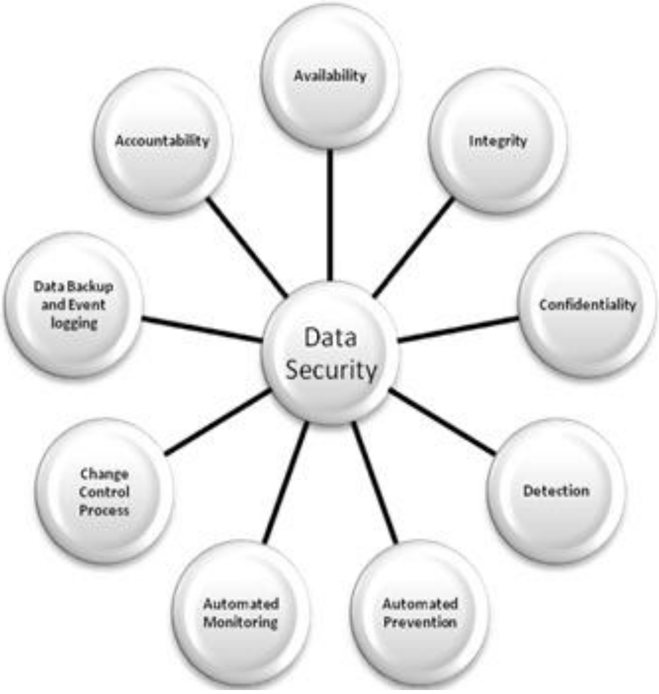


Fig.19. Components of CAD Security System

Nine different components that are used to ensure the security of a network and it resources are described below.

4. *Confidentiality*

This feature ensures the protection of data throughout organization‗s information architecture.As data confidentiality is the basic feature that can be ensured by the implementation of encryption techniques while transferring data on the network. This is equivalent to using data hidden policy as the data can only be decrypted and viewed by authorized user.According to the analysis done on security breach incidents database data loss due to stolen laptops was identified as high frequency breach type. The proposed CAD security system provides a solution to this problem by centralizing the data to be used by the laptop users such that the data does not needs to be present on the laptop it can be accessed from the central server using a Virtual Private Network connection from the authorized laptop. Such an arrangement of data usage is helpful in case if a laptop is stolen there will be no data available on the laptop because in current scenario laptop will only be acting as a data processing machine taking encrypted data from central server and then saving the processed data back to central server instead of saving it on laptop.

5. *Integrity*

This feature ensures unauthorized alteration or destruction of data and data providing services. The implementation of this feature refers to the use of Access control list for identification of authorized users such that the resources on the network are dedicated to users according to their access levels. Therefore CAD system based on the principles of RBAC model maintains centralized access control list of authorized users, a list of access levels assigned to each user and a list of resources assigned to each user. This structure helps in ensuring integrity of data under observation.

6. *Availability*

This feature ensures that the data and other services on the secured network are always available for authorized access.The implementation of this feature is ensured by the implementation of central access control list database that would always be available to the monitoring module of the CAD security system. The feature of data confidentiality requires data resources on a centralized data server where the CAD security system needs to ensure that the data resources are always available for processing.

7. *Accountability*

This feature ensures control over malicious and ambiguous events occurring within in a network. The implementation of this feature is ensured by assigning access control roles to the authorized user active in the network. As access control lists are maintained for each user, the monitoring module can easily detect an event of any authorized user with in the network trying to access the resource that is not dedicated for its use. Thus inside accidental malicious attacks could be controlled by efficient implementation of this feature.

8. *Detection*

This feature ensures control over unauthorized access into the security system, thus breaking/ hacking the system security.The implementation of this feature provides the functionality of detecting the attacks being launched from outside the network. As CAD security system provides protection to unauthorized access by the usage of access control lists so the monitoring module validate the access of the resources and data on network by detecting the combinations allowed by access control lists and in case an unknown combination is detected an alarm will be generated by the monitoring module for CAD security system.

9. *Automated Prevention*

This feature ensures the immediate control over response system once detection of a threat is announced. CAD security system provides automated prevention to unauthorized access by blocking the access of malicious user to the resources on the network. According to the analysis done on security breach incidents database maximum numbers of records are related to outside attacks. As breach methods like hacking are launched from outside the network and target data resources, so CAD security system provides encryption mechanisms to protect data such that an encrypted data will be not reveal the actual information. In addition to encryption techniques this system controls access by using access control lists that are controlled centrally and consist of access rights for every authorized user, so in case an authorize user tries to access a protected resource or data on the network that the user is not authorized to access, such an access will automatically be denied by the system.

10. Automated Monitoring

This feature ensures that the system is being monitored continuously without any delay, such that the immediate detection and prevention procedures are executed before a threat becomes a problem.CAD security system provides automated monitoring by implementation of a state based monitoring module that keeps record of active states of the users registered within the network.

11. Change Control Process

This feature ensures effective management of authorized changes when ever required in a system. Addition of this feature results in a configurable system where the roles of authorized users could be re-defined and the system can be easily updated for monitoring of new threats.

12. Data Backup and Event logging

According to the findings of analysis 95% of times data was not recovered after data breach incidents. CAD Security System supports data backup mechanism and event logging for purpose of data recovery in case of data loss, where system event logging would also help in tracking any loss of data in case a data breach attack is launched.

XV. Findings

(1) A total of 334 million people have been affected by the data breach incidents during years 2006 to 2009. There is an increase in number of people getting affected by data breach incidents recorded in year 2009, as the percentage ratio for people getting affected in 2009 is 41% highest in comparison to the records of years 2006 to 2008.

(2) In four different business domains mentioned in the records, Private businesses are the most affected by data breach incidents with a percentage ratio 52% as the highest percentage of incidents reported from this domain in comparison to other domains. According to statistics about 274 million out of the total number of people affected are related to Private business domain. It shows Private business domains are more vulnerable to data breach attacks as compared to other business domains.

(3) Data breach due to stolen laptops has the highest count of 441 out of 1663 records, showing that most of the times a major reason of data being compromised or leaked because of unprotected confidential data available on stolen laptops.

(4) The Breach type Hacking with a count of 299 is recorded as the second highest method of data breach attacks after stolen laptops, but according to the statistics observed after comparison of total affected versus breach types show that method of hacking has affected about 255 million people and is ranked as highest among other breach methods. This shows that a security system should have control over malicious and ambiguous events occurring within the network with features of active monitoring of resources under observation.

(5) Out of 1663 incidents reported 914 were related to Social Security Numbers, which is about 55% in total. According to statistics the attacks related with data type of Social Security Numbers have been ranked as high frequency reported incidents.

(6) In comparison of attacks on Business types and data types, it was observed that attacks on the private businesses targeted Social Security Numbers data and Financial data with frequencies of 345 and 295 (i.e. highest in comparison to frequencies of other data types) respectively.

(7) Although the highest number of attacks launched targeted Social Security Numbers data but in comparison of total people affected with Data types shows that the attack on financial data type has affected about 77% of 334 million people.

(8) Analysis of sources of attacks (i.e. Attack types) shows that out of 1663 incidents recorded 1113 are recorded as outside attacks. According to the comparison of total affected versus attack types outsider attacks have affected 90% of 334 million people resulting in a major threat of data security affecting a large amount of people.

(9) Out of 1663 incidents analyzed data lost in 95% of data breach incidents data was not recovered which shows that the features of data logging and feedback are missing from most security systems. This shows the requirement of efficient data recovery mechanisms to be supported by the security systems.

(10) Highest frequency outside attacks have affected all four types of business domains where a maximum of 473 incidents out of 1663 records used stolen laptops to compromise data and 281 incidents out of 1663 records outside attacks used method of hacking to launch data breach attack. This shows that a security system must support the features of threat detection, prevention and automated monitoring.

XVI. Conclusions

This paper aims to provide a detailed analysis of data breach incidents database and identify the real world problem in order to propose a solution that should be able to address the problems being currently faced by the industry and affecting millions of people. The identified core problems include threats to data confidentiality, unauthorized access of resources on the network, control over accidental exposure of data by authorized resource and lack of features for data recovery. In this paper a solution to these identified problems is proposed. The proposed Centralized Access Distribution security system is based on the role based access control model for basic data security features and in addition to the usage of this traditional model, nine components for achieving data security have been added to the CAD security system. Each component individually solves the problems identified after data breach records analysis and enhances the security on a CAD based system. The implementation of this CAD security system would help in protecting a networked business environment in terms of data confidentiality, data integrity, detection, prevention and monitoring of data breach attacks, easy configuration of system to protect against new threats and finally the event logging mechanism helpful in monitoring malicious activities going on the network.

XVII. REFERENCES

1) Xiaoni Liu Luyan Chen Cuiqin Duan, "Access control in Network Management System," Proceedings of 2nd International Conference on Power Electronics and Intelligent Transportation System (PEITS), 2009, Vol. 1, pp. 227 – 230.
2) Cheng Zang Zhongdong Huang Gang Chen Jinxiang Dong, "A Network Access Control Architecture Using State-Transfer-Based Dynamic Policy," In CSCWD '06: Proceedings of 10th International Conference on Computer Supported Cooperative Work in Design, 2006, pp. 1 – 5.
3) M.J.Moyer and M.Ahmad, "Generalized role-based access control," In ICDS '01: Proceedings of the 21st International Conference on Distributed Computing Systems, pp. 319-398.
4) Shih-Chien Chou, "Embedding role-based access control model in object oriented systems to protect privacy," The Journal of Systems and Software, Vol. 71, pp 143 – 161, 2002.
5) Bindiganavale, V. Jinsong Ouyang, "Role Based Access Control in Enterprise Application – Security Administration and User Management," Proceedings of IEEE International Conference on Information Reuse and Integration, 2006, pp. 111 – 116.
6) Wu Kehe Zhang Tong Li Wei Ma Gang, "Security Model Based on Network Business Security," In ICCTD'09: Proceedings of International Conference on Computer Technology and Development, 2009, Vol. 1, pp. 577 – 580.
7) Shucheng Yu Kui Ren Wenjing Lou, "Attribute-Based Content Distribution with Hidden Policy," In NPSec 2008: 4th Workshop on Secure Network Protocols, 2008, pp. 39 – 44.
8) G.A.S. Torrellas D.V. Cruz, "Security in PKI-based Networking Enviornment: AMulti-Agent Architecture for Distributed Security Management System & Control," In ICCC 2004: Proceedings of Second IEEE International Conference on Computational Cybernetics, 200, pp. 183 – 188.
9) Onno, S. Thomson R&D, Security Labs, Cesson-Sevigne, "A Federated Physical and Logical Access Control Enforcement Model," In ARES 08: Proceedings of Third IEEE International Conference on Availability, Reliability and Security, 2008, pp. 683 – 692.
10) Bao-Chyuan Guan Ping Wang Chen, S.-J. Chang, R.-I, "An Extended Object-Oriented Security Model For High Secure Office Environment," Proceedings of IEEE 37th Annual 2003 International Carnahan Conference on Security Technology, 2003, pp. 57 – 61.
11) Anwar, M.M. Zafar, M.F. Ahmed, Z, "A Proposed Preventive Information Security System," In ICEE '07: Proceedings of International Conference on Electrical Engineering, 2007, pp. 1 – 6.
12) Open Security Foundation DataLossDB website http://datalossdb.org/ breach
13) Wilde, E. Nabholz, N, "Access Control for Shared Resources," Proceedings of International Conference on Computational Intelligence for Modeling, Control and Automation, 2005, Vol. 1, pp. 256 – 250.
14) Gopinath, K, "Access Control in Communication Systems," Comsware 06: Proceddings of First International Conference on Communication System Software and Middleware, 2006, pp. 1 – 8.
15) Yue Zhang Joshi, J.B.D, "Temporal UAS: Supporting Efficient RBAC Authorization in Presence of the Temporal Role Hierarchy," EUC '08: Proceedings of IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2008, Vol. 2, pp. 264 – 271.
16) Harn, L. Lin, H.-Y, "Integration of user authentication and access control," IEE Proceedings of Computers and Digital Techniques, 2005, Vol. 139, Issue 2, pp. 139 – 143.
17) Yi Deng Jiacun Wang Tsai, J.J.P. Beznosov, K. Sch, "An Approach for Modeling and Analysis of Security System Architectures,"IEEE Transactions on Knowledge and Data Engineering, 2003, Vol. 15, Issue 5, pp. 1099 – 1119.
18) Yeu-Pong Lai, Po-Lun Hsia, "Using the vulnerability information of computer systems to improve the network security," Computer Communications, 2007, Vol. 30, Issue 9, pp. 2032 – 2047.
19) Denning, D.E, "An Intrusion-Detection Model," IEEE Transactions on Software Engineering, 2006, Vol. SE-13, Issue 2, pp. 222 – 232.
20) Felicia A. Durán, Stephen H. Conrad, Gregory N. Conrad, DavidP. Duggan, and E. Bruce Held, "Building a System for Insider Security," IEEE Security and Privacy, 2009, Vol. 7, Issue 6, pp. 30 – 39.