International Journal of u- and e- Service, Science and Technology
Vol.8, No.3 (2015), pp.163-170
http://dx.doi.org/10.14257/ijunesst.2015.8.3.15

Survey on Fraud Detection Techniques Using Data Mining

[1,2]Muhammad Arif and [2]Amil Roohani Dar

[1]*Faculty of Computer Science and Information Technology, University of Malaya 50603 Kuala Lumpur, Malaysia*
[2]*Computer Science Department, Comsats Institute of Information and Technology, Pakistan*

Abstract

Now a days, fraud is a million dollar business and every year it is increasing more and more. In a crime survey in 2009, tells that close to 30% of the company's worldwide reported falling victim to fraud in the past year. Fraud involves individual or in a form of groups who intentionally act secretly to rob another of something of worth, for their own profit. Fraud is as against the humanity and it is unlimited variety of different forms. So in this paper, we introduce different methods and techniques to tackle the fraud and how to prevent the fraud into the organization, businesses, and hospital and insurance companies. Fraud prevention is a continuing battle. Many website owners must continually fight against many kinds of crime ranging from stealing identity theft and credit cards and many other types of fraud related to that. Internet Fraud is also very popular, where fraudster can steal the credit card number and buy thing from the different websites.

Keywords: *Intentionally, Fraud, revenues, Bayesian, Immune, KDD, Subsidies, Communal*

1. Introduction

Fraud detection is very tough job because its types and natures are totally different and there's a millions of methods. So for a long time the traditional ways of data analysis have been in use to detect fraud. They require tough and time consuming task that deals with different domains of knowledge like business practices, finance, economics and law. Normally fraud instances can be similar in appearance and content, but usually are not identical. So fraud detection is very tough task. In this paper, we introduce different methods and techniques to detect it. There' use multilayer perceptron neural network, Neural Nets (NN), Bayesian Nets (BN), Naive Bayes (NB), Artificial Immune Systems (AIS), Decision Trees (DT), to detection the credit card fraud, financial statement frauds (FSF), Artificial Immune Systems (AIS) etc. These are the different techniques and methods to detect fraud on the organization, banks, credit cards companies etc. On this paper, we present the different techniques, their advantages and also explain those algorithm and different system, which are faster than previous to detect the fraud. These are efficient and give the demanded result. These systems perform very well according to their domain.

2. Different Techniques for Fraud Detection

This paper describes an effective medical claim fraud/abuse detection system based on data mining [1, 21]. This is used by a Chilean private health insurance company. On their Fraud/abuse is detecting when the large number of losses in revenues. Basically when this company loses the revenues which are much higher than previously then they detect it. In medical claims has become a major concern with health insurance companies which are

ISSN: 2005-4246 IJUNESST

belong in Chile. On there, this organization carried out by a few medical experts, who have the liability of approving, modifying or rejecting the subsidies requested within a limited period from their reception. The proposed detection system which is used in this paper uses multilayer perception neural networks (MLP). This MLP has each one of the entities involved in the fraud/abuse problem like that medical claims, affiliates, medical professionals and employers, *etc*. So on the Results of the fraud detection system, there's show a recognition rate of around 75 fraudulent and abusive cases per month, while without the using of that MLP system, there were approximate 6.6 months detection. So this is the real industrial problem, an implementation of an automatic fraud detection system [1].

This paper addresses many important questions like wise, what are the main identity about fraud and its category? And secondly, what are the current Information Systems (IS) [2]. So in the case of current Information Systems (IS), in there what are the facilitated attack channels and methods used, to identify fraud perpetrators? Thirdly, what are the effects sustained by targeting victim organizations? The major part of this paper is the development the identity fraud perpetrator framework, which is used to detect the fraud and the understanding of the model's elements and relationships which is used. This framework will be useful in business, law enforcement and government organizations [2]. This paper describes a quick technique which is communal analysis suspicion scoring (CASS) [3]. So on the CASS; there we generate numeric doubt scores on streaming credit applications based on understanding relations to each other, over both time and space. CASS includes pairwise shared scoring of the identifier attribute for application, description of categories of dubiousness for application pairs, the merging of temporal and spatial weights, and smoothed k-wise scoring of several linked application pairs. Results on mining numerous hundred thousand real credit applications show that CASS reduces fake alarm rates while maintaining reasonable hit rates. CASS is scalable for this huge data sample, and can fast detect early symptoms of detect crime. In addition, new ways have been observed from the associations between applications [3].

This paper defines that automated adversarial detection systems can fail when this is under attack by adversaries. As part of a resilient data stream mining system, this is reducing the possibility of such failure [4]. The first part of the adaptive spike detection requires weighing all attributes for spikiness and then this adaptive spike detection rank the attributes. The second part involves filtering, so that there are some attributes with extreme weights, and then we choose the best ones for computing each example and their suspicion score. Within a crime detection domain, this adaptive spike detection is validated on a few million real credit applications. The results reinforce adaptive spike detection and its effectiveness for ranking and selection [4]. In This Paper [5], they apply Arterial Immune Systems (AIS) for credit card fraud detection and compare it to other methods such as Bayesian Nets (BN) and Neural Nets (NN), Decision Trees (DT) and Naive Bayes. Genetic Algorithm (GA) and Exhaustive search are used to select optimized parameters sets, which minimizes the fraud cost basis on a credit card database, which is provided by a Brazilian card issuer. This fraud database is taken into account, such as skewness of data and deferent costs associated with false positives and negatives. These tests are done with sample sets, and all executions related that test is run using Weka (publicly available software). Our results are based on Bayesian Nets, which is better than Neural Nets. Neural Nets is usually widely used in the market today. So this Arterial Immune Systems has given the best performance when parameters optimized by Genetic Algorithm are used[5].

This paper [6] presents a system which is able to prevent subscription fraud in fixed telecommunications with the high impact on long distance carriers. So on this system, there's consists of a classification module and a prediction module. On the classification module, classifies subscribers according to their previous historical behaviour divided into four different categories: subscription fraudulent, otherwise fraudulent, insolvent and

normal. On the prediction module, this allows us to identify potential fraudulent customers at the time of subscription. On the classification module, this was implemented using fuzzy rules. This classification module was applied to a database containing information of over 10,000 real subscribers of a major telecom company. In this database, a subscription fraud detected round about 2.2. This prediction module was implemented as a multilayer perceptron neural network. While on its implementation, this multilayer perceptron neural network was able to identify 56.2% of the true fraudsters, screening only 3.5% of all the subscribers in the test set. This study shows the achievability of preventing fraud in telecommunications by analysing the application information and the customer past history at the time of application [6].

Identity crime mining [21] has increased extremely [7] over the modern years. So on this situation, Spike detection is important because it highlights rapid and quick rises in intensity relative to the current identity attribute value. On this paper, there's proposes the new spike analysis framework for monitoring sparse personal identity streams. For each identity pattern, it detects spikes in single attribute values and integrates many spikes from different attributes to produce a numeric suspicion score. Even if only the temporal representation is examined here, experimental results on artificial and real credit applications disclose some conditions on which the framework will perform well [7].

GSM (Global Services of Mobile Communications) 1800 licenses, this was approved in the start of the 2000's in Turkey [8]. Especially in the starting when the installation phase is running on the wireless telecom services, fraud usage can be an important source of revenue loss. Fraud can be defined as a dishonest or prohibited use of services, with the purpose to avoid service charges. Fraud detection is the activities', where we identify illegal usage and prevent losses for the mobile network operators'. Mostly mobile phone user's intentions may be predicted or check by the call detail records by using data mining techniques. On this paper, there's compares various data mining techniques to get the best practical solution for the telecom fraud detection and offers the Global Services of Mobile Communications, to measure the efficient fraud detection. In the experiment run, shown that ANFIS has provided sensitivity of 97% and specificity of 99%, where it classified 98.33% of the instances correctly [8].

Now a day, security is the most vital topic about internet banking [9]. The Primary objective of banks is ensuring their customers' electronic transactions. Fraudsters are becoming more complicated because to detect those is very crucial and they proceed really clever to achieve their target. So that ankhs have this knowledge of fraud so that the banks try to optimize their detection systems in order to recognize fraud and check the unexpected online transactions and behaviour. The objective of this paper is to show fraud detection. Separately from the offline internet banking, our scope is to present its role in fast and consistent detection of any strange transaction including fraudulent ones [9].

We apply five classification methods, Bayesian Nets (BN), Neural Nets (NN), Naive Bayes (NB), Artificial Immune Systems (AIS) and Decision Trees (DT), to detection the credit card fraud [10]. For a fair relationship, we fine adjust the parameters for each technique either through full search, or through Genetic Algorithm (GA). Furthermore, we evaluate these sorting methods in two training modes, a cost sensitive training mode where dissimilar cost for false negatives and false positives are considered in the training period, and a plain training mode. The study of possible cost sensitive meta heuristics to be functional is not in the domain of this work and all executions are run using Weka. Although Neural Network is claimed to be extensively used in the market these days, the evaluated completion of Neural Network in training gives quite poor results. Our experiments are consistent with the premature result of Maes, which conclude that BN is better than NN, by comparison of result. Cost sensitive training significantly improves the performance of all categorization methods separately from NB and, separately of the DT, training mode and AIS with, optimized parameters, is the best methods in our experiments [10].

Financial statement frauds (FSF) have usual significant attention from the public, the financial community and regulatory bodies because of numerous high profile frauds reported at large corporation such as Lucent, Enron, and WorldCom and Satam computers over the last few years. Falsify financial statements mainly consist of elements manipulating by overstating assets, profit, or understating liabilities [11]. First, there is a lack of knowledge about the characteristics of management fraud. Second, most auditors require the experience needed to detect it. Finally, financial managers and accountants are intentionally trying to mislead the auditors. These limitations propose the need for extra analytical events for the effective detection of false financial statements. Statistics and data mining methods which is defined have been applied successfully to identify behaviour such as telecommunications fraud, money laundering, e-commerce credit card fraud, insurance fraud, and computer intrusion [11].

This paper describes that for e-commerce companies, there is provided that online services, fraudulent access resulting from theft of identity credentials is a serious concern [12]. Such e-commerce companies' providers of organize a variety of defences and invest important time and effort to the analysis of a large amount of log data to detect spiteful activities and their impact. To reduce this burden of checking the log file, we explore the efficiency of an anomaly detection based approach that relies on uniqueness credential usage log records. More of the time, we use an anomaly based metric to achieve the risk of each identity credential usage, e.g., a login request etc. So for that, we make use of actual log data of login attempts to a university portal to evaluate the effectiveness of this approach. So our approach can work in combination with disturbance or fraud detection systems, which can detect the log file. It is also possible that if there is need to gain high risk then stronger verification can be required, which can help balance security and usability demands [12].

Fraud is one of the major ethical issues in the credit card industry [13]. The main purposes are, firstly, to recognize the different types of credit card fraud because this is most important and main thing, and, secondly, to analysis other techniques that have been used in fraud detection. The associate aim is to present, compare and analyse newly published findings in credit card fraud detection. This is depending on the type of fraud which is faced by banks or credit card companies. So for that purpose, various measures can be adopted and implemented to identify the fraud. The proposals of that paper, is expected to have valuable attributes in terms of cost savings and time efficiency. However, there are still moral issues when authentic credit card customers are misclassified as fraudulent [13].

Fraud detection is a massive problem for health insurance companies. The only way to fight with fraud makes a power mechanism and efficient fraud management systems [14]. Existing research society has paying attention great efforts on different fraud detection techniques, while neglecting other aspects is also important activities of fraud management. We suggest a holistic approach that focuses on 6 actions of fraud management, namely, (1) prevention, (2) deterrence, (3) detection, (4) investigation, (5) sanction and redress, and (6) monitoring. The main role of this paper, are 15 key characteristics of a fraud management system, which allow successful and efficient support to all fraud management activities. Keywords which are using are fraud management system, characteristics, and activities, insurance, health care [14].

Fraud detection is a key activity with serious socio economical impact [15]. Inspection behaviour linked with this task is usually forced by limited available resources. Methods of data analysis can give help in the task of deciding where to assign these limited resources in order to optimize the outcome of the inspection activities. In this paper, presents a multi strategy learning method to tackle the question of which cases to inspect first. The proposed methodology is based on the function theory and provides a ranking ordered by decreasing estimated outcome of inspecting the candidate cases. The proposed methodology is general and can be helpful on fraud detection activities with partial

inspection resources. We experimentally evaluate our proposal on both an artificial domain and on a real world task 15]. Now a days, payment flows take place on line, So we need effective and well-organized systems for the finding of credit card fraud [16]. A main feature of this problem is that it is extremely dynamic and active, as fraudsters continually adjust and adopt their strategies in response to the increasing superiority of detection systems. Hence, system training by experience to examples of previous examples of fake transactions can lead to fraud detection systems which are vulnerable to new pattern of fraudulent transactions. Problem of the nature suggests that Artificial Immune Systems (AIS) may have exacting utility for inclusion in fraud detection systems as AIS can be constructed which can flag' non standard' transactions without having seen examples of all possible such transactions during training of the algorithm. In this paper, we study the efficiency of Artificial Immune Systems (AIS) for credit card fraud identification using a huge dataset obtained from an online retailer. Three AIS algorithms were implemented and their act was benchmarked against a logistic regression model. The results propose that AIS algorithms have possible for addition in fraud detection systems but that extra work is necessary to realize their full possible in this domain [16]. Payment frauds are a form of intrusions where money is transfer from one bank account to the other bank account of a fraudster [17]. It is neither promising nor efficient to prevent 100 percent of payment frauds. It therefore becomes significant to sense payment frauds and to control their cost. The paper describes two unique insights into the type of payment fraud. This proposes a new risk based payment fraud detection method. This system does not try to sense individual fraudulent payments but a little seeks to calculate the expected loss from frauds over a given time period. This predictable loss is the risk posed by frauds, and fraud managers only need to interfere if this risk exceeds a maximum satisfactory loss threshold. Below this threshold, payment fraud related losses signify a limited risk, which should be viewed as an operating cost just like stealing is an operating cost in retail. The paper vitally appraises the risk based method and discusses its applicability in practice [17]. Fraud is a very harsh problem that expenditure the global economy trillions of dollars annually [18]. So, fraud detection is difficulties as perpetrators keenly attempt to wrap up their actions. In this paper, we observe the fraud detection problem and observe how learn classier systems can be useful to it. We convey the frequent properties of fraud, which can be tuned to display those characteristics. We report experiments on this theoretical problem with a accepted real time learning classier system algorithm [18]. The results from our experiments indicate that this method can prevail over the difficulties inherent to the fraud detection problem. At the end, when we apply the e algorithm to a real world problem (KDD Cup 1999 network intrusion detection), then we show that it can realize that we gain very good result in this domain [18].

The aims of this paper are to assess the use of technique of decision trees. In combination with the management model CRISP-DM, this technique helps in the prevention of bank fraud [19]. On this article, offers to study on decision trees, an important idea in the field of artificial intelligence. The study is paying attention on discuss, how these trees are able to support in the decision making process of identify frauds by the analysis of information concerning bank transactions. This information is captured with the utilize of techniques and the CRISP-DM management model of data mining in huge databases logged from internet bank transactions [19].With the developments in the IT (Information Technology) and improvements in the communication channels, fraud is scattering all over the world, ensuing in huge financial victims [20]. Still fraud avoidance mechanisms such as CHIP&PIN are developed; these mechanisms do not stop the most ordinary fraud types such as fraudulent credit card usages over virtual POS terminals or mail orders. As a result, fraud detection is the necessary tool and maybe the best way to stop such fraud types. In the is study, there's present classification models based on decision trees and support vector machines (SVM) are developed and functional on credit card fraud detection problem. Due to the study,

compare the performance of SVM and decision tree method in credit card fraud detection with a real data set [20].

For Fraud Detection, Techniques and Methods

Ref	Publication Year	System Name	Techniques	Reasons
[1]	2010	Subscription Fraud Prevention in Telecommunications using Fuzzy Rules and Neural Networks	multilayer perceptron neural network	subscription fraud detected
[2]	2008	Temporal Representation in Spike Detection of Sparse Personal Identity Streams	Spike Analysis Framework	Identity crime
[3]	2009	Fraud Detection Using an Adaptive Neuro-Fuzzy Inference System in Mobile Telecommunication Networks	Global Services of Mobile Communications	Detect the fraud on the installation phase
[4]	2007	Offline Internet Banking Fraud Detection	Offline internet banking fraud detection system	Detect the Fraud via offline internet bank detection
[5]	2011	Comparison with Parametric Optimization in Credit Card Fraud Detection	Neural Nets(NN),Bayesian Nets(BN), Naive Bayes(NB), Artificial Immune Systems(AIS) and Decision Trees (DT), to detection the credit card fraud	Credit Card Fraud Detection
[6]	2009	Financial Statement Fraud Detection by Data Mining	Financial statement frauds (FSF)	Detect fraud in financial activities
[7]	2006	Using Identity Credential Usage Logs to Detect Anomalous Service Accesses	anomaly based metric	Prevent the log records
[8]	2011	Holistic Approach to Fraud Management in Health Insurance	(1) deterrence, (2) prevention, (3) detection, (4) investigation, (5) sanction and redress, and (6) monitoring.	dEtect fraud on health insurance companies
[9]	2006	Credit card fraud and detection techniques	Genetic algorithms and other algorithms.	Detect fraud on banks or credit card companies
[10]	2008	Utility Based Fraud Detection	Utility-based Rankings	Outlier Ranking`
[11]	2009	Identifying Online Credit Card Fraud using Artificial Immune Systems	Artificial Immune Systems (AIS)	Identifying Online Credit Card Fraud
[12]	2008	Risk-Based Payment Fraud Detection	Risk-Based Payment Fraud Detection system	Identify fraud from one bank account to the other bank account
[13]	2010	Learning Classier Systems for Fraud Detection	Detected Fraud	
[14]	2008	IDENTIFYING BANK FRAUDS USING CRISP-DM AND DECISION TREES	Detecting fraud on bank transactions	Using CRISP-DM AND DECISION TREES
[15]	2011	Detecting Credit Card Fraud by Decision Trees and Support Vector Machines	classification models based on decision trees and support vector machines (SVM)	Detect and stop the fraud in the credit card.
[16]	2010	A Medical Claim Fraud/Abuse Detection System based on Data Mining: A Case Study in Chile	multilayer perceptron neural networks (MLP)	To detect fraud in medical domain

[17]	2010	An Identity Fraud Model Categorising Perpetrators, Channels, Methods of Attack, Victims and Organisational Impacts	identity about fraud and its category	
[18]	2010	On the communal analysis suspicion scoring for identity crime in streaming credit applications	communal analysis suspicion scoring (CASS)	identity crime in streaming credit applications
[19]	2007	Adaptive Spike Detection for Resilient Data Stream Mining	adaptive spike detection	crime detection domain
[20]	2011	Credit Card Fraud Detection with Artificial Immune System	Artificial Immune Systems(AIS)	credit card fraud detection and compare it to other methods

3. Conclusions

Now these days, fraud is a million dollar business and every year it is increasing more and more. In a crime survey in 2009, tells that close to 30% of the company's worldwide reported falling victim to fraud in the past year. Fraud involves individual or in a form of groups who intentionally act secretly to rob another of something of worth, for their own profit. Fraud is as against the humanity and it is unlimited variety of different forms. So in this paper, we introduce different methods and techniques to tackle the fraud and how to prevent the fraud into the organization, businesses, and hospital and insurance companies. Fraud prevention is a continuing battle. Many website owners must continually fight against many kinds of crime ranging from stealing identity theft and credit cards and many other types of fraud related to that. Internet Fraud is also very popular, where fraudster can steal the credit card number and buy thing from the different websites.

References

[1] P. A. Ortega, C. J. Figueroa and G. A. Ruz, "A Medical Claim Fraud/Abuse Detection System based on Data Mining: A Case Study in Chile", Proceedings of the 2006 International Conference on Data Mining, DMIN 2006, Las Vegas, Nevada, **(2006)**, pp. 224-231.
[2] P. A. Ortega, C. J. Figueroa and G. A. Ruz, **(2006)**, "A Medical Claim Fraud/Abuse Detection System based on Data Mining: A Case Study in Chile", Proceedings of the 2006 International Conference on Data Mining, DMIN 2006, Las Vegas, Nevada, USA, June 26-29, **(2006)**, pp. 224-231.
[3] C. Phua, R. Gayler, V. Lee and K. Smith-Miles, **(2009)**, "On the communal analysis suspicion scoring for identity crime in streaming credit applications", European journal of operational research, vol. 195, no. 2, pp. 595-612.
[4] C. Phua, R. Gayler, V. Lee and K. Smith-Miles, "On the communal analysis suspicion scoring for identity crime in streaming credit applications, "European journal of operational research", vol. 195, no. 2, pp. 595-612.
[5] M. F. A. Gadi, X. Wang and A. P. Do Lago, "Credit card fraud detection with artificial immune system", Artificial immune systems, **(2008)**, pp. 119-131.
[6] P. A. Estévez, C. M. Held and C. A. Perez, "Subscription fraud prevention in telecommunications using fuzzy rules and neural networks", Expert Systems with Applications, vol. 31, no. 2, **(2006)**, pp. 337-344.
[7] C. Phua, V. Lee, R. Gaylerand K. Smith, "Temporal representation in spike detection of sparse personal identity streams", Intelligence and Security Informatics **(2006)**, pp. 115-126.
[8] M. Sanver and A. Karahoca, "Fraud Detection Using an Adaptive Neuro-Fuzzy Inference System in Mobile Telecommunication Networks", Multiple-Valued Logic and Soft Computing, vol. 15, no. 2-3, **(2009)**, pp. 155-179.
[9] V. Aggelis, "Offline Internet banking fraud detection", Availability, Reliability and Security, 2006. ARES 2006. The First International Conference, **(2006)**.
[10] M. F. A. Gadi, X. Wang and A. P. do Lago, "Comparison with parametric optimization in credit card fraud detection", Machine Learning and Applications, ICMLA'08. Seventh International Conference, **(2008)**.
[11] G. Apparao, A. Singh, G. S. Rao, B. L. Bhavani, K. Eswar and D. Rajani, "Financial statement fraud detection by data mining", Corporate governance, vol 3, no. 4, **(2009)**.
[12] D. Mashima and M. Ahamad, Using identity credential usage logs to detect anomalous service accesses, Proceedings of the 5th ACM workshop on Digital identity management, ACM, **(2009)**.
[13] D. Mashima and M. Ahamad, "Using identity credential usage logs to detect anomalous service accesses", Proceedings of the 5th ACM workshop on Digital identity management, **(2009)**, pp. 73-80.

[14] Š. Furlan and M. Bajec, "Holistic approach to fraud management in health insurance", Journal of Information and Organizational Sciences, vol. 32, no. 2, , **(2008)**, pp. 99-114.
[15] L. Torgo and E. Lopes, "Utility-based fraud detection", IJCAI Proceedings-International Joint Conference on Artificial Intelligence, vol. 22, no. 1, **(2011)**, p. 1517.
[16] A. Brabazon, J. Cahill, P. Keenan and D. Walsh, "Identifying online credit card fraud using artificial immune systems", 2010 IEEE Congress on Evolutionary Computation (CEC), **(2010)**.
[17] K. Julisch, "Risk-based payment fraud detection", Computer Science, **(2010)**.
[18] M. Behdad and T. French, "Online learning classifiers in dynamic environments with incomplete feedback", Evolutionary Computation (CEC), 2013 IEEE Congress, **(2013)**, pp. 1786-1793.
[19] B. C. Da Rocha and R. T. de Sousa Júnior, "Identifying Bank Frauds Using Crisp-DM And Decision Trees", International journal of computer science & information Technology (IJCSIT), vol, 2, **(2010)**.
[20] Y. Sahin and E. Duman, "Detecting credit card fraud by decision trees and support vector machines", International MultiConference of Engineers and Computer Scientists, vol. 1, **(2011)**.
[21] M. Arif, K. Amjad Alam and M. Hussain, "Crime Mining: A Comprehensive Survey", International Journal of u- and e- Service, Science and Technology (IJUNESST), vol. 8, **(2015)**.
[22] M. Arif, K. Amjad Alam and M. Hussain, "Application of Data Mining Using Artificial Neural Network: Survey", International Journal of Dataabase Theory and Application (IJDTA), vol. 8, **(2015)**.

Author

Muhammad Arif is a PhD student at Faculty of CS and IT, University of Malaya. Currently he is working on Medical image Processing. His research interests include image processing, E learning, Artificial intelligence and data mining. He joined UM as a Bright Spark Scholar in September 2013 for the period of 3 years. Before this he completed masters and bachelor degrees in Pakistan. He received his BS degree in Computer Science from University of Sargodha, Pakistan in 2011. He obtained his MS degree in Computer Science from COMSATS Islamabad 2013 Pakistan.

Amil Roohani Dar is a Lecturer at Faculty of CS and IT, Comsats Institute of Information Technology (CIIT), Lahore. Currently he is working as Lecturer. His research interests include Semantic Web, E learning, Artificial intelligence and data mining. He joined CIIT Lahore as a Lecture in August 2014. Before this he completed masters and bachelor degrees in Pakistan. He received his BS degree in Computer Science from University of Azad Jammu & Kashmir (UAJ&K), Pakistan in 2010. He obtained his MS degree in Computer Science from COMSATS Islamabad 2014 Pakistan

