International Journal of Scientific Research in Computer Science and Engineering
Technical Paper Vol-1, Issue-4 ISSN: 2320-7639

Convergence of IT and Data Mining with other technologies

Shilpa Mahajan

School of Engineering and Technology, Ansal University, India

Available online at www.isroset.org

Received: 03 July 2013 Revised: 10 July 2013 Accepted: 07 August 2013 Published: 30 August 2013

***Abstract*—** In this age of technology and communication convergence, we cannot help but be impacted by technologies and innovations that center on computers. This paper examines the growing need for a secure environment and a general-purpose analytics engine. The process need for secure environment is Physical or It security and the process used for analysis is called Data Mining. This paper will also give us the review towards the convergence of various technologies such as IT and Physical Security and data mining with biology, computing, mobility, knowledge management, etc. for human values like privacy, recognition, operational intelligence, etc. and also relationship between data mining/IT security.

Keywords- IT security, physical security, convergence; mobility data mining; genomics; proteomics; RMS; process management

I. INTRODUCTION

A. Physical Security and IT Security- Physical security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism. It is often overlooked (and its importance underestimated) in favor of more technical and dramatic issues such as hacking, viruses, Trojans, and spyware. However, breaches of physical security can be carried out with little or no technical knowledge on the part of an attacker. Moreover, accidents and natural disasters are a part of everyday life, and in the long term, are inevitable.

IT security also known as cybersecurity or computer security) is information security as applied to computers and networks. The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction.

B. Data Mining- Data mining also called data discovery or knowledge discovery is the process of analyzing data from different perspectives and summarizing it into useful information.Data mining is used in many industries where there is a need to find patterns in vast amounts of data. It is being used to find sequences in DNA, predict manufacturing defects, identifying drivers of student performance, optimize transportation logistics, forecast energy consumption, and, most recently, to identify threats to national security.

Data Mining Consists of Five MajorEelements

- 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.

Different Levels of Analysis are Available

1) Artificial neural networks: Non-linear predictive models that learn through training and resemble biological neural networks in structure.

2) Genetic algorithms: Optimization techniques that use process such as genetic combination, mutation, and natural

3) selection in a design based on the concepts of natural evolution.

4) Decision trees: Tree-shaped structures that represent sets of decisions. These decisions generate rules for the classification of a dataset. Specific decision tree methods include Classification and Regression Trees (CART) and Chi Square Automatic Interaction Detection *(CHAID).* CART and CHAID are decision tree techniques used for classification of a dataset. They provide a set of rules that you can apply to a new (unclassified) dataset to predict which records will have a given outcome. CART segments a dataset by creating 2-way splits while CHAID segments using chi square tests to create multi-way splits. CART typically requires less data preparation than CHAID.

5) Nearest neighbor method: A technique that classifies 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. Sometimes called the k-nearest neighbor technique.

6) Rule induction: The extraction of useful if-then rules from data based on statistical significance.

Corresponding Author: *Shilpa Mahajan*

7) Data visualization: The visual interpretation of complex relationships in multidimensional data. Graphics tools are used to illustrate data relationships.

C. Convergence- It is a coming together of two or more distinct entities or phenomena. Convergence is increasingly prevalent in the IT world; in this context the term refers to the combination of two or more different technologies in a single device.

II. PHYSICAL AND IT SECURITY CONVERGENCE

The Open Security Exchange(SM) (OSE) is a not-for-profit association of security experts that provides a forum for end-users, manufacturers, integrators, consultants and allied organizations to mutually define opportunities for converging physical and IT security. Its goal is to help improve enterprise security through the collaborative development of reusable models, definitions, vendor-neutral interoperability specifications and best practice guidelines that accelerate the convergence of security systems.

A. The Coming of Physical/IT Security Convergence

Today, virtually all organizations with physical and IT assets protect those assets in a variety of ways. There are alarm systems to protect facilities and their contents from unlawful entry. There are firewalls to stop intrusion into corporate networks. Corporate assets may also be safeguarded by the use of employee ID badges, software application passwords, and a growing number of technologies, from magnetic cards and readers to biometric finger scans. The scope of security systems spans physical access, logical access, video surveillance and storage, identity management, and more. While all of these security technologies share a common purpose, those that protect physical assets and those that protect IT assets have virtually nothing else in common. They have always existed in parallel, evolving separately and residing under the control of separate organizations. This has resulted in a lack of integration and interoperability between physical and IT security systems. With today's heightened security concerns, this lack of integration is no longer simply an inconvenience. It increases security risks by preventing technologies from working in concert with one another. It limits corporations' efforts to establish centralized control of security and develop integrated risk management strategies. It prevents coordinated responses to security breaches by physical and IT security systems. With no integration between physical and IT security systems, organizations cannot pursue cost synergies, fully address privacy issues, or ensure compliance with a growing number of government and industry regulations. The solutions to these problems will come from the convergence of physical and IT security technologies.

B. Convergence as the migration of Physical and IT security towards common objectives, processes and architectures

The OSE defines convergence as the migration of physical and IT security towards common objectives, processes and Architectures. This migration includes:

1. Objectives:
   - Cost reduction/Revenue enhancement/Regulatory compliance
   - Improve asset/personnel protection
   - Improve operational efficiency of physical/IT security staff
2. Processes:
   - Collaborative planning between physical/IT staff on security strategy
   - Identify/eliminate security gaps
   - Best practices and policies for converged security
3. Architecture:
   - Strategic, tactical and operational security modeling
   - Interoperability standards and policies for physical and IT systems
   - Combined credentials for physical and logical security

Physical/IT security convergence will enable vendor-neutral interoperability among diverse security components to support overall enterprise risk management needs. As physical and IT security merge, networked computer technology and associated applications will provide enterprises with increased operational efficiencies and intelligent security.

III. RECOGNITION, MINING, SYNTHESIS

It is extraordinarily difficult to accurately predict which next-generation applications will become popular. The ability to have computers intelligently understand and interpret data will help us in business, medicine, sociology, science, and personal hobbies. There are some reasons why systems that can help us understand and interpret data will be important:

The web is shifting its focus from "data presentation to end-users" to "automatic data processing on behalf of end-users." Today's World Wide Web is a distributed data repository, a distributed compute infrastructure, and a composable service infrastructure. Most of the Web's current contents are intended for humans to read, not for computer programs to analyze. However, the Web has recently begun to transform into the "Semantic Web" [7]. This will change the Web's functionality from "delivering data to users" to "processing data for users." Computers will use automated reasoning to help us understand and interpret structured collections of information via sets of inference rules.

There is an inherent gap between a user's conceptual model of a problem they want solved and his/her computer's model of the problem. One of the primary goals of any computer system is to interact with its user and respond to user commands efficiently. "Fig. 1" shows a major challenge to achieving this goal is bridging the gap between the user's and computer's model of the underlying problem

to be solved. This gap is also known as Norman's gulf [6]. As noted by Norman in his seminal paper, a typical everyday problem requires multiple iterations of "execute and evaluate" between the user and the system. Iteration consists of the user's deciding which command he/she believes will result in the computer's solving the problem and constructing the command in a machine-readable format; then the computer's executing the command and generating user readable output. Each such iteration normally narrows the modeling gap. Given the increasing complexity of emerging end-user compute scenarios, Norman's gulf has been growing.

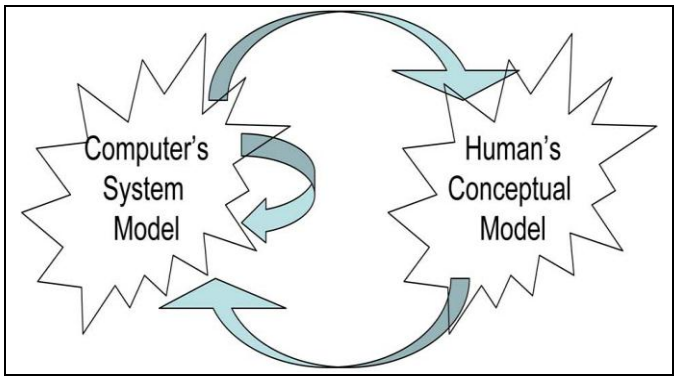

Figure 1. Norman's Gulf

Fortunately, emerging computer usage models are introducing new ways to bridge Norman's gulf. Instead of involving the end-user in every iteration, an alternative is to depend on a computer's ability to refine model instances by itself. This allows a reduction in the number of interactions between a user and his/her computer, and therefore an increase in the system's efficiency.

The above two are examples of the tasks of an "analytics engine" that can model events, objects, and concepts based on what we show the computers and on the data accessible to them. Hence, we must be able to communicate with computers in more abstract terms (high-level concepts or semantics). We believe that an analytics engine must have the capability to construct, manipulate, and evaluate mathematical models. These capabilities can be classified as three distinct classes: recognition, mining, and synthesis (RMS).

A. Recognition

Computers examine data and images and construct mathematical models based on what they "see." Depending on the data provided, that model could be of a valuable vase, a terrorist's behavior pattern, the right time to sell a particular type of stock, or the qualities needed by an actor to successfully play the part of Othello. This is a type of machine learning called recognition. Recognition is the "what is." It is identifying that a set of data constitutes a model and then constructing that model.

B. Mining

Once a computer has recognized the "what is" and turned that data into a model, the computer must be able to search for instances of the model. This is mining. Mining refers to searching a data set, such as the Web, and asking "is it?" to find instances of a model.

C. Synthesis

Synthesis is discovering "what if" cases of a model. If an instance of the model does not exist, a computer should be able to create a potential instance of that model in an imaginary world. In other words, synthesis is the ability to create an instance of a model where one does not exist. For example, if a director is considering switching an actor in some play, synthesis will show how that new actor would appear in the play and possibly predict the success of making the switch. "Fig. 2" shows RMS taxonomy.

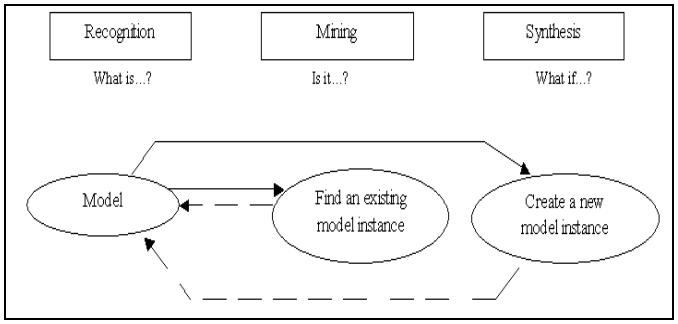

Figure 2. RMS Taxonomy

Beyond its use as taxonomy, RMS offers a view of the underlying technologies [14]. Traditionally we have treated "R," "M," and "S" components as independent application classes. For example, graphics applications used by animation movie studios to render high-quality animated movies are primarily synthesis applications. Similarly, data warehousing primarily involves mining. In contrast, emerging interactive applications use a combination of technologies that span the RMS spectrum.
"Fig. 3" shows how RMS used in Medicine?

Through RMS, a Tumor could be:

- Recognized as a model.
- Identified through mining patient data as the type of tumor in a particular patient.
- Synthesized in a way that would predict the effects of the tumor's progression for a particular patient and whether treatment is advisable.

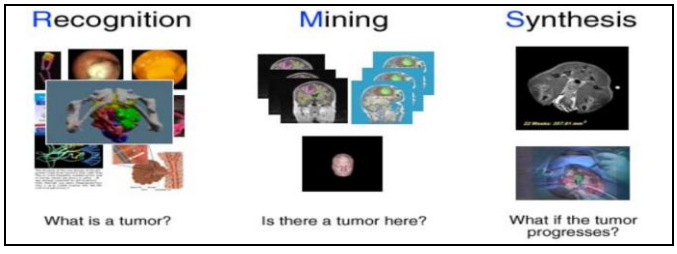

Figure 3. Example of how RMS used in Medicine

IV. DATA MINING WITH MOBILITY AND PRIVACY

A. Mobility

Mobility data means the data made available by the wireless and mobile communication technologies. Our everyday actions, the way people live and move, leave digital traces in the information systems of the organizations that provide services through the wireless networks for mobile communication. This mobility data is turned in to mobility knowledge, that is, useful models and patterns that abstract away from the individual and shed light on collective movement behavior, pertaining to groups of individuals that is worth putting in to evidence.

This conversion of mobility data into mobility knowledge is done with the help of Mobility Data Mining [6]. It is the process of automatically discovering useful information in large data repositories. The traditional data analysis tools and techniques cannot be used because of the massive volume of data gathered. Data Mining is a step of Knowledge discovery in databases, so-called KDD process for converting raw data into useful knowledge.

The three most popular types of data mining techniques can be used for turning mobility data to mobility knowledge:

1) Predictive modeling: The goal is to develop classification models, capable of predicting the value of a class label or target variable as a function of other variables or explanatory variables; the model is learnt from historical observations, where the class label of each sample is known: once constructed, a classification model is used to predict the class label of new samples whose class is unknown.

2) Association analysis: Also called pattern discovery, the goal is precisely to discover patterns that describe strong correlations among features in the data or associations among features that occur frequently in the data. The discovered patterns are presented in the form of association rules.

3) Cluster analysis: The goal is to partition a data set into groups of closely related data in such a way that the observations belonging to the same group, or cluster, are similar to each other, while the observations belonging to different clusters are not.

So, Mobility data mining is a novel geographic discovery process composed of three main steps:

a) Trajectory reconstruction: The stream of raw mobility data has to be processed to obtain trajectories of individual moving objects, the resulting trajectories should be stored into appropriate repositories, such as trajectory database or data warehouse.

b) Knowledge extraction: Spatiotemporal data mining methods are needed to extract patterns out of trajectories.

c) Knowledge delivery: It is necessary to reason on patterns, evaluate patterns' interestingness, refer them to geographic information and find out appropriate presentations and visualizations.

B. Privacy

There is a little path from opportunities to threats: we are aware that the donors of the mobility data are the citizens, and making this data publicly available for the mentioned purposes would put at risk our own privacy, our natural right to keep secret the places we visit, the places we live or work at and the people we meet- all in all, the way we live as individuals. The personal mobility data, as gathered by the wireless networks, are extremely sensitive information; their disclosure may represent a brutal violation of the privacy protecting rights. So the problem is to find an optimal trade-off between two conflicting goals; from one side, we would like to have precise, fine-grained knowledge about mobility, which is useful for the analytic purposes; from the other side, we would like to have imprecise, coarse-grained knowledge about mobility, which puts us in repair from the attacks to our privacy. It is interesting that the conflict between opportunities and risks can be read as a mathematical problem or as a social challenge. Indeed, the privacy issues can only be addressed through an alliance of technology, legal regulations and social norms.

V. DATA MINING WITH BIOLOGY AND COMPUTING

A. Biology

Biology is in the middle of a data explosion. The technical advances achieved by the genomics, metabolomics, transcriptomics and proteomics technologies in recent years have significantly increased the amount of data that are available for biologists to analyze different aspects of an organism [13]. Modern biology studies generate a large amount of data that require dedicated computational tools for their analysis. Data integration is also gaining importance given the need for extracting knowledge from multiple data types and sources, with the aim of inferring insights from the genetic processes underlying them. In fact, since the completion of genome sequences, functional identification of unknown genes has become a principal challenge in systems biology. Bioinformatics plays an important role here, allowing biologists to make full use of the advances in computer science in analyzing large and complex datasets.

B. Data Mining in Genomics

Genomics is the study of an organism's genome and deals with the systematic use of genome information to provide new biological knowledge. Many data mining techniques have been proposed to deal with the identification of specific DNA sequences. The most common include neural networks, Bayesian classifiers, decision trees, and Support Vector Machines (SVMs,) [4]. Sequence recognition algorithms exhibit performance tradeoffs between

increasing sensitivity (ability to detect true positives) and decreasing selectivity (ability to exclude false positives). However state, traditional data mining techniques cannot be directly applied to this type of recognition problems. Thus, there is the need to adapt the existing techniques to this kind of problems. Attempts to overcome this problem have been made using feature generation and feature selection [9]. Another data mining application in genomic level is the use of clustering algorithms to group structurally related DNA sequences.

C. Data Mining in Proteomics

Many modification sites can be detected by simply scanning a database that contains known modification sites. However, in some cases, a simple database scan is not effective. The use of neural networks provides better results in these cases. Similar approaches are used for the prediction of active sites. Neural network approaches and nearest neighbor classifiers have been used to deal with protein localization prediction. Neural networks have also been used to predict protein properties such as stability, globularity and shape. Data mining has been applied for the protein secondary structure prediction. This problem has been studied for over than 30 years and many techniques [8] have been developed. Initially, statistical approaches were adopted to deal with this problem. Later, more accurate techniques based on information theory, Bayes theory, nearest neighbors, and neural networks were developed. Combined methods such as integrated multiple sequence alignments with neural network or nearest neighbor approaches improve prediction accuracy.

VI. DATA MINING WITH PROCESS MANAGEMENT FOR OPERATIONAL INTELLIGENCE

A. Process Management

Process management systems automate processes and manage the flow of work between workflow participants. A workflow defines process steps, their order, under which conditions and when who will carry them out, within an organization, with which tools and define the flow of data within these process steps [2]. In most circumstances, business process determines the context for data eventually used in data mining. Context is very important in business decision-making and when data is taken out of context, the result are, at least, limited, if not downright misleading. Therefore, by combining data mining and process management technologies, organization can leverage from context relevant information in mining methods for producing more concise knowledge. This knowledge can be of utmost importance- not for only decision makers in order to increase business benefit- but also for automated systems like workflow management system (WfMS) to become operational intelligent.

B. Operational Intelligence

Operational Intelligence is a form of real-time dynamic, business analytics that delivers visibility, insight into business process and delivers actionable information. The purpose of operational intelligence is to monitor business process and activities to detect situations relating to inefficiencies [16]. For instance, data mining techniques can be integrated with in WfMS to remove inefficiency related to workflow resource management.

1) Workflow management[2]*:* The WfMS automates processes according to a process model which, according to, consists of five major perspectives.

a) Functional: This perspective defines the skeleton of the process. It identifies process steps and their purpose. A process step can either be atomic or it can be composite and serves as a container to constitute a process hierarchy.

b) Data: This perspective defines input and output data of a process. It defines flow of data between processes and relates it to external data models.

c) Operational: This perspective describes tools that are required for the execution of a process.

d) Behavioral: This perspective determines the control flow, i.e. the order in which the single steps of a process are being scheduled for execution by a WfMS.

e) Organizational: This perspective determines agents who are eligible to perform a certain process in order to achieve the business goal.

"Fig. 4" shows the process model of a garment production process modeled in i>PM process modeling environment [15] where process steps (e.g. Market Making, Cutting, etc.) are depicted as a rectangle; the *Functional* perspective is represented within that rectangle in a text box. Small text at the lower left corner of the process step represents the *Organizational* perspective; here the role e.g. "Cutters" was assigned to the process step Cutting. The Goal construct is described by the small text at the lower right corner ("Cutters Goal"). *Data and Data Flow* are described by small boxes (data) that are placed on the black arrows (data flow) which connect two steps of a process; a data flow arrow always starts at the producer side of a data item and ends at the consumer side. The execution order of a process is, when this is not specified by data dependencies, defined with the help of the *Behavioral* perspective represented by grey arrows. A text just above the upper left corner of a process step denotes information about the *Operational* perspective.

2) Agent assignment strategies: WfMS defines assignment policies to allocate eligible agents to processes, mostly expressed in terms of roles. Roles are defined during process design time on the basis of similar capabilities and skills of individuals within an organization [12]. For example a Cutting process of a garment industry is assigned to cutters. During the execution of a process all of the eligible agents are selected that fit into the role assigned to the process step in execution and are informed about the task to perform. Any eligible agent, not only the efficient one, can select the process and execute it.

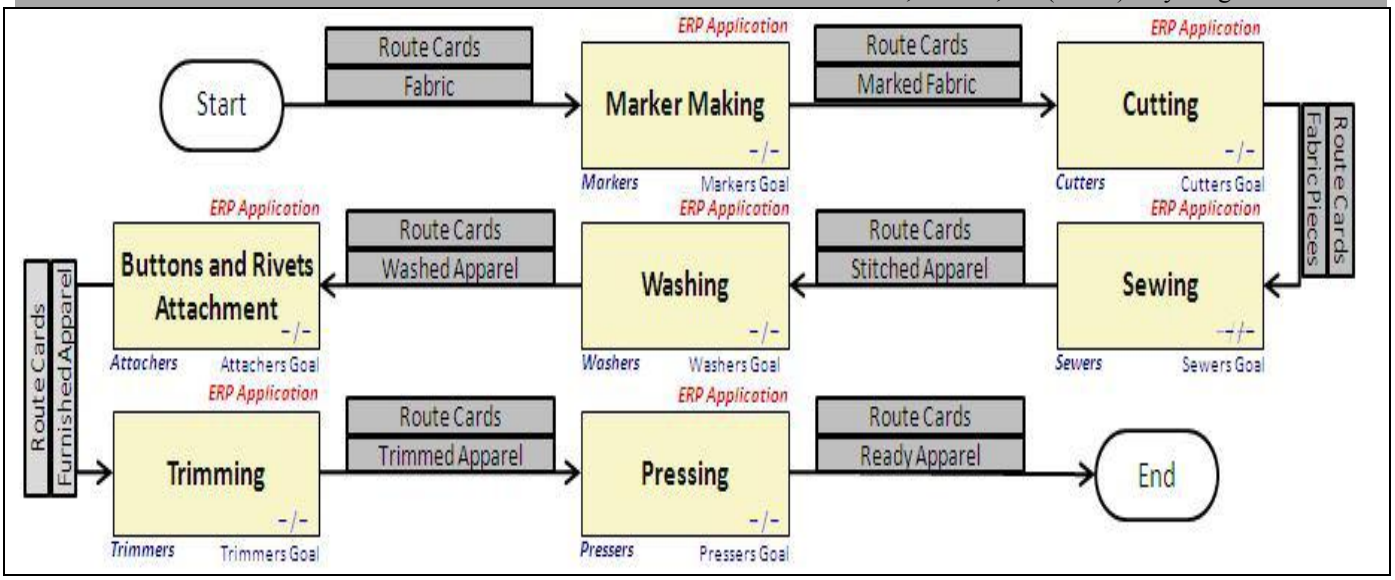

Figure 4. Production Process of an Apparel Division

VII. DATA MINING FOR CYBER SECURITY

Data mining is being applied to problems such as intrusion detection and auditing. For example,

- Anomaly detection techniques could be used to detect unusual patterns and behaviors.
- Link analysis may be used to trace self-propagating malicious code to its authors.
- Classificatio n may be used to group various cyber attacks and then use the profiles to detect an attack when it occurs.
- Prediction may be used to determine potential future attacks depending in a way on information learnt about terrorists through email and phone conversations

Data Mining is also used for E-mail worm detection, for counter-terrorism[19], for surviellance problems.

A. Data Mining for Intrusion Detection[17][18]

An intrusion can be defined as "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource". Attacks are: Host-based attacks Network-based attacks Intrusion detection systems are split into two groups: Anomaly detection systems and Misuse detection systems. Data mining can help automate the process of investigating intrusion detection alarms. Data mining on historical audit data and intrusion detection alarms can reduce future false alarms.

Anomaly Detection Systems - Build models of normal data, Detect any deviation from normal data, Flag deviation as suspect and Identify new types of intrusions as deviation from normal behavior.

Misuse detection - Label all instances in the data set ("normal" or "intrusion"), Run learning algorithms over the labeled data to generate classification rules and Automatically retrain intrusion detection models on different input data

VIII. CONCLUSION

The aim of this paper was to introduce the concept of convergence of new technologies and human values. We have studied what advantages physical and IT security convergence gives, how data mining is converged with other technologies to give a new value or a new technology and how data mining is related with IT security:

- Convergence of data mining, biology and computing leads into a new bio-data enterprise called Genomics.
- New multi-disciplinary research frontier is emerging at the crossroads of Mobility, data mining and privacy.
- Through the convergence of data mining and process management, an organization can produce more concise knowledge for operational intelligence.
- Using the RMS-recognition, mining and synthesis taxonomy, we can mine a dataset for company's financials, for successful investments; we can identify particular potential candidates by constructing a model of a successful employee fro a particular job position; surveillance can be done for business use; information monitoring an sorting to help people stay current with a particular subject or interest is another excellent use of RMS; we can predict tumor's progression for a particular patient , use in medicine.
- Data mining can aid law enforcers in identifying criminal suspects as well as apprehending these criminals by examining trends in location, crime type, habit, and other patterns of behaviors.
- Physical and IT Security convergence leads to new objectives, processes and architectures such as cost reduction, improve asset/personnel protection, eliminate security gaps, collaborative planning, etc.
- There are many practical uses of data mining and the value it provides to those who use this technology to mine their data:

  - Fraud Detection

- Inventory Logistics
- Defect Analysis
- Focused Hiring

REFERENCES

[1] G. Piatetsky-Shapiro, G. Frawley, and W. Frawley. "Knowledge Discovery in Databases". AAAI Press, Menlo Park, California, 1991.

[2] S. Jablonski, C. Bussler, "Workflow management, Modeling concepts, architecture and implementation", Thomson, London, UK, 1996.

[3] A. Abecker, A. Bernardi, K. Hinkelmann, O. Kühn and M. Sintek, "Toward a Technology for Organizational Memories". IEEE Intelligent Systems, vol. 13, no. 3, pp. 40-48, 1998.

[4] Q. Ma, and J.T.L. Wang, "Biological Data Mining using Bayesian Neural Networks: A case study. International Journal on Artificial Intelligence Tools, Special Issue on Biocomputing, 1999, vol. 8, no. 4, pp. 433-451.

[5] R. Tibshirani, T. Hastie, M. Eisen, D. Ross, D. Botstein, and P. Brown, "Clustering methods for the analysis of DNA microarray data (Tech. Rep.). Department of Statistics", Stanford University, Stanford, California, USA, 1999.

[6] H.J.Miller and J.Han(eds). Geographic Data Mining and Knowledge Discovery. Taylor & Francis, 2001.

[7] T. Berners-Lee, J. Hendler, and O. Lassila, "The Semantic Web: A new form of Web content that is meaningful to computers will unleash a revolution of new possibilities",Sci. Amer., May 2001.

[8] D.S. Whishart, "Tools for protein technologies. In Sensen, C.W. (Ed.), Biotechnology, Genomics and Bioinformatics, vol. 5b, Wiley-VCH, 2002, pp. 325-344.

[9] F. Zeng, C.H.R. Yap and L. Wong, "Using feature generation and feature selection for accurate prediction of translation initiation sites". Genome Informatics, 2002, vol. 13, pp. 192-200.

[10] G. Piatetsky-Shapiro, and P. Tamayo, "Microarray Data Mining: Facing the Challenges". SIGKDD Explorations, 2003, vol. 5, no. 2, pp. 1-5.

[11] M. zur Muehlen, "Organizational management in workflow applications", Informational Technology and Management Journal. Kluwer Academic Publisher, 2004, vol. 5, no. 3, pp. 271-291.

[12] R. Bino, R. Hall, O. Fiehn, J. Kopka, K. Saito, J. Draper, B. Nikolau, P. Mendes, U. Roessner-Tunali, M. Beale, R. Trethewey, B. Lange, E. Wurtele, and L. Sumner, "Potential of metabolomics as a functional genomics tool." Trends Plant Sci, vol. 9, no. 9, pp. 418–425, September 2004.

[13] B. Liang and P. Dubey, "BRecognition, mining and synthesis", Intel Technol. J., vol. 9, May 2005.

[14] ProDatO "Integration Technology GmbH: Handbuch iPM Integrated Process Manager"' Software documentation (in German), Erlangen, Germany, 2005, www.prodato.de.

[15] O. Marjanovic, "The next stage of operational business intelligence – creating new challenges for business process management", in Sprague", R.H. Jr (Ed.), Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07), 2007, IEEE Computer Society, Los Alamitos.

[16] Y. Xia, A. Campen, D. Rigsby, Y. Guo, X. Feng, E. Su, M. Palakal, and S. Li, DGEM, "Mining Gene Expression database for primary se tissues, Molecular Diagnosis & Therapy, Issue 3, 2007

[17] B. Thuraisingham. Managing threats to web databases and cyber systems: Issues, solutions and challenges. In V. Kumar et al, editor, Cyber Security: Threats and Countermeasures. Kluwer

[18] B. Thuraisingham. Data mining, national security, privacy and civil liberties. SIGKDD Explorations, January 2003

[19] F. Bolz et al. The Counterterrorism Handbook: Tactics, Procedures, and Techniques. CRC Press, 2001

AUTHORS PROFILE

Shilpa Mahajan is an assistant professor in Ansal University, Gurgaon, Haryana, India. She received her B.Tech degree from Beant College of Engineering and Technology, Gurdaspur, Punjab and M.Tech degree from University Institute of Engineering and Technology, Panjab University, Chandigarh, India.