Volume 4, Issue 6, June 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Data Mining Modeling Techniques and Algorithm Approaches in Privacy Data

[1]Mohammed Younus
Lecturer at College of Computer and Information Sciences in
King Saud University.
(Al-Muzahimiyah Branch)
Saudi Arabia

[2]Dr.Ahmad A.Alhamed
Director of College of Computer and Information Sciences at
King Saud University,
(Al-Muzahimiyah Branch)
Saudi Arabia

[3]Khazi Mohammed Farooq
Lecturer at College of Computer and Information Sciences in
King Saud University
(AlMuzahmiyah Branch), KSA
Saudi Arabia

[4]Fahmida Begum
Associate Professor in
Dr. K.V Subba Reddy
college of MCA,
Kurnool, (Dt)
Saudi Arabia

Abstract: Data mining is the process of queries and extracting patterns from date. Data mining is important tool to transform the data from large quantities of data using pattern matching. Data mining has many applications in security including national security, terrorist activates and fraudulent behavior and cyber security. N recent years, advances in hardware technology have lead to an increase in the capability to store and record personal data of consumers and individuals. This has lead to concerns that the personal data may be misused for a variety of purposes. In order to alleviate these concerns, a number of techniques have recently been proposed in order to perform the data mining tasks in a privacy-preserving way. These techniques for performing privacy –preserving data mining are drawn from a wide array of related topics such as data mining, cryptography and information hiding. The field of privacy-preserving data mining has been explored independently by the cryptography, database and statistical disclosure control communities.

Piracy has seen rapid very fast in recent years because of the increase in the ability to store data. Privacy has been traditionally studies in the context of cryptography and information hiding recent emphasis on data mining has lead to renewed interest in the field. A number of techniques such as randomization and K-anonymity have been discussed in multiple communities such as the data base community. the statistical disclosure control community and the cryptography community,

In this paper we have describe important models, algorithms and applications in the privacy field in a structured and concise way and also privacy-preserving data mining and understanding the practical and algorithmic aspects of the area.

Keywords: ***Data Mining, Data mining issues, Randomization method, K-Anonymity.***

I. INTRODUCTION

Data mining is a recent emerging led, connecting the three worlds of Databases. Artificial Intelligence and Statistics. The information age has enabled many organizations to gather large volumes of data. However, the usefulness of this data is negligible if "meaningful information" or "Knowledge" cannot be extracted from it. Data mining, otherwise known as knowledge discovery, attempts to answer this need. In contrast to standard Statistical methods, data mining techniques search for interesting information without demanding a priori hypotheses. Now a day, advances in hardware technology have lead to an increase in the capability to store and record personal data about consumers and individuals is the confidentiality issues in data mining. The problem of privacy-preserving data mining has become more important in recent years because of the increasing ability to store personal data about users, and the increasing sophistication of data mining algorithms to leverage this information. The need of privacy is sometimes due to law or can be motivated by business interests. However, there are situations where the sharing of data can lead to mutual gain. This has lead to concerns that the personal data may be misused for a variety of purposes.

A number of techniques such as randomization and K-anonymity have been suggested in recent years in order to perform privacy-preserving data mining. Furthermore, he problem has been discussed in multiple communities such as the data base community, the statistical disclosure control community and the cryptography community. The technique is not even effective with increasing dimensionality, since the data can typically be combined with either public or background information to reveal the identity of the underlying record owners.

II. DATA MINING ISSUES

Data mining issues are not limited to, data quality, interoperability, missing creep and privacy . As with other aspects of data mining, while technological capabilities are important factors also influence the success of goal outcome.

Data Quality

Data quality is an issue that represents one of the biggest challenges for data mining. Data quality refers to the accuracy and completeness of the data. Data quality can also be affected by the structure and consistency of the data being analyzed. Now a day's duplicate records have the lack of data standards, the timeliness of updates, and human error can significantly impact the effectiveness of the more complex data mining techniques, which are sensitive to subtle differences that may exist in the data. To improve data quality, it is sometimes necessary to "clean" the data. which can involve the removal of duplicate records, normalizing the values used to represent information in the database (e.g.., ensuring that "no" is represented as a 0 throughout the data bas, and not some times as a 0, sometimes as an N, etc) accounting for missing data points, removing unneeded data fields, identifying anomalous data points and standardizing.

Privacy-Preserving

The issues of privacy is sharing of information and data mining initiatives have been announced, increased attention has focused on the implications for privacy, privacy focus both an actual projects proposed, as well as concerns about the potential for data mining applications to be expanded beyond their original purposes (mission creep). In some cases, anti-terrorism data mining application might also be useful for combating other types of crime as well. So far there has been little consensus about how data mining should be carried out, with several competing points of view being debated. Some observers contend that tradeoffs may need to be made regarding privacy to ensure security. Other observers suggest that existing laws and regulations regarding privacy protections are adequate, and that these initiatives do not pose any threats to privacy. Still other observers argue that not enough is known about how data mining projects will be carried out, and that greater oversight is needed. There is also some disagreement over how privacy concerns should be addressed, The in contrast, some privacy advocates argue in favour of creating clearer policies and exercising stronger oversight. As data mining variety of questions including, the degree to which government agencies should use and mix commercial data with government data, whether data sources are being used for purposes other than those for which they were originally designed, and the possible application of the Privacy Act to these initiatives.

Interoperability

The issue of interoperability of different data bases and data mining related software. It refers to the ability of computer system and/or data to work with other systems or data using common standards are processes. Interoperability is a critical part of the larger efforts to improve interagency collaboration and information sharing through e-government and homeland security initiatives. For data mining, interoperability of data bases and software is important to enable the search and analysis of multiple data base simultaneously, and to help ensure the compatibility of data mining activities of different agencies. Data mining applications that are trying to take advantage of existing legacy data bases or that are initiating first-time collaborative efforts with other agencies or levels of government (e.g., police departments in different states) may experience interoperability problems. Similarly, as agencies move forward with the creation of new data base and information sharing efforts, they will need to address interoperability issues during their planning stages to better ensure the effectiveness or their data mining application.

Mission Creep

Mission creep is one of the big risks of data mining cited by civil libertarians, and represents how control over one's information can be tenuous proposition. It refers to the use of data for purposes other than that for which the data was originally collected. This can occur regardless of whether the data was provided voluntarily by the individual or was collected through other means. Data holders may feel obligated to make any information available that could be used to prevent a future attack or track a known terrorist.

Government officials responsible for ensuring the safety of others may be pressured to use and/or combine existing data bases to identify potential threats. Unlike physical structures or the detention of individuals, accessing information for purposes other than originally intended may appear to be a victimless or harmless exercise. Those information uses can lead to unintended outcomes and produce misleading results outcome.

Quantification of Privacy

A key issue in measuring the security of different privacy-preservation methods is the way in which the underlying privacy is quantified. The idea in private quantification is to measure the risk of disclosure for a given level of perturbation.

Unit Based privacy –Preserving Data Mining

Most privacy-preserving data mining methods apply a transformation which reduces the effectiveness of the underlying data when it is applied to data mining methods or algorithms. Infect there is natural tradeoffs between privacy and accuracy, through this tradeoffs is affected by the particular algorithm which is used for privacy-preservation.. A key issue is to maintain maximum utility of the data without compromising the underlying privacy constraints.

Cryptographic Methods for Information sharing and Privacy

In some cases, multiple parties may wish to share aggregate private data, without leaking any sensitive information as their end [14]. A key problem that arises in any en masse collection of data is that of confidentiality. However, there are situations where the sharing of data can lead to mutual gain. A key utility of large data bases today is research, whether it is scientific or economic and market oriented. Thus, for example, the medical fields has much to gain by pooling data for research; as can even competing business with mutual interests. Despite the potential gain, this is often not possible due to the confidentiality issues which arise. Another example, different superstores with sensitive sales data may wish to coordinate among them in knowing aggregate trends without leaking the trends of their individual stores. This requires secure and cryptographic protocols for sharing the information across the different parties. The data may be distributed in two ways across different sites:

Horizontal Partitioning: In this case, the different sites may have different sets of records containing the same attributes.
Vertical Partitioning: In this case, the different sites may have different attributes of the same sets of records. The challenges for the horizontal and vertical partitioning case are quite different.
Privacy Attacks: It s useful to examine the different ways in which one can make adversarial attacks on privacy-transformed data . This helps in designing more effective privacy-transformation methods. Some examples of methods which can be used in order to attack the privacy of the underlying data include SVD-based methods, spectral filtering methods and background knowledge attacks.

Privacy-Preservation of Data Streams

A new topic in the area of privacy preserving data mining is that of data streams, in which data grows rapidly at an unlimited rate. In such cases, the problem of privacy-preservation is quite challenging since the data is being released incrementally. In addition, the fast nature of data streams obviates the possibility of using the past history of the data. We note that both the topics of data streams and privacy-preserving data mining are relatively new, and there has not been much work on combining the two topics.

III. THE KEY FIELDS OF PRIVACY –PRESERVNG IN DATA MINING

Privacy – Preserving Data Viewer

The technique used to study different transformation methods associated with privacy, those techniques are randomization [1], K-anonymity [16] and diversity [11]. How the perturbed data can be used in conjunction with classical data mining methods such as association rule mining [15], other related problems include that of determining privacy-preserving methods to keep the underlying data useful (utility-based methods), or the problem of studying the different definitions of privacy, and how they compare in terms of effectiveness in different scenarios.

Privacy – Privacy Changing the Data Mining Applications Results

The privacy changes in the database application result of such as association rule or classification rule mining can compromise the privacy of the data. This has spawned a field of privacy in which the result of data mining algorithms such as association rule mining are modified in order to preserve the privacy of the data.

Privacy-Privacy Methods for Distributed Cryptographic

In cryptographic distributed methods the data may be distributed multiple sites and the owners of the data across these different sites may wish to compute a common function. In this such cases, a variety of cryptographic protocols may be used in order to communicate among the different sites, so that secure function computation is possible without revealing sensitive information.

IV. DATA MINING METHODOLOGY

It should be clear from the above that data mining is not a single technique: any method that will help to get more information out of data is useful. Different methods serve different purposes, each method offering its own advantages and disadvantages. However most methods commonly used for data mining can be classified into the following groups. Statistical Methods: Historically, statistical work has focused mainly on testing of preconceived hypotheses and on fitting Models to data statistical approaches usually rely on an explicit underlying probability model. In addition it is generally assumed that these methods will be used by statisticians, and hence human intervention is required for the generation of candidate hypotheses and models.

Case based Reasoning

Case-based reasoning (CBR) is a technology that tries to solve a given problem by making direct use of past experiences and solutions. A case is usually a specific-problem that has been previously encountered and solved. Given a particular new problem, case based reasoning examines the set of stored cases and finds similar ones. If similar case exist, their solution is applied to the new problem, and the problem is added to the case base for future reference.

Neural Networks

Neural Networks (NN) are a class of systems modeled after the human brain. As the human brain consists of millions of neurons that are interconnected by synapses, neural networks are formed from large numbers of simulated neurons,

connected to each other in a manner similar to brain neurons. Like in the human brain, the strength of neuron interconnections may change (or be changed by the learning algorithm) in response to a presented stimulus or an obtained output , which enables the network to "learn". Decision Trees: A decision tree is a tree where each non-terminal mode represents a test or decision on the considered data item. Depending on the out come of the test, one chooses a certain branch. To classify a particular data item, we start at the root node and follow the assertions down until we reach a terminal node (or leaf). When a terminal node is reached, a decision is made. Decision trees can also be interpreted as a special form of a rule set, characterized by their hierarchical organization of rules.

Role induction

Rules state a statistical correlation between the occurrences of certain attributes in a data item, or between certain data items in a data set. The general form of an association rule is XI..Xu..,Y [C, S], meaning that the attributes X1..Xn..predict Y with a confidence C and significance S. Bayesian Belief Networks. Bayesian belief networks (BBN) are graphical representation of probability distributions, derived from co-occurrence counts in the set of data items. Specifically, a BBN is a directed, acyclic graph, where the nodes represent attributes variables. And the edges represents probabilistic dependencies between the attributes variables. Associated with each node are conditional probability distributions that describe the relationships between the node and its parents.

V. CONFIDENTIAL ISSUES IN DATA MINING

When the key problem arises in any en masse collection of data is that of confidentiality. The need for privacy is sometimes due to law (e.g., for medical data base) or can be motivated by business interests. There are situation where the sharing of data can lead to mutual gain. A key utility of large databases today is research, whether it is scientific or economic and market oriented. Thus, for example, the medical field has much to gain by pooling data for research, as can even competing business with mutual interests. Despite the potential gain, this is often not possible due to the confidentiality issues which arise. Our scenario is the following.

Let a1 and a2 be parties owning private databases D1 and D2. Both parties wish to apply a data – mining algorithm to the joint database D1UD2 without revealing any unnecessary information about their individual database. The only information learned by a1 about D2 is that which can be learned from the output of the data mining, algorithm, and vice versa.. We do not assume any "trusted" third party who computes the joint output. In our model there exists a secure-protocol for any probabilistic polynomial – time functionality [10,17], However, as we discuss in Section 3.3 these generic solutions are very inefficient, especially when large inputs and complex algorithms are involved. Thus, in the case of private data mining, more efficient solutions are required. It is clear that any reasonable solution must have the individual parties to the majority of the computation independently. Our solution is based on this guiding principle and in fact, the number of bits communicated is dependent on the number of transactions by a logarithmic factor only. We remark that a necessary condition for obtaining such a private protocol is the existence of a (non-private) distributed protocol with low communication complexity. In any multi-party computation setting, a malicious adversary can always alter its input. The data mining setting, in fact can be very damaging since the adversary can define I its input to be the empty database. The output obtained is the result of the algorithm on the other party's database alone. Although this attack cannot be prevented, we would like to prevent a malicious party from executing any other attack. However, for this initial work we assume that the adversary is semi-honest. That is, it correctly follows the protocol specification, yet attempts to learn additional information by analyzing the transcript of messages received during the execution. We remark that although the semi-honest adversarial model is far weaker than the malicious model. This is because deviating from a specified program which may be buried in a complex application is a non-trivial task. Semi-honest adversarial behavior also models a scenario in which both parties that participate in the protocol are honest.

VI. PRIVACY- PRESERVING DATA MINING ALGORITHMS

We discuss the key stream data mining problems and will discuss the challenges associated with each problem in privacy-preserving. To solve the problem there are lot algorithms. That algorithms are statistical disclosure control method, measure of Anonymity method, K-anonymity method, Randomization method.

Measures of Anonymity

There are very large number of definitions of anonymity in the privacy-preserving data mining field. This is partially because of the varying goals of different privacy-preserve data mining algorithms. For example methods such as K-anonymity I-diversity and t-closeness are all designed to prevent identification, though the final goal is to preserve the underlying sensitive information. Each of these methods is designed to prevent disclosure of sensitive information in a different way.

The K-anonymity method

An important method for privacy de-identification is the method of K-anonymity [16]. The motivating factor behind the K-anonymity technique is that many attributes in the data can often be considered Pseudo-identifiers which can be used in conjunction with public records in order to uniquely identify the records. For example, if the identifications from the records are removed., attributes such as the birth date and zip-code and be used in order to uniquely identify the

identities of the underlying records. The idea in K-anonymity is to reduce the granularity of representation of the data in such a way that a given record cannot be distinguished from at least (k-1) sector records.

The Randomization method

The randomization technique uses data distortion methods in order to create private representation of the records [1, 4]. In most cases, the individual records cannot be recovered, but only aggregate distributions can be used for the data mining purposes. Two kinds of perturbations are possible with the randomization method.

Additive Perturbation

In this case randomized noise is added in the data records. The overall data distribution can be recovered from the randomized records. Data mining and management algorithms re designed to work with these data distributions.

Multiplicative Perturbation

In this case, the random projection or random rotation techniques are used in order to perturb the records.

VII. APPLICATIONS OF PRIVACY- Preserving Data Mining

The applications of privacy -preserving data mining has numerous applications in homeland security, medical database, mining and customer transaction analysis. Some of these applications such as those involving bio-terrorism and medical database mining may intersect in scope. In this section, we will discuss a number of different applications of privacy-preserving data mining methods.

Medical Databases – The scrub and Data Fly Systems

The scrub system [11] was designed for de-identification of clinical notes and letters which typically occurs in the form of textual data. The clinical data's are typically in the form of text which contains references to patients, family members, addresses, phone numbers or providers . Traditional techniques simply use a global search and replace procedure in order to provide privacy. However clinical notes often contain cryptic references in the form of abbreviations which may only be understood either by other providers or member of seems to suggest that the method becomes increasingly infeasible to implement effectively with increasing dimensionality.

Bioterrorism Applications

It is used in application on bioterrorism applications, we would like to analyze medical data for privacy-preserving data mining purposes. Often a biological agent such as anthrax produces symptoms which are similar to other common respiratory deceases such as the cough, cold and the flu. In the absence of prior knowledge of such an attack, health care's providers may diagnose a patient affected by an anthrax attack to have symptoms from one of the more common respiratory diseases. In many cases, an unusual number of such cases in a given locality may indicate a bio-terrorism attack. Therefore in order to identify such attacks it is necessary to track incidences these common dioceses as well. Therefore, the corresponding data would need to be reported to public health agencies. The common respiratory deceases are not reportable deceases by law. The solution proposed that is of "selective revelation" which initially allows only limited access to the data. However, in the event of suspicious activity it allows a drill down" into the underlying data. This provides more identifiable information in accordance with public health law.

Credential Validation Problem

In this problem, we are trying to match the subject of the credential to the person presenting the credential. For example, the theft of social security numbers present a serious threat to homeland security. In the credential validation approach [7], it is made to exploit the semantics associated with the social security number to determine whether the person presenting the SSN credential truly owns it.

Identity Theft

A related technology [15] is to use a more active approach to avoid identity theft. The identity angel system [5] crawls through cyberspace and determines people who are at risk from identity theft. This information can be used to notify appropriate parties. We note that both the above approach to prevention of identity theft are relatively non-invasive and therefore do not violate privacy.

Web Camera Surveillance

The possible method for surveillance is with the use of publicly available webcams which can be used to detect unusual activity. This is a much more invasive approach that the previously discussed techniques because of person specific information being

Captured in the webcams. The approach can be made more privacy—sensitive by extracting only facial count information from the images and using these in order to detect unusual activity. It has been hypothesized in that unusual activity can be detected only in terms of facial count rather than using more specific information about particular individuals. This kind of approaches uses a domain specific downgrading of the information available in the webcams in order to make the approach privacy-sensitive.

Genomic Privacy

Now a days the database of collected DNA are growing very fast in the both the medical and law enforcement communities. DNA data is considered extremely sensitive since it contains almost uniquely identifying information about an individual. As in the case of multi dimensional data simple removal of directly identifying data such as social security numbers is not sufficient to prevent. It has used a software called Clean Gene can determine the identification of DNA entries independent of any other demographic or other identifiable information.. The software relies on publicly available medical data of particular diseases in order to assign identifications to DNA entries. It was shown in [13] that 98-100 % of the individuals are identifiable sing this approach. The identification is done by taking the DNA sequence of an individual and then constructing a genetic profile corresponding to the sex, genetic diseases, the location where the DNA was collected etc. This genetic profile has been shown in to be quite effective in identifying the individual to a much smaller group. One way to protect the anonymity of such sequences is with the use of generalization lattices which are constructed in such a way that an entry in the modified database cannot be distinguished from at least (k-1) other entries. Another approach is constructs synthetic data which preserves the aggregate characteristics of the original data, but preserves the privacy of the original records. Another method for compromising the privacy of genomic data is that of trail-re identification, in which the uniqueness of patient visits patterns in exploited in order to make identifications. The premise of this work is that patients often visit and leave behind genomic data at various distributed locations and hospitals. The hospitals usually separate out the clinical data from the genomic data and make the genomic data available for research purposes.

VIII. CONCLUSION

Today, most enterprises are actively collecting and storing large database. Many of them have recognized the potential value of these data as an information source for making business decisions. The dramatically increasing demand for better decision support is answered by an extending availability of knowledge discovery and data mining products, in the form of research prototypes developed at various universities as well as software products from commercial vendors. In this paper we provide an overview of common knowledge discovery tasks-approaches to solve these tasks and available software tools employing these approaches. In this paper, we discussed a variety of data modification techniques such as randomization and k-anonymity based techniques. We discussed methods for distributed privacy-preserving mining and the methods for handling horizontally and vertically partitioned data. We discussed the issue of downgrading the effectiveness of data mining and data management applications such as association, rule mining, classifications and query processing.

We discussed some fundamental limitations of the problem of privacy preservation in the presence of increased amounts of public information and knowledge. Finally we discussed a number of diverse application domains for which privacy-preserving data mining methods are useful. We introduced the problem of privacy-preserving data mining and discussed the broad areas of research in the field. The broad areas of privacy are corresponds to sanitizing the data, so that its privacy remains preserved and corresponds to designing data management and mining algorithms in such a way that the privacy.

REFERENCES

[1] Adam N, Wortmann J,C. Security –control methods for Statistical Database: A Comparison Study, ACM Computing Surveys, 21(4),2009

[2] Agarwal R.Srikant R. Privacy-Preserving Data Mining, Proceedings of the ACM SIGMOD Conference, 2009

[3] Agarwal R.Srikant R.Thomas D Privacy-Preserving OLAP, Proceedings of the ACM SGMOD Conference, 2010.

[4] Bertino E Fovino L Provenza L-A Framework for Evaluating Privacy-Preserving Data Mining, Algorithms, Data Mining and Knowledge Discovery Journal , 11(2), 2005

[5] DARPA, Report to Congress Regarding the Terrorism Information Awareness Program, May 20, 2005 [http://www.eff,org/privacy/TIA/IIA-report.pdf]

[6] CRE Report RL31786, Total Information Awareness Program : Funding . Composition and Oversight Issues by Anny Belasco.

[7] IBM Corporation Intelligent Miner 2-1.http://www.softwareibm.com /data/intelli-mine,1968.

[8] IBM Corporation.PVE1.0.http://www.ibm.com/news/950203/pre-01.html,1995.

[9] Information Discovery Inc The IDS Information Discovery System , http://datamining.com,1997.

[10] Integral Solution Ltd Clementine 5.0 http://www.isl.co.uk/clen-html1998.

[11] Isoft S.A Alice 3.1 http://www.alice-soft.com, 2000

[12] Kamber M.Han J.and Chiang I.Y Using Data Cubes for Meta Rule – Guided Mining of Multi-Dimensional Association Rules, Technical Report U SFraser-CMPT-TR:1997-10, Simon Fraser University, Burnaby, May 1997

[13] Kohavi, R., Sommer field, D., and Doughrety J. Data Mining using MLC++: A Machine Learning Library in C++ . Tools with AI'96, 234-245, November 1996.

[14] Kovach Computing Services, MYSP.0.

[15] http://www.kovcomp.co.uk /mvsp.html.2000. [15] Lippmann, R.P.. An introduction to computing with Neural Nets.IEEE ASSP Magazine, 4-22, April 1987.

[16] Megaputer Intelligence Ltd. Poly analyst 3.5 http://www.megaputer.com, 1998
[17] Meta Group Inc. Data Mining: Trends, Technology, and implementation Imperatives. Stamford CT, February, 1997.
[18] Microsoft Corp. MSBN 1.0.
[19] Brooks, P. Visualizing Data – Sophisticated Graphic Visualization and Development Tools Tailored for Business Applications in DBMS, Miller Freeman Inc., Sanmateo , CA, August, 2003.
[20] Brunk, C. Kelly. J and Kohavi, R. Mineset: An Integrated System for Data Mining. In Proceedings of the Third International Conference on Knowledge Discovery and Data Mining, August, 1997. (Can be retrieved from http://robotics.stanford.edu/users/ronnyk/ronnyk-bip.html)
[21] Business Objects S.A. BusinessMiner 4.1.http://www.businessobjects.com. San Jose, CA, 1998.
[22] Clark, P., and Boswell, R. Rule Induction with CN2 some recent improvements. In Kodratoff, Y (ed.), Machine Learning – EWSL – 91 Springer – Verlag, Berlin 151-163-1991.
[23] Cohen, W. Fast effective rule induction. Proceedings of the Twelfth International Conference on Machine Learning , Lake Tahoe, California, 1995.
[24] Data Distilleries Inc. Online Data Mining (tm)-Data Distilleries' vision on data mining technology. White paper DD-R9704, Amesterdam, May 1997
[25] Dehaspe, L., Van Laer, W, and De Raedt, L. Claudies, the Clausal Discovery Engine – User's Guide 3.0. Technical Report CW239, Department of Computing Science, K.U.Leuven, 1996.

AUTHOR PROFILE

1) MOHAMMED YOUNUS did M.S (IT) from University of East London in 2010. I have 4 years of experience in Academics worked as a lecturer in London College of Human Resource and Management At present working as Lecturer at College of Computer and Information Sciences in KING SAUD UNIVERSITY.(AL-MUZAHIMIYAH BRANCH).

2) DR.AHMAD A.ALHAMED is the Director of College of Computer and Information Sciences at KING SAUD UNIVERSITY(AL-MUZAHIMIYAH BRANCH)

3) Khazi Mohammed Farooq did Master of Computer Applications (MCA) from Osmania University in 1998. I have total 15 years experience of Academic Teaching and working as Senior System Network Administrator Engineer in Data Center at College of Telecommunication and Information, Riyadh KSA. At present working as Lecturer at College of Computer and Information Sciences in King Saud University (AlMuzahmiyah Branch), KSA. My area of Interest in Data Center and Networks.

4) Fahmida Begum did his MCA from Osmania University, and Ph.D from MJPRU , U. P. Her interested areas are mobile computing and cloud computing . she has 9 years experience of Teaching in various colleges. At present she is working as an Associate Professor in Dr. K.V Subba Reddy college of MCA, Kurnool.(Dt).

