IITM Journal of Information Technology

Annual Journal of Institute of Innovation in Technology & Management

Volume 1 **Issue 1** **January-December, 2015**

CONTENTS

Research Papers & Articles

BLANK

Discovering Rule Dynamics in Real Estate on Hetrogeneous Data Sets

Dr. Geetali Banerji*
Dr. Kanak Saxena**

Abstract

This Paper deals with the prediction of investment power of customers in the Real estate, as it is a field that is budding day by day and where the changes are taking place recurrently. The paper concerns on factors, which the prediction of investment power is possible. The investment power considers three major aspects i.e. social constraints, Income and bank transactions. The combined customer data with preprogrammed offering that aims at customer meeting certain criteria, when the demand is sensitive and stochastic to customer interest with social constraints. In this paper, concept of ruled dynamics is used. It is proved to be more efficient and accurate in terms of rules efficiency and accuracy to facilitate the real estate domain and not only to identify the investment power but also in setting of cost, structure, facilities etc. which fulfills the day-by-day need of customer with their desired profits.

Key Words: Association Rules, CobWeb, DBSCAN, K-means, preprocessing, unsupervised learning.

I. Introduction

In Real estate domain, a real estate broker who sends a direct mail catalog to its current customer database promoting various schemes. Customer Interest is recorded in a transactional database recording his demographic, educational and professional information. The customers need or requirements keep on changing that is of more dynamic in nature. There can be three groups of customers namely "willing to invest", "may invest" and "not at all interested". The major reason of its dynamic nature is income, demographic data and his social constraints, which can be identified and analyzed by his day to day transactions for this we have found data mining techniques has a great impact in prediction to find out the future trends of customer in Real Estate.

Data mining or the efficient discovery of interesting patterns from a large collection of data is an important area of database research. The most commonly sought patterns are association rules as introduced by Rakesh et al. in [16]. Intuitively, an association rules identifies a frequently occurring pattern of information in a database. When mining association rules from a large non-transactional data, we may find hundreds or thousands of rules [15] corresponding to specific attribute values. In this paper, we have introduced a model, which does the unsupervised learning prior to finding association rules from the data set. It proves to be more accurate. If a Marketing person wants to find out who are the target customers for various products the exact rules as per the interest, location, status, he will now be able to find and target its products to the specific group of customers not on to the total mass. Our model is a customize model, where the rules are of dynamic nature. The problem, we consider is how to mine efficient rule dynamic on bank transactions and construction plans in Real estate.

Dr. Geetali Banerji*
Professor, Department of IT
IITM, Janakpuri, New Delhi
E-mail: hod.csdept@iitmjp.ac.in

Dr. Kanak Saxena**
Professor, Department of Computer Applications
Samrat Ashok Technological Institute, Vidisha (M.P.)
E-mail: kanak.saxena@gmail.com

In practice, it is very important that the rules mined from a database are understandable and useful to the user. Dynamic rules are helpful in reducing the large number of rules that typically computed by existing algorithm, therefore introducing rule dynamics is much easier to interpret and visualize. A practical used of these rules is to perform segmentation on large customer oriented database. As an example, the company could use rule dynamics on the attributes of customer. The company can then use these rules to identify their future customers who are likely to invest and deal with them in a personalize manner. This paper discusses about proposed model, unsupervised learning, Association rules and empirical results. The proposed model rules are compared with the traditional association rules using WEKA version 3-6-2, regression and data mining tool [3], [17].

II. Proposed Model

There is an underlying structure in most real estate data available to users or customers including locations, brokers, income, religions etc. A related phenomenon is the recurrence of certain semantically well-defined temporal events that often act as major or minor constraints come to life e.g., especially in Indian scenario, a customer who wants to invest but occurred a major health problem in the family, or if he or she belongs to a posh location or religion as current status. All these problems assume importance in the wake of an increasingly analysis environment.

Finding the semantic as well as structure in real estate is very difficult. The major problem that has been addressed is in the data available which doesn't give any information regarding the responsibilities on the shoulders of the interested customers with other constraints. In this paper we proposed a novel unsupervised approach to detect the recurring events and structure in the investors life. The main objective of proposed algorithm is its ability to account for short term as well as long-term continuity and its ability to detect the constraints pattern automatically without supervision. The algorithm attempts to perform association and temporal or structural clustering [12] - [13].

We now present a probabilistic architecture for discovering the constraints patterns in the data. The approach is to detect the patterns in the data that is in customer's life. Initially unsupervised clustering algorithms are applied and then further preprocessed by finding the association rule. Fig. 1 is the block analysis model to illustrate the complete process.

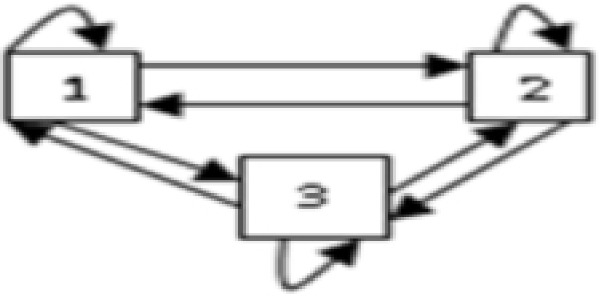


Fig. 1: Block Analysis Model

In Fig. 1, block 1 represents the customer's transaction, block 2 represents the corresponding bank transactions and block 3 represents the design specifications.

A byproduct is the use of transitions between blocks to denote current transactions situations of customers. Earlier the problem was that the cluster was able to model only short term statistics, but we are interested to enhanced the work in relatively long term statistics as well as which not only facilitate the customer but also helps the colonizers to keep track of the customers who are really interested. In long term and more importantly they can plan accordingly to generate the price, performance and facilities ratio in upward direction. Fig. 2 actually illustrates the transition graph of the blocks in the proposed architecture.

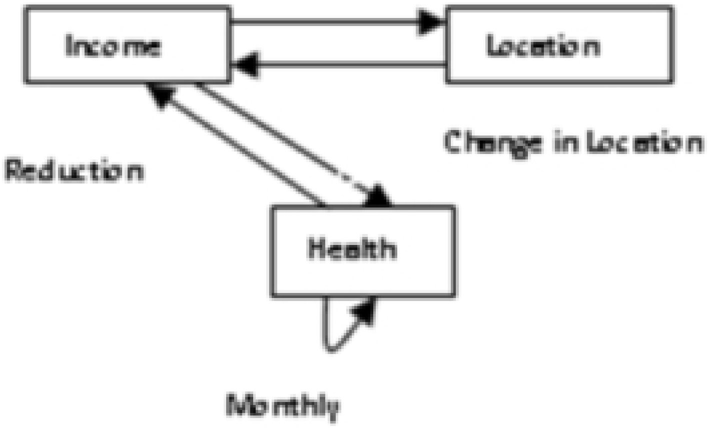


Fig. 2: Blocks Description

To make the connection between the models in Fig. 1 and 2 one could expand each block attribute with transition within blocks and between blocks.

The exact number of transition and number of block is a matter of current dependent experimental selection situation in the real estate. If it is believed that there are M possible events with sufficient data, it can be expected that these are learned automatically without the need for manual interactions. Fig. 3 depicts the traditional clustering block model. Fig. 4 is block representation of the proposed model. The model thus significantly improves the modeling of the long-term statistics. The proposed model preprocessed by Apriori and then trained by using K-means, DBSCAN and COBWEB techniques.

We believe that this gives the relationship among the various attribute within the state as well as between the states for long term statistics. The following experiments shows the result of constraints pattern rules applied on the three data sets (i) Real estate (ii) Bank Transaction and (iii) Design specifications

The empirical study suggests that proposed model performs significantly better than traditional clustering methods on the real estate domain for long term period to give the benefits to customers as well as brokers.

III. Concepts Used

A. Association Rules

Mining association rules is particularly useful for discovering relationships among items from large databases. In general, the association rule is an expression of the form X=>Y, where X is antecedent and Y is consequent. Association rule shows how many times Y has occurred if X has already occurred depending on the support and confidence value [1], [2],[5],[18].

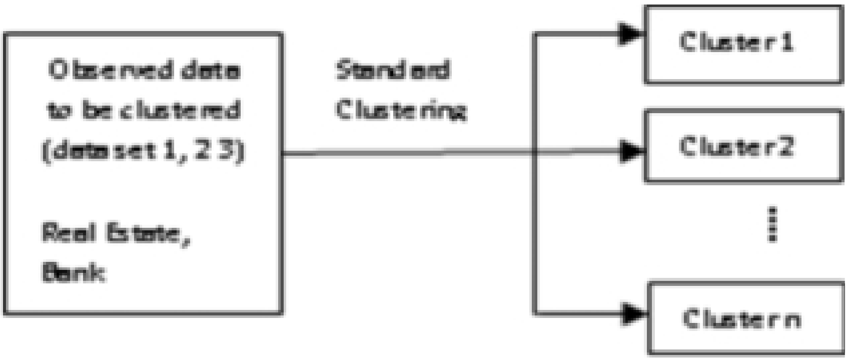
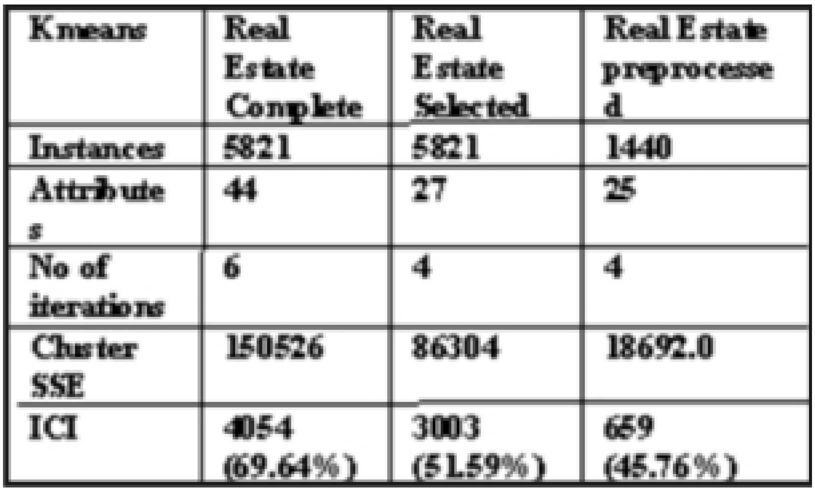


Fig. 3: Traditional Clustering block model.

Table I: Kmeans on Real Estate (Complete, Selected and Preprocessed data set)



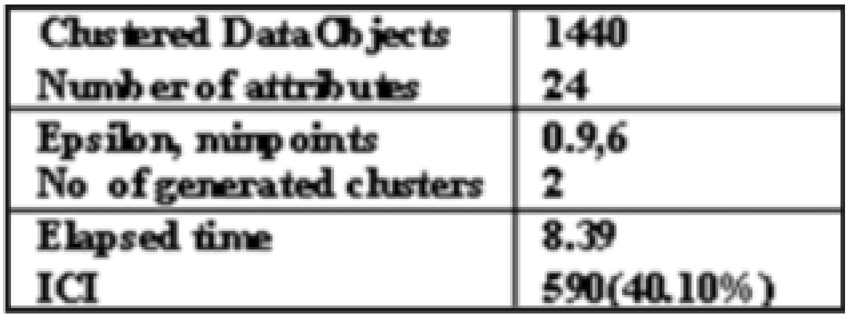
Kmeans	Real Estate Complete	Real Estate Selected	Real Estate preprocessed
Instances	5821	5821	1440
Attributes	44	27	25
No of iterations	6	4	4
Cluster SSE	150526	86304	18692.0
ICI	4054 (69.64%)	3003 (51.59%)	659 (45.76%)

B. Clustering

Clustering is a division of data into groups of similar objects. Representing the data by fewer clusters necessarily loses certain fine details, but achieves simplification. It models data by its clusters. There exists a variety of algorithms that meet these requirements and were successfully applied to real-life data mining problems.

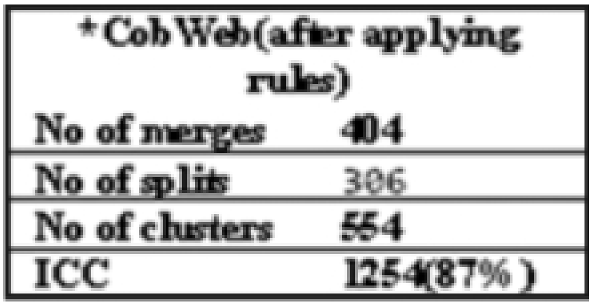
The two main types of clustering techniques are those that create a hierarchy of clusters and those that do not.

- Hierarchical: The hierarchical clustering techniques create a hierarchy of clusters from small to big. With a hierarchy of clusters defined it is possible to choose the number of clusters that are desired.
- Non-Hierarchical Clustering: The non-hierarchical techniques in general are faster to create from the historical database but require that the user make some decision about the number of clusters desired or the minimum "nearness" required two records to be within the same cluster. The non-hierarchical techniques most of the times are run multiple times starting off with some arbitrary or even random clustering and then iteratively improving the clustering by shuffling some records around.
- WEKA: WEKA is a data mining system developed by the University of Waikato in New Zealand that implements data mining algorithms. It is a state-of-the-art facility for developing machine learning (ML) techniques and their application to real-world data mining problems. It is a collection of machine learning algorithms for data mining tasks.



Clustered Data Objects	1440
Number of attributes	24
Epsilon, minpoints	0.9,6
No of generated clusters	2
Elapsed time	8.39
ICI	590(40.10%)

Table II: Dbscan on Real Estate (Preprocessed)



*CobWeb(after applying rules)	
No of merges	404
No of splits	306
No of clusters	554
ICC	1254(87%)

Table III: Cobweb on Real Estate (Preprocessed)

WEKA implements algorithms for data preprocessing, classification, regression, clustering, association rules; it also includes a visualization tools. WEKA is open source software issued under the GNU General Public License [3], [17].

IV. Empirical Results

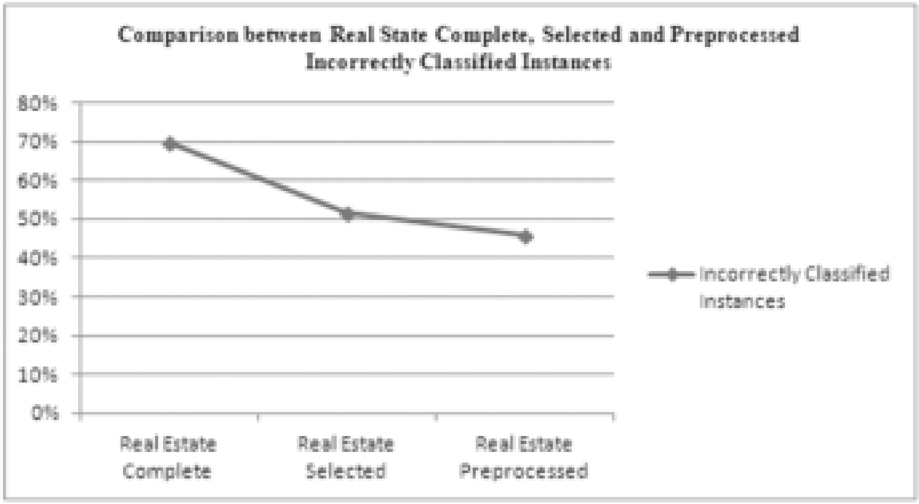
A. Modeling

Our data set contains customer's personal, educational, professional and social status (Fig. 6). It is not sufficient to identify the investing interest of a potential customer as published in paper [6], [7], [9], [10]. We have taken into consideration customer bank transactions and Design specifications which prove better results. Fig. 5, the proposed model, initially does the preprocessing by incorporating the customer bank details and property details to preprocess and remove the noise. Next it performs clustering by applying various algorithms and selects the best with lowest error rate. The last step is to generate association rule as per the specific cluster [8].

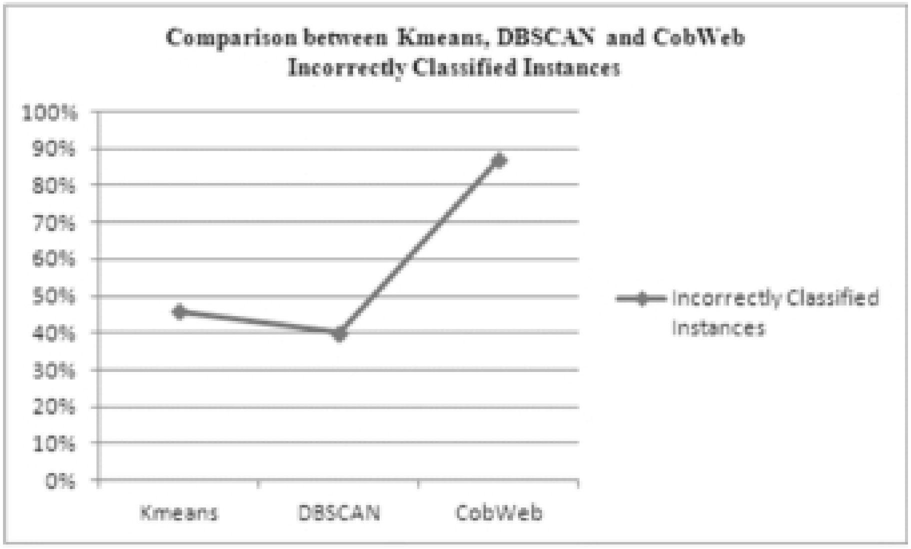
B. Testing

Testing is done on three clustering algorithms k-means, DBSCAN and CobWeb on test mode, classes to cluster evaluation on training data and association rules were generated using Apriori, using WEKA version 3-6-2.

- K-means: K-means clustering is a method, which aims to partition n observations into k clusters in which each observation belongs to the cluster with the nearest mean. This results in a partitioning of the data space into Voronoi cells. It use cluster centers to model the data, and tends to find clusters of comparable spatial extent [11].



Graph 1: Real Estate Incorrectly Classified Instances



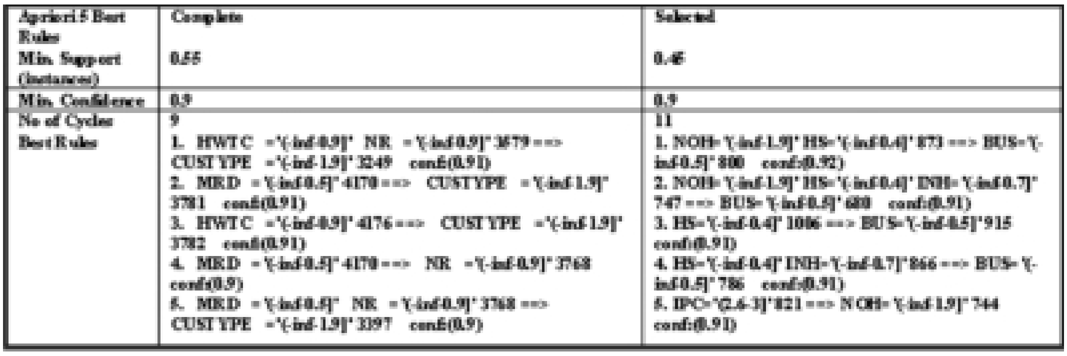
Graph 2: Clustering Incorrectly Classified Instances

- DBSCAN: DBSCAN stands for density-based spatial clustering of applications with noise. It finds a number of clusters starting from the estimated density distribution of corresponding nodes. DBSCAN is one of the most common clustering algorithms and most cited in scientific literature [14].
- CobWeb: CobWeb incrementally organizes observations into a classification tree. Each node in a classification tree represents a class (concept) and labeled by a probabilistic concept that summarizes the attribute-value distributions of objects classified under the node [4], [11].

C. Results

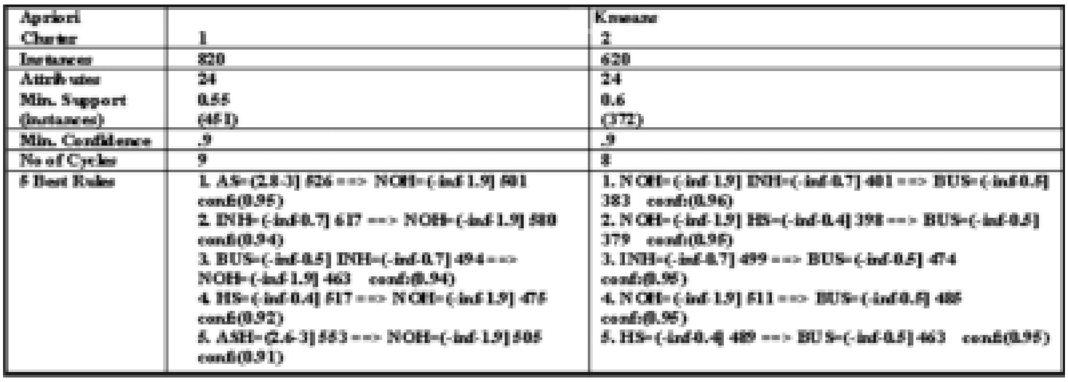
- Clustering based on the K-Means (Table 1): We have applied kmeans on real estate complete (1st column), real estate selected (after removing demographic details 2nd column), on real estate after preprocessing (3rd column) and found that as we clean the data the results are improving. Incorrectly classified Instructions (ICI) are reduced from 69.74% to 45.76% and Sum of Square Error (SSE) also reduced significantly. Hence it can be proved, that after preprocessing the results are improved tremendously.
- Clustering based on the DBSCAN (Table 2): Table 2 shows results of clustering on real estate (preprocessed). If we compare it with k-means results are better (40%). It means that DBSCAN is better than k-means.
- Clustering based on the CobWeb (Table 3): Table 3 shows results of clustering on real estate (preprocessed). If we compare it with k-means and DBSCAN, CobWeb results are not good. It signifies that CobWeb is not suitable for this domain.
- Association Rules induction from Real Estate (Complete, Selected), Kmeans, DBSCAN and CobWeb clusters (Table 4, 5, 6, 7): As per Table 4, the rules induced from real estate complete are somehow jumbled, it consider marital status, no. of children and customer type, which doesn't play any significant role in deciding the capacity of customer who can invest. In case of real estate selected, it take care of no. of houses, higher income (123.00 per Annum) and business which plays certain role in deciding the potential customer. In both the cases the rules are of static nature, it is not customize according to interest.
- In case of rules induced from clusters (Table 5, 6 & 7) using various clustering algorithm we found that each cluster is having a different set of rules as per

Table IV: Association Rules on Real Estate (Complete and Selected Data Sets)



Apriori 5 Best Rules	Complete	Selected
Min. Support (instances)	0.55	0.45
Min. Confidence	0.9	0.9
No of Cycles	9	11
Best Rules	1. HWTC ='(-inf-0.9]' NR ='(-inf-0.9]' 3679 ==> CUSTTYPE ='(-inf-1.9]' 3249 conf:(0.91) 2. MRD ='(-inf-0.5]' 4170 ==> CUSTTYPE ='(-inf-1.9]' 3781 conf:(0.91) 3. HWTC ='(-inf-0.9]' 4176 ==> CUSTTYPE ='(-inf-1.9]' 3782 conf:(0.91) 4. MRD ='(-inf-0.5]' 4170 ==> NR ='(-inf-0.9]' 3768 conf:(0.9) 5. MRD ='(-inf-0.5]' NR ='(-inf-0.9]' 3768 ==> CUSTTYPE ='(-inf-1.9]' 3397 conf:(0.9)	1. NOH='(-inf-1.9]' HS='(-inf-0.4]' 873 ==> BUS='(-inf-0.5]' 800 conf:(0.92) 2. NOH='(-inf-1.9]' HS='(-inf-0.4]' INH='(-inf-0.7]' 747 ==> BUS='(-inf-0.5]' 680 conf:(0.91) 3. HS='(-inf-0.4]' 1006 ==> BUS='(-inf-0.5]' 915 conf:(0.91) 4. HS='(-inf-0.4]' INH='(-inf-0.7]' 866 ==> BUS='(-inf-0.5]' 786 conf:(0.91) 5. IPC='(2.6-3]' 821 ==> NOH='(-inf-1.9]' 744 conf:(0.91)

Table V: Association Rules on K-Means Clusters



Apriori Cluster	 1	Kmeans 2
Instances	820	620
Attributes Min. Support (instances)	24 0.55 (451)	24 0.6 (372)
Min. Confidence	.9	.9
No of Cycles	9	8
5 Best Rules	1. AS=(2.8-3] 626 ==> NOH=(-inf-1.9] 601 conf:(0.96) 2. INH=(-inf-0.7] 617 ==> NOH=(-inf-1.9] 580 conf:(0.94) 3. BUS=(-inf-0.5] INH=(-inf-0.7] 494 ==> NOH=(-inf-1.9] 463 conf:(0.94) 4. HS=(-inf-0.4] 517 ==> NOH=(-inf-1.9] 475 conf:(0.92) 5. ASH=(2.6-3] 553 ==> NOH=(-inf-1.9] 505 conf:(0.91)	1. NOH=(-inf-1.9] INH=(-inf-0.7] 401 ==> BUS=(-inf-0.5] 383 conf:(0.96) 2. NOH=(-inf-1.9] HS=(-inf-0.4] 398 ==> BUS=(-inf-0.5] 379 conf:(0.95) 3. INH=(-inf-0.7] 499 ==> BUS=(-inf-0.5] 474 conf:(0.95) 4. NOH=(-inf-1.9] 511 ==> BUS=(-inf-0.5] 485 conf:(0.95) 5. HS=(-inf-0.4] 489 ==> BUS=(-inf-0.5] 463 conf:(0.95)

specific customer category i.e. of dynamic nature.

Graph 1 shows a comparison between incorrectly classified instances in Real estate complete, selected and preprocessed.

From Graph 1, we can establish that when we considers only real estate complete, Incorrectly classified instances is maximum, after removing the demographic details from the data set, it is reduced, after preprocessing and cleaning it got reduced drastically. It means that, customer type, social status, marital status etc. doesn't have any relation to identifying the behavior of a customer. But in context to Indian scenario these attributes play very significant roles.

Graph 2 shows a comparison between incorrectly classified instances in Kmeans, DBSCAN and COBWEB clustering algorithms.

From Graph 2, it is very much clear that DBSCAN is best among the rest in real estate domain with the minimum percentage of identifying incorrectly classifying instances.

V. Conclusions

This paper discusses about the preprocessing, association rules, clustering algorithm along with their merits and demerits. It also highlights the problem with association rule that is, it generates static rule set for the underlying domain, which is not a very accurate one and not gives a clear picture about the existing domain. To overcome this, we have suggested a model that deals with preprocessing and cleaning prior to clustering, followed by dynamic rule generation. The rule set inducted on various clusters using different clustering algorithm shows that they are of dynamic nature.

That is, if we keep on refining our data set by considering the various factors affecting them, we get more specific. Hence the proposed model proves to be better in terms of accuracy than traditional one. It also proves that the model, suits the real estate scenario which is of dynamic nature.

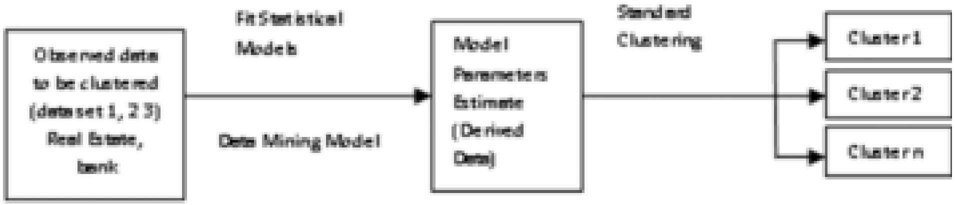

Observed data to be clustered (data set 1, 2 3) Real Estate, bank
Fit Statistical Models
Data Mining Model
Model Parameters Estimate (Derived Data)
Standard Clustering
Cluster 1
Cluster 2
Cluster n

Fig. 4: Block representation of proposed model

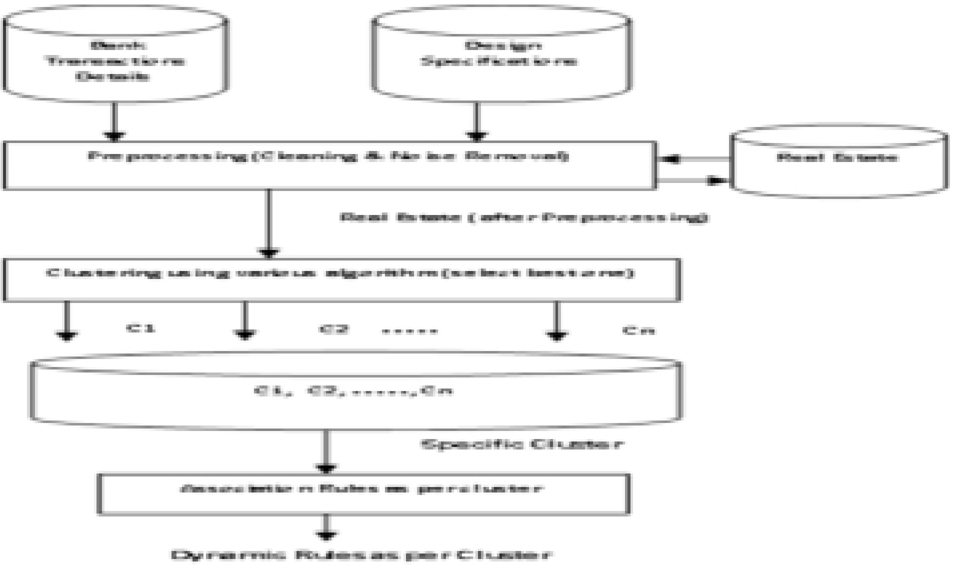
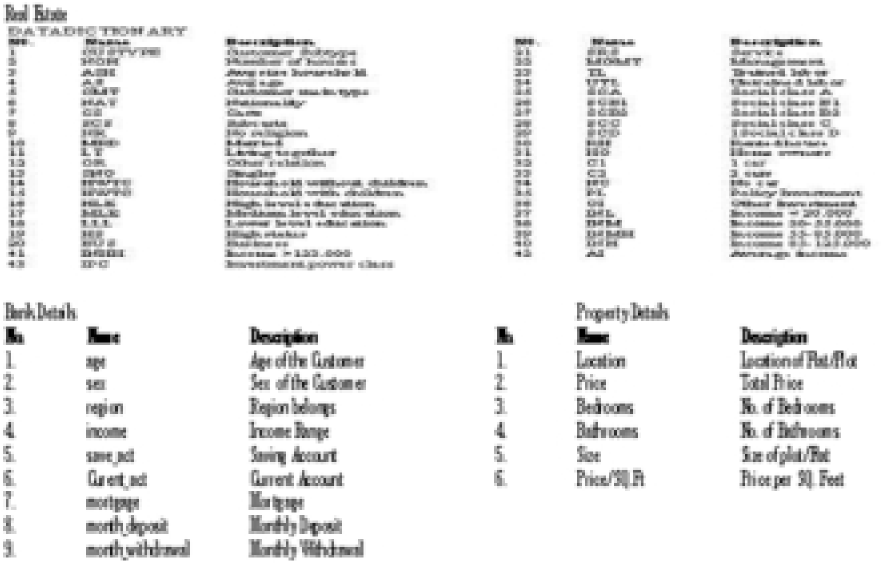

Bank Transactions Details
Design Specifications
Preprocessing (Cleaning & Noise Removal)
Real Estate
Real Estate (after Preprocessing)
Clustering using various algorithm (select best one)
C1
C2 .....
Cn
C1, C2,.....,Cn
Specific Cluster
Association Rules as per cluster
Dynamic Rules as per Cluster

Fig. 5: Proposed Model


Real Estate

DATADICTIONARY

Nr.	Name	Description
1	CUSTYPE	Customer Subtype
2	NOH	Number of houses
3	ASH	Avg size household
4	AA	Avg age
5	CMT	Customer main type
6	NAT	Nationality
7	[illegible]	[illegible]
8	[illegible]	[illegible]
9	NR	No religion
10	MRD	Married
11	LT	Living together
12	OR	Other relation
13	SNG	Singles
14	[illegible]	Household without children
15	[illegible]	Household with children
16	HLE	High level education
17	MLE	Medium level education
18	LLE	Lower level education
19	HS	High status
20	[illegible]	Business
41	[illegible]	Income >123,000
42	IPC	Investment power class

Nr.	Name	Description
21	SRV	Service
22	MGMT	Management
23	TL	Trained labor
24	UTL	Untrained labor
25	SCA	Social class A
26	SCB1	Social class B1
27	SCB2	Social class B2
28	SCC	Social class C
29	SCD	(Social) class D
30	RH	Rented house
31	HO	Home owners
32	C1	1 car
33	C2	2 cars
34	NC	No car
35	PI	Policy Investment
36	OI	Other Investment
37	[illegible]	Income < 20,000
38	[illegible]	Income 20-35,000
39	[illegible]	Income 35-65,000
40	[illegible]	Income 65-123,000
43	AI	Average Income

Bank Details

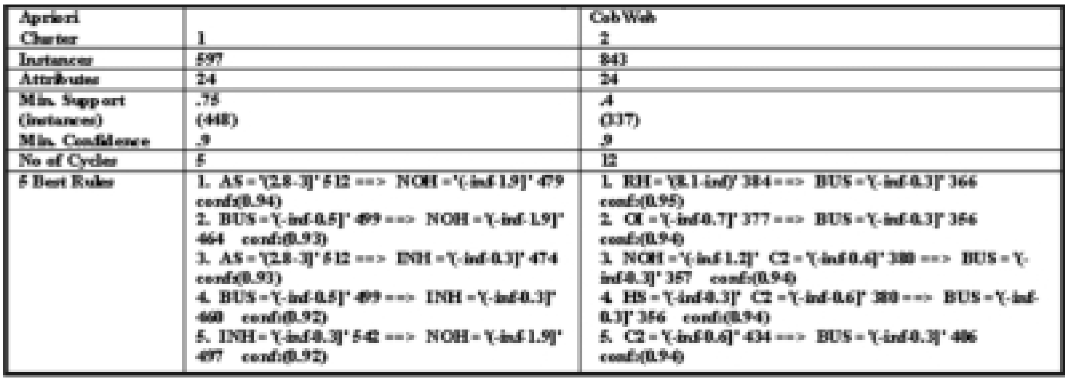
No.	Name	Description
1.	age	Age of the Customer
2.	sex	Sex of the Customer
3.	region	Region belongs
4.	income	Income Range
5.	save_act	Saving Account
6.	Current_act	Current Account
7.	mortgage	Mortgage
8.	month_deposit	Monthly Deposit
9.	month_withdrawal	Monthly Withdrawal

Property Details

No.	Name	Description
1.	Location	Location of Plot/Flat
2.	Price	Total Price
3.	Bedrooms	No. of Bedrooms
4.	Bathrooms	No. of Bathrooms
5.	Size	Size of plot/Flat
6.	Price/SQ.Ft	Price per SQ. Feet

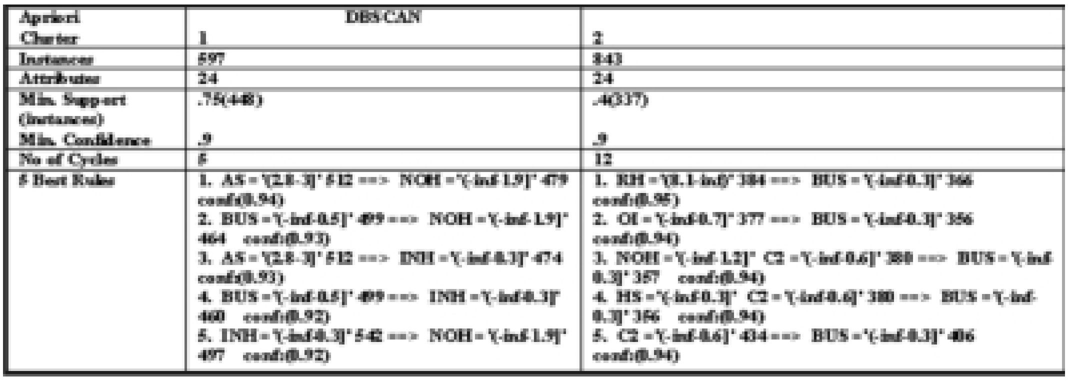
Fig. 6: Data Sets

Table VI: Association Rules on Cob Web Clusters



Apriori		Cob Web
Cluster	1	2
Instances	597	843
Attributes	24	24
Min. Support (instances)	.75 (448)	.4 (337)
Min. Confidence	.9	.9
No of Cycles	5	12
5 Best Rules	1. AS = '(2.8-3]' 512 ==> NOH = '(-inf-1.9]' 479 conf:(0.94) 2. BUS = '(-inf-0.5]' 499 ==> NOH = '(-inf-1.9]' 464 conf:(0.93) 3. AS = '(2.8-3]' 512 ==> INH = '(-inf-0.3]' 474 conf:(0.93) 4. BUS = '(-inf-0.5]' 499 ==> INH = '(-inf-0.3]' 460 conf:(0.92) 5. INH = '(-inf-0.3]' 542 ==> NOH = '(-inf-1.9]' 497 conf:(0.92)	1. RH = '(8.1-inf)' 384 ==> BUS = '(-inf-0.3]' 366 conf:(0.95) 2. OI = '(-inf-0.7]' 377 ==> BUS = '(-inf-0.3]' 356 conf:(0.94) 3. NOH = '(-inf-1.2]' C2 = '(-inf-0.6]' 380 ==> BUS = '(-inf-0.3]' 357 conf:(0.94) 4. HS = '(-inf-0.3]' C2 = '(-inf-0.6]' 380 ==> BUS = '(-inf-0.3]' 356 conf:(0.94) 5. C2 = '(-inf-0.6]' 434 ==> BUS = '(-inf-0.3]' 406 conf:(0.94)

Table VII: Association Rules on Dbscan Clusters



Apriori	DBSCAN	
Cluster	1	2
Instances	597	843
Attributes	24	24
Min. Support (instances)	.75(448)	.4(337)
Min. Confidence	.9	.9
No of Cycles	5	12
5 Best Rules	1. AS = '(2.8-3]' 512 ==> NOH = '(-inf-1.9]' 479 conf:(0.94) 2. BUS = '(-inf-0.5]' 499 ==> NOH = '(-inf-1.9]' 464 conf:(0.93) 3. AS = '(2.8-3]' 512 ==> INH = '(-inf-0.3]' 474 conf:(0.93) 4. BUS = '(-inf-0.5]' 499 ==> INH = '(-inf-0.3]' 460 conf:(0.92) 5. INH = '(-inf-0.3]' 542 ==> NOH = '(-inf-1.9]' 497 conf:(0.92)	1. RH = '(8.1-inf)' 384 ==> BUS = '(-inf-0.3]' 366 conf:(0.95) 2. OI = '(-inf-0.7]' 377 ==> BUS = '(-inf-0.3]' 356 conf:(0.94) 3. NOH = '(-inf-1.2]' C2 = '(-inf-0.6]' 380 ==> BUS = '(-inf-0.3]' 357 conf:(0.94) 4. HS = '(-inf-0.3]' C2 = '(-inf-0.6]' 380 ==> BUS = '(-inf-0.3]' 356 conf:(0.94) 5. C2 = '(-inf-0.6]' 434 ==> BUS = '(-inf-0.3]' 406 conf:(0.94)

References

1. Alaa AI Deen Mustafa Nofal and Sulieman Bani-Ahmad, Classification Based on association Rule Mining Techniques: A general survey and Empirical Comparative Evaluation.
2. B. Tunc and H. Dag, "Generating Association Rules with Modified Apriori Algorithm", in Proc.of the 5th WSEAS Int. Conf. on Artificial Intelligence, Knowledge Engineering and Data Bases, Madrid, Spain, February 15-17, 2006
3. WEKA Manual for Version 3-6-2, January 11, 2010
4. Breiman L., Friedman J.H., Olshen R.A., Stone C.J. Classification and Regression Trees, Wadsforth International Group, 1984.
5. Geetali Banerji, Kanak Saxena, "An Improved Apriori Based Algorithm with Single Scan of Database", in Proc. National Conferenceon Converging Technologies Beyond 2020, UIET, Kurukshetra University, India, April 2011
6. Geetali Banerji, Kanak Saxena, ""Predictive Test model- A Boon for Real Estate" , International Journal for Wisdom Based Computing Volume(1) 2, pp. April 2012
7. Geetali Banerji and Kanak Saxena, "An Algorithm for Rule based Classification", in Proc. National Conference on Emerging Trends in Information Technology 2012,p.

8. Geetali Banerji, Kanak Saxena,, “Analysis of Data Mining techniques on Real Estate”, International Journal of Soft Computing and Engineering (IJSCE) ISSN:2231-2307 Volume-2, Issue-3,pp. July 2012

9. Geetali Banerji, Kanak Saxena, “A comparative analysis of Bayesian methods for Real Estate domain, International Journal of Management, IT and Engineering”, ISSN 2249-0558 pp

10. Jiawei Han, Usama M. Fayyad. Proceedings of the Second International Conference on Knowledge Discovery and Data Mining (KDD-96). AAAI Press. pp. 226–231.ISBN1-57735-004-9.

11. Han J. and Kamber M., Data Mining: Concepts and Techniques, 6th ed., San Francisco, Morgan Kauffmann Publishers, 2009

12. Hillol Kargupta, Anupam Joshi et. al., Data Mining Next Generation Challenges and Future Directions, PHI Learning Private Limited

13. Mahesh Kumar and Nitin R. Patel, Clustering Data with Measurement Errors, Statistical Methods in E-Commerce, a John Wiley and Sons Publication, pp 245

14. Martin Ester, Hans-Peter Kriegel, Jörg Sander, Xiaowei Xu., A density-based algorithm for discovering clusters in large spatial databases with noise. In Evangelos Simoudis, 1996.

15. M. Klemettinen, H. Mannila, P. Ronkainen, and H. Toivonen, “Finding interesting rules from large sets of discovered association rules”, 3rd international Conference on Information and Knowledge Management (CIKM), Nov. 1994.

16. R. Agrawal, T. Imielinski, and A. Swami, “Mining association rules between sets of items in large Databases”, in proc. of the 1993 ACM SIGMOD International Conference on Management of Data, Washington, D.C., 1993

17. Witten I. frank, E., *Data Mining: practical machine learning tools and techniques with Java implementations*, Morgan Kaufmann, San Francisco, 2000

17. Yu-Chiang Li, Jieh-Shan Yeh, Chin-Chen Chang, “Efficient Algorithms for Mining Shared-Frequent Itemsets”, in Proc. of the 11th World Congress of Intl. Fuzzy Systems Association, 2005.

Cyber Terrorism – A Framework of Destruction

Vaibhuv Sharma*
Vansh Sharma**
Ankit Verma***

Abstract

It is more than clear that the method for leading terrorism with the time is getting to be more refined. The Cyber terrorism is real threat to fast technology development. Cyber Terrorism can destroy a nation's infrastructure just by taking control over virtual frameworks. As we are bounded to technologies, new methods of Cyber attacks are being developed over time. It is necessary to understand the Cyber attacks in order to control the terrorism by knowing its background details.

Key Words: Cyber Terrorism, Cyber Security, Cross Site Scripting, SQL Injection, Cyber Attacks.

I. Introduction

There are numerous definitions that define Cyber Terrorism, but in simple words "It's a way of attacking a nation's infrastructure without the utilization of weapons." The infrastructure of the modern world has started relying heavily on computer networks without giving a single though on its security. A nation, for example, the United States, whose national security is so intensely dependent on machine systems, could find itself crippled if an attack against the military or budgetary division of the nation was dispatched, the risk of cyber terrorism is genuine and greatly hazardous. Thus, this gives a new chance to attackers in order to exploit a country virtually. Hackers that inspire terrorists have exhibited that people can get access to delicate data by using critical attacks on a network. Only government sector is not vulnerable to cyber attacks, now cyber terrorists are also targeting well known celebrities in order to gain attention. It also means that technology needs to be upgraded time to time. Though, government is working on new technologies in order to safeguard private networks such as financial sectors etc. We cannot predict the future of cyberspace but we can try to implement more secured security layers in order to protect the data virtually. Cyber Terrorism can come in various forms, including but not limited to Viruses, Emails, Pop-ups, unknown executable files etc. Cyber Terrorism is a wide concept and it has various impacts. Either it can be used for personal gains, cyber wars, information breach or to check security flaws in a network. Still cyber criminals are using it to provide mass destruction to one's nation.

II. Cyber Terrorism

Nowadays, Cyber-war seems to be the new trend of showing or finding the weakness of countries. Nations are indulged in Cyber-war by using cyberspace as a medium, by this terrorist organization are being motivated and thus leads to Cyber Terrorism. Terrorism doesn't mean weapons; infect Cyber Terrorism is much more devastating than Physical wars. As confidential data is being leaked and misused for personal gains. Today, terrorist doesn't need Media in order to reach Mass audience; they are simply using Cyberspace as medium to gain attention. As there is

Vaibhuv Sharma*
Student of BCA
IITM, Janakpuri, New Delhi
vaibhuvsharma@gmail.com

Vansh Sharma**
Student of BCA
IITM, Janakpuri, New Delhi
vanshsharma95@gmail.com

Ankit Verma***
Assistant Professor
IITM, Janakpuri, New Delhi
ankit.verma.aquarius@gmail.com

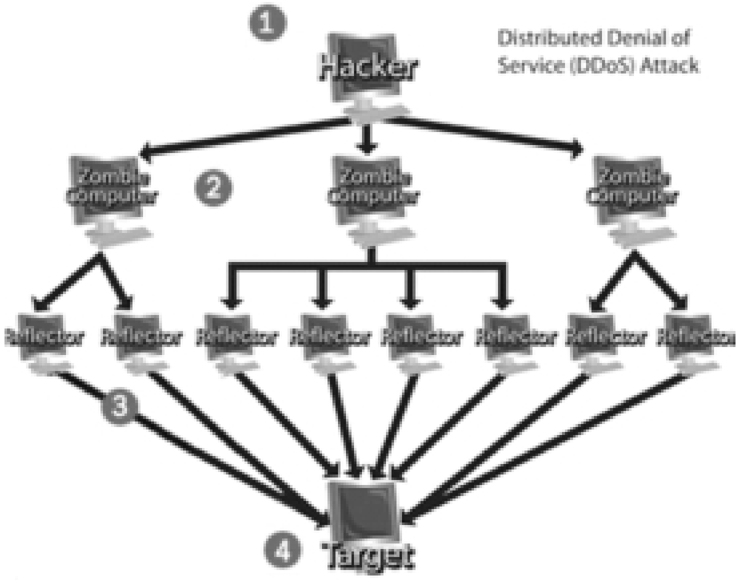


Figure 1: Working of DDOS Attack

no limit, today cyber terrorists are lurking behind Social Media websites in order to attack innocent internet users, and use their personal information online without any permission. To control that, government had created a sector in the field of Information Technology, widely known as 'Cyber Cells'. These cells are working hard to stop Cyber Criminals by tracking them worldwide.

A. Techniques of Cyber Attacks

Cyber terrorists are so smart that they use different methods while attacking. So, even if one method gets patched then they are ready with their next method to continue the destruction.

1. Cross Site Scripting

Cross Site Scripting is also known as 'XSS'. It's a great way of destroying a website completely. Here, an attacker injects malicious scripts on a website and tests the vulnerability. If the vulnerability exists then he keeps on exploiting it. This vulnerability is of two types:

- ***Persistent***

When the script is injected by the attacker on a website and it gets mixed with the website's source code, then the vulnerability is known to be persistent. Then the changes made on the website by the attacker will be visible to anyone who visits it. Therefore, it's more devastating as the attacker can also redirect the website to any third party website with the help of scripts. Or he can simply deface the website to leave a message of his presence.

- ***Non-Persistent***

The scripts executed by an attacker are visible to him only, then the vulnerability known to be Non-Persistent. It will be less exploitable yet destructive. As the attacker can grab cookies of those users who visit the website and can use those cookies against them?

2. Structured Query Language Injection

Structured Query Language Injection is also as 'SQLi' and it's a great of exploiting a website's database. Today, a website is nothing without a database as it contains a lot of data that can be used time to time as per the needs. This attack focuses on Database, where an attacker inserts malicious SQL statements into an entry field by exploiting the security layers of a website. This type of attack can be done while combining different vulnerabilities together, such as SQLi + XSS. i.e.., By using SQL commands and malicious scripts.

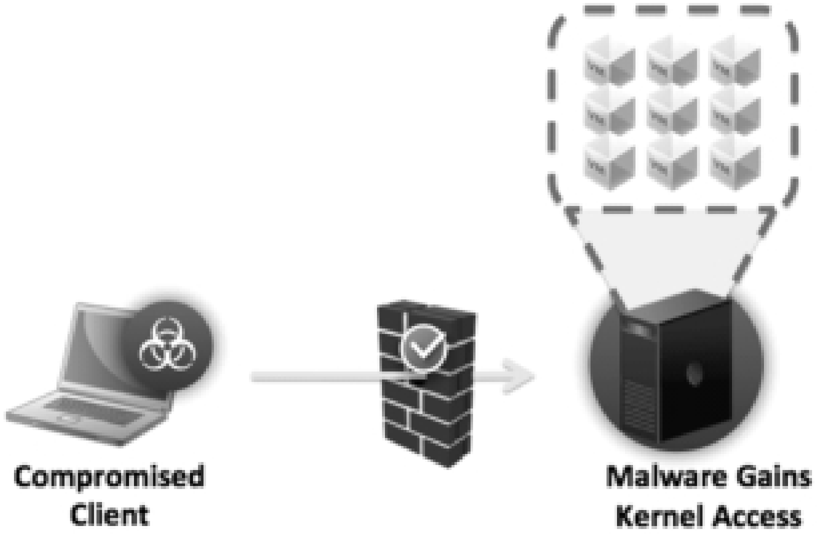


Figure 2: Working of RAT

3. Distributed Denial of Service Attack

Distributed Denial of Service (DDOS) Attack is used to make an online service unavailable for a limited time, it is done when multiple infected system networks also known as 'Botnets' send multiple packets to a single system network, while network attempts to catch each package in order to grab the signal but it fails and shutdowns the network completely. This attack can be used to shutdown Home Connections, LAN, and Servers etc. And to shutdown each network, different layers and protocols are being used such as SSYN, UDP/IP are examples of protocols.

4. Remote Administration Tools (RAT)

Remote Administration Tools popularly known as RAT is a remote software that is being used by cyber criminals to grab personal and confidential information of an individual. This tool is widely available on the internet and can be installed on a victims system by attaching it with fake files with different extensions like PDF, DOC etc. RAT is so powerful that it can take over all control of a system and can misuse it. This tool provides an attacker with the following capabilities:

- Record Screen
- Download or execute anything
- Shell control through Command Prompt
- Access to computer registry
- Hardware over-clock
- Show fake system errors
- Kill task manager

A well designed RAT will allow the attacker to destroy the system physically as well.

Once the victim downloads or receives the infected file i.e., RAT, his system gets compromised by attacker. As the malware gains the Kernel Access and can break through firewalls easily. If victim is connected to the Internet, that means his system can be used by attacker and the attacker can download or execute anything on victims system, as attacker gets the personal access.

RAT is one of the most dangerous tools that can be used by cyber criminals against an individual.

B. Current Scenario

Recently the most famous and the wealthiest terrorist group ISIS (Islamic State of Iraq and Syria) is working to seek a cyber attack against western countries while mainly targeting the dams, electric grids, airports, hospitals, banks etc. As many militants of ISIS group are high profile hackers, especially one who hacked into the Gmail account of Former British Prime Minister. So chances are high that they will soon launch a cyber attack in order to damage the western infrastructure.

Also, ISIS have clear targets in mind, the group has publicly announced their plans on the internet that they will make proper use of Encryption software's and some custom made tools that will destroy the USA's Financial and Infrastructure System. The situation is getting very critical as ISIS is getting popular day by day and they are trying to expand their force into Cyberspace by targeting big gaming companies like Sony and Microsoft.

C. Current Cyber Laws

The current cyber laws emphasis on Internet. Many Cyber laws are implemented in order to protect the crucial information and help in Human Rights Issues.

In India "Information Technology Act, 2000" is a act which applies to whole India and it comes in action when crimes like Hacking, Data Theft, Spreading of virus, Identity theft etc are violated. It is implemented by various rules such as Data Security, Blocking of websites and also observing ISP's.

Conclusion

The paper gives a brief overview of the term "Cyber Terrorism" and shows the various forms of attacks used by the cyber criminals in order to prevent the damage to a nation's infrastructure. The government must implement strong cyber laws in a country in order to avoid the cyber warfare and cyber threats. Such laws will prevent cyber criminals from targeting internet users and government agencies. This will result in less cyber-crime. Implementation of network security devices will also help in tracking the cyber criminals, while protecting the data. As cyber criminals use Internet as a medium to spread their terror on Individual and government sectors.

If the above strategies are implemented correctly, then there will less cyber crimes and people will feel safe while accessing the internet from anywhere in the world.

As crimes are getting more advanced then security layers must be upgraded time to time for the survival of cyberspace. Cyber Terrorism may pose the greatest threat to a nation's security infrastructure, although, cyber-crimes can be reduced.

References

1. Matusitz,Jonathan(April2005). "Cyberterrorism:" American Foreign Policy Interests 2: 137–147.
2. DOD – Cyberspace. Dtic.mil. Retrieved 8 November 2011.
3. Russia Today, 26 January 2012, "US Launched Cyber Attacks on Other Nations,"
4. Grossman, Jeremiah (July 30, 2006). "The origins of Cross-Site Scripting (XSS)". Retrieved September 15, 2008.
5. Sean Michael Kerner (November 25, 2013). "How Was SQL Injection Discovered? The researcher once known as Rain Forrest Puppy explains how he discovered the first SQL injection more than 15 years ago.
6. Kevin J. Houle, CERT/CC; George M. Weaver, CERT/CC, in collaboration with: Neil Long, Rob Thomas, "Trends in Denial of Service Attack Technology," V1.0, October 2001.
7. Clarke:More defense needed in cyberspace" Hometown Annapolis.com, 24 September 2010
8. Remote Server Administration Tools for Windows 7". Microsoft Technet June 4, 2009. Retrieved 4 February 2011.
9. Kelley, Michael B. (20 August 2014). "One Big Question Surrounds The Murder Of US Journalist James Foley By ISIS". Business Insider. Retrieved 20 August 2014. ... the de facto ISIS capital of Raqqa, Syria .
10. "You Can't Understand ISIS If You Don't Know the History of Wahhabism in Saudi Arabia". August 2014. Retrieved February 2015.
11. Hassan, Hassan. "The secret world of Isis training camps – ruled by sacred texts and the sword". Sunday 25 January
12. Emerging Technologies and the Law: Forms and Analysis, by Richard Raysman, Peter Brown, Jeffrey D. Neuburger and William E. Bandon, III. Law Journal Press, 2002-2008.ISBN 1-58852-107-9
13. "Law and Borders - The Rise of Law in Cyberspace". Cli.org. Retrieved 2013-11-05.

Role of Information Assurance Practices in Cloud Computing-Cloud Assurance

Kavita Mittal*

Abstract

Information assurance and business organizations realize well that technology disasters come in all shapes and sizes. While infinite solutions exist to help with disaster recovery, business continuity, and an ever-growing number of intruder/malware prevention practices, it's apparent that in-house IT professionals are overwhelmed by the sheer volume of choices and complexity of integration. Cloud computing is in demand today, but has this approach simplified information assurance. Are cloud solutions too new to trust, or are the concepts and methods mature enough to match or even enhance information assurance planning and practice? An emerging technology with a number of different applications, the global move to cloud computing stands to significantly affect the way we access and share data across multiple devices. The movement to online storage carries inherent risks. On-demand access to files that are stored on distant servers requires file transmission over the Internet, without the protection of an individual or enterprise firewall system. Cloud-based applications, where complete programs are stored on servers and streamed to individual computers as needed, present additional challenges. While there are significant advantages to a cloud-based application in facilitating access for all users to a single, updated software version, the question arises as to the consequences if security of this server-based program is compromised. With the inherent security risks of online storage systems, organizations face an apparent need to hire dedicated teams of information security professionals. Information assurance at the cloud level, however, has the added benefit of encouraging security management by the providers of cloud services. As cloud computing continues to develop, so too will the sophistication of hacking attempts. This paper attempts to highlight the importance of assurance for any organization's data security system.

Key Words: Cloud Technology, Models in cloud computing, Cloud Information Assurance.

I. Introduction

Computer storage has seen major amendments in recent years with the development of cloud-based storage technology. Where collaboration across multiple devices previously required manual uploading and tracking of new file versions, server-side storage allows multiple users to access their files from nearly any device connected to the Internet. No longer limited by what is or is not stored on an individual computer, cloud computing keeps users in sync with each other and up-to-date in terms of both individual files and cloud-based applications.

In cloud computing a safe and secure data storage environment can be obtained despite the increased level of risk. Cloud computing services are well developed and equipped to address concerns as they arise, and in some cases services can handle security issues more effectively than the organizations whose data they host. Providers of cloud-based applications are also well positioned to handle the inherent risks of compromised software. Prior to the advent of cloud computing, organizations were required to patch each instance of their applications as flaws became apparent. A cloud-based storage solution allows organizations

Kavita Mittal*
Assistant Professor, Department of IT
IITM, Janakpuri, New Delhi
kavitamittal.it@gmail.com

to delegate responsibility for upgrades to a team of focused professionals, all but eliminating the need for organizations to keep track of software versions. It may be the case that hosting an application or desktop environment "in the cloud" constitutes a risk in itself, but if an information assurance team can respond more quickly and effectively at the server level than cloud hosted organizations, then a net benefit may be seen in cloud software usage. In these cases is a shift in responsibility for information assurance from organizations to cloud computing providers may be seen. There certainly are inherent security risks to an increasingly online storage system, but in many cases the providers of these systems are in a position to address any concerns. With this shift in responsibility in mind, it becomes crucial for businesses to research their providers with care. Cloud computing providers must have sufficient information assurance policies and personnel in place to handle the risks of online data storage, including well documented and implemented best practices and "disaster response" plans.

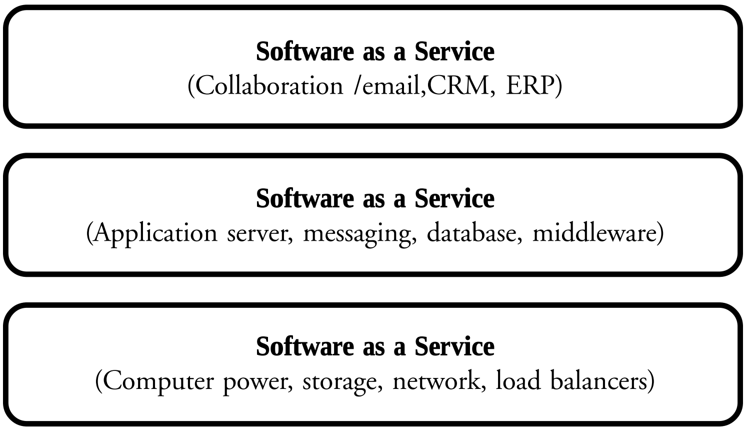
II. Cloud Technology

Cloud computing is an emerging trend which has progressed to the point of serious adoption in both public and private sector organizations, yet it remains a relatively immature paradigm, one which dictates a revision to the traditional characterization of risk in information technology environments. As a means of an introduction to those changes, this paper offers an overview of the information assurance aspects of cloud computing with a focus on potential security advantages and pitfalls. The intended audience is anyone who is considering the adoption of cloud computing and who needs to understand the security risks and potential opportunities cloud computing provides as part of a risk management process. Cloud computing is an evolving concept and various definitions have been offered, some with widely varying scope. Cloud computing can be described as a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the network.

Examples of cloud computing delivery models vary from *infrastructure as a service* (IaaS) where one can lease capabilities such as storage or computing resources (e.g., Amazon Simple Storage Service and Elastic Compute Cloud), *platform as a service* (PaaS) where one can lease an application development environment (e.g., The Microsoft Azure Services Platform) and *software as a service* (SaaS) which offers network based applications (e.g., Facebook, Google docs). The figure below illustrates how these various classes of cloud computing offerings build upon one another and offers additional examples from the commercial space.

A. Service Models in Cloud Computing

Service delivery in Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The three service models



Software as a Service
(Collaboration /email,CRM, ERP)

Software as a Service
(Application server, messaging, database, middleware)

Software as a Service
(Computer power, storage, network, load balancers)

Figure 1: Cloud Service Delivery Models

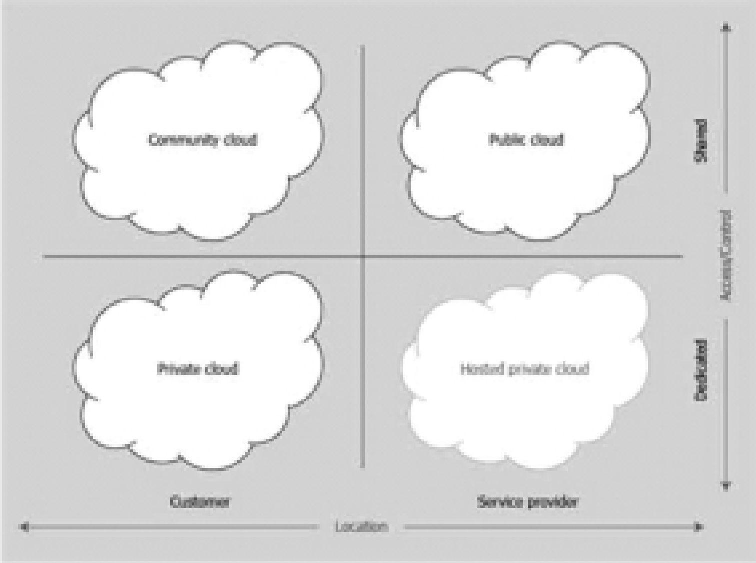


Figure 2: Cloud computing deployment models

or layer are completed by an end user layer that encapsulates the end user perspective on cloud services. The model is shown in figure 1.

- **Software as a Service**: Builds upon PaaS to offer complete applications customize by the user to a limited degree and utilizing a security model developed by provider.
- **Platform as a Service**: Builds upon IaaS to offer development environments which are leveraged by the user to build custom applications.
- **Infrastructure as a Service**: Includes the foundational elements such as storage, operating system instances, networking, and identify management upon which development platforms and applications can be layered.

III. Deployment Models

Deployment models (shared or dedicated, and whether internally hosted or externally hosted) are defined by the ownership and control of architectural design and the degree of available customization. (Loeffler, Bill, 2011)

- **Private cloud** — The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise
- **Community cloud** —The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise
- **Public cloud** —The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services
- **Hybrid cloud—** The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)

Two dimensions are used to classify the various deployment models (see **Figure 2**) for cloud computing:

- *Where the service is running*: On customer premises or in a service provider's data center
- *Level of access*: Shared or dedicated

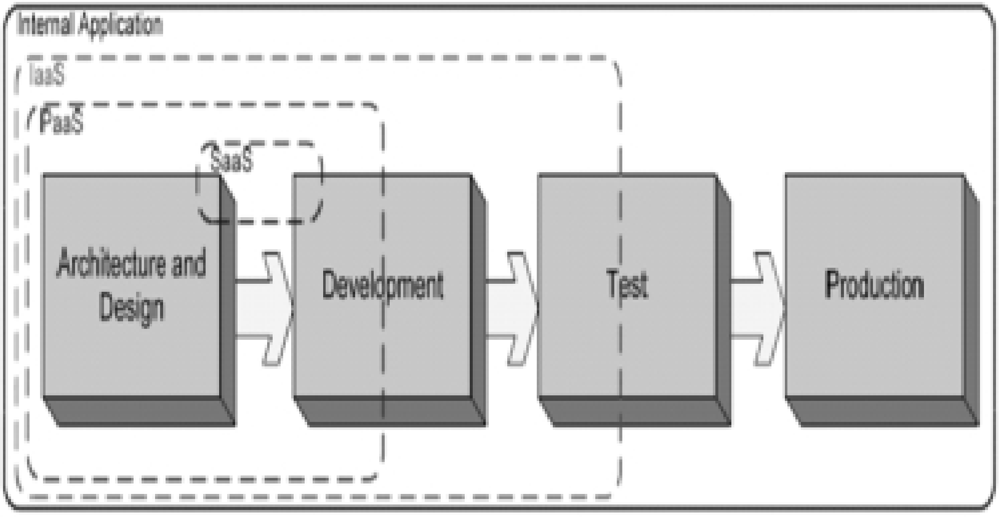


Figure 3: Public Cloud Trust Boundaries

IV. IA Concerns

When considering the risk associated with cloud computing, the most fundamental element that must be considered is how the cloud environment affects the trust boundary. In thinking about this question, first consider a traditional computing model, one where applications reside on client machines or somewhere else on the infrastructure owned and controlled by the enterprise. In this environment it is possible to levy a host of countermeasures to mitigate the security risks that exist in the information technology world. Those countermeasures can include firewalls, data encryption, antivirus solutions, tight access permissions, separation of networks either virtually or physically, and more. Coupled with those technical countermeasures are the use of trusted administrators, trusted application developers, and internal processes which should reflect the value of the network and the data which resides on it. Now consider what happens when the application is moved to a cloud infrastructure provided by an outside provider, one whose business model is typically driven by the provision of a common service to a wide variety of customers.

The trust boundary will vary depending on the type of cloud service in question as shown in Figure 3, a presentation adopted from one offered by the Cloud Security Alliance (2009). This illustrates the software development process and notes that for traditional applications which are developed and deployed in-house, the architecture and design, development, testing, and deployment can be accomplished with trusted individuals using tools and processes integral to the enterprise. Certainly risks remain, even outside of the application development process, but the high degree of control and ownership allows a layering of process and technical countermeasures. At the other end of the spectrum, SaaS allows the user very limited control over the application, with customizations typically limited to a narrow set.

Due to this issue of the movement of the trust boundary, public clouds (whereby cloud resources are dynamically provisioned over the Internet) represent the greatest challenge from a security perspective. While the specific concerns will vary somewhat depending upon the type of cloud service (IaaS, PaaS, or SaaS), the key aspects to consider when looking defining assurance in Cloud sourcing is (Gerry O'Neill, 2013):

- ***Privileged user access***

As stated earlier, the movement of any sensitive data outside the organization carries with it an inherent level of risk, because outsourced services can bypass the traditional security control frameworks that internal IT and security departments may insist on.

As your data is now going to be in someone else's hands, it is imperative that you ask questions about who will be managing your data. You should, therefore, request potential providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access.

- ***Regulatory compliance***

*Customer*organizations are ultimately responsible for the security and integrity of their own data, even when it is processed or stored by an external service provider. Traditional service providers are subjected to external audits and security certifications. Cloud computing providers now increasingly recognize the value of trust and assurance, but processes are still developing, Any Content Security Policy (CSPs) who refuse to undergo independent assurance are 'signaling that customers can only use them for the most trivial functions', according to Gartner.

- ***Data location***

It is imperative, if organisations aim to meet customer, business or regulatory requirements that they know exactly where their data is to be hosted in the Cloud. In such circumstances, they must ask CSPs if they will commit to storing and processing data in specific jurisdictions, and whether they will give contractual commitments to complying with local privacy regulations on behalf of their customers

- ***Data segregation***

Data held in the Cloud is typically in a shared (multi-tenancy) environment alongside data from other clients, and so there must be effective access separation and confidentiality protection. Encryption can be an effective response but isn't a panacea. It is important that you find out what is done to segregate data 'at rest'. The CSP (Content Security Policy) should be asked to provide evidence that their access control mechanisms and their encryption solutions were designed by experienced specialists and also tested by independent experts.

- ***Recovery***

The ability to recover your data and systems in the event of a serious outage is these days regarded as a fundamental control. The organization should require the CSP to outline what will happen to the data and service in the event of a disaster. Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure, so you should ask the potential provider if they have the ability to undertake a complete restoration and how long it is likely to take.

- ***Investigative support***

Security incidents are on the increase and are becoming more complex. The ability to investigate inappropriate or illegal activity is taken as core ability in-house, but this may be difficult to achieve in a Cloud solution. Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If you cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then you're only safe assumption is that investigation and discovery requests will be impossible.

- ***Long-term viability***

There are many new entrants to the Cloud services market. Hopefully, the chosen CSP will never go out of business, but customer organizations must ensure that their data will remain available even after such an event. You should, therefore, ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application. Of course, there are also the additional costs and disruption that would ensue in having to set up business all over again with any new supplier – just something else to be taken into account.

B. Countermeasures

So, how does one counter the uncertainty and risk of using public cloud resources? (NSA, Report, 2009).There is a range of options:

- **Limit Use***:* Don't use the public cloud for sensitive data. For example, one might limit the data placed on a social networking site to data that one truly intends to be publicly available and not rely on any privacy or data confidentiality features the provider might offer. User training is a key element here.

- **Encryption**: Encrypt data before uploading it to the cloud. This could be a good solution for folks who are looking at the cloud as a means of data storage.
- **Characterize the Vendor**: Attempt to gain confidence in the provider and obtain answers to the security concerns posed by this document and others that may be unique to a situation. The question of enforcement of the expectations one obtains through such insight is paramount and, while service level agreements and contract mechanisms can play a role, such legal distinctions are well beyond the scope of this document. Note there may be a practical limit to the insight and control one can gain through such means when dealing with providers who are in the business of providing a common service to the masses.
- **Utilize Safe Web Surfing Practices**: Since that attacker's motivation is not focused solely on compromising cloud services, but using those services as a platform for compromising client computers, following safe web surfing practices is paramount
- **Use Private Clouds**: Avoid, or limit, dependence on public cloud services by utilizing a private cloud. While in a public cloud, the service is open to possible exploitation by the internet community at large; moving to a private cloud has the effect of limiting the threat exposure by restricting access to a much greater degree through layers of protection mechanisms such as firewalls and routing restrictions. Practically speaking, for many organizations a mix of public and private clouds will prove optimal. In essence, organizations might use their risk management and return on investment analysis to choose the most cost effective architecture that meets their security needs.

V. Need For Information Assurance Framework

To obtain a safe and secure data storage environment despite the increased level of risk in cloud computing, one of the most important recommendations is the Information Assurance Framework, a set of assurance criteria designed to:

- Assess the risk of adopting cloud services (comparing the risks of maintaining a 'classical' organization and architecture with risks to migrate in a cloud computing environment)
- Compare different Cloud Provider offers.
- Obtain assurance from the selected cloud providers. The preparation of effective security questionnaires for third party service providers is a significant resource drain for cloud customers and one which is difficult to achieve without expertise in cloud-specific architectures.
- Reduce the assurance burden on cloud providers. Many cloud providers find that a large number of customers request audits of their infrastructure and policies. This can create a critically high burden on security personnel and it also increases the number of people with access to the infrastructure, which significantly increases the risk of attack due to misuse of security-critical information, theft of critical or sensitive data etc. Cloud providers will need to deal with this by establishing clear framework for handling such requests.

The Framework provides a set of questions that an organization can ask a cloud provider to assure themselves that they are sufficiently protecting the information entrusted to them. These questions are intended to provide a minimum baseline any organization may therefore have additional specific requirements not covered within the baseline. Equally this paper does not provide a standard response format for the cloud provider, so responses are in a free text format. However it is intended to feed into a more detailed comprehensive framework which will be developed as a follow-up to this work, allowing a consistent, comparable set of responses. Such responses will provide a quantifiable metric as to the Information Assurance maturity of the provider.

VI. Cloud Information Assurance Baseline

Organizations considering cloud-based services must understand the associated risks and define acceptable use cases and necessary compensating controls before allowing cloud services to be used for regulated or sensitive information. Cloud computing environments have information technology risks in common with any externally provided service. There are also some unique attributes that require risk assessment in areas such as data integrity, recovery and privacy, and an evaluation of legal issues in areas such as e-discovery, regulatory compliance and auditing. The baseline would be governed by the current Federal Cloud Computing Initiative cross agency organization and include the following key areas: Privileged User Access, Compliance, Data Location, Data Segregation, Availability, Recovery, Investigative Support, Viability, Support in Reducing Risk.

VII. Success Factors And Recommendations

Reducing these risks areas will require the detailed diminishing strategies along with people and process changes. Certain IT and business roles will be needed to define appropriate risk mitigation plans. It is critical to include application development and security subject matter experts, and to address information assurance, security and risk. The following critical success factors and recommendations should guide any Federal Government agencies investigating the use of cloud computing technologies.

A. Critical Success Factors:

- The most practical way to evaluate the risks associated with using a service in the cloud is to get a third party to do it.
- Cloud computing information technology risks in areas such as data segregation, data privacy, privileged user access, service provider viability, availability and recovery should be assessed like any other externally provided service.
- Location independence and the possibility of service provider "subcontracting" result in information technology risks, legal issues and compliance issues that are unique to cloud computing.
- If agencies are making unauthorized use of external computing services, then they are circumventing security policies and creating unrecognized and unmanaged information related risks.

B. Recommendations:

- Agencies that have information technology risk assessment capabilities and controls for externally sourced services should apply them to the appropriate aspects of cloud computing.
- Legal, regulatory and audit issues associated with location independence and service subcontracting should be assessed before cloud-based services are used.
- Demand transparency. Think seriously before contracting for information technology services with a cloud provider that refuses to provide detailed information on its security and continuity management programs.
- Develop a strategy for the controlled and secure use of alternative delivery mechanisms, so that agencies know when they are appropriate to use and have a recognized approval process to follow.

References

1. Amazon Web Services: "Overview of Security Processes".http://s3.amazonaws.com/aws_blog/AWS_Security_Whitepaper_2008_09.pdf

2. Capturing the Private Cloud. A description of the fiscal motivations driving some to choose private clouds over public. http://gcn.com/Articles/2009/07/13/Private-cloud-computing-for-government.aspx.

3. Gerry O'Neill,(2013),"Security and Assurance in the Cloud, Chartered Accountants" Hall, UK

4. Loeffler, Bill, (2011),ISD IX, in Microsoft's Windows Server & Solutions. Retrieved from http://technet.microsoft.com/enus/magazine/hh509051.aspx(30/10/2014)

5. NSA(2009), Mitigation Monday #2 Defense against Drive-By Downloads. A set of guidelines for safer web surfing. Retrieved from http://www.nsa.gov/ia/guidance/security_configuration_guides/fact_sheets.shtml(30/10/2014)11

6. Pearson, S. (2009). Taking Account of Privacy when Designing Cloud Computing Services. In Proceedings of the ICSE Workshop on Software Engineering Challenges of Cloud Computing (CLOUD'09), pp. 44-52, Vancouver, British Columbia, Canada, May 2009.

7. Security Guidelines for Critical Areas of Focus in Cloud Computing. Cloud Security Alliance.http://www.cloudsecurityalliance.org/guidance/csaguide.pdf 13.

8. Vouk, M. A. (2008). "Cloud Computing – Issues, Research and Implementations". In Proceedings of the 30th International Conference on Information Technology Interfaces (ITI'08), pp. 31-40, Cavtat, Croatia,June 2008

9. Why Cloud Computing Needs Security. Describes the challenges that consolidated cloud computing sites pose for security. http://gigaom.com/2008/06/10/the-amazon-outage-fortresses-in-the-clouds/17.

A Critical Analysis of Various Data Mining Techniques in Educational Assessment and Feedback

Ms. Zinnia Ohri*

Abstract

There is pressure in higher educational institutions to provide quality education to its students to improve their performance as well as institutional effectiveness. The student's academic performance is affected by many factors, therefore it is essential to develop predictive data mining model for students' performance so as to identify the difference between high learners and slow learners. This paper is designed to justify the capabilities of data mining techniques in context of higher education. Here, we will also specify the data mining process to evaluate student's performance in higher education. This study will help the teacher to reduced drop-out ratio to a significant level and improve the performance of students.

Key Words: Data Mining (DM); Knowledge Discovery in Databases (KDD); Educational Data Mining (EDM).

I. Introduction

Data Mining (DM), or Knowledge Discovery in Databases (KDD), is an approach to discover useful information from large amount of data. DM techniques apply various methods in order to discover and extract patterns from stored data. The pattern found will be used to solve a number of problems occurred in many fields such as education, economic, business, statistics, medicine, and sport. The large volume of data stored in those areas demands for DM approach because the resulting analysis is much more precise and accurate. In recent years, there has been increasing interest in the use of DM to investigate educational field. Educational Data Mining (EDM) is concerned with developing methods and analyzing educational content to enable better understanding of students' performance. It is also important to enhance teaching and learning process [1]. EDM methods and algorithms used to discover hidden patterns and relationships which include prediction, classification, clustering and relationship mining. In this research, the classification task is used to evaluate student's performance. By this task we extract knowledge that describes students' performance in end semester examination. It helps earlier in identifying the dropouts and students who need special attention and allow the teacher to provide appropriate advising/counseling.

II. Related Work

While data mining has been applied in a variety of industries, government, military, retail, and banking, data mining has not received much attention in educational contexts (Ranjan & Malik, 2007). Application of specific data mining techniques such as web mining, classification, association rule mining, and multivariate statistics are also key techniques applied to educationally related data (Calders &Pechenizkiy, 2012) [4]. These data mining methods are largely exploratory techniques that can be used for prediction and forecasting of learning and institutional improvement needs. Also, the techniques can be used for modeling individual differences in students and provide a way to respond to those differences thus improve student teaching (Corbett, 2001).Lin (2012) applied machine learning algorithms to improve student retention efforts. Researchers at Bowie State University developed a system based on data mining that supports and improve retention (Chacon, Spicer,

Ms. Zinnia Ohri*
Assistant Professor, Department of IT
IITM, Janakpuri, New Delhi
zinnia.sardana13@gmail.com

and Valbuena, 2012) [5]. Their system helps the institution identify and respond to at-risk students. Data mining was used to assess the efficacy of writing center in an effort to analyze student achievement and student progress to the next grade (Yeats, Reddy, Wheeler, Senior, and Murray, 2010). Their work demonstrated the ability to assess a specific educational support process, i.e., the writing center, in an effort to improve institutional effectiveness. The research by Yeats et al. (2010) took a different approach to analyzing student achievement in that it made the connection between writing center attendance and student grades. It did not make the link to student retention issues, but a future study could examine the relationship between these three concepts: writing center attendance, student grades, and retention. In another study, three different data mining techniques were used to determine predictors of student's retention. Yu, DiGangi, Jannesch-Pennell and Kaprolet (2010) applied classification trees, multivariate adaptive regression splines (MARS), and neural networks to educational data which resulted in finding transferred hours, residency, and ethnicity as critical elements in retention efforts (Yu, DiGangi, Jannesch-Pennell and Kaprolet, 2010).

One research team used data mining to classify students into three groups (which include low-risk, medium-risk and high-risk students) as early as they could in the academic year. In a related study, researchers examined whether the demographic background of students had any influence on their performance (Yorke et al., 2005). The drawback with the research (Yorke et al., 2005) used these phrases, but never applied any classification, regression, or other data mining techniques. Contrary to the Yorke et al. (2005) study, a different research team noted that demographic characteristics are not significant predictors of student satisfaction or success (Thomos and Galambos, 2004) [7].

Personal learning environments (PLEs) and personal recommendation systems (PRS) also directly relate to educational data mining. PLEs focus on proving the various tools, services, and artifacts so that the system can adapt to students' learning needs on the fly (Modritsher, 2010). One research team examined this issue by applying PRS in an effort to improve student prediction results (Thai-Nghe, Drumond, Krohn-Grimberghe, and Schmidt-Thieme, 2010). It focuses on underlying algorithms and methods to improve recommender system. It provides an analysis of which analytical methods are more accurate when predicting student performance.

A large number of researchers within education data mining focus directly on course management system (CMS) and how they can be improved to support student learning outcomes and student success. CMS such as open source Moodle can be mined for usage data to find interesting patterns and trends in student online behavior. A systematic method for applying data mining techniques to Moodle usage data was established (Cristo‘bal Romero, Ventura, and Garci‘a, 2008). The benefit to mining usage data is that it contains data about every user activity, such as testing, quizzes, reading, and discussion posts. Romero et al. (2008) discuss the importance of pre-processing the data and then discuss specifics on how to apply data mining techniques to Moodle data. Their research results demonstrated how straight forward it is to mine data, even if a reader does not have much experience in this area. The authors also use both Keel &Weka as their data mining software packages. These software programs are open source and are built on the Java language, so they are extendable as well.

III. Data Mining Techniques

Data mining refers to extracting or "mining" knowledge from large amounts of data. Data mining techniques apply various methods in order to discover hidden patterns and relationships helpful in decision making [4]. The sequences of steps used for extracting knowledge from data repository are shown in Figure 1.

Various techniques used in data mining process are as follows:-

A. Classification

Classification is the most commonly applied data mining technique, which employs a set of pre-classified examples to develop a model that can classify the large set of records. This approach frequently employs decision tree or neural network-based classification

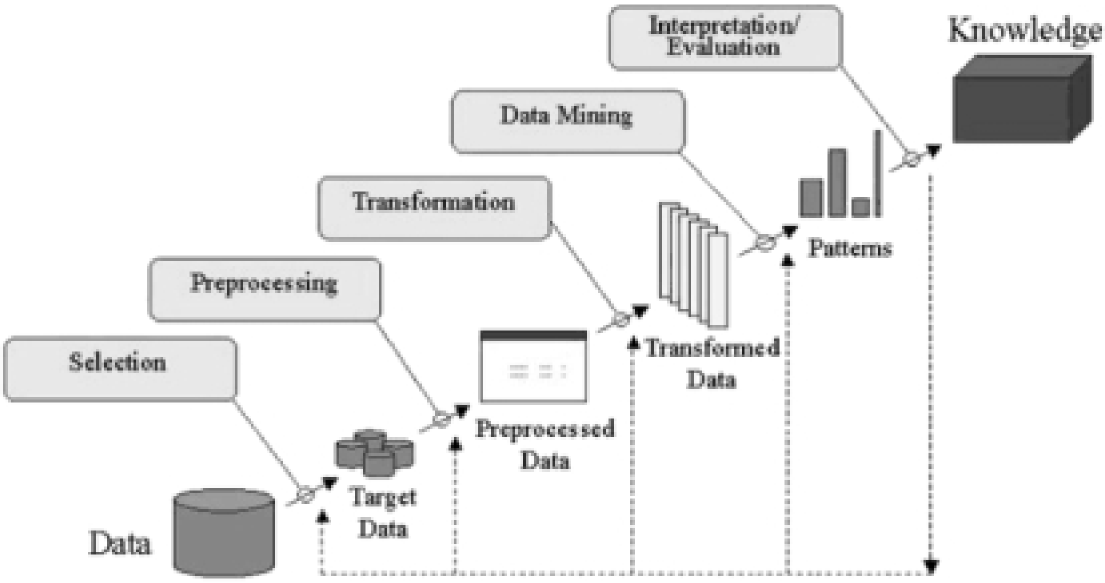


Figure 1: The steps of extracting knowledge from data

algorithms. The data classification process involves learning and classification. In Learning the training data are analyzed by classification algorithm. In classification test data are used to estimate the accuracy of the classification rules. If the accuracy is acceptable the rules can be applied to the new data tuples. The classifier-training algorithm uses these pre-classified examples to determine the set of parameters required for proper discrimination. The algorithm then encodes these parameters into a model called a classifier.

B. Clustering

Clustering is defined as grouping of similar classes of objects. We can classify dense and sparse regions in object space using the clustering method of data mining and can discover overall distribution pattern and the relationships among data attributes [4]. Classification approach also helps us to distinguish groups or classes of object but it is an expensive process as compared to clustering which can be used as preprocessing approach for attribute subset selection and classification.

C. Predication

For prediction about the unknown data sets, we can use regression technique. Regression analysis is done to analyze the relationship between one or more independent variables and dependent variables. In data mining independent variables are attributes already known and response variables are what we want to predict. Unfortunately, many real-world problems are not simply prediction. Therefore, more complex techniques (e.g., logistic regression, decision trees, or neural nets) may be necessary to predict future values. The same model types can often be used for both regression and classification.

D. Association rule

Association and correlation is usually to find frequent item set findings among large data sets. This type of finding helps businesses to make certain decisions, such as catalogue design, cross marketing and customer shopping behavior analysis [6]. Association Rule algorithms need to be able to generate rules with confidence values less than one. However the number of possible Association Rules for a given dataset is generally very large and a high proportion of the rules are usually of little (if any) value.

E. Neural networks

Neural network is a set of connected input/output units and each connection has a weight present with it. During the learning phase, network adjusts weights so as to be able to predict the correct class labels of the input tuples. Neural networks have the capability to discover meaning from complicated data and can be used to extract patterns and detect trends that are too complex to be noticed by either humans or other computer techniques. These are well suited for continuous valued inputs and outputs.

F. Decision Trees

Decision tree is tree-like structures that represent sets of decisions. These decisions help us to generate rules for the classification of a dataset. The most common decision tree methods are Classification and Regression Trees (CART) and Chi Square Automatic Interaction Detection (CHAID).

G. Nearest Neighbor Method

This is a technique that groups each record in a dataset based on a combination of the classes of the k record(s) most similar to it in a historical dataset (where k is greater than or equal to 1). This approach is also known as the k-nearest neighbor technique.

These techniques can be used to discover and extract patterns from stored data so as to analyze the performance of students and improve their skills and efficiency.

IV. Conclusion

In this paper, we analyzed the importance of using data mining approach for improving the performance of students. We also analyzed the various techniques that can be used for effective functioning of the higher education system and controlling the drop-out rate of the students. By adopting these techniques; we can analyze the current educational system and fill the gaps in higher education system. This study will help to the students and the teachers to improve the division of the student. This study will also work to identify those students which needed special attention to reduce fail ration and taking appropriate action for the next semester examination.

V. Future Scope

There is always scope for improvement. We can use the effective strategies for improving the feedback system of educational domain that will help the educational system to be accurate, up-to-date, reliable, and valid. We can also analyze and suggest adaptive predictive model based on some analytical tool.

References

1. Baker, R., & Yacef, K, "The State of Educational Data mining in 2009: A Review and Future Visions, Journal of Educational Data Mining", 2009.
2. Berson, A., Smith, S., & Thearling, K., "An Overview of Data Mining Techniques Retrived", November 28, 2011.
3. Blikstein, P., "Using learning analytics to assess students' behavior in open-ended programming tasks", 2011.
4. Calders, T., & Pechenizkiy, M., "Introduction to the special section on educational data mining", 2012.
5. Campbell, J., & Oblinger, D.(20 07), Academic analytics. Washington, DC: Educause. ,Chacon, F., Spicer, D., &Valbuena, A. (2012). , "Analytics in Support of Student Retention andSuccess", (Research Bulletin 3, 2012 ed.).
6. Chrysostomou, K., Chen, S. Y., & Liu, X., "Investigation of Users' Preferences in Interactive Multimedia Learning Systems: A Data Mining Approach"., 2009.
7. Nemati, H., & Barko, C., "Organizational Data Mining (ODM): An Introduction. In H.Nemati & C. Barko (Eds.), Organizational Data Mining (pp. 1-8). London: Idea Group Publishing", 2004.

Network Security Using Divergent Firewall Technologies

Sonali Ghai*
Ankit Verma**

Abstract

If your PC is connected to internet you are a potential target to an array of cyber threats such as Trojans, malware, key loggers and hackers that attack through un-patched security holes. These threats are responsible for the loss and manipulation of data, hijacked networks, leaks of security and personal data etc. for these reasons one of the critical component of network security has been deployed which works as a barrier between your PC and cyber space. Firewall filters the packets of sent and received data to check whether it meets certain criteria of rules and thereafter blocks or allows the data.

Key Words: Firewall technologies, network security, access control, proxy firewall.

I. Introduction

Through internet a large amount of data is available to an average computer used in business, in education and at home. For more people having access to this, information is no longer just an advantage, it is essential. But connecting a private network to the internet can expose critical and confidential data to malicious attack. Users who connect their computer to the internet must be aware of all the risks and should know how to protect their personal data [1]. The best way that ensured the security of their personal data is firewall. These can be used in number of ways to provide security to home or business computers. Large company uses very complex firewalls to protect their confidential or extensive data. Extensive configurations are to be maintained by the highly trained IT-professionals. But for home use firewalls work much more simply. The main work of the personal firewall is to save computer networks from the malicious mischief or viruses. A virus can be transmitted to your computer through email or over the Internet and can quickly cause a lot of damage to your files. There are two ways in which firewall can prevent this from happening i.e. by restricting the traffic from entering the network which does not follow the criteria, and by restricting traffic from going out unless it meets criteria.

II. Firewall

A firewall provides protection to the networked computers getting hostile from getting into computers which can compromise privacy and security or leads to data corruption or denial of service? It works as a filter between the network and the internet [2]. It can be programmed according to us that which traffic we can allow or we should send. Firewall uses different methods to filter the traffic some of them are used individually and some in combinations these methods work on different levels of network layer which determines how specific filtering options can be. Also firewall doesn't allow the outside computers to access the data of computers inside the network. It can be a software program (see Figure 1) or a hardware device (see Figure 2) running on a secure host computer. In either case, it must at least have two network interfaces,

Sonali Ghai*
Student of BCA
IITM, Janakpuri, New Delhi
sonali.ghai19@gmail.com

Ankit Verma**
Assistant Professor, Department of IT
IITM, Janakpuri, New Delhi
ankit.verma.aquarius@gmail.com

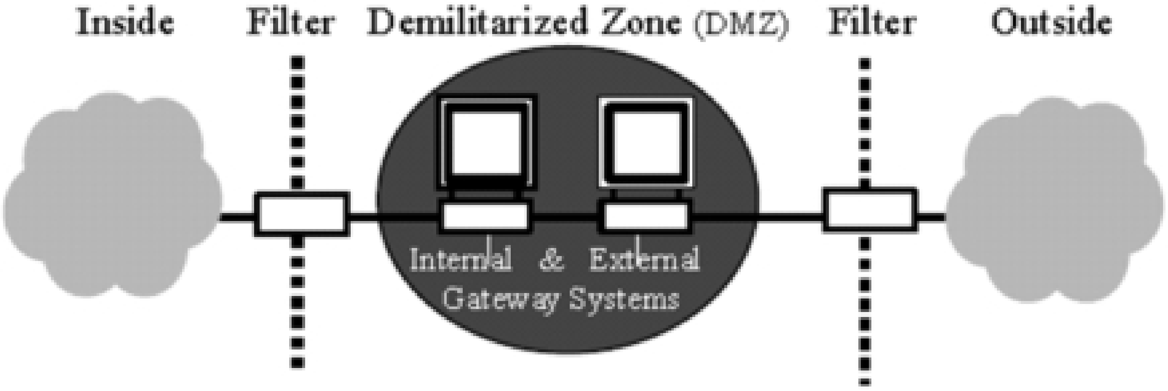


Figure 1: Firewall Schematics

i.e. one for the network it is trying to protect, and one for the network it is being exposed to [3]. A firewall exists at the junction point or gateway between the networks, it usually consist of public network and a private network such as the Internet. Earliest firewalls were simply routers. The term firewall comes from the fact that by dividing a network into different physical sub networks, they limited the damage that could spread from one sub network to another just like firewalls.

III. Firewall Working

There are two methodologies that are used by the firewalls for access denial. A firewall can allow all the data packets through, or it may deny all data packets unless it meets certain criteria (see figure 3). The criteria that are used to determine whether data packets should be allowed through varies from one firewall type to another. They may be concerned with the type of data packets or destination addresses and ports. They may use complex rule bases that analyze the application data to determine whether the data packets should be allowed through or not. A firewall determines which data packets are allowed, it depends on which network layer it is operating at [4].

IV. Firewall Types

Firewalls are broadly classified into the following different categories on the basis of their applications:

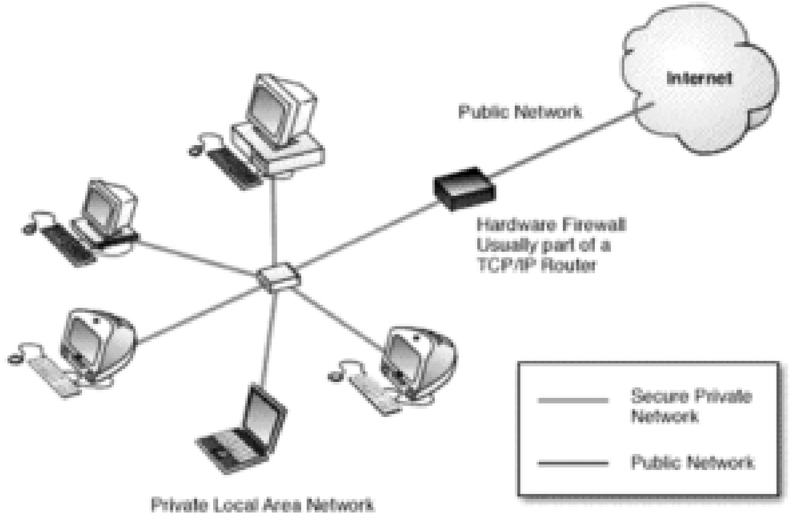


Figure 2: Local Network Hardware Firewall Protection

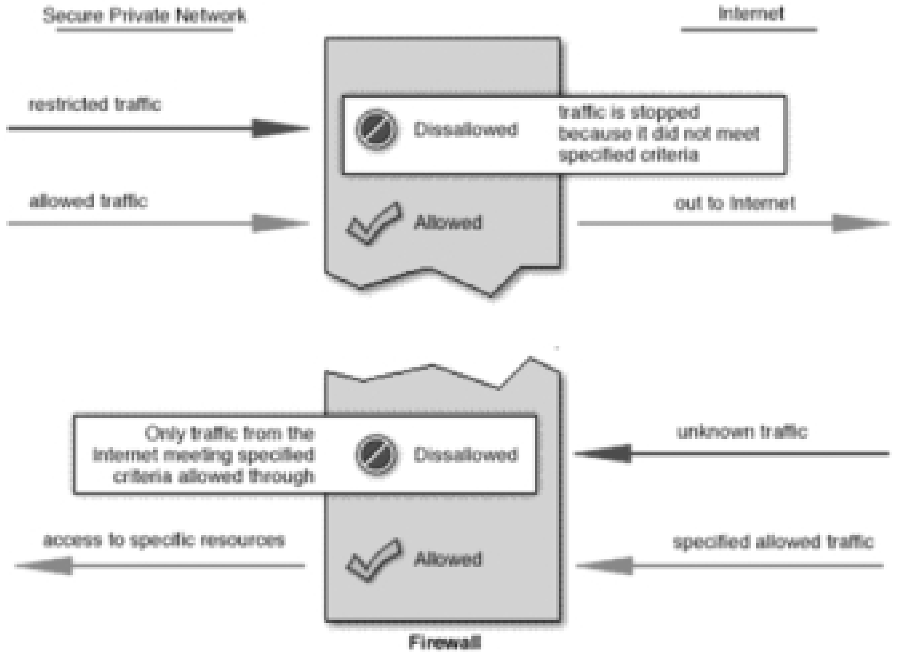

Secure Private Network
Internet
restricted traffic
Dissallowed
traffic is stopped because it did not meet specified criteria
allowed traffic
Allowed
out to Internet
Only traffic from the Internet meeting specified criteria allowed through
Dissallowed
unknown traffic
access to specific resources
Allowed
specified allowed traffic
Firewall

Figure 3: Basic Firewall Operation.

A. Packet Filters

When the internet is on computer receiver and sends data continuously this process is monitored by the firewall i.e. our computer receives only those data packets that satisfy the rules of the firewall (see Figure 4). The rules of the firewall are either set by the administrator or it uses default criteria [5]. In computer packet filtering is done through a program known as packet filter. It examines the header of each data packet and decides whether to accept the data packet or to drop it. Packet filter can be considered in 3 ways. In the first method it accepts only those packets that it is

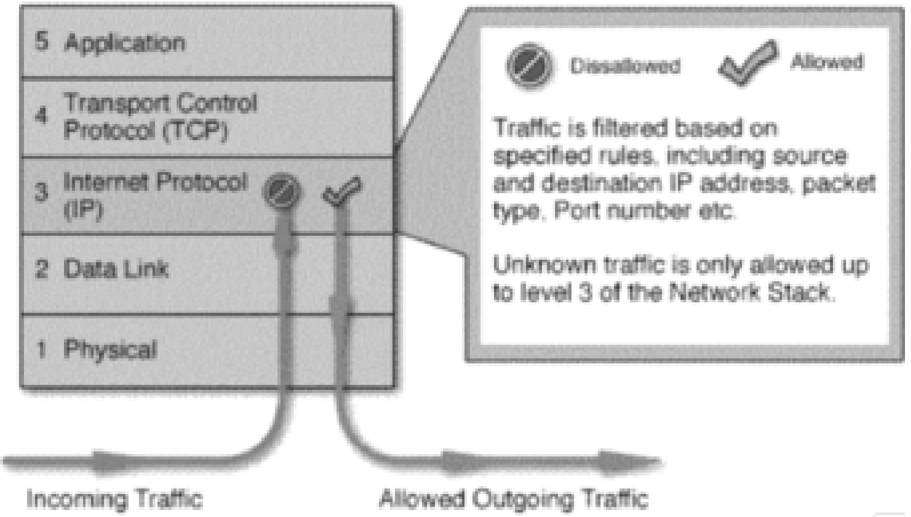

5 Application
4 Transport Control Protocol (TCP)
3 Internet Protocol (IP)
2 Data Link
1 Physical
Dissallowed
Allowed
Traffic is filtered based on specified rules, including source and destination IP address, packet type, Port number etc.
Unknown traffic is only allowed up to level 3 of the Network Stack.
Incoming Traffic
Allowed Outgoing Traffic

Figure 4: Packet Filter Operation

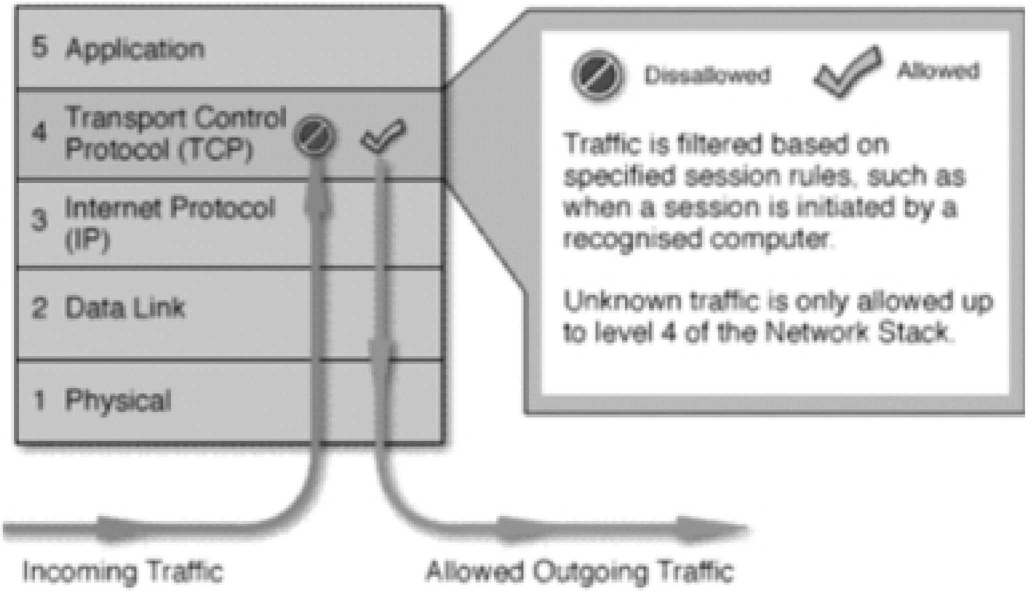

5 Application
4 Transport Control Protocol (TCP)
3 Internet Protocol (IP)
2 Data Link
1 Physical
Dissallowed
Allowed
Traffic is filtered based on specified session rules, such as when a session is initiated by a recognised computer.
Unknown traffic is only allowed up to level 4 of the Network Stack.
Incoming Traffic
Allowed Outgoing Traffic

Figure 5: Circuit Level Gateway's Operation

sure of are safe and drops all the other packets. This is the most secure method but this can cause inconvenience to the user because it can drop some of those packets that are required by user. In the second method it drops that packet, it is sure are unsafe and allows all others. It is least secure method but doesn't create inconvenience for the user. In third method if the filter finds and packets that is not according to its set rules it will take the authentication from the user whether to allow it or not.

B. Circuit Level Gateways

Circuit level gateway is a type of firewall which provides User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) connection security. It works

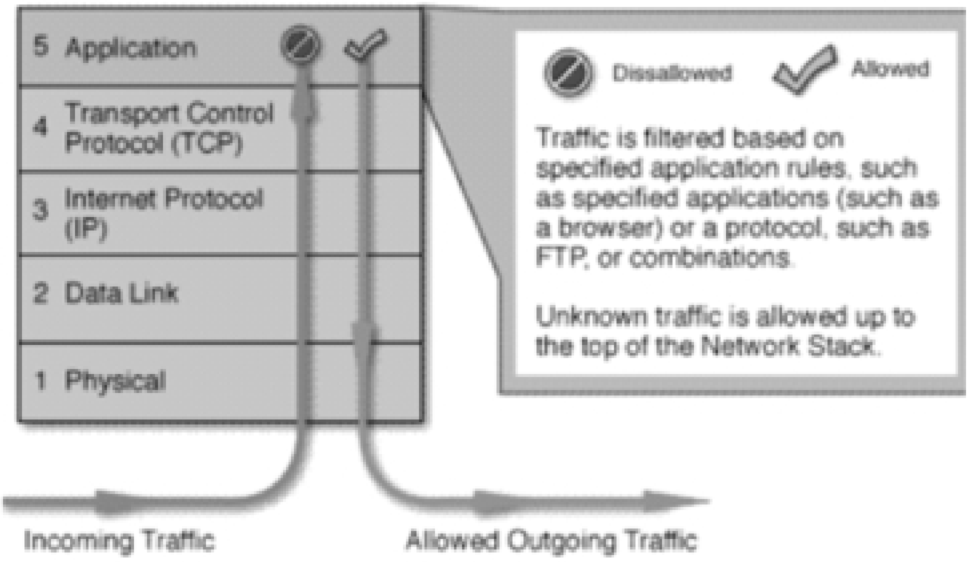

5 Application
4 Transport Control Protocol (TCP)
3 Internet Protocol (IP)
2 Data Link
1 Physical
Dissallowed
Allowed
Traffic is filtered based on specified application rules, such as specified applications (such as a browser) or a protocol, such as FTP, or combinations.
Unknown traffic is allowed up to the top of the Network Stack.
Incoming Traffic
Allowed Outgoing Traffic

Figure 6: Application Level Gateway's Operation

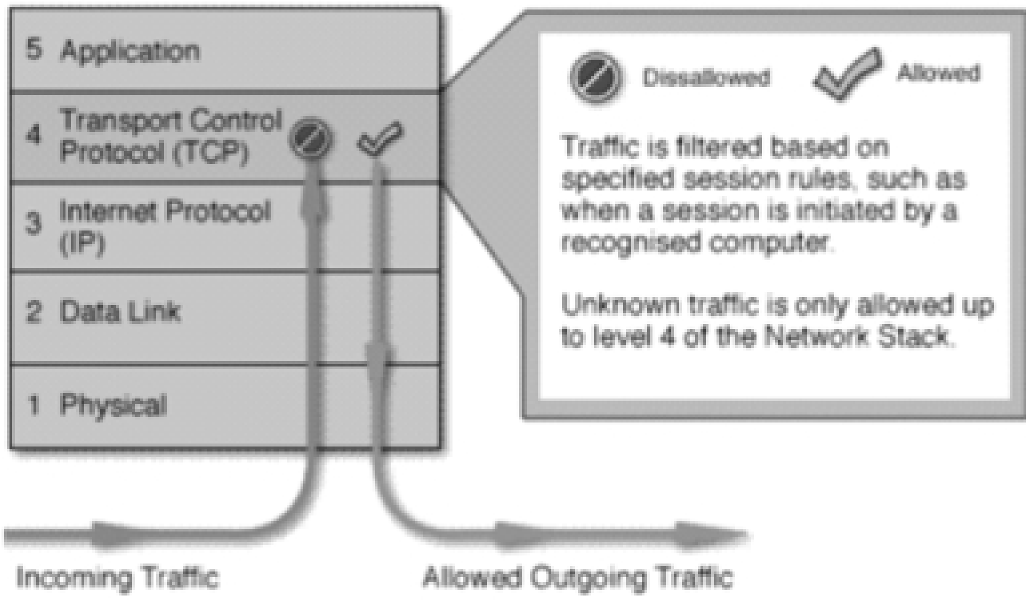

5 Application
4 Transport Control Protocol (TCP)
3 Internet Protocol (IP)
2 Data Link
1 Physical
Dissallowed
Allowed
Traffic is filtered based on specified session rules, such as when a session is initiated by a recognised computer.
Unknown traffic is only allowed up to level 4 of the Network Stack.
Incoming Traffic
Allowed Outgoing Traffic

Figure 7: Stateful Multilayer Inspection's Operation

at the session layer of OSI model. Unlike application gateways, circuit-level gateways monitor TCP data packet handshaking and session fulfillment of firewall rules and policies (see Figure 5). It is simple to implement. It doesn't require a separate proxy server for each application.

C. Application Level Gateways

Packet filleting alone cannot provide the protection. In order to effectively block one-to-one related network traffic, here, there is a requirement of application filtering. They are slower than the Stateful inspection. They are sometimes implemented using application proxies [6]. In this two TCP connections are established one between the source packet and firewall and another between the firewall and the destination packet.

D. Stateful Multilayer Inspection Firewalls

It is a type of firewall which keeps track of the state of the network connections that travel across it. Only data packets matching the known active connection will be allowed by the firewall else others will be dropped [6]. It is also known as dynamic packet filtering. This security feature is often included in business networks.

E. Proxy Firewall

It is a network security system that filters data packets at the application layer. It can also be known as application firewall or gateway firewall. Just like proxy server a proxy firewall acts as a intermediary between the client and server on the internet. It also monitors the incoming traffic for 7 layer protocols, such as HTTP and FTP. Also for determining which traffic is allowed and which is denied, a proxy firewall uses Stateful inspection technology and deep packet inspection to analyze incoming traffic for signs of attack.

V. Conclusion

Throughout the paper firewall topics are discussed like what firewall is, how they work and what the types of firewalls are. We have studied firewall is the main component of network security. It acts as a filter that filters the traffic coming inside the network and going outside network and denies all other traffic that does not follow the preset criteria of the firewall. It saves the data from the viruses, malicious activities, from getting lost and from getting manipulated. This is helpful for both home users and corporate users.

References

1. Briand, L. C., Daly, J., and Wüst, J., "A unified framework for coupling measurement in objectoriented systems", *IEEE Transactions on Software Engineering*, 25, 1, January 1999, pp. 91-121.
2. Maletic, J. I., Collard, M. L., and Marcus, A., "Source Code Files as Structured Documents", in *Proceedings 10th IEEE International Workshop on Program Comprehension (IWPC'02)*, Paris, France, June 27-29 2002, pp. 289-292.
3. Marcus, A., *Semantic Driven Program Analysis*, Kent State University, Kent, OH, USA, Doctoral Thesis, 2003.
4. Marcus, A. and Maletic, J. I., "Recovering Documentation-to-Source-Code Traceability Links using Latent Semantic Indexing", in *Proceedings 25th IEEE/ACM International Conference on Software Engineering (ICSE'03)*, Portland, OR, May 3-10 2003, pp. 125-137.
5. Salton, G., *Automatic Text Processing: The Transformation, Analysis and Retrieval of Information by Computer*, Addison-Wesley, 1989.
6. M. Frantzen, F. Kerschbaum, E. Schultz, and S. Fahmy, "A framework for understanding vulnerabilities in firewalls using a dataflow model of firewall internals," Computers and Security, vol. 20, no. 3, pp. 263–270, May 2001.

TNA Methods & Evaluation of training Program a Study at TCS e-serve

Dr. Suniti Chandiok*

Abstract

This paper shows that how the deficiency in the interview process of team leaders of TCS e-serve led to the poor performance of newly promoted team leaders of the organization. Their performance appraisal indicates low scores in the general areas of competency attributes. This is also a hindrance for their talent management program. The team-leader of an organization is expected to have some team leading qualities like self-motivation& the ability to motivate others, taking initiative, stress tolerance, leadership, etc. But in this particular organization, while selecting the team leader emphasis was paid more on process knowledge rather than team leading qualities. Candidates were not systematically checked for the required competencies listed above, and even if checked, it was done in an unstructured manner. There was no systemic behavior assessment of the candidates. Although this cannot be construed as a singular reason for the Team Leaders falling short during the performance appraisal on team leading issues. The current interview process was deficient in identifying the right candidate, hence involving a change in the structure of the interview process. So, Training Need Analysis was done and after that employee was trained in their deficient areas and evaluation was also conducted to check training programme.

Key Words: Training need Analysis; Evaluation of training; Analysis of training; Task analysis.

I. Introduction

Training Needs Analysis (TNA) is a process for analysing the specific training (or developmental) needs of individuals and groups. TNA is often used by organisations to uncover and bridge the gap between adequate and inadequate job performance, or to prepare existing workers for new challenges as outlined in strategic plans. A well conducted TNA will allow you to determine the precise training need and consider appropriate learning strategies to meet it. A Training Needs Analysis will assist you to make sure that it really is a training need you are responding to, rather than a policy or procedure need or perhaps a support need. Know your learner's needs and design your training to meet them and start with what your learner's know. It is important not to teach skills and knowledge that your learner's already have. This is not only a waste of time and money, but will often alienate learner's who feel patronize. A well conducted Training Needs Analysis will assist you to undertake all aspects of planning to train, including:

- Developing the objectives for undertaking the training.
- Preparing assessments based on the objectives derived from the need.
- Developing program plans specifying who will be taught what and when.
- Selecting content and delivery methods based on learner's needs.
- Marketing the program and curricula to relevant people by addressing their needs.
- Preparing detailed instructional materials intended to meet their needs.
- Evaluating training based upon the objectives derived from the needs.

Dr. Suniti Chandiok*
Associate Professor, Department of Management
Banarsidas Chandiwala Institute of Professional Studies,
Dwarka, New Delhi

A. Determining a training need

Stage 1: Determining the purpose of the TNA

- Deficiency model - the purpose is bridging the gap between current performance and desired performance
    - ➢ To compare current staff skills with current or future skill requirements
    - ➢ To assess how successful previous training initiatives have been
    - ➢ To identify the skills required for new positions
    - ➢ To find out why you are getting complaints, loss of business or other negative indicators
- Opportunity model - the purpose is providing opportunities for staff and organisational development rather than in response to noted deficiencies.
    - ➢ To identify the skills required for a planned organisational development
    - ➢ To identify competence, capability and potential when succession planning
    - ➢ To find out what might motivate your staff to stay and continue development

Stage 2: Selecting appropriate method/s for determining training needs for undertaking the TNA will have an effect on the methods you use to determine training needs and the learning strategies you design to meet the determined training needs. A detailed description of methods is included later in this paper.

Stage 3: Carry out the TNA to determine the Needs: At this stage you gather your data, analyze it. Are the needs you have identified training needs, needs that are linked to a specific job or role requirement with a focus on the current or future job performance of the individual, educational needs linked to more general or transferable skills and knowledge's or developmental needs linked to the overall development of the individual over a long time period.

Stage 4: Determine appropriate learning strategies to meet the need. Some identified needs are not best resolved through training. In a deficiency based TNA for example, it may be a better option to transfer workers whose identified skills do not meet job requirements to positions that will utilize their existing skills. In an opportunity based TNA the sort of skills identified might be more easily acquired through a mentoring process than through a short course. The learning strategies are usually then documented in a Training Plan. This is not a session plan, but rather lists the training needs and learning strategies in an action plan format times, dates, responsibilities etc. and can be made for an individual or for a group.

Stage 5: Consult with learners to negotiate training requirements: Stage 4 and 5 are actually interchangeable, depending on the context, it may be better to consult with potential learners prior to determining strategies, particularly if you are working within an opportunity model. Traditionally, however, HR professionals determine the best strategy or range of strategies and then inform workers about the training they will be undertaking.

In an opportunity based TNA the sort of skills identified might be more easily acquired through a mentoring process than through a short course. The learning strategies are usually then documented in a Training Plan. This is not a session plan, but rather lists the training needs and learning strategies in an action plan format– times, dates, responsibilities etc. and can be made for an individual or for a group.

Evaluation literature refers to the “dimensions of evaluation” as process, outcome and impact. These concepts are fundamental and this will be discussed in other contexts more fully (P-O-I).

- **Process evaluations**: Process Evaluations describe and assess programme materials and activities. Establishing the extent and nature of programme implementation is an important first step in studying programme outcomes; that is, it describes the interventions to which any findings about outcomes may be attributed. Outcome evaluation assesses programme achievements and effects.
- **Outcome evaluations**: Outcome Evaluations study the immediate or direct effects of the

programme on participants. The scope of an outcome evaluation can extend beyond knowledge or attitudes, however, to examine the immediate behavioural effects of programmes.

- **Impact evaluations**: Impact Evaluations look beyond the immediate results of policies, instruction, or services to identify longer-term as well as unintended programme effects. Very useful reports on this subject have notably been made by the Center for Global Development and comprehensive review of the three dimensions–process, outcome and impact.

II. Literature Review

It has been recognized that training and development is related with the successful performance of workers, organizations and nations. The nations which spend significantly on training and development are relatively more developed. For the macro level analysis the economists use the term human capital development. (Berker 1980). The researchers, (Barro 1989. Buechtemann and Sooloff 1994) believe that the productivity of human resource is taken as more important than natural resources, physical equipment or any other form of wealth. Human capital is conceptualized as sum total of skills and knowledge acquired by the people of one country. Human capital is a significant factor to explain different rates of economic growth of nations.

Analyzing various government laws and policies on training and development, the authors conclude that training and development infrastructure is still weak and under construction. Various surveys and the reports of "Ministry of Education" indicate that there is restrained spending on training and development in public owned enterprises mainly due to the lack of capabilities of individual entrepreneurs ,while there is a good deal of investment in human capital at private enterprises. The research of Technology Commission indicates that there is low practice of training and development and consequently low labor productivity and industrial efficiency. By using secondary data from the books and journals, the author has explored public policy and strategy for reduction of poverty and unemployment; corporate policies and strategies and has provided a list of various organizations, associations and institutions which are working for the promotion of training and development in the country. The author has analyzed the data provided in Economic survey 1998-99 of India to describe educational and research infrastructure and training and development in the country. Lastly, the findings of his research on HRD policies and practices in 252 Indian industries suggest that organizations have shifted to target-based to need-based training and that there is growing realization among the managers and policymakers to consider the expenditure on training as an investment in human capital.

III. Research Methodology

This is an descriptive research in which objective is to find out how the deficiency in the interview process of team leaders of TCS e-serve led to the poor performance of newly promoted team leaders of the organization. The research is done by the survey method/interview of focused group, skill audit of different domains are conducted in the organization. For survey, SBU Head, Line Managers, Incumbent Team Leaders, Trainers etc. All the data was collected by primary source. The response rate is 85% in TCS E-serve, Mumbai location has 52 process managers and around 165 Team leaders with approximately 3 Team Leader's reporting to 1 process manager and in this survey consultation with the SBU head.TCS e-Serve, known formerly as Citigroup global services is the back-office processing centre for all entities of Citigroup around the world. Located in suburban Mumbai, they provide IT enabled services and solutions to their client. Being a captive BPO for Citigroup, they have robust financials and are supported by a world-class infrastructure and have stringent quality and delivery norms. TCS e-Serve provides clients with outsourcing benefits and mitigating off-shoring risks.

Objective of the Study: A trend that is emerging in the organization is that many newly promoted Team Leaders are not replicating the performance that they were displaying in their previous roles and on the basis of which they were promoted.

IV. Data Finding and Analysis

The data was analysed and assessed Training Needs Assessment: Before the delivery and design of any effective training, we need to ascertain the necessity for that training. Needs assessment is the process for the determination of the necessity of the training. The needs assessment flows in the following manner:-

- **Organizational Analysis:** As discussed, the organization is facing an issue with the performance of newly promoted team leaders. Their performance appraisal indicates low scores in the general areas of competency attributes that are outlined below after the competency mapping. This is a cause of concern for the top management as they believe that a lacuna exists between potential and performance of the Team leaders and this is also an hindrance for their talent management program as the continuous poor performance appraisal of the Team Leaders makes them ineligible to be groomed from a long term view. Having effective Team leaders is also important for the organization, as they are core to the activities inside the organisation since they are considered to be the bridge between management and the employees in the Team member position. The organisation believes this to be a delicate balancing act and having the right person for the job is crucial.
- **Task Analysis:** The existing Competency Mapping of the job of the Team Leader reveals the following job performance aspects that they need to possess while handling a team:
- **Taking Initiative** – Employee actively makes an attempt to influence situation and people for the attainment of goals. Rather than passively accepting the event, employee makes a conscious effort to direct the event.
- **Self -Motivation and to motivate others** – Employee is intrinsically directed to perform and achieve results and is capable of energizing his team to follow suit.
- **Stress Tolerance**- Employee is able to perform under job related constraints and able to effectively handle disappointment and/or rejection.
- **Leadership** – Employee can utilize appropriate methods and leadership styles in guiding subordinates and groups.
- **Decision Making** – Employee displays readiness to make informed decisions after carefully considering the available alternatives and its consequences.
- **Persuasiveness** – Employee displays the ability to convince for the attainment of results.
- **Communication** – Employee can succinctly express verbal and written information to others. And able to provide timely information to the concerned people.

We also concentrated on the interview process held to select candidates for Team Leader position. The interview process involves 3 roles: HR in-charge of the process, the line manager (process manager) and the internal shortlisted candidate or an external candidate with Team Leader experience. There is an aptitude test followed by interview with the line manager and then the HR process in-charge. We found that while the HR round is basically a discussion about remuneration and career prospects, it is the line manager who has the vital task of selecting the Team leader. Interviews with the line manager revealed that the questions asked of the candidates were process oriented rather than behaviour oriented and candidates who excelled in technical skills were usually selected. So emphasis was paid more on process knowledge rather than team leading qualities. Candidates were not systematically checked for the required competencies listed above, and even if checked, it was done in an unstructured manner that was subjected to the biases of the line manager.

- **Person Analysis:** Based from the task analysis, we identified that there was a gap in the manner in which Team Leaders were selected for that role, as there was no systemic behaviour assessment of the candidates. Although this cannot be construed as a singular reason for the Team Leaders falling short during the performance appraisal on team leading issues; the HR process in-charge role can also be under scrutiny as ideally they should have intervened in the interview process if they observed that the current interview process was deficient in identifying the right candidate, hence involving a change in the structure of the interview process; the lack of skill on the part of the line manager to identify the suitable candidate can be considered significant enough for us to identify that line managers need to undergo training on conducting behavioural interviews. We also believe that the HR process in-charge should also be included in the training so as to create the initial buy-in from the line managers, as there is a general belief that it is the HR manager's job to identify suitable candidate behaviours. Convincing the line manager that the onus is on him/her to identify the suitable candidate is therefore very essential for the training to be successful.

A. Participants in Needs Assessment:

- SBU Head
- Line Managers (Process Managers)
- Incumbent Team Leaders
- Internal potential candidates identified for the role of Team Leader's
- Trainers

Since it is not feasible to include all the line managers and incumbent Team Leaders in the needs assessment process (TCS E-serve, Mumbai location has 52 process managers and around 165 Team leaders with approximately 3 Team Leader's reporting to 1 process manager), in consultation with the SBU head, we will identify the processes that have Team Leaders with below expectation performance appraisals and conduct our TNA in those processes.

B. Methods of Needs Assessment

- **Documentation:** Checking the Performance Appraisals of the Team leaders from the sample processes selected.
- **Interviews:** This would be done with the SBU head regarding the problem of underperforming Team Leaders and whether the magnitude of the problem is large enough to mandate allocation of financial resources for training purposes. Interviews would be held with the HR process in-charge and process managers regarding the selection interviews. We prefer the interview mode rather than the questionnaire technique, as this will let us explore unanticipated issues that come up during the interviews. This is not possible with the questionnaire as it is uni-dimensional in the response that it seeks.

C. Principles of Learning

The adult learning model propounded by Malcolm Knowles was kept in mind when designing the training programme. In the **Andragogy** developed by Knowles, the following assumptions are made:

- Adults need to know the reason for which they are learning.
- Adults prefer to be self-directed
- Use of work based experience in the learning context is preferred by adults
- Adults have an approach to learning that is problem centered.
- Intrinsic and extrinsic motivators induce adults to learn (Knowles, Holton & Swanson, 2005)

All the above assumptions were kept in mind when designing the training program. The training objective will inform the managers what they are going to learn and linking the objectives to the needs assessment will create the buy-in from the managers as to why they need to undergo these training and different learning styles available. We have attempted to incorporate in our training different modes to accommodate the learning approaches of the four different learning styles in VARK:

- Visual Learners: PowerPoint Presentation
- Aural Learners: Discussion
- Read - Write Learners: Handouts
- Kinesthetic Learners: Role Play.

D. Instructional Objectives and Outcomes

At the end of the course, Trainee will be able to demonstrate the following:

- To understand what is behavioural Interview

- Understand the benefits of Behavioural Interview as applicable to TCS E-serve
- Ask relevant Behavioral questions to potential Team Leaders
- Use the Evaluation criteria to measure candidate response

E. Training Evaluation

The evaluation of the training outcomes will be done using Kirkpatrick's four level framework. For the training programme, the evaluation criteria using Kirkpatrick's framework will be as follows:

F. Level Criteria Outcome

4. Results Presence of Team Leaders with high scores on the competency traits as determined by the organisation

3. Trainee Behaviour (Skill Transfer Outcome) Trainee's use Behavioural Interview technique as a part of the selection process

2. Trainee Learning (Cognitive / Skill Learning Outcome) Trainee's understood the behavioural Interview technique

1. Trainee Reaction (Affective Outcome) Trainee's are satisfied with the training module and content

Level 1 (reaction) and 2 (learning) outcomes and can be measured during and immediately after the training. Level 3 (Behaviour) and 4 (Results) assist in determining the transfer of training and measure the usage of training content by the trainees while on the job.

Level 1 information will be collected by means of a questionnaire (attached in Appendix) to be filled by trainees at the end of the programme.

Level 2 outcome can be measured during the training programme itself by means of role play, discussion and Q&A sessions than are incorporated in the training.

Level 3 outcomes will be measured by observation of the managers during interviews.

Level 4 outcomes will be measured from the performance appraisal of Team Leaders who had been subjected to the behavioural interview technique trained to process managers to be used during the selection process.

V. Conclusions

After analyzing we found that while the HR round is basically a discussion about remuneration and career prospects, it is the line manager who has the vital task of selecting the Team leader. Interviews with the line manager revealed that the questions asked of the candidates were process oriented rather than behaviour oriented and candidates who excelled in technical skills were usually selected. So emphasis was paid more on process knowledge rather than team leading qualities. Candidates were not systematically checked for the required competencies listed and even if checked, it was done in an unstructured manner that was subjected to the biases of the line manager. Based from the task analysis, we identified that there was a gap in the manner in which Team Leaders were selected for that role, as there was no systemic behaviour assessment of the candidates.

References

1. Bhatia, S.K. (1989). "Challenges in Human Resource Development". The Management Review iii (1989).
2. Bremmer, B. (1998, Nov.30). "Japan- Special Report: Wanted - A new economic model". Business Week, 62-63, 66, 71.
3. Caroli, Paine &Nancovich (1972). "The Relativeness of training methods experts opinion and research". Personnel Psychology, Vol. 25(1), pp 12-25.
4. Cascio, W.F. (1995). "Managing Human Resources - productivity, quality of work life, profits". 4th Edition. New York: McGraw-Hill.
5. CGSL (2009). TCS E-serve. Retrieved on September 25, 2009 from, www.citigroup global services.com/

6. Fisher, C.D., Schienfeldt, L.F, & Shaw, J.B. (1999). Human Resource Management, Boston: Houghton Mufflin Company, P.389.

7. Harrison, R. (1993). "Human Resource Management: Issues and Strategies". Addison-Wesley.

8. Hawk, F. T., & Shah, J.A. (2007). Using Learning Style Instruments to Enhance Student Learning. Decision Sciences Journal of Innovative Education.5(1). Retrieved from Ebsco Database on September 25, 2009 fromhttp://web.ebscohost.com/ehost/pdf?vid=2&hid=111&sid=3b29939a-f796-4d7e-8835-6786cfc0 ce9e%40rep licon 103

9. Human Technology, Inc. (1993). "Department of justice training and development project task 3 report: training and development framework and descriptions of best practices". Human technology, Inc.: McLean, VA.

10. Khan Parveen (2001). "Training Employees for total quality". IJTD, Vol.XXXI, No. 2, April-June 2001.

11. Kunder Holder Linda (1998). "Employees perception of the Status and Effectiveness of the Training and Development system and the Value ofTraining and Development". Virginia Polytechnic Institute and State University.

12. Knowles, M, Holton, E ,& Swanson R.(2005). The Adult Learner: the definitive classic in adult education and human.(6thed). Boston : Elsevier

13. Lajuria Kumar, B.A. (2002). "Management And Training" Sundaysupplement of Greater Kashmir, Oct. 13, 2002.

14. Morita, Akio (1987). "Made in Japan.".London: Harper Collins Publishers.

15. Noceraz, J. (1996). "Living with Layoff. Fortune, 6(133): 69-71.

16. Noe, R.A. (1998). "Employee Trainingand Development." Boston: Irwin, McGrawHill.

17. Rothwell&Kazans, H. (1994). "Planningand managing human resources:Strategic planning for personnelmanagement" (rev.ed).

18. Sodhi, J.S. (1999). "Industrial Relationsand Human Resources Management in Transition", Indian Journal of Industrial Relations.

19. Targeted Selection (2009). Targeted Selection. Retrieved on September 25,2009 from,www.ddiworld.com/products_services/targetedselection.asp

20. Wexley, K.N. & Latham, G.P. (2000). "Developing and Training Human Resources in Organisations".Vol.3, Englewood Cli.s, NJ:Prentice-Hall.

Technology- A Panacea for Financial Sector Reforms in India

Ms. Shikha Gupta*

Abstract

This paper takes the view that financial sector reforms are not only a matter of jettisoning old regulations nor even simply a matter of prudential regulation accompanying structural deregulation; it is intimately bound up with various issues and has changed considerably since the 1990s. Since then the Indian equity market has become world-class. Interest rates have been deregulated and new entrants are allowed in the banking and the securities business. New private banks have come forward that are more customer-oriented than the older state-owned banks. There is further need for adds on financial sector reforms due to substantial expansion in the scale of saving within the economy much as in East Asian economies during their high-growth period. In particular, more freedom is required in asset allocation in banking sector. During 2007-2008, Public sector banks did appear sounder to public in comparison with the private ones due to implicit government backing. They ought to be privatised to improve their governance and minimise the recurrent need for recapitalisation. Also the remaining obstacles for new entrants have to be abridged along with financial inclusions. Other priorities include precluding restrictions on microfinance. The legal and regulatory framework also needs to be revamped. Such reforms would have positive spill over effects on the rest of the economy and help sustain rapid growth along with improving financial sector efficiency. This adds to the need for further financial-sector reform.

Key Words: Bank Privatisation; Financial Sector Reform; Regulatory Framework; Financial Inclusion; Financial Regulation; Interest Rates; Microfinance; Asset Allocation.

I. Introduction

A powerful and efficient financial sector is crucial for the optimal allocation of capital not just in highly developed economies but also in emerging market economies, especially in fast-growing ones. Financial sector reforms are at the centre stage of the economic liberalization that was initiated in India in mid 1991.

Financial sector reform is an important component of the ongoing process of liberalization of the Indian economy. Since 1990s, India's financial sector has undergone major reforms and a remarkable transformation but, in many respects, it still reflects the institutional set-up that was put in place when India was run as a directed economy. This paper, gauge at the extent and impact of the reforms so far before considering where further legal, institutional and regulatory changes are needed.

The Indian economy has grown swiftly over the past decade, with a sharp rise in investment and saving rates (Table 1). Also reforms of the financial intermediation between firms and households have played a crucial role which is evident by cross-state studies of the influence of banking competition on the efficiency of traditional industry and the impact of the stock market on high-tech industries in India[7]. The saving rate had already pep up in the late 1980s (Figure 1) in relation with earlier economic reforms, but it rose more rapidly in the early 2000s, to levels comparable to those in a number of East Asian economies during their phase of rapid growth (with the remarkable exception of China, where GDP growth is higher along with the

Ms. Shikha Gupta*
Assistant Professor, Department of Management
IITM, Janakpuri, New Delhi
shikhaguptardias@gmail.com

Table 1: Saving and investment rates % of GDP

	1998-99	2008-09
Gross private saving	24.7	33.1
Household sector	20.4	24.1
Private corporate sector	4.3	9.0
Foreign saving	0.6	0.5
Gross private investment	15.1	24.9

saving rates which have been an order of higher magnitude).

II. Credit Market

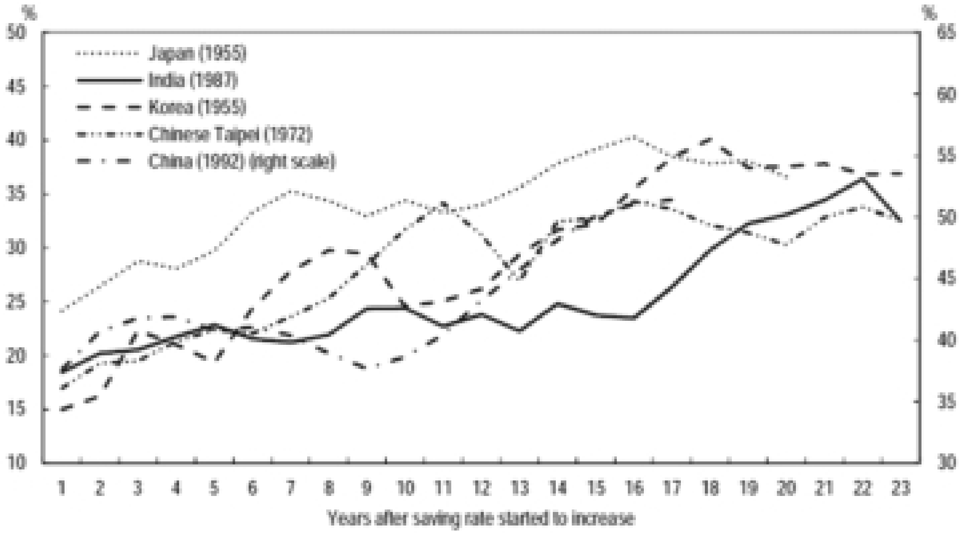
Credit markets perform the critical function of intermediation of funds between savers and investors and improve the allocative efficiency of resources. The banking sector embraces three groups of public sector banks, private banks and foreign banks. On the whole, three-quarters of the total assets of deposit-taking institutions and non-bank financial institutions of the credit market is dominated by public sector. (Fig. 2)

The RBI (Central Bank) as part and parcel of the financial sector deregulation, attempted to enhance the transparency of the annual reports of Indian banks by, among other things, introducing various measures like stricter income recognition and assets classification rules, improving the capital adequacy norms, and by requiring a number of added disclosures sought by investors to make advanced cash flow and risk assessment.

The Banking Sector

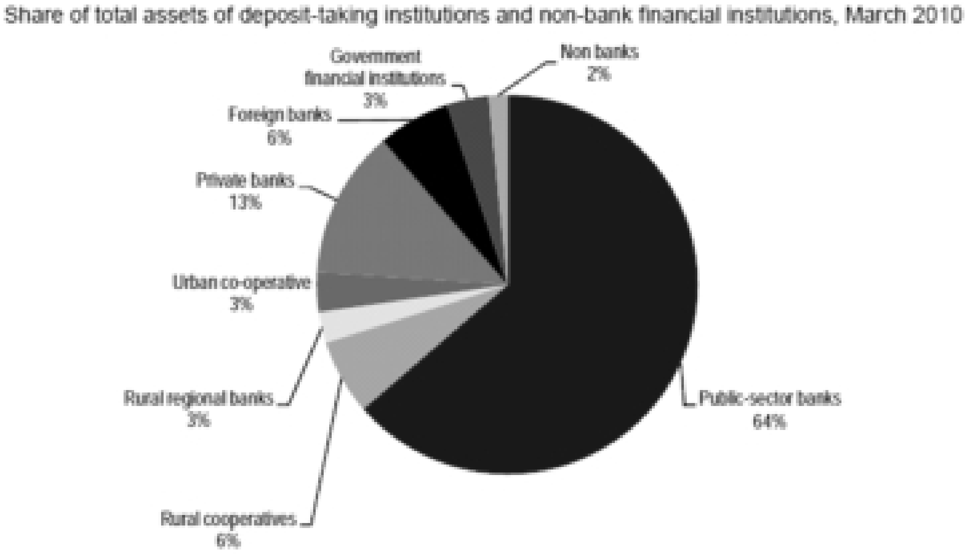
The Indian banking industry is the backbone of the country's economy which has always played a vital role in preventing the economic catastrophe from reaching terrible volume in the country. It has achieved enormous appreciation for its strength, as in the wake of the worldwide economic disasters, which pressed its worldwide counterparts to the edge of fall down. The Indian banking system is among the healthier performers in the world, if we compare the business

Figure 1: National saving rates in India and selected East Asian economies



Source: National Statistical Offices.

Figure 2: Structure of the credit market



Source: RBI.

of three top most banks in terms of total assets and return on assets. This sector is immensely competitive and recorded as growing in the right trend [15]. Indian banking industry has multiplied its total assets more than five times between March 2000 and March 2010, i.e., US$250 billion to more than US$1.3 trillion. Also CAGR growth of 18 percent has been recorded in this industry as compared to country's average GDP growth of 7.2 percent during the same period. The commercial banking assets to GDP ratio has increased to nearly 100 percent while the ratio of bank's business to GDP has recorded nearly twofold, from 68 percent to 135 percent. The overall development has been lucrative with enhancement in banking industry efficiency and productivity.

In the banking world, the Indian banking industry is measured as a flourishing and the secured one. Our banking industry is a mixture of public, private and foreign ownerships of which the major dominance of commercial banks can be easily found in Indian banking, although the co-operative and regional rural banks have little business segment.

Literature Review

Joshi (1986) in his study of profitability and trends in profits of commercial banks nationalization of all scheduled commercial banks operating in India relating to the period 1970-1982. The factors leading to the deterioration of profitability are also highlighted.

Minakshi and Kaur (1990) quantitatively measure the impact of several monetary policy instruments on the profitability of commercial banks. The empirical study proves that pre-liberalization banking being highly regulated and controlled industry, has suffered a lot so far as profitability concerned. The reserve requirements ratio and bank rates has played a significant role in having a negative impact on the bank's profitability.

Ojha (1992) measure the productivity of Indian public sector commercial banks. After identifying various measures of productivity like total deposits per employee, total assets per employee, net profit per employee, total credit per employee, pre-tax profits per employee, working funds per employee, ratio of establishment expenses to working funds and net interest per employee, comparison is made with the banks at the international level. The study concludes that the Indian public sector commercial banks have comparatively very less productivity ratio in against with western countries.

The study of Raut, Kishore and Das, Santosh (1996) empirically examine and analysed the profitability trend of Indian commercial banks operating over a time-frame. The study showed the relationship among the expenses factors and earning factors which are endogenous and exogenous in nature.

Tarapore, S.S.(1990) reviews RBI's policy and its promising effect on banking sector reforms.

Misra (2003) studied for three broad sectors of each State viz, agriculture, industry and services. The study recommends improvement in the overall allocative efficiency in the post reform period for the majority of the States.

Kumar and Gulati (2008) analyse and provide that the factors like market share, profitability, and asset quality do not have any significant impact on the overall technical efficiency of Indian public sector banking industry by applying Logistic Regression Analysis, Slacks and Targets Setting Analysis and input-oriented efficiency scores.

Athanasoglou et al (2009) assesses the evolution of output and productivity in the Greek banking industry for the period 1990– 2006 by using the production approach; the intermediation approach; and the user-cost approach. The study finds that the capital and total factor productivity have also improved remarkably mainly since 1999, due to the structural changes that took place within the industry, capital (mainly IT) investments and improvement in the quality of human capital.

Das & Ghosh (2009) uses non-parametric DEA methodology, univariate analysis and determinants of inefficiency. The study indicate high levels of efficiency in costs and lower levels in profits, reflecting the importance of inefficiencies on the revenue side of banking activity, The proximate determinants of profit efficiency appear to suggest that big state-owned banks performed reasonably well and are more likely to operate at higher levels of profit efficiency. A close relationship is observed between efficiency and soundness as determined by bank's capital adequacy ratio.

II. The Impact of Deregulation on the Sector

Undeniably, liberalization in post reform era has improved the efficiency of the banking sector. Studies based on the estimation of production functions advocate that following deregulation banks moved much closer to the efficient frontier in terms of profits maximization [7].

The higher efficiency of the new private banks explains their rapid market share. These banks are highly regarded by capital markets with market capitalization to book value ratios of 3 against ratios of close to one for public-sector banks and have high capital ratios.

In 1999/2000 and 2007/08, two-thirds of the nationalized banks performed worse within the public sector than the least efficient member of the State Bank group. The dispersion of cost-efficiency narrowed markedly during the 1990s but no longer did between 2000 and 2007. Overall, the remaining cost inefficiency appears to twig mainly from a failure in asset allocation in line with their rates of return [10]. Indeed, Indian public-sector banks have been more probable to invest in government securities even after statutory requirements to hold government securities were lowered [8].

Extreme competition has also squashed intermediation margins. In the immediate aftermath of deregulation, the net interest margin plunge from 4.2% in 1992 to 3.2% in 2000. It has continued to crash since, albeit more slowly, to 2.8% by 2009. This was helped by a fall in employee compensation costs from 2.0% to 0.9% of earning assets in the decade to 2009/10, which was more marked amongst public-sector banks. While the latter were able to trim down costs through voluntary separation schemes.

Balance Sheet Quality

On average, strong balance sheet positions have been observed among Indian banks. The build-up of poor quality assets, which sparked the deregulation of the banking sector in the early 1990s, was largely absorbed in the first half of the past decade. As per International Monetary Fund (2010b) and Reserve Bank (2010b), more recently gross non-performing loans (NPLs) have been rising slightly faster than total loans, to falling to 2.58% of total loans in September 2010, against 2.39%, a year earlier, but still one quarter the level seen at the turn of the century.

In early 2010, Stress tests were conducted by the RBI [15], which suggested that NPLs would have to soar to pose a major threat to the system as a whole. A more recent set of RBI stress tests quantifies the impact of hypothetical adverse macroeconomic shocks on capital adequacy and NPL ratios [16]. The RBI test concluded that the financial system would be most sensitive to an external shock but that it could withstand a serious economic downturn.

Meeting Basel III capital adequacy regulations

On an average, Indian banks are well placed to meet the new regulatory requirements of Basel III (Table 2). This agreement calls for much higher minimum basic capital, whose definition will be restricted to common equity. The ratio of basic to risk-weighted assets rises from 2.0% to 4.5%. However, the RBI has always persisted on a higher level of common equity and, as outlined above, the banks have chosen to have a much larger common equity capital base than demanded by the RBI.

As a result, Indian banks collectively have adequate capital to ensure compliance with the requirements for equity capital and for the conservation buffer. Their existing capital is also sufficient to deal with the average level of the macro-prudential capital requirement. Considering total capital (which includes general loss reserves, undisclosed reserves and subordinated debt), Indian banks have on an average, a greater margin.

Table 2: Capital Adequacy

Norm	Existing RBI standard	Basel III Standard	Actual as of 31st March, 2010
	% of risk-weighted assets		
Common equity (after deductions)	3.6	4.5	8.8.
Conservation Buffer	0	2.5	-
Countercyclical buffer (on average)	0	1.25	-
Common equity + conservation buffer + countercyclical buffer	3.6	8.25	8.8
Tier 1 (including the buffer)	6	9.75	10
Total capital (including the buffers)	9	11.75	14.5

Source: ICRA (2010).

Indian banks are also quite well positioned relative to banks in OECD countries. Core common equity is higher relative to risk-weighted assets than in the euro area and even more so than in Japan (Table 3). The major private banks have equity levels above those seen in the United States and are even better capitalized. The same holds for leverage ratios. Indian private banks appear to have come to this conclusion, as they maintain a core equity capital ratio that is almost twice that found in public sector banks.

Resolving weak banks

Post liberalizations of the banking system, some banks were absorbed by stronger ones as they became too weak to continue to take deposits, sometimes voluntarily but mostly under instructions from the government and the RBI. Event studies show that even though the possibility of forced mergers had been anticipated, the share prices of the absorbing banks fell on the day of the announcement of the terms of merger [9]. This suggests that minority private shareholders underwent a levy as the result of the

Table 3: Various capital adequacy ratios: an international comparison

	Tier 1 common equity capital	Leverage ratio
India	8.8	19.6
Private	12.4	14.3
Public	7.7	21.4
United States	10.5	12.9
Euro area	8.0	25.4
Japan	4.1	35.1

Source: ICRA (2010) for domestic Indian banks; Institute of International Finance (2010) for other banks.

forced merger. Supporting this finding, a comparison of the efficiency of Indian banks pre and post merger indicates that in forced mergers the acquiring bank has usually been weakened by the merger [10].

III. Constraints Facing the Banking System

The RBI has the power to decide where the banks open branches. Before deregulation, it was necessary for banks to open four rural branches for every new urban branch. After deregulation, this ratio was reduced to one for one. In 2010, these restrictions were eased but restrictions on opening banks in areas with a population of above 50 000 remain in place. Moreover, the restrictions are not just nation-wide, the number of branches each bank shall have in each area is also decided by RBI. Banks are required to obtain a license for branch opening and seek permission for selling or exchanging branches with other banks. The RBI now allows banks to install ATMs in locations separate from their branches without prior permission, but reserves the right to make banks move the ATMs once it knows where they have been installed. Only banks are permitted to own ATMs. In addition, the RBI determines the maximum amount that a client of one bank can withdraw from all third-party banks. It also determines the fees that all banks can charge their client for withdrawals.

A. Portfolio Management

Severe constraints on portfolio management are also faced by Indian banks. They have to keep deposits amounting to 6% of assets with the central bank, RBI and have to invest further 23% of their assets in government securities. Finally, domestic banks have to channel 40% of net bank credit to priority sectors. Of these loans, 45% have to go to the agricultural sector and 55% to a diverse group of other sectors. For this type of lending there are no interest rate limits. However, a lower limit is set for the interest rate which is received from the official rural bank on their deposits with this institution. Lending under this category usually resulted in above-average bad loans.

B. Agriculture as a target for lending

The primary objective of policy since 1960s has been to direct credit to the agricultural sector, which was seen as crucial to the growth of the economy. However, in recent years, growth in agriculture has been much slower than in the rest of the economy (OECD, 2011). The agricultural sector does of course need adequate access to credit to supplement or make up for the absence of equity investment in farms from sources other than the farmer and his family. It is important, however, that bank lending to the agricultural sector does not become a concealed form of fiscal subsidy to farmers, through repeated debt write-offs.

C. Administered interest rates

While the interest rates of the banking system are now largely deregulated, the interest rates on small savings schemes operated by the Post Office are determined by the government and change very infrequently (most recently, in 2003). In addition, interest income on these deposits is tax-free whereas for bank deposits it is subject to income tax. Banks thus find themselves borrowing expensively when market rates are falling. Measuring the precise differential in favour of small savings schemes is difficult, but if one-year small savings rates are compared to the three-month interbank bid rate, then the government has paid an interest rate about 1.5 percentage points higher than the banking system – mainly resulting from the income tax advantage.

IV. New entry policies

The RBI suggested favoring doorway of small banks by keeping low absolute capital requirements and limiting bank size through insisting on a high capital adequacy ratio. The new policy would assist the entry of small banks that could perhaps serve lower-income clients more cheaply. This in turn would greatly facilitate their ability to offer savings and credit products to their customers. The prime objective of new entry is to spur competition. New investment from overseas banks should also be allowed freely. Since new banks are at added risk failing, their formation needs to be accompanied by that of a strong deposit insurance institution and by legislation that levels the playing field between deposits at public and private-sector banks. Furthermore, winding-up methods for failing banks need to change.

Rural co-operative credit societies

The co-operative credit system could have played an extremely crucial role in bringing financial services to the poor and underprivileged across rural India. However, over time it became heavily dependent on State governments. As per 2004 government report, State policy came to be premised on the view that the government should ensure adequate supply of cheap institutional credit to rural areas through co-operatives. The State took liability for strengthening the institutions, by inculcating additional capital and professional workforce. The sheer magnitude of resources and assistance channeled through the societies, makes control of decision-making and management attractive to parties in power, for accommodating their members, to influence decisions through directives, and for individual politicians to be on the management boards of the co-operatives" [20]. The National Agricultural and Rural Development Bank (NABARD) and the RBI are there to deal with the banking issues. A clearer demarcation of responsibilities is needed. First, the RBI should sell the NABARD to the government. And secondly, the regulatory and supervisory roles must be transferred to the RBI. Finally, the Registrar of Co-operative Societies should only oversee societies with zero banking or credit activities.

In 1975, Regional rural banks (RRBs) were launched in order to increase the availability of banking in rural areas. They were instituted by a sponsoring state-owned commercial bank which held 35% of their capital and the remainder was held jointly by the central government (50%) and the state government in the area of the bank served. They quickly expanded and by 1991 there were 196 banks with 14,443 branches till 2005. In this sector, it has proved extremely thorny to align the incentives of politicians, stockholders and policymakers [2]. Further progress would probably be easier to achieve if the banks were moved into the private sector.

Microfinance

To cope with high income variability, poor do need financial instruments. A study shows that low-income groups use various strategies to that effect, which involve informal financial activities [6]. These activities have a cost structure that is adapted to the local area rather than based on national salary scales. Amongst the lower-income quartile, two-thirds of borrows outside the circle of friends and family using moneylenders. While the rates of interest appear high at over 3% per month [3], the actual return was comparatively much lower due to repeated rescheduling of loans [6].The bulk of the high lending cost is due to the intense client monitoring needed to ensure that loans are repaid. Akin results are found in Pakistan [1] and in the "pay-day" money lending business in the US [18].

The power of microfinance appears to fall short of some of the poverty-reducing claims that are meant for the system. Randomized attempts in Andhra

Pradesh show slight impact of microfinance on development goals such as improved health and education and lower poverty – at least for a two-year span [4].

Mobile Phone Banking

Mobile penetration is high in India and banks are now also allowed to have a wider range of agents in present. Improvements are coming from new technology as MFIs have greatly raised financial inclusion. Mobile banking is used to make money transfers and other financial transactions without the requirement of physical presence at a bank branch or even in absenteeism of own bank account (via the use of so-called mobile wallets). The best-known example of such a service is in Kenya where the density of banks is less than one third that in India. In India, the major mobile companies are forming coalition with banks in order to gain access to enter the market.

However, with present regulations, it may be hard for mobile banking to act as a vehicle for financial inclusion despite crashing call charges and the fact that at 31% in December 2010, the penetration rate for mobile phones far outnumbers that of bank account holders (Telecom Regulatory Authority of India, 2010). Given the absence of identity cards in India, the RBI must consider reducing KYC regulations for people using mobile banking services and permit banking correspondents to open bank accounts, subject to a low use threshold for such accounts.

V. Conclusion

The Indian financial system has made substantial progress since its liberalization in the 1990s. The banking sector has been transformed by allowing a confined number of new entrants into the market. A world-class stock exchange has come out complementing a large and vibrant equity derivatives market. A considerable microfinance industry has bounce up providing credit to low-income households in a way that the banking system cannot, which helps in promoting financial inclusion. But remains of the former policy regime still remain in place. The potential financial market (government bonds) is anemic and suffers from having the holder, operator and regulator all in one and the same institution. This hinders the development of a bond-currency-derivative nexus and obstructs the transmission of monetary policy impulses. At the same time, the legal framework is dated and to a large extent relies on laws drafted long before current financial markets came into existence; moreover, and partly for that reason, there is a tendency not to rely on the rule of law but to use administrative decisions that are without appeal.

References

1. Aleem, I. (1990), “Imperfect Information, Screening and the Costs of Informal Lending: A Study of a Rural Credit Market in Pakistan”, World Bank Economic Review, Vol. 4, No. 3.
2. Baht, N. and Y. Thorat (2001), “India’s Regional Rural Banks: The Institutional Dimension of Reforms”, Journal of Micro Finance, Vol. 3, No. 1.
3. Banerjee, A. and E. Duflo (2007), “The Economic Lives of the Poor”, Journal of Economic Perspectives, Vol. 21, No. 1.
4. Banerjee, A. and E. Duflo (2010), “Giving Credit Where it is Due”, Mimeo, March, MIT.
5. Banerjee, A., E. Duflo, R. Glennerster and C. Kinnan (2010), “The Miracle of Microfinance? Evidence from a Randomized Evaluation”, mimeo, MIT.
6. Collins, D., J. Morduch, S. Rutherford and O. Ruthven (2009), Portfolios of the Poor: How the World’s Poor Live on $2 a Day, Princeton, NJ: Princeton University Press.
7. Das, D. (2009), “Role of Financial Intermediation in Promoting Productivity Growth: Evidence from India”, presentation to the Indira Gandhi Institute of Development Research, Annual Money and Finance Conference, January, Mumbai.

8. Gupta, P., K. Kochhar and S. Panth (2011), "Bank Ownership and the Effects of Financial Liberalization: Evidence from India", Working Paper 11/50, International Monetary Fund, Washington D.C.
9. Jayadev, M. and R. Sensarma (2007), "Mergers in Indian Banking: An Analysis", mimeo, Indian Institute of Management, Bangalore.
10. Kaur, P. and G. Kaur (2010), "The Impact of Mergers on the Cost Efficiency of Indian Commercial Banks", Eurasian Journal of Business and Economics, Vol. 3, No. 5.
11. Ministry of Finance (1991), Report of the Committee on the Financial System (Narasimham Committee), New Delhi, Government of India.
12. Ministry of Finance (1993a), Economic Reforms: Two Years After and the Tasks Ahead, New Delhi, Government of India.
13. Ministry of Finance (1993b), Public Sector Commercial Banks and Financial Sector Reforms: Rebuilding for a Better Future, New Delhi, Government of India.
14. Ram Mohan T. T. (2002), "Deregulation and Performance of Public Sector Banks", Economic and Political weekly", Vol. 37, pp. 393.
15. Reserve Bank of India (2010a), Financial Stability Report, March, Mumbai.
16. Reserve Bank of India (2010b), Financial Stability Report, December, Mumbai.
17. Telecom Regulatory Authority of India (2010), Consultation Paper on Quality of Service Requirements for Delivery of Basic Financial Services Using Mobile Phones, Consultation Paper No. 13.
18. Skiba, P. and J. Tobacman (2007), "The Profitability of Payday Loans", Vanderbilt University Law School, mimeo.
19. Standard and Poor (1997), "Financial System Stress and Sovereign Credit Risk", Standard and Poor's Credit Week, December 10, 1997.
20. Vaidyanathan, A. (2004), Final Report of the Task Force on the Revival of Cooperative Credit Institutions, 30 December, Ministry of Finance, New Delhi.

Optimized Digital Image Watermarking Technique using modified Difference Expansion

Tejna Patodi*

Abstract

This paper gives a modification of the existing Difference Expansion for Digital watermarking an image. Digital Watermarking hides data inside another media. In Difference Expansion, the difference between the adjacent pixels is calculated and accordingly, the payload is selected and embedded into the original pixels. In this paper, a modification is introduced into the Difference Expansion method. After calculating the difference in the pixel values, the average and difference of the pixels are interchanged. This ensures a level of encryption, improving the quality of the watermark image and preventing the thwarts. The proposed method has been checked for different image sets from Berkeley illustrating good quality of watermarked image obtained.

Key Words: Digital Watermarking, Difference Expansion, Digital Media, Data Embedding

I. Introduction

With the increase in the usage of internet on a world wide scale, the images, audio, video etc. has been made available on the internet easily.

Therefore, the protection to this multimedia has become important. This concern has caused lot of research work in the field of Digital Media protection schemes. One of the most accurate schemes is Digital Watermarking. Digital Watermarking [1] is a technique for data hiding where data or message is hidden inside another multimedia transparent to the user. This Technique differs from Encryption. In watermarking, the user is allowed to view access and analyse the media whereas in Encryption, the access to the media is denied.

The data is hidden in such a way that the receiver can decode the media and restore back the image, audio, video. Hence, the motivation is distortion-free watermarking [2]-[5].

In this paper, the modification to data embedding technique i.e. Difference Expansion for digital media is proposed. The difference between adjacent pixel values is calculated and some values are selected for Difference Expansion [6]. Along with the different values, some additional data is also sent like information regarding content restoration, date/ time (optional), and Message Authentication code. With the application of modified Difference Expansion on the watermarked media, optimization can be obtained.

II. Digital Watermarking

Digital watermarks are embedded in to the text, image, audio or video to facilitate data protection [7]-[8]. The data carried out by digital means falls into two categories: 1. Triggers (flags) that tells whether some action is to be taken 2. Identifiers that tells about the information content and distribution service. Some requirements for watermarking are[9]:

1. Security- Watermark is accessible only to the authorized parties. Only they can alter the watermarked content. To prevent unauthorized access, Encryption is the best option.
2. Transparency- The watermarking method should be transparent to the users. Only watermark detector should show up the watermark.

Tejna Patodi*
Department of IT
Delhi Technological University, New Delhi
patoditejna@gmail.com

3. Embed and Retrieval easiness-algorithm should be complex such that it can be retrieved also. More complexity can make it harder to access.
4. Robustness- Watermark must be able to withstand various attacks, whether intentional or not.

Different types of Watermark are [8]:

1. Perceptibility
   a. Visible/audible
   b. Invisible/inaudible
2. Robustness
   a. Fragile
   b. Semi Fragile
   c. Robust
3. Necessary data for Extraction
   a. Blind
   b. Informed
4. Inserted Media
   a. Text
   b. Audio
   c. Video
5. Inserting Watermark Type
   a. Noise
   b. Image
6. Processing Method
   a. Spatial
   b. Spectral

III. The Proposed Algorithm

In general, generation of watermark involves three steps:

1. Generating the mark
2. Embedding the mark
3. Creating the key file
4. Producing the watermarked image

Now, we introduce the optimization of watermark with Difference Expansion. This technique [6] makes use of the Least significant bits of neighboring pixels of an image and embedding the payload into it and original vales into it. For example, assume two values,

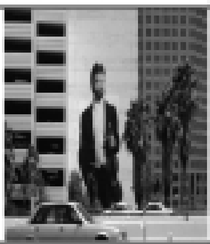
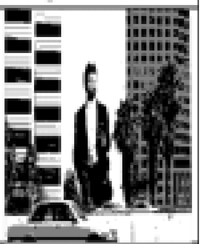
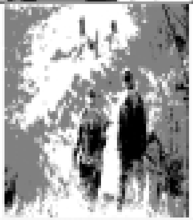
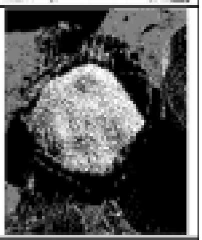
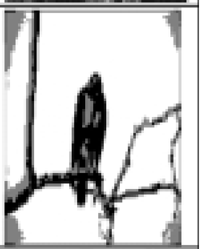
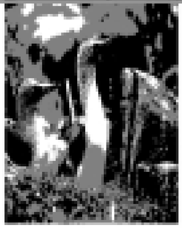
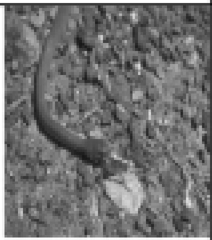
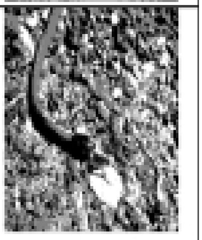
Image Identity	Original Image	Watermarked Image
119082		
170057		
58060		
42049		
103070		
175043		

Figure 1: Test Images & images after watermarking

x =206, y =201. To embed 1 bit b=1, integer average l and difference h is computed as

$$l=\left\lfloor\frac{206+201}{2}\right\rfloor=\left\lfloor\frac{407}{2}\right\rfloor=203 \qquad ------(1)$$

$$h=206-201=5 \qquad -----(2)$$

That means, $h=5=101_2$. Now, appending b=1 to h, we get $h'=1011_2$ = 11.

So, the new values become,

$$x'=203+\left\lfloor\frac{11+1}{2}\right\rfloor=209$$

$$y'=203-\left\lfloor\frac{11}{2}\right\rfloor=198$$

The reverse is also easy, in the same way.

The proposed algorithm is as follows:

1. Select the Host image (512X512 pixels) and a watermark image (128X128 pixels). Scan the image in the raster-scanning manner excluding the rightist corner and the lowest row. Calculate the bit representation of all the pixels. Let the binary representation be stored in Bimg. Take the first pixel, B_1 and B_2 and calculate the difference between the two. If LSB is 0, set payload=1, else payload=0. Similarly, the payload is calculated with all the pixels of the image.
2. Calculate the average and difference between the pixel values and interchange the two values with each other. Embed the payload and construct the new values as per equation (1) and (2) above.

Consequently the original values of the pixels remain hidden and the new values are transferred across. The original values can be regenerated at the receiver's end by the reverse of equation (1) and (2). Therefore, Watermark Extraction is exact reverse of Watermark Embedding.

IV. Results and Observations

By exchanging the values of average and difference of neighboring pixel values, we can an advanced level of encryption. By this, it becomes difficult to identify the original pixel values and hence, thwarts can be prevented and Quality is achieved.

The experiments are performed on MATLAB, 2.50GHz Intel i5 processor.

These images include Berkeley segmentation data set [10] and the popular tested images like 119802, 170057, 58060, 42049, 10370, 175043. Fig. 1 shows the original images and the images obtained after watermark. After applying the modified Difference Expansion algorithm, the results obtained are of good quality and low time complexity.

V. Conclusion

The updated Difference Expansion is introduced where an advanced level of encryption is applied on the pixels. This improves the quality of image and ensures low time complexity. The original Difference Expansion took more time to compute the results and form the watermark. The proposed algorithm gives better and accurate results for image watermarking as compared to other algorithms.

References

1. Jonathan K. Su, Frank Hartung, Bernd Girod; University of Erlangen-Nuremberg (Digital Watermarking of Text, Image and Video documents).
2. J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding—new paradigm in digital watermarking," EURASIP J. Appl. Signal Processing, vol. 2002, no. 2, pp. 185–196, Feb. 2002.
3. A.A.Zaidan, B.B.Zaidan, Fazidah Othman, "New Technique of Hidden Data in PE-File with in Unused Area One", International Journal of Computer and Electrical Engineering (IJCEE), Vol.1, No.5, ISSN: 1793- 8198, pp 669-678.
4. A.A.Zaidan, B.B.Zaidan, Fazidah Othman, "New Technique of Hidden Data in PE-File with in Unused Area One", International Journal ofComputer and Electrical Engineering (IJCEE), Vol.1, No.5, ISSN: 1793-8198, p.p 669-678.

5. A.A.Zaidan, B.B.Zaidan, Anas Majeed, "High Securing Cover-File of Hidden Data Using Statistical Technique and AES Encryption Algorithm", World Academy of Science Engineering and Technology(WASET), Vol.54, ISSN: 2070-3724, P.P 468-479.

6. Jun Tian, "Reversible Data Embedding Using a Difference Expansion" , IEEETRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 13, NO. 8, AUGUST 2003 .

7. Hamid.A.Jalab, A.A Zaidan, B.B Zaidan, "New Design for Information Hiding with in Steganography Using Distortion Techniques", International Journal of Engineering and Technology (IJET)), Vol 2, No. 1, ISSN: 1793-8236, Feb (2010), Singapore.

8. Mahmoud Elnajjar, A.A Zaidan, B.B Zaidan, Mohamed Elhadi M.Sharif and Hamdan.O.Alanazi, "Optimization Digital Image Watermarking Technique for Patent Protection", JOURNAL OF COMPUTING, VOLUME 2, ISSUE 2, FEBRUARY 2010, ISSN 2151-9617.

9. Biswajit Biswas, "Digital Watermarking for MPEG video", Tata Elxsi Engineering Creativity, pp 3-10.

10. [Online]. Available: http://www.eecs.berkeley.edu/Research/Projects/ CS/vision/bsds/s

Security Infrastructure of Cloud Computing

Sahaj Arora*
Dr. Geetali Banerji**

Abstract

Security Infrastructure is all about giving the security to the network layer which is most attacked by the "hackers", although the central attraction for security threats is increasingly shifting towards the application layer. This paper, discuss about the attacks by the attackers and how to give security to our applications in different ways.

Key Words: Cloud Security, Cyber Security, Security Infrastructure

I. Introduction

Security infrastructure, in context of cyber security, relates to the security provided to the particular organization [3]. Now-a-days, everything is now on internet whether it is playing games, chatting, sharing of information even while searching for any information, everything needs security. Think what will happen if you put no locks on your house and there is no member in there, your house will be at high risk of getting mugged. In reality thieves are the one who attacks to the house (In example) but in security world 'Hackers' do this job.

Hacker is the person who attacks over a system to take out important information. Hacker can attack in many ways and that's why we need to be aware of the security to the systems. Security infrastructure lets you know about:

- How the security internally is working.
- Why do we need to provide security to our system?
- In how many ways we can secure our systems?
- Places where high security is needed, etc.

Sahaj Arora*
Student of BCA
IITM, Janakpuri, New Delhi
asahaj1894@gmail.com

Dr. Geetali Banerji**
Professor, Department of IT
IITM, Janakpuri, New Delhi
hod.csdept@iitmjp.ac.in

II. Cloud Security

There is no such definition made on cloud computing but it refers to the safety of the cloud itself for running applications, storing data and processing transactions. This is a concern of more companies as they try to leverage the low-cost advantages of cloud security solutions without compromising corporate or customer information. Cloud computing refers to a network of computers, connected through internet, sharing the resources given by cloud providers catering to its user's needs like scalability, usability, resource requirements. The USA National Institute of Standards and Technology (NIST) defines it as follows: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Cloud computing allows users to access software applications and computing services. They might be stored off-site at locations rather than at local data centre or the user's computer. In general cloud providers offer three types of services i.e. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). There are various reasons for organizations to move towards IT solutions that include cloud computing as they are just required to pay for the resources on consumption basis. In addition, organizations can easily meet the needs of rapidly changing markets to ensure that they are always on the leading edge for their consumers. The cloud or the network specially the public one, raises many security concerns for companies that are accustomed to hosting their data and applications within their own four walls. Within a traditional internal IT security infrastructure, it is comparatively easy to ensure proper security mechanisms such as authentication, authorization, non repudiation, privacy, confidentiality. These mechanisms must be accompanied by proper security policies and processes that are followed by employees [4]-[5].

III. Cloud Security Models

A. SaaS

This particular model is focused on managing access to applications. For example, policy controls may dictate that a sales person can only download particular information from sales CRM applications. For example, they are only permitted to download certain leads, within certain geographies or during local office working hours. In effect, the security officer needs to focus on establishing controls regarding users' access to applications.

B. PaaS

The primary focus of this model is on protecting data. This is especially important in the case of storage as a service. An important element to consider within PaaS is the ability to plan against the possibility of an outage from a Cloud provider. The security operation needs to consider providing for the ability to load balance across providers to ensure fail over of services in the event of an outage. Another key consideration should be the ability to encrypt the data whilst stored on a third-party platform and to be aware of the regulatory issues that may apply to data availability in different geographies.

C. IaaS

In this model the focus is on managing virtual machines. The CSOs priority is to overlay a governance framework to enable the organization to put controls in place regarding how virtual machines are created and spun down thus avoiding uncontrolled access and potential costly wastage.

IV. Cloud Security Checklist

The following list a checklist of cloud security[1]:

- Continuous web application scanning to detect vulnerabilities.
- Boot and data volume encryption with external key management to protect data at rest and keep control of the keys.
- SSL certificates to protect data-in-motion with encryption.
- Intrusion Prevention with virtual patching to protect against vulnerabilities even before you patches.

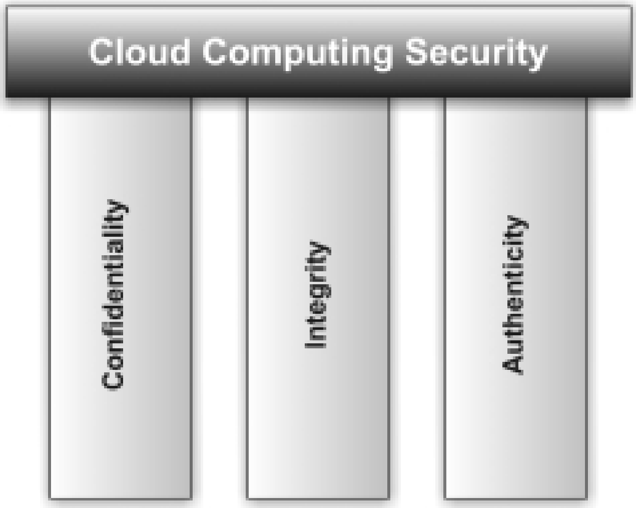


Figure 1: Cloud Computing Security Issues

- Host-based bi-directional firewall to prevent unauthorized outbound communication – with logging and alerting capabilities to make it easier to manage.
- File integrity monitoring to catch unauthorized system component changes.
- Anti-malware with web reputation to protect against viruses and malicious URLs.

V. Cloud Security Issues

The three issues of cloud computing security are [2]:

A. Availability

Availability is the attestation that data will be available to the user in a perpetual manner irrespective of location of the user. It is ensured by: fault tolerance, network security and authentication.

B. Integrity

Integrity is the assurance that the data sent is same as the message received and it is not altered in between. Integrity is infringed if the transmitted message is not same as received one. It is ensured by: Firewalls and intrusion detection.

C. Confidentiality

Cloud computing can offer many advantages when it comes to security. Because security is such a 'hot button' issue, in many cases cloud computing solutions over compensate for security risks, sometimes dedicating entire security teams to monitor the system. Security elements are also often able to be delivered in real time. Furthermore, data is monitored in real time due to the nature of cloud computing.

Below is a list of the security advantages and challenges associated with cloud computing:

Table I. Advantages and Challenges of Security

Advantages	Challenges
Dedicated Security Team	Data dispersal and international privacy laws
Greater Investment in Security Infrastructure	Quality of service guarantees
Fault Tolerance and Reliability	Dependence on secure hypervisors
Greater Resiliency	Attraction to hackers (high value target)
Hypervisor Protection Against Network Attacks	Security of virtual OSs in the cloud
Reduction of Assessment and Authorization Activities (FedRAMP)	Possibility for massive outages
Simplification of Compliance Analysis	Encryption needs for cloud computing
Data Held by Unbiased Party (cloud vendor assertion)	Encrypting access to the cloud resource control interface
Low-Cost Disaster Recovery and Data Storage Solutions	Encrypting administrative access to OS instances
On-Demand Security Controls	Encrypting access to applications
Real-Time Detection of System Tampering	Encrypting application data at rest
Rapid Re-Constitution of Services	Public cloud vs internal cloud security
	Data ownership issues
	Need for isolation management
	Multi-tenancy
	Logging challenges
	Data retention issues
	Exposure of data to foreign government and data subpoenas

VI. Conclusions

Security Infrastructure of Cloud Computing has become one of the top most concerns in Cyber World. It becomes very important for cyber citizen to be aware as well to be secure. This paper throws a light on cloud computing, its models, measures to be taken for securing oneself in cyber world. It also discusses about the issues, advantages and challenges to face for getting secure infrastructure.

References

1. Security Guidelines for Critical Areas of Focus in Cloud Computing. Cloud Security Alliance.http://www.cloudsecurityalliance.org/guidance/csaguide.pdf 13.
2. Vouk, M. A. (2008). “Cloud Computing – Issues, Research and Implementations”. In Proceedings of the 30th International Conference on Information Technology Interfaces (ITI’08), pp. 31-40, Cavtat, Croatia,June 2008
3. Why Cloud Computing Needs Security. Describes the challenges that consolidated cloud computing sites pose for security. http://gigaom.com/2008/06/10/the-amazon-outage-fortresses-in-the-clouds/17
4. Alexa Huth, James Cebula, “The Basics of Cloud Computing, United State Computer Emergency Readiness Team (US-CERT)
5. Grace Walker, Cloud Computing Fundamentals – A different way to deliver computer resources, IBM.

Cyber Crime and its Types

Nalci*
Charul Nigam**

Abstract

As we all know that Cyber crime has been one of the common practices made by the computer expert. Cyber crime is that activities made by the people for destroying organization network, stealing others valuable data, documents, hacking bank account and transferring money to their own. This paper gives detailed information regarding Cyber crime, its types, including prevention to deal effectively with Cyber crime.

Key Words: Cyber Crime, Drug Trafficking, Hacking

I. Introduction

Criminal activities carried out by means of computers or the Internet. Computer crime, or Cyber crime, refers to any crime that involves a computer and a network [1]. The computer may have been used in the commission of a crime, or it may be the target.Cyber crime is the latest and the most complicated problem in the cyber world. "Cyber crime is a big problem in which either the computer is an object or subject of the conduct constituting crime". "Any criminal activity that uses a computer either as an instrumentality or target it cause a problem called Cyber crime". Definition of Cyber crime may be "unlawful acts wherein the computer is either a tool or target or both"**.** The computer may be used as a tool in the following kinds of activity- financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking. The computer may however be target for unlawful acts in the following cases- unauthorized access to computer and computer system and also computer networks, theft of information contained in the electronic form, e-mail bombing, logic bombs, Trojan attacks, internet time thefts, web jacking, theft of computer system, physically damaging the computer system. In Cyber crime when an attacker wants to hack data from a particular system across the internet network is called Cyber crime. The computer can be considered as the tool rather than the target. Cyber crime is a crime that involves a computer and a network. Example of crime is Scams, theft etc.

A. History of Cyber Crime

When computers and networks came into being in the 1990s, hacking was done basically to get more information about the systems. Hackers even competed against one another to win the tag of the best hacker. As a result, many networks were affected, hacking started making networks and systems slow. As hackers became more skilful, they started using their knowledge and expertise to gain benefit by exploiting and victimizing others [7].

II. Types of Cyber Crime

When any crime is committed over the Internet it is referred to as a Cyber crime [4]. There are many types of Cyber crimes and the most common ones are explained below:

A. Hacking:

This is a type of crime wherein a person's computer is broken into so that his personal or sensitive

Nalci*
Student of BCA
IITM, Janakpuri, New Delhi
nalci.kumari@gmail.com

Charul Nigam**
Assistant Professor, Department of IT
IITM, Janakpuri, New Delhi
charul.nigam@gmail.com

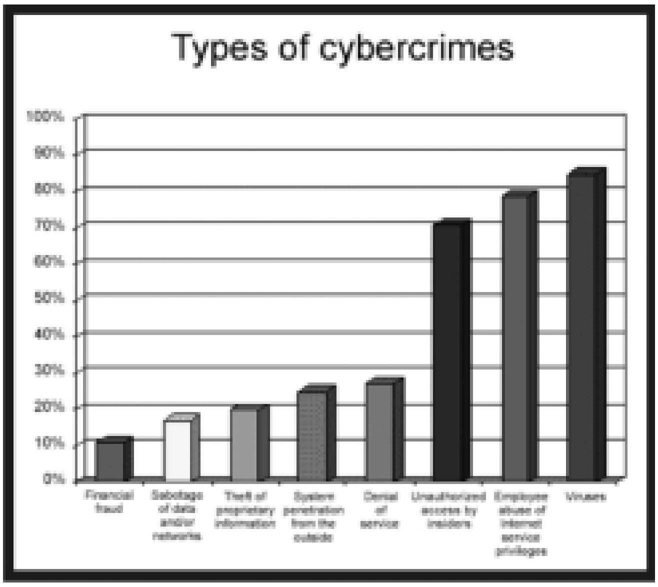


Figure 1: Types of Cyber Crime Statistics

information can be accessed. In hacking, the criminal uses software to enter a person's computer and the person may not be aware that his computer is being accessed from a person that is hacker. Hacker is a person or human being who tries to break into computer systems. Hacker is a clever programmer who might be able to access your personal details. He will be able to misuse your personal detail or any other secret information.

B. Theft:

Theft is the taking of another person's property without that person's permission with the objective to steal the rightful owner of it. This crime occurs when a person downloads music, movies, games and software.

C. Malicious Software:

These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data in the system.

D. Child Abuse:

This is also a type of Cyber crime; in this kind of crime criminals solicit minors via chat rooms for the purpose of child pornography.

E. Harassment:

Harassment is the Cyber crime most commonly encountered in chat rooms or through newsgroups comments directed towards a specific individual e.g. on gender, race, religion & nationality.

F. Drug Trafficking:

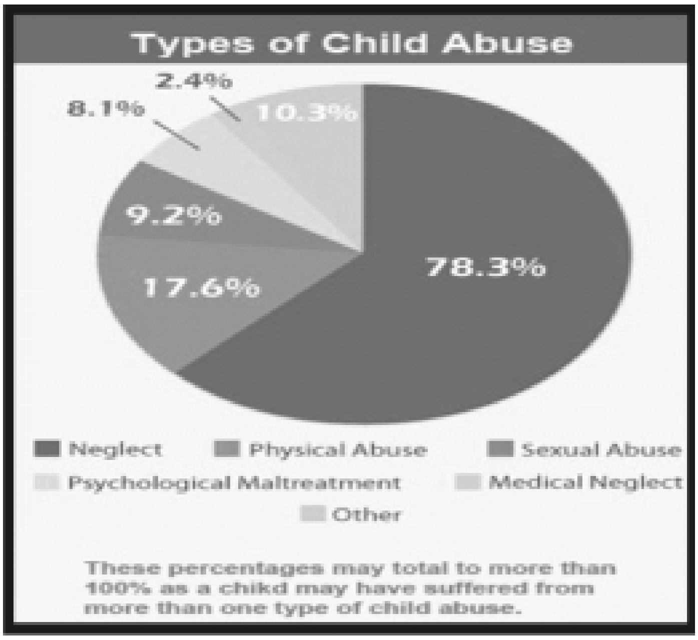
Drug traffickers use the Internet as a medium for trading their illegal substances or any useful information and data by sending out email & other Internet technology. Most of the drug traffickers can be found arranging their illegal deals at internet cafes.

G. Cyber Terrorism:

Due to the increase in cyber terrorism, hacker can crash the official websites and they can also steal the information from the government official website.

III. Impact of Cyber Crime

The impact of Cyber crime is financial losses, theft of intellectual property and loss of customer confidence and trust. The first step of Cyber crime is too aware and gives training to all the peoples, citizen, consumer and employee and students as well. They all should be aware of these attacks and they can take action to protect their own information and personal details.



Types of Child Abuse

These percentages may total to more than 100% as a chikd may have suffered from more than one type of child abuse.

Figure 2: Types of Child Abuse Statistics

IV. Conclusion and Future Scope

This paper discuss about the current scenario of Cyber crime. How it has become a problem in our country. It also becomes very important to be aware of the security risks of Cyber crime that can be done on the internet side. We have to know about Cyber crimes that now become a problem to us. The internet can open the door to a world of entertainment and education, but you could be at risk if you don't know how to use it safely. "If you ever feel uncomfortable, tell your parents or a trusted adult."

References

1. searchsecurity.techtarget.com/definition/cybercrime
2. infosecawareness.in/cyber-crime-cells-in-india
3. www.cyberlawsindia.net/cases.html
4. www.naavi.org/pati/pati_cybercrimes_dec03.html
5. http://www.crossdomainsolutions.com/cyber-crime/
6. http://drmzz.blogspot.in/2013/07/abstract-of-cyber-crime.html
7. www.indiancybersecurity.com/.../8_history_of_cyber_law_in_india.html

Rule Extraction in Data Mining Techniques

Pramod Kumar Soni*
Govind Murari Upadhyay**

Abstract

In this paper, the concept of data mining is summarized and its significance towards its methodologies is illustrated. The data mining based on Neural Network and Genetic Algorithm is researched in detail and the key technology and ways to achieve the data mining on Neural Network and Genetic Algorithm are also surveyed. This paper also conducts a formal review of the area of rule extraction from ANN and GA.

Key Words: Data Mining, Neural Network, Genetic Algorithm, Rule Extraction

I. Introduction

Data mining refers to extracting or mining the knowledge from large amount of data. The term data mining is appropriately named as 'Knowledge mining from data' or "Knowledge Mining". Data collection and storage technology has made it possible for organizations to accumulate huge amounts of data at lower cost. Exploiting this stored data, in order to extract useful and actionable information, is the overall goal of the generic activity termed as data mining. The following definition is given: Data mining is the process of exploration and analysis, by automatic or semiautomatic means, of large quantities of data in order to discover meaningful patterns and rules. In [1], the following definition is given:

Data mining is the process of exploration and analysis, by automatic or semiautomatic means, of large quantities of data in order to discover meaningful patterns and rules Data mining is an interdisciplinary subfield of computer science which involves computational process of large data sets' patterns discovery. The goal of this advanced analysis process is to extract information from a data set and transform it into an understandable structure for further use. The methods used are at the juncture of artificial intelligence, machine learning, statistics, database systems and business intelligence.

Data Mining is about solving problems by analyzing data already present in databases [2]. Data mining is also stated as essential process where intelligent methods are applied in order to extract the data patterns.

Data mining consists of five major elements:

- Extract, transform, and load transaction data onto the data warehouse system.
- Store and manage the data in a multidimensional database system.
- Provide data access to business analysts and information technology professionals.
- Analyze the data by application software.

Present the data in a useful format, such as a graph or table. Data mining functionalities are used to specify the kind of patterns to be found in data mining tasks. Data mining tasks can be classified in two categories-descriptive and predictive. Descriptive mining tasks characterize the general properties of the data in database. Predictive mining tasks perform inference on the current data in order to make

Pramod Kumar Soni*
Asst. Professor, Department of IT
IITM, Janakpuri, New Delhi
Pramod.soni0007@gmail.com

Govind Murari Upadhyay**
Asst. Professor, Department of IT
IITM, Janakpuri, New Delhi
Govindmurari.upadhyay@gmail.com

predictions. The purpose of a data mining effort is normally either to create a descriptive model or a predictive model. A descriptive model presents, in concise form, the main characteristics of the data set. It is essentially a summary of the data points, making it possible to study important aspects of the data set. Typically, a descriptive model is found through undirected data mining; i.e. a bottom-up approach where the data "speaks for itself". Undirected data mining finds patterns in the data set but leaves the interpretation of the patterns to the data miner. The purpose of a predictive model is to allow the data miner to predict an unknown (often future) value of a specific variable; the target variable. If the target value is one of a predefined number of discrete (class) labels, the data mining task is called classification. If the target variable is a real number, the task is regression.

The predictive model is thus created from given known values of variables, possibly including previous values of the target variable. The training data consists of pairs of measurements each consisting of an input vector x (i) with a corresponding target value y(i). The predictive model is an estimation of the function y=f(x; q) able to predict a value y, given an input vector of measured values x and a set of estimated parameters q for the model f. The process of finding the best q values is the core of the data mining technique [3].

At the core of the data mining process is the use of a data mining technique. Some data mining techniques directly obtain the information by performing a descriptive partitioning of the data. More often, however, data mining techniques utilize stored data in order to build predictive models. From a general perspective, there is strong agreement among both researchers and executives about the criteria that all data mining techniques must meet. Most importantly, the techniques should have high performance. This criterion is, for predictive modeling, understood to mean that the technique should produce models that will generalize well, i.e. models having high accuracy when performing predictions based on novel data.

Classification and prediction are two forms of data analysis that can be used to extract models describing the important data classes or to predict the future data trends. Such analysis can help to provide us with a better understanding of the data at large. The classification predicts categorical (discrete, unordered) labels, prediction model, and continuous valued function.

II. Methodologies of Data Mining

A. Neural Network

Neural Network or an artificial neural network is a biological system that detects patterns and makes predictions. The greatest breakthroughs in neural

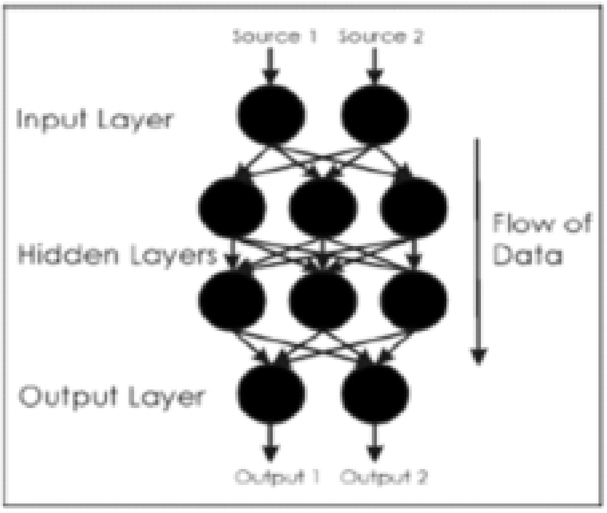


Fig. 1: Neural Network with hidden layers

network in recent years are in their application to real world problems like customer response prediction, fraud detection etc. Data mining techniques such as neural networks are able to model the relationships that exist in data collections and can therefore be used for increasing business intelligence across a variety of business applications [4]. This powerful predictive modeling technique creates very complex models that are really difficult to understand by even experts. Neural Networks are used in a variety of applications. It is shown in fig.1. Artificial neural network have become a powerful tool in tasks like pattern recognition, decision problem or predication applications. It is one of the newest signals processing technology. ANN is an adaptive, non linear system that learns to perform a function from data and that adaptive phase is normally training phase where system parameter is change during operations. After the training is complete the parameter are fixed. If there are lots of data and problem is poorly understandable then using ANN model is accurate, the non linear characteristics of ANN provide it lots of flexibility to achieve input output map. Artificial Neural Networks, provide user the capabilities to select the network topology, performance parameter, learning rule and stopping criteria.

B. Decision Trees

A decision tree is a flow chart like structure where each node denotes a test on an attribute value, each branch represents an outcome of the test and tree leaves represent classes or class distribution. A decision tree is a predictive model most often used for classification. Decision trees partition the input space into cells where each cell belongs to one class. The partitioning is represented as a sequence of tests. Each interior node in the decision tree tests the value of some input variable, and the branches from the node are labeled with the possible results of the test. The leaf nodes represent the cells and specify the class to return if that leaf node is reached. The classification of a specific input instance is thus performed by starting at the root node and, depending on the results of the tests, following the appropriate branches until a leaf node is reached [5].Decision tree is represented in figure 2.

Decision tree is a predictive model that can be viewed as a tree where each branch of the tree is a classification question and leaves represent the partition of the data set with their classification. The author defines a Decision Tree as a schematic tree-shaped diagram used to determine a course of action or show a statistical probability [6]. Decision trees can be viewed from the business perspective as creating a segmentation of the original data set. Thus marketing managers make use of segmentation of customers, products and sales region for predictive study. These predictive segments derived from the decision tree also come with a description of the characteristics that define the predictive segment. Because of their tree structure and skill to easily generate rules the method is a favoured technique for building understandable models.

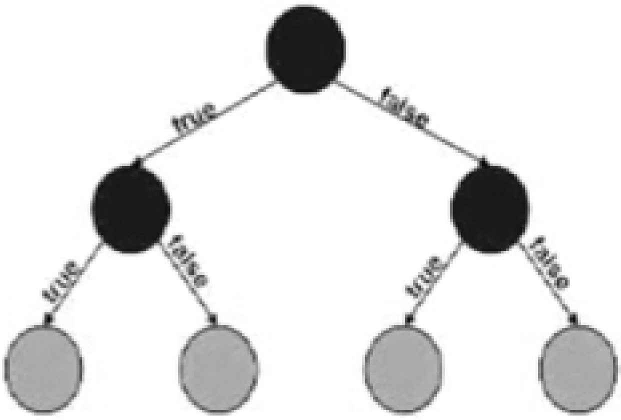


Fig. 2: Decision tree

C. Genetic Algorithm

Genetic Algorithm attempt to incorporate ideas of natural evaluation The general idea behind GAs is that we can build a better solution if we somehow combine the "good" parts of other solutions (schemata theory), just like nature does by combining the DNA of living beings [7]. Genetic Algorithm is basically used as a problem solving strategy in order to provide with a optimal solution. They are the best way to solve the problem for which little is known. They will work well in any search space because they form a very general algorithm. The only thing to be known is what the particular situation is where the solution performs very well, and a genetic algorithm will generate a high quality solution. Genetic algorithms use the principles of selection and evolution to produce several solutions to a given problem. In fig. 3

Genetic algorithms (GAs) [8] are based on a biological applications; it depends on theory of evolution. When GAs are used for problem solving, the solution has three distinct stages:

- The solutions of the problem are encoded into representations that support the necessary variation and selection operations; these representations, are called chromosomes, are as simple as bit strings.
- A fitness function judges which solutions are the "best" life forms, that is, most appropriate for the solution of the particular problem. These individuals are favored in survival and reproduction, thus giving rise to generation.
- Crossover and mutation produce new gene individuals by recombining features of their parents. Eventually a generation of individuals will be interpreted back to the original problem domain and the fit individual represents the solution.

D. Rule Extraction

The taxonomy of Rule extraction contains three main criteria for evaluation of algorithms: the scope of dependency on the black box and the format of the extract description. The first dimension concerns with the scope of use of an algorithm either regression or dimension focuses on the extraction algorithm on the underlying black-box: independent algorithms. The third criterion focuses on the obtained rules that

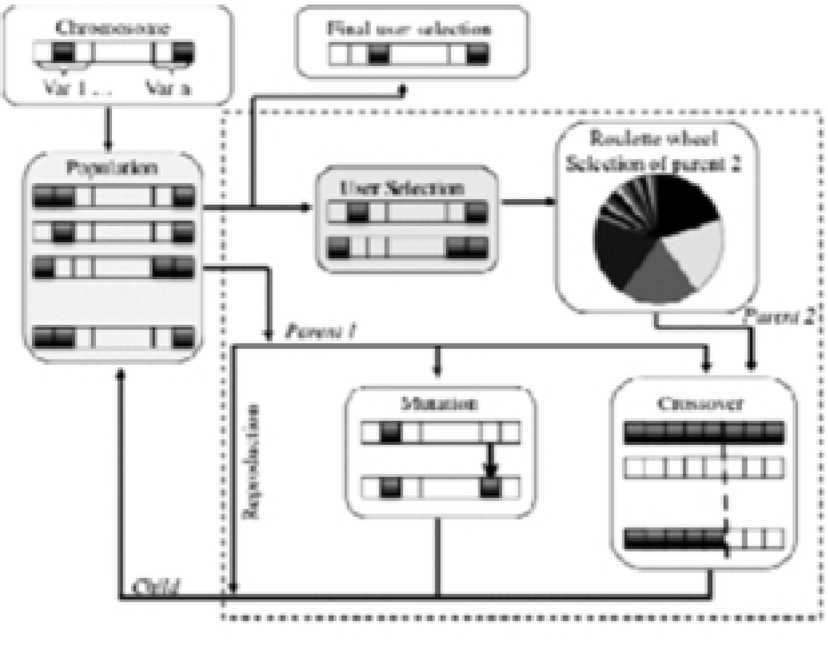


Fig. 3: Structural view of Genetic Algorithm

might be worthwhile algorithms. Besides this taxonomy the evaluation criteria appears in almost all of these surveys rule; Scalability of the algorithm; consistency [9].

Generally a rule consists of two values. A left hand antecedent and a right hand consequent. An antecedent can have one or multiple conditions which must be true in order for the consequent to be true for a given accuracy whereas a consequent is just a single condition. Thus mining a rule from a database antecedent, consequent, accuracy, and coverage are all targeted. Sometimes "interestingness" is also targeted used for ranking. The situation occurs when rules have high coverage and accuracy but deviate from standards. It is also essential to note that even though patterns are produced from rule induction system, they all not necessarily mean that a left hand side ("if "part) should cause the right hand side ("then") part to happen. Once rules are created and interestingness is checked they can be used for predictions in business where each rule performs a prediction keeping a consequent as the target and the accuracy of the rule as the accuracy of the prediction which gives an opportunity for the overall system to improve and perform well.

For data mining domain, the lack of explanation facilities seems to be a serious drawback as it produce opaque model, along with that accuracy is also required. To remove the deficiency of ANN and decision tree, we suggest rule extraction to produce a transparent model with accuracy. It is becoming increasingly apparent that the absence of an explanation capability in ANN systems limits the realizations of the full potential of such systems, and it is this precise deficiency that the rule extraction process seeks to reduce. Experience from the field of expert systems has shown that an explanation capability is a vital function provided by symbolic AI systems.

In particularly, the ability to generate even limited explanations is absolutely crucial for user acceptance of such systems. Since the purpose of most data mining systems is to support decision making, the need for explanation facilities in these systems is apparent. But many systems must be regarded as black boxes; i.e. they are opaque to the user.

For the rules to be useful there are two pieces of information that must be supplied as well as the actual rule:

- Accuracy - How often is the rule correct?
- Coverage - How often does the rule apply?

Only because the pattern in the data base is expressed as rule, it does not mean that it is true always. So like data mining algorithms it is equally important to identify and make obvious the uncertainty in the rule. This is called accuracy. The coverage of the rule means how much of the database it "covers" or applies to.

Craven and Shavlik in there paper [11] listed five criteria for rule extraction, and they are as follows:

- Comprehensibility: The extent to which extracted representations are humanly comprehensible.
- Fidelity: The extent to which extracted representations accurately model the networks from which they were extracted.
- Accuracy: The ability of extracted representations to make accurate predictions on previously unseen cases.
- Scalability: The ability of the method to scale to networks with large input spaces and large numbers of weighted connections.
- Generality: The extent to which the method requires special training.

III. Conclusions

If the conception of computer algorithms being based on the evolutionary of the organism is surprising, the extensiveness with which these methodologies are applied in so many areas is no less than astonishing. At present data mining is a new and important area of research and ANN itself is a very suitable for solving the problems of data mining because its characteristics of good robustness, self-organizing adaptive, parallel processing, distributed storage and high degree of fault tolerance. The commercial, educational and scientific applications are increasingly dependent on these methodologies.

References

1. Xingquan Zhu, Ian Davidson, “Knowledge Discovery and Data Mining: Challenges and Realities”, ISBN 978-1-59904-252, Hershey, New York, 2007.

2. Joseph, Zernik, “Data Mining as a Civic Duty – Online Public Prisoners Registration Systems”, International Journal on Social Media: Monitoring. Measurement, Mining, vol. - 1, no.-1, pp. 84-96, September2010.

3. Zhao, Kaidi and Liu, Bing, Tirpark, Thomas M. and Weimin, Xiao,”A Visual Data Mining Framework for Convenient Identification of Useful Knowledge”, ICDM ’05 Proceedings of the Fifth IEEE International Conference on Data Mining, vol.-1, no.-1,pp.- 530- 537,Dec 2005.

4. R. Andrews, J. Diederich, A. B. Tickle,” A survey and critique of techniques for extracting rules from trained artificial neural networks”, Knowledge-Based Systems,vol.- 8,no.-6, pp.-378-389,1995.

5. Lior Rokach and Oded Maimon,”Data Mining with Decision Trees: Theory and Applications(Series in Machine Perception and Artificial Intelligence)”, ISBN: 981-2771-719, World Scientific Publishing Company, 2008.

6. Venkatadri.M and Lokanatha C. Reddy ,”A comparative study on decision tree classification algorithm in data mining” , International Journal Of Computer Applications In Engineering ,Technology And Sciences (IJCAETS), Vol.- 2 ,no.- 2 , pp. 24- 29 , Sept 2010.

7. AnkitaAgarwal,”Secret Key Encryption algorithm using genetic algorithm”, vol.-2, no.-4, ISSN: 2277 128X, IJARCSSE, pp. 57-61, April 2012.

8. Li Lin, Longbing Cao, Jiaqi Wang, Chengqi Zhang, “The Applications of Genetic Algorithms in Stock Market Data Mining Optimisation”, Proceedings of Fifth International Conference on Data Mining, Text Mining and their Business Applications,pp- 593-604,sept 2005.

9. Fu Xiuju and Lipo Wang “Rule Extraction from an RBF Classifier Based on Class-Dependent Features “, ISNN’05 Proceedings of the Second international conference on Advances in Neural Networks ,vol.-1,pp.-682-687,2005.

10. H. Johan, B. Bart and V. Jan, “Using Rule Extraction to Improve the Comprehensibility of Predictive Models”. In Open Access publication from Katholieke Universiteit Leuven, pp.1-56, 2006

11. M. Craven and J. Shavlik, “Learning rules using ANN “, Proceeding of 10th International Conference on MachineLearning, pp.-73-80, July 1993.

Deep Web: The Susceptible Network

Akshat Kapoor*
Raman Solanki**

Abstract

The Deep Web, Deep Net, Invisible Web or Hidden Web are search terms referring to the content on the World Wide Web that is not indexed by standard search engines. Recent advances of internet over the two decades of more than two billion users. The expansion resulted in developing applications for the cyber world, however there are various applications not accessible. This hidden web over the past years been used as an invariable tool and is not regulated or monitored. The future of the deep web is still uncertain.

Key Words: Deep Web, dark Web, TOR network

Introduction

Deep Web can be delineated as an ambiguous description of the internet not necessarily accessible to search engines. Dark web and the Deep web are used interchangeably however they are not same. Dark web refers to any web page that has been cancelled to hide in the plain sights or reside within a separate but public layer of standard internet. The internet is constructed around web pages that refer other web pages, if you have a destination web page which has no inbound links you have cancelled that page and it cannot be found by users or search engines. Virtual Private Networks (VPN) are another outlook of the crepuscular web that exists within the public internet which require additional software to access.TOR (The Onion Router) is a vivid example. Hidden within the public web is an entire network of different content which can only be accessed using the TOR network. While personal freedom and privacy are admirable goal of the TOR network the ability to travel over the internet with complete anonymity nurtures a platform ripe for what is considered illegal activity in countries like India and China. Dynamic web pages, blocked sites, unlinked sites, private sites, non HTML /-contextual/-scripted contents and limited access networks is not indexed by known search engines like Bing and AOL. The surface web which people use routinely consist of data that search engine can find and then offer a in response to queries, this is only the tip of the iceberg. A traditional search engine sees about 0.3% of the information that is available [1]. Much of the rest is embedded which is called the Deep Web also known as 'Hidden Web', 'Invisible Web', and the 'Undernet'. Most of the content located in the deep web exists in the websites that require a search that is not implicitly illicit. Dark web is a very dynamic place; an online forum can be at a specific URL one day and gone the next day. The naming and addressing schemes in the dark web often change this means that the information be harvested two weeks ago is no longer relevant today.

Dark Web

The dark Web is the sector of the deep Web that has been purposely hidden and is inaccessible through standard Web browsers. Dark Web sites serve as a platform for anonymity as essential for Internet users, since they not only provide safety from unauthorized users , but also usually include encryption to prevent monitoring.

Akshat Kapoor*
B.Tech; Apprentice
IPEC, U.P.-201010
akshat1011@rediffmail.com

Raman Solanki**
BCA,
IITM, Janakpuri, New Delhi-110058
solanki_raman@aol.com

A comparatively known source for content that stays on the dark Web is found in the TOR network. The Tor network is a group of operated servers who have volunteered to allows people to upgrade their privacy and security on the Internet that can only be accessed with a special Web browser. First came up as The Onion Routing (TOR) project in 2002 by the US Naval Research Laboratory, it was a method for online communication anonymously. Another network, I2P, provides many of the same features that Tor does. Though, I2P was designed to make a network within the Internet, with traffic staying contained in its borders. Tor provides superior anonymous access to the open Internet and I2P provides a more robust and reliable "network within the network" [2][4][10].

How to access dark web?

- One widely used is TOR browser is one way to access dark web sites as they are in .onion extension that cannot be accessed by normal browsers so TOR Browser is used for browsing the web to withhold some information about your computer's configuration.
- Tor2web created by Aaron Swartz and Virgil Griffith. It is bridge between public internet and untraceable sites. However it won't be anonymous in the way they would be if they used Tor [7].

How does TOR network works?

TOR protects you against a familiar form of Internet surveillance that is traffic analysis. Traffic analysis can be used to deduce who is interacting to whom over a public network. As the source and destination of your Internet traffic is known this allows others to track your behavior and interests. TOR distributes your transactions over several places on the Internet that reduces risks of both simple and complex traffic analysis, so no single point can link you to your destination. This is similar to adopting a swirly, hard-to-follow route in order to get rid of somebody who is tailing you and then systematically erasing your footprints. Rather than taking a direct route from source's database to destination, data packets on the TOR network take's a random pathway through many relays that cover's your tracks so that no observer at any single point can tell from where the data came or where it's going to create a private network pathway. In TOR, the user's software incrementally produces a circuit of encrypted connections by relaying on the network. The circuit is elongated one bounce at a time, and each relay along the way knows only which relay gave it data and which relay it is giving data to. No individual relay can ever know the complete path that a data packet has withdrawn. The client accommodates a separate set of encryption keys for each bounce along the circuit to ensure that each bounce can't trace these connections as they pass through dark web site [6].

Languages used in Dark web

After scouting 500 domains about 310 domains used English as their main language followed by 33 domain used Russian and 157 domain used other languages. That is around 62% domain used English.

If we take language distribution on basis of URLs Russian betas English as there are huge Russian forums not directly linked to various activities but mirrored in both tor and I2P .[3]

Deep Web

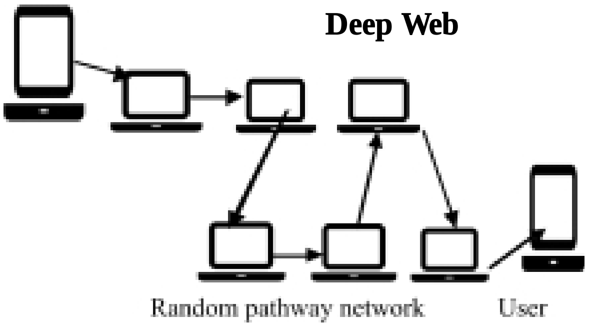


Figure 1: Working of TOR network

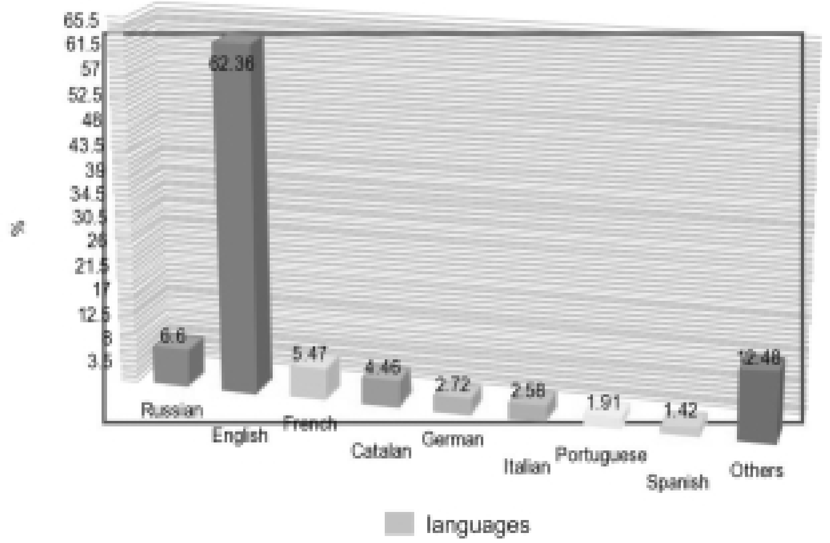


Figure 2: Popular languages based on the number of domains containing pages that use them

The deep web is that part of the internet not accessible to link-crawling search engines like Google; the only way the user can access this portion of the internet by typing a directed query into a web search form thereby retrieving the content from the database that is not associated. The only way to access the Deep Web is by conducting a search that is within a particular website. Surface web search engines can lead you to website that has unstructured deep web contents. For instance if one need to search for a published article, there are certain papers that are only accessible if one has access to the Google Scholar web pages, which lead to the database connected to it, there is no other way; a person or an organization can access the database if they don't have the correct en-route to it. If you are searching for some government grants the search engine, will direct you to the website www.grats.gov, researchers can search thousands of grants by searching the database via the website search box. In this surface search engine lead users to the deep web websites where the directed query to the search box brings back Deep web content not found via the search engine.[8][9]

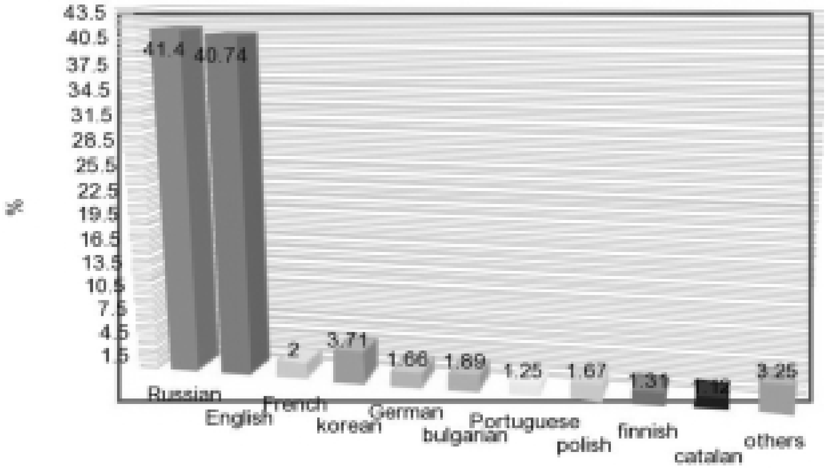


Figure 3: Popular languages based on the number of URLs with content using them

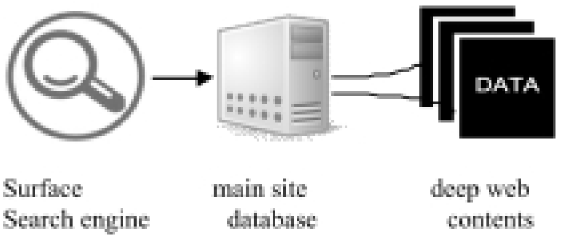


Figure 4: Deep web location

Deep web search engines

Search engines such as Google indexes over a trillion pages on the World Wide Web, but there are information on the web that common search engines are unreachable. Most of them are in databases that needed to be searched directly from the particular website. A small pocket of the deep web is filled with hyper-secret communities who gather there in order to escape identification from authorities. To discover content on the Web, search engines use web crawlers that uses a technique to follow hyperlinks. This technique is ideal for discovering resources on the surface Web but is often feckless in finding deep Web resources. For example, these crawlers do not attempt to find dynamic pages that are the result of database queries because of the infinite number of queries that are possible. It has been acclaimed that this can partially be overcome by providing links to query results, but this could unintentionally inflate the popularity for a member of the deep Web example is the PageRank. In 2005, Yahoo made a small part of the deep web searchable by the release of Yahoo Subscriptions. This search engine searches through a few subscription-only web sites. Some search tools such as Pipl are purposely designed to retrieve information from the deep web their crawlers are set to identify and interact with searchable databases that aim to provide access to deep Web content. Deep web harvesting service provided by Bright Planet .They harvest each and every big data from deep web for the client . It extracts every single word every time it accesses a web page. Plus, the Deep Web Harvester stores every single page harvested as a separate. [7][4][9]

Deep web crawling

Crawling the deep web automatically has been a major aim for some researchers these days. Raghavan and Garcia-Molina presented an architectural model in 2001 for a Deep Web crawler that used key terms provided by users or collected from the query interfaces to query a Web form and crawl into the deep Web resources. Ntoulas et al. created a hidden-Web crawler in 2005 that automatically generated meaningful queries to issue against search forms. Even though crawler generated favourable results, but the problem is far from being solved. [5][9]

Conclusions and Suggestions

Since a huge amount of useful information and data reside in the deep web; its engine has begun exploring alternate methods to crawl the deep web. Google site map protocols and mod oai are the mechanism that allows the search engine and other search parties to discover the deep web resources on particular web servers. Both mechanisms allow the web server to advertise the URL's that are accessible on them thereby allowing automatic discovery of the resources that are not linked directly to the surface web.

Another way to reach the deep web is to crawl it by subject category or vertical. Since traditional search engine have huge difficulties in crawling deep web pages and their content. Deep web search engines like CloserLookSearch, Alacra, and Northern light develop specialty engines by topic to search the deep web because these search engines are narrow in their data focus, they are built to access the specified deep web contents by topic, these engines can search dynamic or password protected databases that are otherwise close to search engines. In the near future, the deep web will be explored to all its content and further deep web will develop.

References

1. UNDERSTANDING THE DEEP WEB IN 10 MINUTES, Steve Pederson, CEO.
2. BELOW THW SURFACE EXPLORING THE DEEP WEB, Dr. Vincenzo Ciancaglini, Dr. Marco Balduzzi, Robert McArdle, and Martin Rösler Forward-Looking Threat Research Team
3. THE IMPACT OF THE DARK WEB ON INTERNET GOVERNANCE AND CYBER SECURITY,Michael Chertoff and Tobby Simon February 2015.
4. Bergman, Michael K. 2001. "White Paper: The Deep Web: Surfacing Hidden Value." http://quod.lib.umich.edu/j/jep/3336451.0007.104?view=text;rgn=main.
5. EFFICIENT, AUTOMATIC WEB RESOURCE HARVESTING Michael L. Nelson, Joan A. Smith and Ignacio Garcia del Campo.
6. TOR:OVERVIEW,https://www.torproject.org/about/overview.html.en.
7. NEW SERVICE MAKES TOR ANONYMIZED CONTENT AVAILABLE TO ALL, http://www.wired.com/2008/12/tor-anonymized/
8. INVISIBLE WEB by closurelooksearch.com.
9. INVISIBLEWEB/DEEPWEB,http://www.voodish.co.uk/articles/invisible-web-deep-web/.
10. THE INVISIBLE INTERNET PROJECT(I2P), https://geti2p.net/en/about/intro.

Electronic Governance: Defiance for India

Biny Pal Sing Gill*
Raman Solanki**

Abstract

The evolution of information and Communication Technology (ICT) has dispensed means for faster and reliable communication, revival/retrieval of data and utilization of information to its user. E-governance is basically the utilization of ICT to provide govt. departments services to the needed citizens through internet. Governments emphasize on providing its citizens efficient, convenient and transparent services through ICT. Governance is an alternative structure of the traditional view of the government. One of the ways in which E-Government hat to work is to transfer confidential information from one point to another. In developing countries like India, Where there more than 65% of its people are below the poverty line and bring up their children with very less of studies and which leads to very low literacy in the whole country in the long run, people are not even aware about the assistance of E-Governance activities and people do not utilize information and communication technology to a further extent, there exist a drastic number of problems to implement E-Governance activities. The purpose of the research paper is to highlight the main challenges related to implementation of E-Governance in India.

Key Words: Cost, different languages, e-readiness rank, e-Governance, ICT, literacy level, per capita income, separation.

1. Introduction

In late 1990s with the making of first government website came in the existence of the term E-Governance. E-Governance or 'Electronic Governance' symbolizes the use of information and Communication Technology (ICTs) for giving its citizens and corporate organizations a convenient access to the government's services and information. In other words, electronic governance involves ICTs, the internet especially, to provide its citizens, government agencies and corporate organizations government services more efficiently and with improved systems. Only the public sector is not the one which is getting the services of this network but it will also benefit the management and administration of policies and procedures in private sector.

The services of the government are given to the citizens in a better and faster way but it is not the only area it affects; it also increases the transparency between the government and its citizens. But India is a developing country and have **65%** of the population illiterate and the people who even know how to operate a computer is very low [10]. E-readiness which is the ability to use information and communication technologies to develop one's economy and wellbeing. India's rank in E-readiness is **69** with a score of **3.95** out of 10 according to Global Information Technology Report 2012, which means the rate of use of ICTs in India is at the ground level. Many Other factors like privacy and Security related to the user's personal information, digital devices etc. are also a huge area of concern for the E-Governance in India[1].

Biny Pal Sing Gill*
B.C.A, IT Department
IITM, Janak Puri, New Delhi
+91-7838813263
gill6688@gmail.com

Raman Solanki**
B.C.A, IT Department
IITM, Janak Puri, New Delhi
+91-9711012908
solanki_raman@aol.com

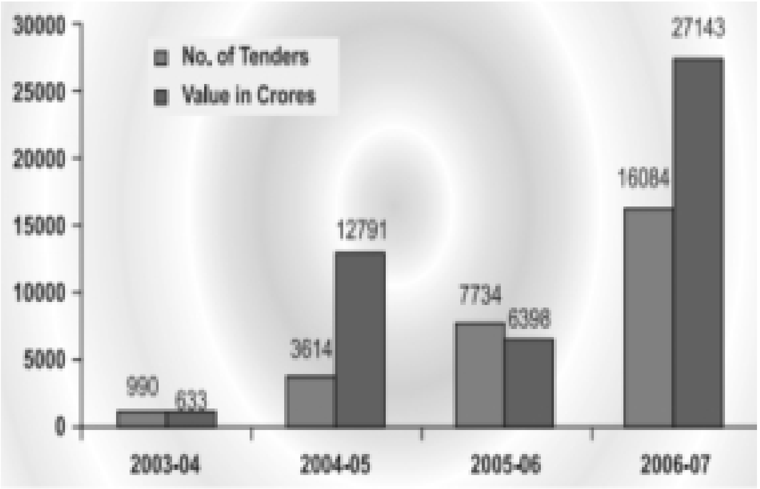


Figure 1: E-Procurement Trends

- Threat Related To The security Of the Network

  1. Natural
  2. Intentional
  3. Unintentional

2. Techniques For Security

2.1 Cryptography

2.2 Steganography and Steganalysis

If these areas are maintained and are looked up to with real depth the E-governance can become a great success [2]

3. Setbacks of E-governance

E-Governance in India has many Obstacles in its implementation and providing its services to the related corporations and citizens [2-3]. The Following Categories can justify these obstacles very well:

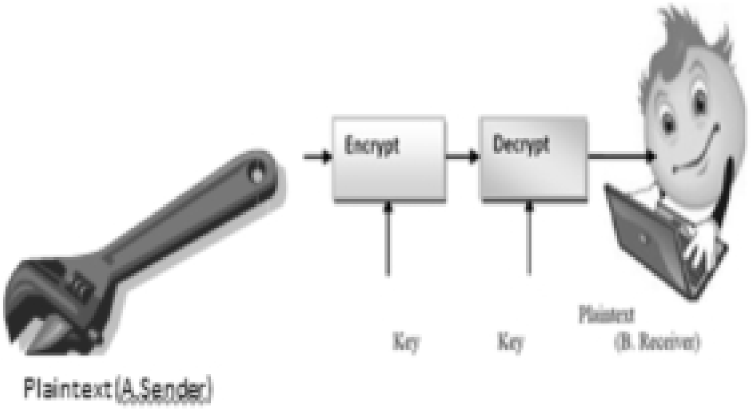


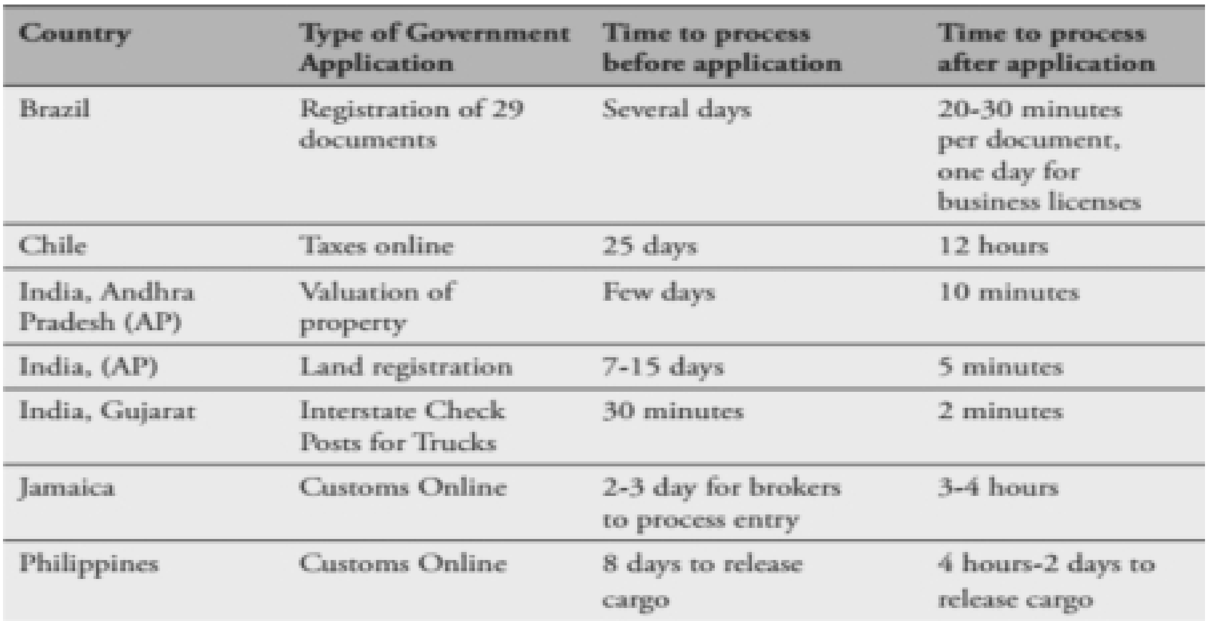
Figure 2: Cryptography

- Environmental and Social Challenges,
- Economic Challenges
- Technical Challenges [3].

These challenges are explained below:

3.1 Environmental and Social Challenges

The Variation in languages: India is a country not of many colors but of many languages as well 22in total. These languages vary form one state to another which is very amazing and drastic in the same place. This is a very serious and huge challenge for implementation



Country	Type of Government Application	Time to process before application	Time to process after application
Brazil	Registration of 29 documents	Several days	20-30 minutes per document, one day for business licenses
Chile	Taxes online	25 days	12 hours
India, Andhra Pradesh (AP)	Valuation of property	Few days	10 minutes
India, (AP)	Land registration	7-15 days	5 minutes
India, Gujarat	Interstate Check Posts for Trucks	30 minutes	2 minutes
Jamaica	Customs Online	2-3 day for brokers to process entry	3-4 hours
Philippines	Customs Online	8 days to release cargo	4 hours-2 days to release cargo

Figure 3: Benefits of E-governance in respect of time taken with applications

of E-Governance projects because of the diversity of people in context of language as e-Governance applications are written in English language mostly. And also, English is not a language that is familiar to most of the people living in India. Therefore, e-Governance applications which are to be implemented for the whole nation have to be in more than one language make it a huge challenge for the government so that the government can ensure that these may be acceptable to the users of a particular language and are of full use to them.[4]

Low Literacy: Reading, writing and having a grasp over any language is known as literacy. A person who can merely read and is real disaster in writing or properly understanding the language cannot be treated as a literate. Any formal education or minimum educational standard is not the requirement for being considered as a literate person. One of the huge obstacles in implementation of E-governance projects is that majority of the population in India Has a very low level of literacy and can even barely read or write. Illiterate people do not have the ability to access a computer how gain will access the E-governance applications; hence the projects do not get much uplift in the views of the Indian citizens [5].

Issues Regarding Awareness And Reliability Of The Government Application: User must be confident and comfortable while using the application that is developed by the government for the implementation of public administration functions via e-Government requires And that is not the case in India. He should also have the trust and faith that the application he/she is using is secured and well build which is not a every governments cup of tea. The government should and will have to provide reform and breakthrough technology to gain the trust of its people. System prevention from fraudulent transactions and the burden that extensive checks can take place on people who are honest is to be made balance between by the government or the concerned authority [6].

3.2 Economic challenges

Expenses: India is a developing country and in countries such as ours, cost is one of the most important throwbacks in the path of implementation of e-Governance where major part of the population cannot afford three meals a day and are residing very below the poverty line. Implementing e-Governance is not even the area of interest for major share of governments and politicians. Implementation, operational and evolutionary maintenance task involve a major amount of investment and time that is difficult for the current position of this country to afford. These costs must be low enough so that to guarantee a good cost/benefit ratio. [7]

Applications must Support and designed for multiple platforms: Hardware and software platforms independence is a must for E-governance applications to touch the lives of the millions and provide them the services they are looking for. Therefore, these applications should not be dependent on the hardware or software and should be able to run from one platform to another irrespective of the hardware or the software. This application should be able to have multiple administrators and should be able to provide services as per there need [8].

Regional Language: English language in not accepted in India very well and is further unknown to most of the population .The applications for E-governance will be written in English. That is why the most of the government projects which are basically related to E-governance get shut down very soon and are able to success that they were designed to achieve. Hence, all the E-governance application should be written in the native regional/local language so that it may be able to aid the local citizen and they are able to use these applications the way they are meant to be used [9].

3.3 Technical challenges

Coverage Area of The application: From day one the applications which are going to e developed for E-governance are to be designed to cover large scales and should be able to reach masses in short span of time. Every person in the country is supposed to be affected by the E-governance application because it is going to be a medium between the government and the local citizens, so the application should be launched at a large scale so that it touches every citizen in the country. [10]

Privacy and Security: Individuals personal data that he/she provides to obtain government services is the most critical obstacle in the way of E-Governance because it is to e transferred through a safe and encrypted line otherwise it can fall in wrong hands and can be used against the well-being of the person. Some effective/efficient measures must be put into place to protect the sensitive personal information of the people to gain the trust of the people and successfully implement E-governance in India. Personal information such as income, medical history etc. are very private and hence, are to be handled with care so there should be standards and lack of these standards can lead to un-effective application and no further development in the field of E-governance [11].

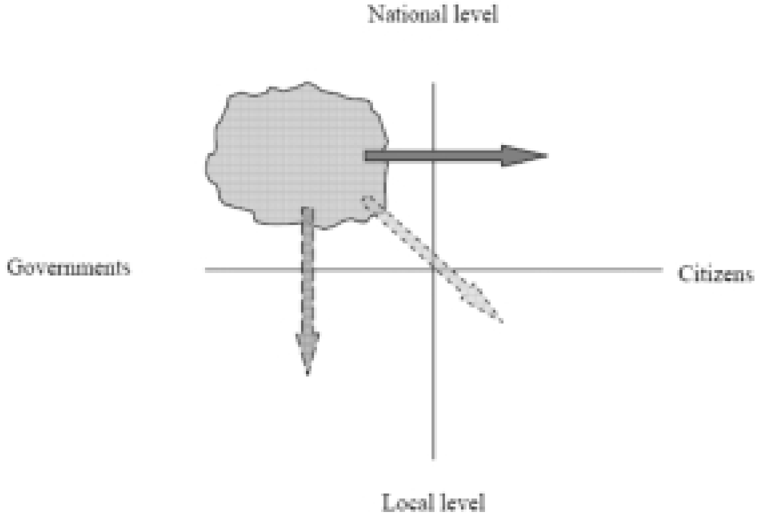


Figure-4: Different research focuses in the field of e-Government [12]

4. Conclusion

Reinventing in the way which governments interact and replies back to the citizens is what E-Governance is all about, this list also includes Industries, Government Agencies, and other stakeholders. It is about making the lives of the people/citizens easier using new ideas and enhancing the democratic process. The term e-Government if from the recent years and has a bright future is used in the right path and the research and practice is still in its starting years hence, will get a lot of breakthrough in the coming future. E-Governance is immature at the current position and many researchers are involved in a range of different research projects that are going to make this applicable in real life very easily in the coming future in different topics in the field.

As the usage of Information Technology is having a fast and great increase in awareness and has a real bright future, Indian government has taken step forward by making lots of efforts to provide services to its citizens through e-Governance. Although a lot of money is being spent on e-Governance projects by the Indian Government but still these projects are having a no success graph in all parts of India. Illiteracy and un-awareness among the people, regional language of the people who are not even familiar to English, privacy for the personal data of the people and its protection/security etc. are main hurdles which are responsible for the downwards slant in the graph for implementation of e-Governance in India. Government must make people aware about the e-Governance activities y take a brighter look at it and conducting awareness campaigns so that people may take full advantage of the services which E-Governance is capable of giving and further e-Governance projects can be implemented successfully. And finally In the nut shell of the above topic, I would like to mention that the participation of people can plays a very important and vital role in implementation of e-Governance and making it great success in India.

5. References

1. Bhatnagar Subhash (2004), e-government from vision to implementation, sage publications, New Delhi.
2. Dey, Bata K. (2000), “E-governance in India: Problems, Challenges and Opportunities – A Futures Vision”, Indian Journal of Public Administration, Vol. XLVI, No. 3.
3. Diwedi S.K., Bharti A.K. “E-GOVERNANCE IN INDIA – PROBLEMS AND ACCEPTABILITY, Journal of Theoretical and Applied Information Technology available at www.jatit.org. [4]E-Readiness Ranking 2012, The Global Information Technology Report 2012 by Economist Intelligence Unit.
5. Gupta, M.P. (2004). *Towards E-Government Management Challenges*, Tata McGraw-Hill Publishing Company Limited, New Delhi.
6. Kaushik, P.D. (2004). E-Governance: Government Initiatives in India, in Bibek Debroy, *Agenda for improving Governance*, Academic Foundation in Association with Rajiv Gandhi Institute for Contemporary Studies, New Delhi.
7. Kochhar Sameer and Gursharan Dhanjal, (2005). E-government Report Card, *Yojna,* Vol.49, August, New Delhi.
8. Prabhu, C S R. “Cost Effective Solution for Effective e-Governance/ e-Panchayat (Example of Exemplary Leadership and ICT Achievement of the year)”, available at http://www.csi-sigegov.org/3/28_284_3.pdf
9. Report of the Working Group on Information Technology Sector Twelfth Five Year Plan (2012 – 17), available at http://planningcommission.nic.in/aboutus/committee/.../cit/wgrep_dit.pdf.
10. Singh, S K. (2008). “Panchayati Raj and Good Governance”, Centre for World Solidarity, Hyderabad.
11. Verma R.K., Kumari A. (2010) “E-Governance at Grassroots Level in South Asia: A Study of Citizen-centric e-Panchayats in India”. Asia-Pacific Journal of Rural Development Vol. XX, No. 1
12. http://www.beep.jepponet.dk/egovIndia/ShowCase.asp?CaseID=1492

HRM to e-HRM: Concept, Application & Applicability

Richa Dixit*

Abstract

With the introduction and development of internet, a new term e-HRM has emerged that changed the HR practices and processes dynamically to sustain in today's competitive environment. This paper aims to follow the evolution and journey of HRM to e-HRM. This study focuses on the impact of application of E-HRM tools on the HRM functions to be performed in an organization. The essence of this study is to understand the applicability of E-HRM towards HRM practices in terms of its advantages and limitations. This is a descriptive research based on secondary data collected from various websites, magazines and journals.

Key Words: E-HRM, ICT, HR functions, HR practices

I. Introduction:

The early part of the century was concerned with improving efficiency through careful design of work. During the middle part of the century emphasis shifted to the availability of managerial personnel, & employee productivity. Recent decades have focused on the demand for technical personnel, responses to new legislation and government regulations, increased concern for the quality of working life, total quality management and a renewed emphasis on productivity.

Personnel or Human Resource Management originated in 1800 B.C. In India, early roots of HRM traced back to period after 1920.Various acts and professional bodies like Factories Act 1948, Indian Institute of Personnel Management Kolkata, NILM, Mumbai have came into existence in 1950s. During 1960s the scope of personnel function expanded to labour welfare, participative management, industrial harmony etc. In 1960s & 1970s, Human resource development has become important. During 1990s, organizational restructuring and cost reduction gain importance. Liberalization, privatization, globalization, attention to employee capabilities, customer satisfaction and work-force diversity became crucial.

With changing needs of organization, Personnel Management became HRM. Further advancement in the arena of HRM resulted in evolution of the concept of strategic HRM. Now in today's dynamic environment sustainability of an organization is crucial and Strategic HRM is not sufficient enough to provide this sustainability. Organizations work in an ever changing society. Changes like economical, social, cultural etc call for a new concept to support these changes. Technological advancements have altogether changed the approach towards practicing different HR functions. All these changes lead to the evolution of e-HRM [5].

Originally e-HRM system was used in the payroll system by the US firms in the year 1950. During this time the organizations started using computers to process enormous data and also to closely follow the Government rules and regulations. In 1990's the organizations started to decentralize the organizational functions yet tried to maintain the control at the centre by following standardized information and processes.

E-HRM was introduced in mid 1990s' with different names like e-HRM, web based HRM, digital HRM etc. The use of e-HRM increased manifolds with the dynamic development of internet. There has been a considerable increase both in the number of organizations implementing e-HRM and also in the scope of e-HRM. The implementation of e-HRM

Richa Dixit*
Astt. Professor
IITM, Janakpuri
iitm.richa@gmail.com

complements the dynamic role of HRM in an organization. E-HRM in any organization should be so that it is in sync with the personnel and general HRM needs of the organization. E-HRM helps in integrating all the functions of HRM at various organizational levels.

II. Review of Literature

In organizational context, human resource includes the resources of all the people who contribute their services to attain the organizational goals. HRM at organizational level means the management of the dynamic components of all the people at all levels of the organization. It is to plan, organize, direct and control the functions of recruitment, selection, development, and compensation etc of human resource in an organization. It is to get the best people, train them and retain them to achieve organizations objectives. Ivancevich & Glueck defined HRM as "a function performed in organisations that facilitates the most effective use of people (employees) to achieve organizational & individual goals." Another definition given by M.L. Cuming states that "Human Resource Management is concerned with obtaining the best possible staff for an organisation & having got them looking after them, so that they want to stay & give their best to their jobs." So basically, HRM is a process to bring people & organizations together so that the goals of each are met. It is to procure, develop and maintain competent work force to attain organizations goal in an effective and efficient manner.

On the other hand, enabling various Human Resource Practices using web-based technologies is termed as e-HRM. The terms like web-based HRM, Intranet-based HRM, HRIS, HRM e-services, virtual HRM etc are used interchangeably for e-HRM. But it is not the same as V-HRM or HRIS. In e-HRM employees access various HR functions using intranet or other web-technology systems. E-HRM consists of HR policies and processes and collaborate individuals and organizations by delivering these policies using computers and electronic network capabilities. It is the application of information and communication technologies for implementation of HR strategies and practices in an organization.

According to Bondarouk and Ruel, e-HRM is "an umbrella term covering all possible integration mechanisms and contents between HRM and Information Technologies aiming at creating value within and across organisations for targeted employees and management." [2]

Strohmeier defined e-HRM as "the application of information technology for both networking and supporting at least two individuals or collective actors in their shared performing of HR activities."[1]

According to Shashank Kumar Shrivastava, "e-HRM is advance business solution which provides a complete on-line support in the management of all processes, activities, data & information required to manage human resource in a modern company."[4]

On reviewing the above definitions, we can say that, e-HRM is to apply IT to perform HR practices so as to enable easy interaction between people at all levels of the organization. E-HRM accumulates and facilitates all the information regarding employee personal data, compensation, performance management, recruitment, training etc. The purpose of e-HRM is to decrease the paperwork in the organization and to process huge volume of data easily.

III. Objectives of the study:

This study is an attempt:

To study and understand the applicability of e-HRM tools and techniques in various HR function.

To analyze and understand the impact of Information-Communication Technology on HRM

To study the advantages and disadvantages of e-HRM to HR personnel.

IV. Research Methodology:

This is a qualitative research paper. Only secondary source of data is used to understand the impact of web based technology on the HR functions of an organisation. Various books, journals, magazines and articles have been referred to analyze the subject.

V. Classification of E-HRM

According to Lepak & Snell E-HRM can be classified as [6]:

A. Operational E-HRM:

It is concerned administrative functions of HRM like employee personal data.

B. Relational E-HRM

It is related to supporting business processes using recruitment, performance management, training etc.

C. Transformational E-HRM:

Strategic HR activities like strategic re-orientation, knowledge management and talent management comes under transformational e-HRM.

VI. Application of e-HRM to HRM functions:

Application of e-HRM enhances the HRM functions in an organization. Application of e-HRM covers all the HRM functions ranging from traditional activities to transformational activities [3]. There are various tools which can be applied to perform HRM functions and the outcome is high competence, cost effectiveness, high commitment and higher compatibility. Following are the prominent e-HRM tools:

A. E-Recruitment:

Recruitment is to attract the potential candidates and making them apply for a job openings in your organization, whereas, E-Recruitment is to use computer and internet connection to search for potential candidates using various job sites and data bank of potential candidates and then communicate with them regarding job opening and other job related details and make them apply for the job available in the organization. This saves time in searching the candidates and is also cost effective and gives access to innumerable resume of prospective candidates for the job.

B. E-Selection:

Selection is the process of choosing the right person for the right job and at the right time. Selection process involves lots of formalities, assessment and paper work. Selection process can be made easy using e-Selection tool. E-selection can minimize the paperwork. It can be used to complete the assessment and other formalities of prospective employee by using the interactive assessment forms and submitting the same to the organization. Auto-generated assessment results, interactive online interviews using web-based technologies etc can be used to make the selection process speedy and cost effective.

C. E-Training & Development

Training and development involves identification of individual potentialities and helping in the development of key competencies through planned learning process. The competencies are to be developed to enable individuals to perform current as well as future jobs. It aimed at bettering the performance of individuals and groups in organizational settings. Organizations can develop their employees by providing them online training programs any time and at any place. E-Training helps the organization to provide training to their employees at reduced cost and also enables its employees to learn and share knowledge at different levels of the organization and also across other companies and departments.

D. E-Performance Management

The performance management system ensures linkages between individual & organizational goals. It aims at ensuring that every individual's efforts and actions support the goal of the organization. It is a collective effort of manager and the employees of delivering successful results in organizations by improving the performance and developing the capabilities. E-Performance management system involves the application of software to record, update, monitor and retrieve the relevant information of the employees. This system helps in linking the performance of the employee with his/her compensation. It can easily provide feedback to the employees on their performance in the organization. This system ensures cost reduction and greater transparency and speed in performance management system.

E. E-Compensation

Compensation Management involves providing monetary and non-monetary benefits to employees to maintain and balance work-employee relation. Bonuses, overtime pay, recognition rewards, profit sharing, perks, sales commission etc are parts of employee compensation. This element focuses on a fair, consistent & equitable compensation & benefits to the work force. E-compensation is also a tool to help management in managing the compensation of employees. It refers to designing a compensation package for the employees using information and communication technologies. It helps the management in fulfilling the objective of giving fair compensation to all the employees working in the organization. It helps the management to analyze the past compensation package data, prepare budget and incentive systems for the current and future needs of the organization. It saves time and is cost effective.

VII. Implementation of e-HRM:

E-HRM implementation process can be described through following steps:

Step 1: Setting of objectives and Accountability:

Personnel from HR department should initiate the E-HRM implementation. They should arrange meetings with all relevant stakeholders such as functional managers, department heads, line managers etc and make a team which includes few experienced and a few fresh personnel having experience from different companies to implement e-HRM in the organization. Personnel involved in the process must assume and announce their accountability regarding various aspects of the implementation.

Step 2: Process Awareness:

Next step is to make the stakeholders aware about the application and applicability of e-HRM. They should know about the various HRM functions it supports. Process awareness sessions should be organized for all the stakeholders.

Step 3: System installation & Configuration:

IT Infrastructure required to install and configure e-HRM application should be provided by the IT infrastructure team. It should provide a stable application. To support the application in case of any technical issue, an IT team representative should be appointed [7].

Step4: Integration and Accessibility: Next step is to integrate E-HRM application with other e-enabled application in the organization if required for larger information and accuracy across the functions for data. Further, the authority and level of access should be defined by HR to avoid post implementation issues.

Step 5: User Acceptance: User acceptance is a big issue for the HR department. Different users may perceive the system differently. There may be various suggestions resulting out of day-to-day use of the application which were not there initially. The user may find the application not up to the expectation. So it becomes more important to involve the users from the beginning.

Step 6: Objective Evaluation: After the installation of e-HRM a survey should be conducted to evaluate the effectiveness of the system in achieving organizational objectives.

Step 7: Change Management: Suggestions received from people after implementation of E-HRM should be evaluated for future enhancement of the system and the feasibility of incorporating these suggestions should also be checked.

Step 8: Removal of system: With time E-HRM system may become outdated if not reviewed and revised regularly. If it is not meeting the organization's objectives, it should be removed after discussing the issue with the stakeholders.

VIII. Applicability of e-HRM:

Evaluation E-HRM depends on the following forces:

Updated, low-cost, high speed automated information communication technologies.

Strategic process reengineering to streamline and improve business processes.

High speed management to be competitive and quicker service delivery.

Networked organizations that use intranet, internet, local area network, emails etc to share information and empower personnel at all levels of the organization.

Learning organization with well informed, self directed, computer savvy, knowledge worker to identify and seize better business opportunities.

A global HR department, using e-HRM to provide service and support to their employees anywhere in the world.

IX. Advantages & Benefits of e-HRM:

Data & information collected and stored helps in strategic decision making.

Helps in managing human resource of the organization effectively and efficiently.

Facilitates quick reporting and analysis.

Result in better business processes, enhanced productivity and increased employee satisfaction.

Paperless office reduces administrative work and reduces the cost of working.

HRM functions like recruitment, performance management, training and development etc are performed using web-technologies which make the work faster and effective.

X. Disadvantages & Challenges of e-HRM:

Security and confidentiality of employee data and information is crucial. Employee may feel insecure to share important information on web-based technologies.

People resist change. Acceptance of e-HRM may be an issue among traditional managers and employees. Change in their mindset is required to accept the usefulness of web based HR application.

To integrate all the departments of an organization it becomes important to align the e-HRM with other systems installed in the organization. Aligning the e-HRM system is a crucial and time consuming task.

Providing training to the users of e-HRM is also a challenge for the HR Department. Not every employee is comfortable in using information and communication technologies.

Installation and implementation of e-HRM system involves high cost.

E-HRM is not very much useful for very small organizations.

XI. Conclusion:

To conclude we can say that e-HRM is a technological way of practicing HR functions. E-HRM is a tool to achieve organizational goals more effectively and efficiently. The outcomes of e-HRM are cost reduction, improved strategic decision making, increased efficiency of employees in performing HR functions, and it also facilitates strategic role of HRM [5]. It enhances the production and productivity of the employees, helps in reducing the administrative work and enables better management in an organization. Finally, E-HRM may help the employees to perform their work with increased speed and efficiency and it surely reduce the administrative burden and operational cost of an organization.

References

1. Strohmeier, Stefan. (2007). e-HRM: Review and implications in Chair for Management Information Systems. Human Resource Management Review, 17, 19-37
2. Ruel, H. J. M., Bondarouk, T., & Looise, J. C. (2004). E-HRM: Innovation or irritation. Management Review. Management Review, 15(3), 364"381.
3. Emma Parry (2011), “An examination of e-HRM as a means to increase the value of the HR functions”, International journal of human Resource Management, Vol. 22, Iss. 5, 2011, pp. 1146-1162
4. Shashank Kumar Shrivatsava (2010), “Shaping organizations with eHRM”, International Journal of Innovations, Management and Technology, Vol. 1, No. 1, April 2010.
5. Gardner, S.D., Lepak, D. and Bartol, K.M. (2003), ”Virtual HR: the impact of information technology on the human resource professional”, Journal of Vocational Behaviour, Vol. 63,pp. 159-79.
6. Lepak, D.P. and Snell, S.A. (1998), “Virtual HR: strategic human resource management in the 21stcentury”, Human Resource Management Review,Vol. 8 No. 3, pp. 215-34.
7. Shrivastava, S. and Shaw, J. (2004), ”Liberating HR through technology”, Human Resource Management, Vol. 42 No. 3, pp. 201-22.

Crimes in Cyberspace: Indian Scenario

Suvrat Bahuguna*
Tanya Raizada**
Ashok Wadje***

Abstract

The recent advances made in the field of information technological all around the world has made people very tech savvy.People have indulged in over use of the technology and have become highly dependent over it.With such advancements and overuse of the technologies there has been observed a high increasein the number of crimes committed in the internet by people as it is considered the safest mediumof committing a crime due to everything being virtual and there being no personal interaction ofthe criminal with the victim. Criminals spread viruses which in turn crash other people'scomputers, steal identities of others, spread pornography etc.Until recently, experts in the field of IT had no knowledge and awareness in the area ofcybercrimes, even the law enforcement officers did not have appropriate tools which wereneeded to tackle such problems as the old laws prevailing in the country were majorly silent onsuch crimes and the new laws introduced were not in accordance to the reality.Fearing that such cyber-attacks may in the future be used by hackers to cripple and disable themilitary, financial and social stability of advanced economies, special care is being taken bymilitary personnel and IT companies to prohibit and fight such crimes.With the passage of time and more technological advancements being made by the human racesuch crimes are on the rise and are spreading at a massive rate all around the world.It can be said that even though the government has introduced measures like these in the societyto stop cybercrimes from rising and exploiting the countries as well as its individuals, yet noeffective result can be expected until and unless action will be taken at an individual level by thecitizens to fight cybercrime by taking full precautions and care.

Key Words: Attacks, Cybercrimes, Technology.

I. Introduction

The recent advances made in the field of information technological all around the world has made people very tech savvy. People have accepted the new technologies introduced in the market which make their life easier and convenient. People have indulged in over use of the technology and have become highly dependent over it. With such advancements and overuse of the technologies there has been observed a high increase in the number of crimes committed in the internet by people as it is considered the safest medium of committing a crime due to everything being virtual and there being no personal interaction of the criminal with the victim. Criminals get easy money by hacking into bank accounts of people using internet banking and not logging out safely and leaving trails for the criminals who can easily hack their accounts and withdraw their money. Criminals spread viruses which in turn crash other people's computers, steal identities of others, spread pornography etc. Until

Suvrat Bahuguna*
BA LLB 4thyear,
Symbiosis Law School, Noida
suvrat2593@gmail.com

Tanya Raizada**
BA LLB 4thyear,
Symbiosis Law School, Noida
tanya.raizada02@gmail.com

Ashok Wadje***
Faculty In charge of Cyber Laws
NLU, Jodhpur
ashokwadje@gmail.com

recently, experts in the field of IT had no knowledge and awareness in the area of cybercrimes, even the law enforcement officers did not have appropriate tools which were needed to tackle such problems as the old laws prevailing in the country were majorly silent on such crimes and the new laws introduced were not in accordance to the reality. There was a constant debate over privacy issues of others which hampered the forensic expert's ability to gather evidence from the victim. There was also a constant misunderstanding and cold war going on between the IT professionals and the Law enforcement personnel. The former had the understanding of computers and networks whereas the latter had the ability to gather evidence and understand the criminal's mindset and know the basics of gathering evidence and bringing offenders to justice but the constant rivalry between the two hampered an effective action against cybercrimes.

Seeing an increase in such criminal activities via the internet due to various legal as well as social factors, the government was forced to introduce a stringent law regarding protection of people with respect to crimes in the area of internet which finally came in the form of the Indian IT Act, 2000[1]. This act provides security to the victims of cybercrimes and provides them ample security. This act segregates different cybercrimes and provides different punishment for each and has been of great help in reducing cybercrimes in India.

II. Cyber Crimes

Any criminal activity that uses a computer either as a target or a mean for perpetuating certain crimes comes within the ambit of cybercrime [2]. Computer crimes started to creep in our society from the latter half of the 19th century. Computer manipulation, sabotage, espionage and the illegal use of the computer system started happening as early as in the 1960's[3].

These sorts of crimes encompass a broad range of criminal activities. However, they can be broadly classified into two categories:

1) Crimes which target the computers directly.
2) Crimes which are facilitated by the use of computer networks or devices and the main target are independent of the computer network or device used.

Crimes which mainly target the computer networks or devices include:

- Computer viruses.
- Denial-of-service attacks.
- Malware (malicious code).
- Crimes using computer networks or devices to commit crimes against others include:
- Cyber stalking.
- Fraud and identity theft.
- Information warfare.
- Phishing scams.
- Spam.

III. Threats of Cyber Crimes:

A. Spam:

Primarily the unsolicited sending of mails in a bulk manner i.e. repeatedly and in a large number for several commercial purposes is illegal in many jurisdictions.Even though anti-spam laws are comparatively newer, the various restrictions and limits levied on unsolicited electronic communications have been existingfor quite some time now.

B. Computer Fraud:

Anyfraud scheme which involves the use of one or more components of the internet to present fraudulent information to victims so as to conduct fraudulent transactions and obtain illegal benefit is computer fraud[4]. To execute such a crime very less expertise or knowledge is required and it is not an uncommon form of theft executed by certain employees of any organization or company by changing the data before making entries or even making false entries.

C. Obscene/Offensive Content:

The word obscene literally means thoughts, books, picture etc. which are indecent, disgusting and offensive [5]. Content of such a nature which is offensive to others is regarded as illegal in most countries of the world.More than 25 jurisdictions all over the world place limits and restrict communications which are racist, slanderous, libelous, blasphemous, seditious or which may incite some kind of riots or crimes in the country.Child pornography is one such area present on the internet which is strongly opposed by everyone due to its highly obscene nature.

D. Harassment:

Electronic media may be used to harass others in an unsolicited fashion [6]. When the matter on the internet is targeted in an obscene and hurting manner against an individual or a whole community it falls under the ambit of harassment. For example posting obscene and derogatory comments related to someone's gender, race, religion, nationality, sexual orientation. This is a common occurrence in chat rooms by sending hate e-mail to targeted parties.

E. Intimidation:

Although freedom of speech is protected by law in most democratic societies yet this freedom does not include all types of speech. In fact spoken or written "true threat" speech/text is criminalized because of "intent to harm or intimidate" and this is applicable to electronic communication. The US Supreme Court definition of "true threat" is "statements where the speaker means to communicate a serious expression of intent to commit an act of unlawful violence to a particular individual or group".

F. Drug Trafficking:

Drug traffickers are increasingly taking advantage of the internet to sell their illegal substances through encrypted e-mail with the help ofinternet. Drug peddlers execute deals at internet cafes and track their package of drugs with the help of courier websites.The lack of face-to-face communication has led to the rise in internet drug trades. The sketchy effects that are often associated with drug trades are severely minimized and the filtering process that comes with physical interaction fades away.

G. Cyber Terrorism:

A cyberterrorist is someone who threatens, coerces or even intimidates a governmental organization in order to promote and advance his or her own personal political and social objectives by launching computerbased attackswhich are aimed atthe vital information stored in the computers and network.[7]

Cyber terrorismis the premeditated use of disruptive activities, or the threat thereof, against computers and/ or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives.[8]Even a small simple propaganda being posted on the internet regarding a series of bomb explosions that will occur during the holidays can be considered to be an act of cyberterrorism. There are also hacking activities which are mainly aimed towards an individualand his family for creating fear amongst people by demonstrating power and collecting scandalous information regarding peoples' lives and then using the same information to blackmail them.

Cyberextortion is basically a cyber-terrorism and in such activities a website, e-mail server, or computer system is subjected to repeated denial of service or other attacks by malicious hackers, who demand money in return for promising to stop the attacks.[9]

H. Cyber Warfare:

The U.S. Department of Defense (DoD) notes that cyberspace has emerged as a national-level concern through several recent events of geo-strategic significance[10]. Among those included the attacks by Russian hackers on Estonia's infrastructure sometime in 2007[11]. In August 2008, Russians allegedly for the second time conducted cyber-attacks and this time in a coordinated and synchronized kinetic and non-kinetic campaign which were targeted against the country of Georgia. Fearing that such cyber-attacks may in the future be used by hackers to cripple and disable the military, financial and social stability of advanced economies, special care is being taken by military personnel and IT companies to prohibit and fight such crimes.[12]

IV. Landmark Cybercrime Cases in India

The Following paragraphs discuss about the landmark cases related to Cybercrime in India:

A. Pune Citibank Call Center Fraud

Some employees gained the confidence of their customers and obtained their PIN numbers so as to commit the crime of fraud. The employees involved in the crime obtained these numbers by helping the customers out of difficult situations. They memorizedthese numbers and accessed the Citibank accounts of the customers andtransferred the money from their clients account to their account in Pune. This transaction left a trail for the police to detect and catch the criminals.

B. Bazee.com case

CEO of Bazee.com was arrested in December 2004 because a CD with objectionable material was being sold on the website. This opened up the question as to what kind of distinction do we draw between internet service provider and a basic content provider and thereby it was decided in this case that the burden for proving innocence rests on the accused that he was the Service Provider and not the Content Provider.

C. State of Tamil Nadu Vs SuhasKatti

This case basically deals with the posting and publication of obscene, defamatory and annoying messages which aimed at a certain divorcee woman in the yahoo message group. After such material was posted on the net, the divorcee/victim started receiving annoying phone calls to the lady in the belief that she was soliciting. After a formal complaint was registered by the victim in 2004, the police started gathering evidence and traced the accused to Mumbai and arrested him within the next few days.

D. SMC Pneumatics Pvt. Ltd. v. Jogesh Kwatra

This is India's first case of cyber defamation. Jogesh Kwatra, an employ of the plaintiff company started sending emails containing derogatory, obscene, derogatory, vulgar, filthy and abusive language and content to his bosses and also to the different branches of the same company present all over the world with the sole motive tospoil the company's reputation and to defame its Managing Director. A suit for permanent injunction was filed by the plaintiff thereby restraining the defendant from carrying on with this his illegal act of sending derogatory and abusive emails to the plaintiff. Further, the Hon'ble Judge completely put restraints on the defendant with regards to his activity of publishing, transmitting or publishing any information in the actual world as well as in cyberspace which is derogatory or defamatory or abusive to the plaintiffs.

E. Andhra Pradesh Tax Case

The computer used by a prominent businessman from Andhra Pradesh exposed the various illegal activities he was involved in and were used as evidence against him. The businessman accused in this case was the owner of a plastics firm and he was arrested by the officials of the vigilance department with Rs 22 crore cash being recovered from his house. An explanation was sought from him by the department regarding the unaccounted cash within a span of 10 days. The accused person submitted before the department approximately 6,000 vouchers in order to show his innocence by proving the legitimacy of trade and the cash recovered from his house.He thought that his offence would go undetected but after careful scrutiny of the submitted vouchers and careful screening of the contents on his computers it came to light thatthese vouchers were made after the raids were conducted.

He was arrested for running 5 illegal businesses and for not paying the taxes.

F. Sony.Sambandh.com Case

A complaint was filed by Sony India Private Ltd, which operates a website called www.sony-sambandh.comfor theNon Resident Indians. This website lets NRI's to pay for a particular Sony product online and send it to their friends and relatives in India. An anonymous person under the identity of Barbara Campalogged onto this site and placed an order for a Sony Colour Television set and a cordless head phone. The payment was made duly made by the user. At the time of delivery, digital photographs showing the acceptance of the delivery by Arif Azim were taken by the company. The transaction was henceforth closed but after one and a half months Sony was informed by credit card agency that this transaction was unauthorizedas the real owner denied any kind of purchase made by her. Investigation started and it was found out that the transaction was wrongly carried out by Arif Azim who had gained access to the credit card number of an American national which he misused for his own benefit. The products which he wrongfully obtained were taken back by the police and he was arrested for the fraud committed by him.

V. Measures to Protect Oneself from Cyber Crimes

One should be sure that he has a latest and effective antivirus installed on his/her computer and should regularly look for the updates available on the net related to the virus and update regularly the anti-virus software installed on the computer. A weekly or monthly scan of the computer should be done to locate and remove any malware, spyware or virus which hampers the functioning of the computer.

Always keep the computer's firewall protection feature on as it is a digitally created barrier that prevents hackers and viruses from entering into the computer system.

Important data on the computer should be encryptedand the computers user should utilize the encryption software as it makes it important data unintelligible to anyone who tries to hack into your computer system.

Net users should refrain from providing his/ her personal information to a website one knows nothing about, especially the ones which ask for the user's name, his bank account number or social security number.

Online shopping must be done on a secure website having a URL that starts with an "http" or has a VeriSign seal. If such features are not there on the site then one runs the risk of putting vital information like some personal information or information about his credit card on a site which may be a fraud.

Avoid getting allured by common scams like winning foreign lotteries and similar other methods used by cyber criminals to attract consumers and get their personal information and money. [13]

Easy access to the internet may expose children to the aggressions of pedophiles and child pornography[14] and therefore the online activities of children and use parental control software to limit the types of sites they can gain access to. The spam blocker should be always on so that you do not receive unnecessary and malicious spams.

VI. Conclusion

The immense increase in the use of internet and the dependency of individuals of every field over it has led to a number of new crimes relating to cyber space being introduced in our society.With the passage of time and more technological advancements being made by the human race such crimes are on the rise and are spreading at a massive rate all around the world. This sudden and drastic growth in cybercrime has led the Indian government to enact and adopt various laws relating to this field in the recent past. The Information Technology Bill is one such effort which has been taken by our government for the same and has led to a substantial drop in the rate of cybercrimes in India but it has still not been fully enacted and adopted by everyone. People are still unaware of their rights and protections given to them by provisions of this act. It can be said that even though the government has introduced measures like these in the society to stop cybercrimes from rising and exploiting the countries as well as its individuals, yet no effective result can be expected until and unless action will be taken at an individual level by the citizens to fight cybercrime by taking full precautions and care.

Acknowledgement

This work was supported in part by a grant from the National Science Foundation.

References

1. The Information Technology Act, 2000 (No. 21 of 2000) [9th June 2000].
2. ParthasarathiPati, http://www.naavi.org/pati/pati_cybercrimes_decoz.htm
3. U.Sieber, Legal Aspects of Computer Related Crime in the Information Society, COMCRIME study, Europeancommission.
4. http://www.usdoj.gov/criminal/fraud/internet/.
5. Barua, Yogesh and P.DayalDenzyl, Cyber Crimes, Notorious Aspects of the humans and the Net.
6. Wayne Petherick, Cyber stalking: Obsessional Pursuit and Digital riminal/http://crimelibrary.com/cyberstalking
7. R.Richardson, CSI Computer Crime and Security Survey (Computer Security Institute,2008).
8. Kevin Coleman, Cyber Terrorism, Technolytics, October 10,2003
9. Praveen Dalal, Cybercrime and cyber terrorism: Preventive defense for cyberspace violations.
10. Cyber protests: The Threat to US Information Infrastructure-October 2001.
11. "Cyber-attack in Estonia- what it really means" http://www.news.com/Cyberattack-in-Estonia-what-it-really-means/2008-7349_3-6186751.html
12. Terror on the Internet: The new Arena, the New Challenges USIP Press Books, 2006.
13. http://www.usdoj.gov/criminal/cybercrime/1030_new.html
14. Agrawal, S.C; Computer ethics, child sexual abuse, pornography and regulation of child pornography on the internet, vol. 10, Jan 2002.

Information Technology and Cyber Crime

Dr. Vatsla Sharma*

Abstract

The last decade of 20th century had witnessed information technology emerge as the most prominent technology, which has a revolutionary effect on the lives of the people across the world. The scientific and technological advancement specifically in the fields of communication and information have created havoc thus, opening new ventures for the human being including the criminals. On the other hand criminal minded people misused the said revolution for the promotion and extension of criminal activities. These activities may be referred as computer crime or cyber crime. Presently, Cybercrime is an ever increasing phenomenon, not only in India but all over the world. Cyber crime is the use of computers and the internet by criminals to perpetrate fraud and other crimes against companies and consumers.

Key Words: Cyber Crime, Cyber Laws, Cyber Fraud, Cyber stalking.

I. Introduction

Computer revolution has given birth to internet culture. Internet is a massive worldwide network of computer connected to each other with the main objective of sharing and transmitting information. The internet is a global network in interconnected computers, enabling users to share information. Typically, a computer that connects to the Internet can access from available servers. A majority of widely accessible information on the Internet consists of inter linked hypertext documents and other resources of the World Wide Web (WWW).

The internet is still at a very nascent stage of development. Being the newest mode of communication, the laws railing them are also at a developing stage. As the internet gain proliferation, so will the complexity of Cyber Laws covering more relevant more relevant issues. With many countries and societies are in the process putting in place the Cyber Laws, a few have already put down Cyber Laws and India is proud to be one among them. India is globalizing its economy.

Dr. Vatsla Sharma*
Heera Lal Yadav Law College, Lucknow
E-mail: vatslasharma@rediffmail.com

II. Information Technology

Information Technology and Information Services have a profound effect on the country's economy, trade and commerce. The Securities and Exchange Board of India has allowed trading on the Internet. The Stock Exchange in India is carrying out different kinds of transaction and information exchange of their networks. The Reserve Bank of India has introduced the electronic payment system. There have been concerns from Intelligence and Law Enforcement Agencies and other about Computer Crime, Computer misuse, data protection, security standards, intellectual property rights, privacy etc [1].

The movement of information in the Internet is achieved via a system of interconnected computer networks that share data by packet switching using the standardized Internet Protocol (TCP/IP). It is a "network of networks" that consists of millions of networks and is linked with wireless connections and other technologies.

Anything related to Internet and computer networks came to be known with the prefix 'Cyber'-Cyber law, cyber café, cyber police, cyber space, cyber stalking and cyber fraud. The list is endless. Internet provides as superhighway for transportation of information. It is popularly known as "World Wide Web" (WWW).

The Internet is fast becoming a way of life for millions of people [2].

The use of computer in law is of recent origin. As late as 1979 Fielder in his work "Functional Relation between Legal Regulation and Software" lamented that "on the side of the legal theory up till now there has been but very little interest in the computerized implementation of law. For legal theory, this lack of interest is a deplorable deficiency. "Now lamentable stage is over. Computer is used and is helping law experts in knowledge acquisition, knowledge representation and knowledge utilization. It is rightly said that technological development in every area is likely to cause drastic effect in every walk of life. It is evident that at present whole world is crazy for spaceman ship involving various adventures and causing revolutionary changes. The scientific and technological advancement specifically in the fields of communication and information have created havoc thus, opening new ventures for the human being including the criminals. On the other hand criminal minded people misused the said revolution for the promotion and extension of criminal activities. These activities may be referred as computer crime or cyber crime. Cyber crime is the most recent type of crime which affects many people. This is the biggest challenge for police, prosecutors and lawmakers.

The tremendous progress made by computer technology during the last quarter of the 20th century has now made it possible for the people to visually chat, send messages, transmit information and conduct business with a person in any part of the world through internet. The computer as an innovative mechanism has increased our capacity to store, search, retrieve, and communicate data as also accessibility to information which has made it possible for us to communicate with any person, anywhere, anytime in the world [3].

III. Cyber Crime

Cyber Crime is a problem which confronts the entire world. Cyber Crime is the most dangerous of all crimes because of the magnitude of the loss it is causing today and its potential, the ease with which it is committed, its invisibility and the disregard for geographical boundaries, the difficulty in investigation, collection of evidence and successful prosecution of the cyber criminals and the costs of dealing with Cyber Crime by effecting law enforcement and protective technology. The Internet being an integral part of daily life, cyber Crime, if not checked would be destructive to civilization itself. The growth of Internet linked with the growth of protective technology and other means to check cyber crime. It would be futile for Internet culture to grow without effective means of checking cyber crime. It would be in the interest of the society for the Internet, e-commerce e-business to grow slowly but steadily.[4]

The term 'cyber crime' is a misnomer. This term has nowhere been defined in any statute/Act passed or enacted by the Indian Parliament. Cyber crime has not been defined in Indian Penal Code, 1860 because it was drafted in 1860 when computers were non-existent. Information Technology Act, 2000 is the only Act which gives legal recognition to computers and matters related thereto. The Information Technology Act, 2000 has for the first time brought cyber crime, punishment and procedure for probing it within a legal framework.

Cyber crime is an amalgamation of two words: 'cyber'-related to internet or other electronic networks and 'crime'-a criminal activity. Literally, the word cyber means "connected with electronic communication networks, especially the internet."

"Cyber crime may be said to those species, of which, is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime".

"Any criminal activity and uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime".

A generalized definition of cyber crime may be "unlawful acts wherein computer is either a tool or target or both". The term "computer" used is in this definition does not only mean the conventional desktop to laptop computer. It includes Personal Digital Assistance (PDA), cell phones, sophisticated watches, cars and a host of gadgets.

Cyber crime is the use of computers and the internet by criminals to perpetrate fraud and other crimes against companies and consumers. Crime committed using a computer and the internet to steal a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs. Cyber crime is a broadly used term to describe criminal activity committed on computers or the Internet. Some of it is punishable by the laws of various countries, where others have a debatable legal status.

The first recorded cyber crime took place in the years 1820. That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 BC in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage [5].

In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of series of steps in the weaving of special fabrics. This resulted in a fact amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from use of the new technology. This is the first recorded cyber crime [6].

In a day and age when everything from microwave ovens and refrigerators to nuclear power plants are being run on computers, cyber crime has assumed rather sinister implications. Cyber Crime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation, and mischief. The abuse of computer has also given birth to a gamut of new age crimes such as hacking, web defacement, cyber stalking, web jacking etc [7].

Prof. S.T. Viswanathan has given three possible definitions of cyber crimes and these are as follows:

Any illegal action in which a computer is a tool or object of the crime; in other words, any crime, the means or purpose of which is to influence the function of computer.

Any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator, by, intention, made or could have made a gain.

Computer abuse is considered as any illegal, unethical or unauthorized behavior relating to the automatic processing and transmitting of data.[8]

Douglas Thomas and Brian D. Loader [9] has attempted the definition of cyber crime in its broadest contours by observing that "cybercrime can be regarded as computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks. Its distinctiveness is derived from the versatile capabilities provided by the new Information & communication technologies ICTs. The global connectivity of the Internet, for example, makes it much easier for criminals to act beyond national boundaries to conduct their illegal affairs. It also makes it possible for existing organized crimes to use more sophisticated techniques to support and develop networks for drugs trafficking money laundering, illegal arms trafficking, smuggling and the like. For hackers with the requisite computer skills, a large market exists for security and trade secrets which can be accessed transmitted electronically. Furthermore, the many-to-many communications which is an essential feature of the Internet enables the production and worldwide dissemination of information and knowledge which could be potentially harmful, threatening or liable to incite violence.

Of even greater significance perhaps is the burring of the distinction between internal and external security. The transforming qualities of ICTs make it increasingly difficult to distinguish between warfare, terrorism and criminal activities. Extremist political groups, for example, may engage in all the three. A country in the post Cold War period may be more under threat from economic espionage than nuclear assault. The use of ICTs by non-government organization and international criminal organizations will therefore clearly have an increasingly important impact upon the functioning of law enforcement and security agencies in the information age [10].

Cyber Space or cyber world is one such virtual world where the machines are connected through information technology; the blood relations of one individual are mirrored here in a computer. Likewise, several networks are like various nation states which are globally connected through Internet. This virtual world has computers or computer systems or a network thereof communicating with each other and giving and receiving data messages [11].

The Internet, touching every nook and corner of modern society, is inescapable and has becomes a means of cultural transmission. In fact, it is even regarded as having cultural dimensions of its own. As a potent instrument of transmission, the Internet has ranked "new uncertainties" not only in the social world but also in the legal world [12].

IV. Conclusion

The unprecedented growth of computers and the Internet is revolutionizing almost all aspects of human life. Increasing use of computers and the Internet in government, military institutions, critical services like power, telecommunication and aviation, education, financial sector and banking is undoubtedly moving the present day society into a new information age parallel only to the Industrial Revolution. Among developed nations, computer has become an item of necessity in every household. India is also catching up with other countries, standing fourth among the top then nations in the world with 81 million internet users. The growth of mobile phone in India has also been phenomenal. In addition to being a communication device, the mobile phone offers connectivity with the Internet. Many new applications, like Twitter's Tweet SMS are also available on cell phone. The global sweep of the Internet, providing a borderless and a relatively anonymous domain has brought many opportunities for activities that are undoubtedly of criminal nature. The Internet has made it possible to commit computer crime from a far off place, often beyond national boundaries.

References:

1. V.D. Dudeja: Crimes in Cyber space Scams & Frauds (issues and remedies), Edn. Ist 2003, pp-221-222.
2. Nandan Kamath: Law Relating to Computer, Intenet& E- Commerce, Edn. 3rd, 2007, p-208.
3. V. Paranjape, Cyber Crimes & Law, Central law Agency, 2010, p-210.
4. V.D. Dudeja: Crimes in Cyber space Scams & Frauds (issues and remedies), Edn. Ist 2003, p-220.
5. Ian J Loyd: Information Technology Law, 3rd Ed Butterworths, London, 2000.
6. Advocate, Prashant Mali: Cyber law & Cyber Crimes, First Edition 2012, Snow white Publication, P-5.
7. Rohas Nagpal: Cyber Crime and Corporate Liability, First print 2008, published by Walters Kluwer (India) pvt.Ltd.New Delhi, p-166.
8. S.T. Viswanathan, The Indian Cyber Law: with Cyber Glossary, (BLH) New Delhi 2001, p-81.
9. Douglas Thomas and Brian D. Loader, Cybercrime: law enforcement, security and surveillance in the information age at p.3.
10. Dr. Gupta & Aggarwal: Cyber Laws, Edn. Ist, p-54.
11. Dr. J.P. Mishra: Introduction to cyber laws, First Edition, 2012, Central law publications, p-9.
12. Talat Fatima: Cyber crimes, First Edition, 2011, Eastern Book Company, p-28.