ISSN No. 2349-8412

Journal of Information Sciences and Application

Volume No. 12

Issue No. 2

May - August 2024

ENRICHED PUBLICATIONS PVT.LTD

JE - 18,Gupta Colony, Khirki Extn,
Malviya Nagar, New Delhi - 110017.
E- Mail: info@enrichedpublication.com
Phone :- +91-8877340707

ISSN No. 2349-8412

Journal of Information Sciences and Application

Aims and Scope

Journal of Information Sciences and Applications has become very important with the ever-increasing demands of the software development to serve the millions of applications across various disciplines. For large software projects, innovative software development approaches are of vital importance. In order to gain higher software standard and efficiency, software process adaptation must be derived from social behavior, planning, strategy, intelligent computing, etc., based on various factors. International Journal of Software Engineering address the state of the art of all aspects of software engineering, highlighting the all tools and techniques for the software development process.

ISSN No. 2349-8412

Journal of Information Sciences and Application

(Volume No. 12, Issue No. 2, May - August 2024)

Contents

M-Commerce In India: Emerging Issues

Dr. Sunil Batra*, Dr. Neenu Juneja*
*Assistant Professor, Chandigarh Group of Colleges Landran. Mohali

ABSTRACT

This paper extends research on mobile commerce in India. It lists the issues being faced by the Indian M-commerce industry. Businesses and its strategies are ever changing with the advancement of time and technologies. Earlier, business strategies were based on limited geographical reach and scope for the growth. But because of rapid advancements in the Internet and communications technologies geographical boundaries are diminishing. M- commerce industry is young in India.9% Indians are using smart phones for the purpose of rapidly consuming contents such as gaming, videos, songs and entertainment on their smart devices and this leads to steady growth in mobile advertising and apps industry. Indian m- commerce industry, however, is yet not developed enough for comparison to the m-Commerce market in the developed countries. Some of the reasons for a contrast is due to some political, social, economical and cultural factors, but rate at which growth is increasing it is expected that the growth would increase in times to come.

Keywords: M-commerce; Mobile Commerce; M-commerce barriers; Mobile Payments; Mobile Governance, M-commerce value chain; Mobile commerce applications; M-commerce applications; Mobile commerce growth drivers; Mobile commerce value chain.

INTRODUCTION

From 1990s onwards E-commerce (electronic commerce)is adding higher values to all types of businesses and academics as well – as a result the users are changing the way business us carried out , people are moving from offline to online transactions. The latter modality is relatively easy, convenient and cheap. But advancement of wireless technology from 2000 onwards has changed and adding new values to business, benefits and conveniences for all its users. And this advanced technology is known as M-commerce or Mobile Commerce. In other words, m-commerce refers to the commerce that is carried out by using wireless devices. Mobile Commerce is the advanced version of e-commerce, mobile commerce, which not only includes all e-commerce transactions, but also provides greater flexibility and convenience to its subscribers. Both the telecommunications industry and the business world are starting to see m-commerce as a major focus for the future.

DEFINITIONS OF M-COMMERCE

"Mobile Commerce is the use of information technologies and communication technologies for the purpose of mobile integration of different value chains an business processes, and for the purpose of management of business relationships.”

(Webagency)

“M-Commerce is the use of mobile devices to communicate, inform transact and entertain using text and data via a connection to public and private networks.”

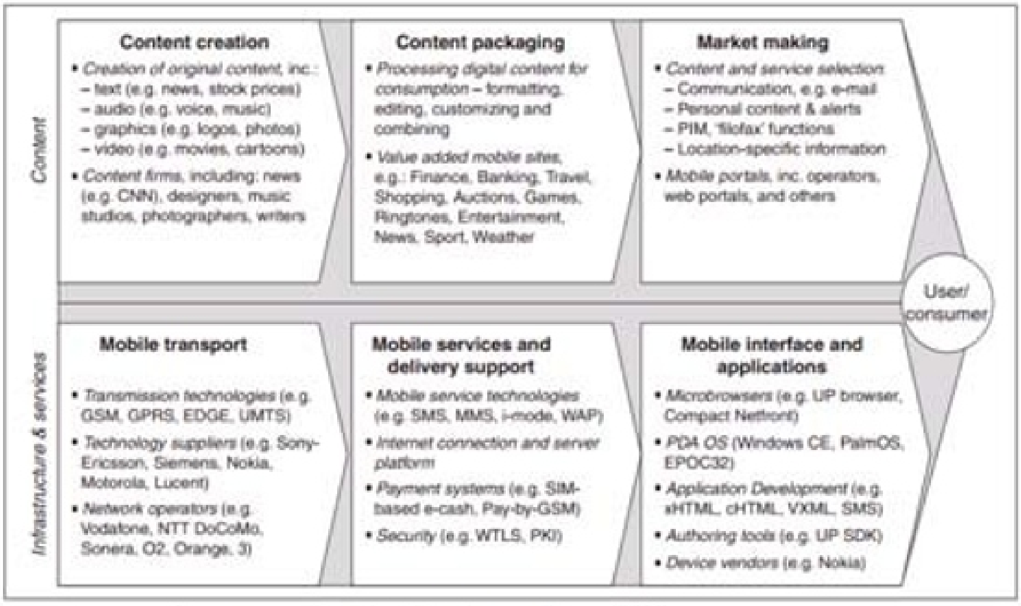
(Lehman Brothers)

"The core of mobile e-commerce is the use of a terminal (telephone, PDA, PC device, or custom terminal) and public mobile network (necessary but not sufficient) to access information and conduct transactions that result in the transfer of value in exchange for information, services or goods.”

(Ovum)

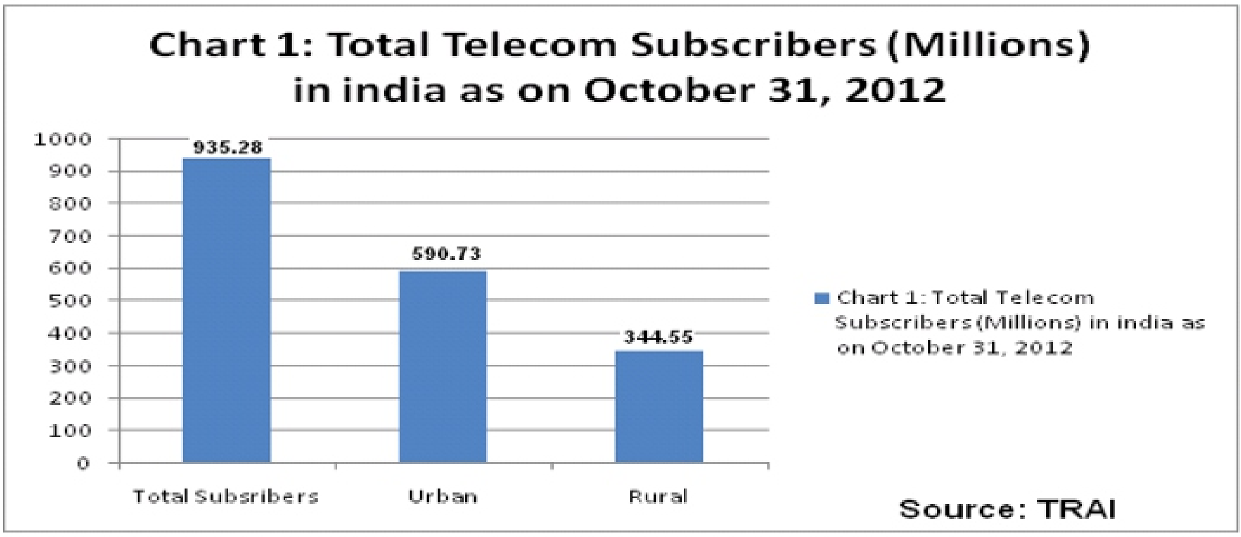
"The use of mobile handheld devices to communicate, interact via an always-on high-speed connection to the Internet.”

(Forrester)


Content
Content creation
• Creation of original content, inc.:
– text (e.g. news, stock prices)
– audio (e.g. voice, music)
– graphics (e.g. logos, photos)
– video (e.g. movies, cartoons)
• Content firms, including: news (e.g. CNN), designers, music studios, photographers, writers
Content packaging
• Processing digital content for consumption – formatting, editing, customizing and combining
• Value added mobile sites, e.g.: Finance, Banking, Travel, Shopping, Auctions, Games, Ringtones, Entertainment, News, Sport, Weather
Market making
• Content and service selection
– Communication, e.g. e-mail
– Personal content & alerts
– PIM, 'filofax' functions
– Location-specific information
• Mobile portals, inc. operators, web portals, and others
User/ consumer
Infrastructure & services
Mobile transport
• Transmission technologies (e.g. GSM, GPRS, EDGE, UMTS)
• Technology suppliers (e.g. Sony-Ericsson, Siemens, Nokia, Motorola, Lucent)
• Network operators (e.g. Vodafone, NTT DoCoMo, Sonera, O2, Orange, 3)
Mobile services and delivery support
• Mobile service technologies (e.g. SMS, MMS, i-mode, WAP)
• Internet connection and server platform
• Payment systems (e.g. SIM-based e-cash, Pay-by-GSM)
• Security (e.g. WTLS, PKI)
Mobile interface and applications
• Microbrowsers (e.g. UP browser, Compact Netfront)
• PDA OS (Windows CE, PalmOS, EPOC32)
• Application Development (e.g. xHTML, cHTML, VXML, SMS)
• Authoring tools (e.g. UP SDK)
• Device vendors (e.g. Nokia)

The m-commerce value chain (source: Barnes, 2002)

As depicted in the figure the M-Commerce value chain includes content creation, content packaging, market making, mobile transport, mobile services and mobile interface and application those are used by the users to practice M-commerce.It is carried out using mobile phone devices, PDAs or other handheld devices. M-commerce applications have 2 major characteristics: broad reach and mobility. Mobility implies portability, for example, users can conduct their businesses in real time via mobile devices. With the help of M- commerce, people can be reached at any time via mobile devices. And by broad reach it means that the reach of M-commerce is more than e-commerce as for the use M-commerce, mobile devices are needed which are already widely spreading all over the world. Such is the extent of adoption of mobile phones that researchers have forecasted that by 2017 the number of mobiles on earth would exceed the population on earth.



A study by Telecom Regularity Authority of India (TRAI), more than 935 million subscribers. As per Chart: 1, in India has the second largest number of mobile phone users in the world. And among these 935 million users there are approximately 18-20 million users who are using smart phones as shown in Chart: 2. Although this is a very small number, that is only 2%(approximately). But it is encouraging to note that the growth of smart phone industry in 2012 is 200% of that in 2011.

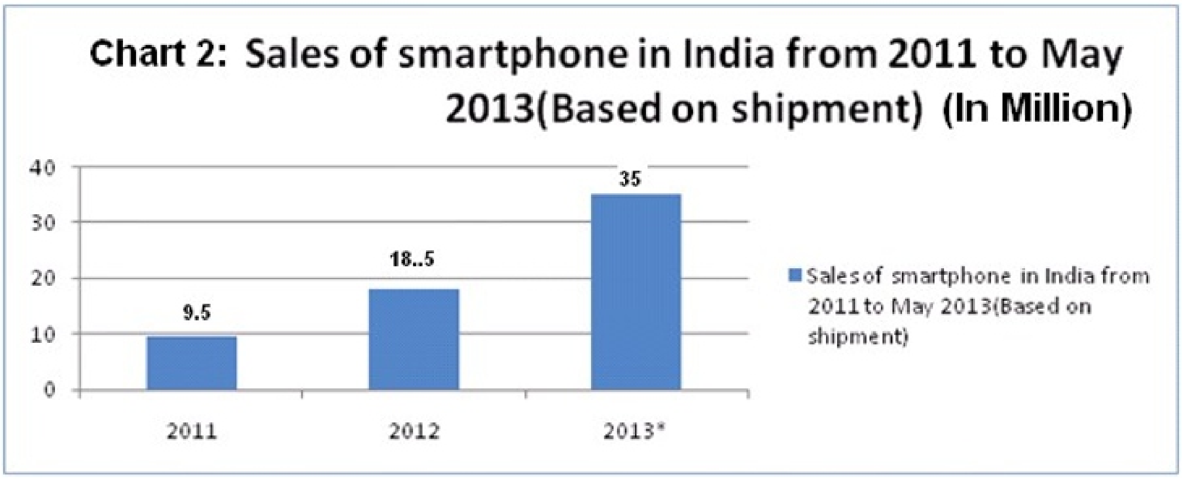


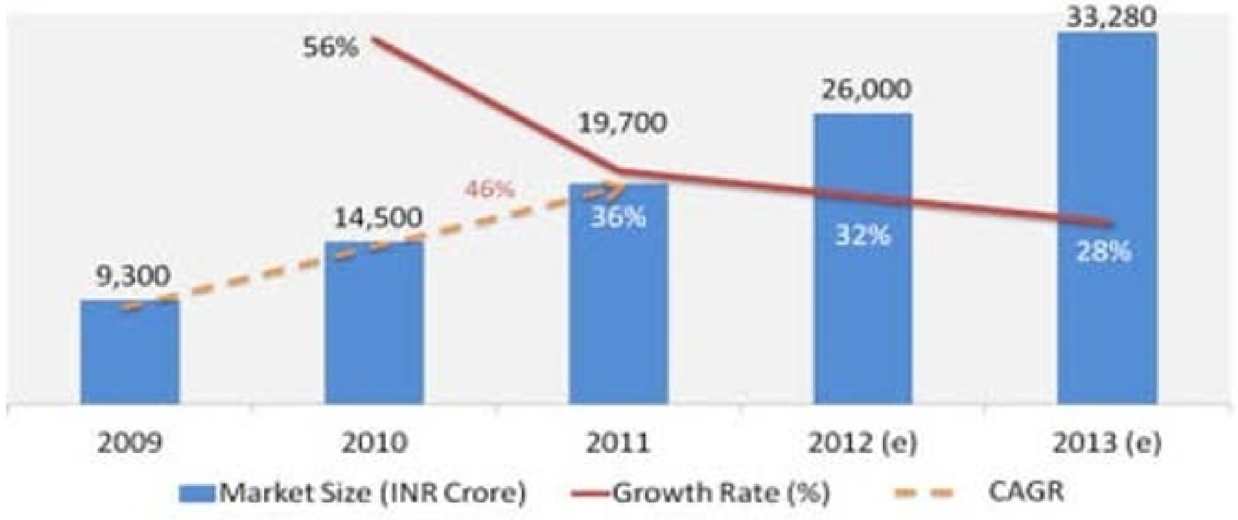
Table 1 Top Five Smartphone Markets and Market Share for 2011, 2012 and 2016 (Based on shipments)

Country	2011 Market Share	2012 Market Share	2016 Market Share	2011 – 2016 CAGR
PRC	18.30%	26.50%	23.00%	26.20%
USA	21.30%	17.80%	14.50%	11.60%
India	2.20%	2.50%	8.50%	57.50%
Brazil	1.80%	2.30%	4.40%	44.00%
United Kingdom	5.30%	4.50%	3.60%	11.50%
Rest of world	51.10%	46.40%	46.00%	18.10%
Total	100.00%	100.00%	100.00%	20.50%

To provide mobile commerce to consumers/businesses three broad aspects work simultaneously, these are: wireless network infrastructure which includes networking requirements & wireless/mobile network, mobile middleware which includes agent technologies, database management wireless & mobile communication systems, wireless & mobile protocols and finally it is the mobile interface and mobile handheld devices.

All these aspects of m-commerce together provide flexibility, convenience, mobility, ease of use and low cost to the businesses as well as to customers. With the help of M-commerce many services like location based services, mobile advertisement, mobile entertainment services, games, mobile financial applications, product locating and searching, wireless reengineering, travel, ticketing, Enterprise Resource Planning, entertainment, healthcare services etc.

Chart 3: Mobile VAS Size and Growth Rate



MVAS Market Size and Growth Rate *Source: IMRB Estimations*

Although M-commerce market has displayed huge growth in recent years but there is a wide gap between technology capabilities and the consumer's expectations. M-commerce players need to improve the user interface soon and implement innovative pricing structures. Despite initial hiccups the users, consumers have envisioned that once the glitches are removed, mobile applications will become an integral part of business as well. But investing in m-commerce has its own risks. While there is potential for a lot of money to be made, there is also potential to lose as well. Organizational and system changes in a business to allow for M-Commerce can be huge, and that means a lot of extra cost. Getting high return on investment can take a long time, and businesses aren't always prepared to stay afloat until they recoup that money. A consumer who uses a device for M-commerce needs to feel secure. Because customers have to provide personal and financial information, hence the reliability and security of the systems must be high.

GROWTH DRIVERS OF M-COMMERCE:

M-commerce is characterized by some special features that generate certain advantages viz- a-viz conventional forms of commercial transactions or as compare to electronic commerce.

Instant connectivity: Ever since the introduction of the GPRS (General Packet Radio Service) mobile devices are offering consistent connectivity and services, which help people to remain always connected with others. This feature brings convenience to the consumers.

Personalization Factor: Since mobile devices are often used by an individual, they are ideal for personal information. Mobile technology provides the benefits to personalize messages to various segment group, based upon time and location etc. For the M-commerce's success mobile databases have become a primary factor by providing personalized services and compiling personalized information.

Mobility factor: Users can easily carry smart phones or mobile devices with them. So any consumer who wants to do monetary transactions need not to go for any cyber to use e- commerce but he/she can perform transactions from anywhere.

Immediacy: Immediacy is the possibility of real-time of services (the “anytime” feature). This feature is significant for some services that need time critical and a quick reaction. For example in the case of stock market a broker need a real time data in a very fast manner.

Localization: The latest positioning technologies, such as the GPS (Global Positioning System), allow companies to offer services and goods to the user based on the current location of the customers. So the location based services meets the consumer's requirement and localized content and services.

Broad reach ability/Ubiquitous computing: Mobile devices or smart phones provide instant connectivity to the users and its reach ability is also very high as compared to other traditional commerce or e-commerce methods.

Ubiquity: Ubiquity means that the user can use services and carry out online transactions independent of his current geographic location. And with the help of this feature a user can use many services such as he/she can check the price of a product online while shopping in a supermarket.

Reach factor: Due to the unprecedented growth in mobile phone sector from the last past 5 years, mobile phones have penetrated deep into the population. And this penetration level is much higher than other areas such as wire line phones, cable television, bank accounts, Internet, PCs, etc. Mobile networks cover rural areas where there are lack of other facilities such as bank branches, land line phones, internet etc.

Cheap 3G services: In the coming few months it is expected that the 3G networks and services expected to be rolled out in India. And with this the user experience for the use of data services over smart phones is expected to improve significantly.

Table 2 Top Five Smart phone Markets and Market Share for 2011, 2012 and 2016 (Based on shipments)

Country	2011 Market Share	2012 Market Share	2016 Market Share	2011 – 2016 CAGR
PRC	18.30%	26.50%	23.00%	26.20%
USA	21.30%	17.80%	14.50%	11.60%
India	2.20%	2.50%	8.50%	57.50%
Brazil	1.80%	2.30%	4.40%	44.00%
United Kingdom	5.30%	4.50%	3.60%	11.50%
Rest of world	51.10%	46.40%	46.00%	18.10%
Total	100.00%	100.00%	100.00%	20.50%

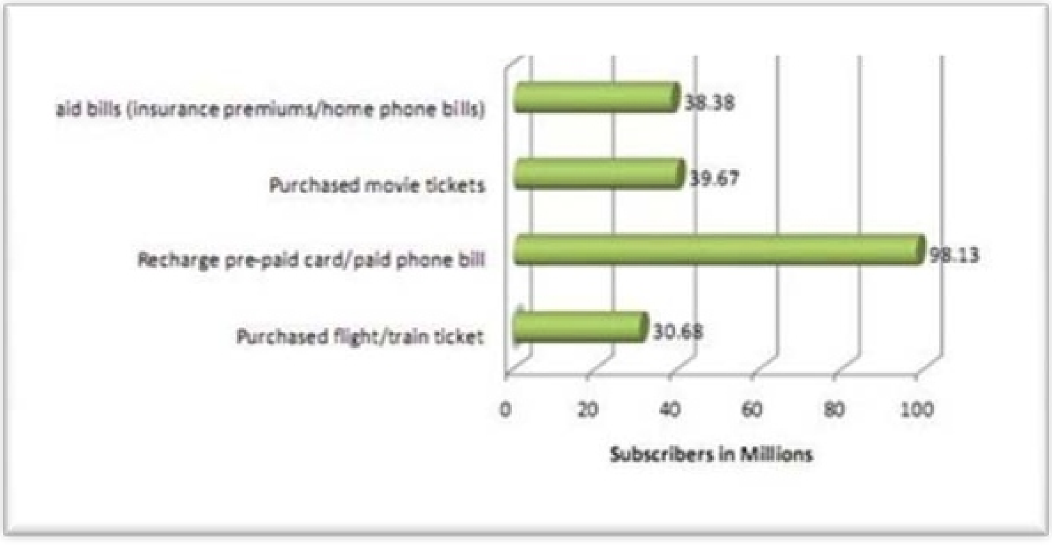
Cheap and Smart handsets: From the last few years the smart phone industry has given a lot to the customers, not only in-terms of latest handsets, even smart handsets on a cheaper and reasonable price. With the advancement and competition in this industry all companies are trying to give latest technology to.

MOBILE COMMERCE APPLICATIONS:

Entertainment: Entertainment on smart phone devices has played an important role in development not only for entertainment industry but also for M-commerce industry, mobile application development industry, mobile hardware industry and many more industries which are directly or indirectly connected with entertainment. Entertainment applications have captured a major share in mobile commerce market and in future this may become the dominated part of mobile commerce. Today it is one of the popular applications for the younger generation. M-commerce has made it possible for us to download images, video, audio and games, data files at anywhere and anytime. On-line games and gambling has become much easier to access and play using latest mobile commerce applications.

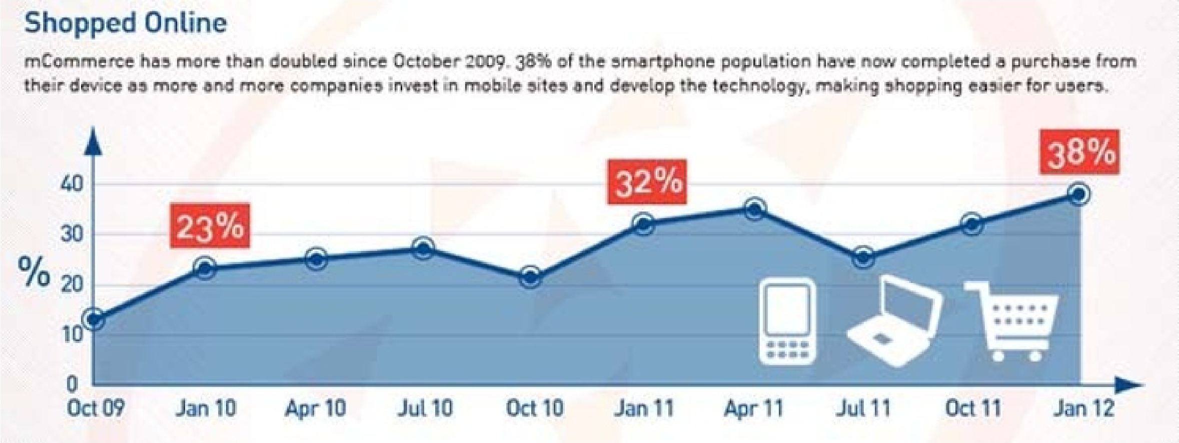
Education: These days education is also available on smart phones. One can access lot of contents while traveling or sitting on somewhere where online contents cannot be accessible through internet. Many of the online journals has their dedicated applicationwhich may help a student or reader to access the contents anywhere. For example Science Direct Journal, The DU Water fowler's Journal, The American Diabetes Association's "ADA Journals", The Wall Street Journal, The Journal of Digital Imaging etc. are some of the well known journals and these journals have a dedicated application for various smart phones platforms.

Travel and Ticketing: Ticketing has been become easy these days. Be it for railways, road or air traveling, all are providing facilities for m-ticketing. Indian Railways has been launched official mobile application which helps consumers to check train schedule, timing, booking etc on their mobile phones. Many road transport companies are also proving latest mobile apps to give facility for the customers to book their tickets online. Almost all airline companies have their mobile applications for various mobile platforms to provide facility to their customers.



E-auction: E-auction is an electronic implementation of the bidding mechanism. It provides the benefits for suppliers and buyers and also increases efficiency and time-savings for both, there is no need for physical transportation until and unless the deal has been established by the supplier and buyer.

M-Shopping: After the success of online shopping on internet, online shopping companies are focusing on mobile shopping as now days this is another booming sector. User wants to spend more time on mobile phone than computer these days so preferably a consumer searches for products and services using mobile phones. As per Nielsons, mobile shopping is increasing 10% to 15% each year and is adding a huge contribution to commerce. And from October 2009 to Jan 2012, 38% growth has been recorded.



Traffic Control: Traffic is the movement of pedestrians or vehicles through an area or route. The passengers in the vehicles and the pedestrians are all mobile objects, ideal clients of mobile commerce. With the help of technology, mobile commerce can improve the problems related to the traffic jam in many ways. For example, usually all smart phones have capabilities of a GPS, these can be used in determining the driver's exact position, and can be used for giving directions, and advising the driver on the current status of traffic in that area. A traffic control center can also control and monitor the traffic according to the traffic signals which are sent from mobile devices in the vehicles.

M-COMMERCE ISSUES:

Mobile commerce growth in India is about 2%. But this growth factor can be high if appropriate policies and other factors come in favor for mobile commerce growth. Mobile commerce is facing many challenges such as security issues, lack of ubiquitous wireless network coverage, lack of standards, and technical mismatches among various wireless devices & smart phones. Furthermore, there are many other issues that indirectly have a huge impact on this industry. These include high cost of smart phones; slow access speed etc creates hurdles in the growth of mobile commerce industry.

MAIN MOBILE COMMERCE CHALLENGES INCLUDE:

DATA TRANSMISSION RATE:

The major growth factor that makes mobile commerce successful is the data transmission bandwidth, which is as compared to other countries is very limited. Due to this factor even with the latest hardware one cannot access web contents faster. With 3Gdata transfer at 14.5 mbps can be attained, but the charges for such services are high.

WIRELESS INTERNET INFRASTRUCTURE:

Wireless internet infrastructure in not sufficient to provide the path the mobile industries for their growth and success. Government is yet to provide such sufficient infrastructure for the growth of wireless industry without such support mobile commerce market could become severely crippled.

SECURITY:

The main issue revolved around mobile commerce is security. Users worry that their devices could be hacked or attacked by some kind of viruses. Usually it came to the notice that while having mobile transactions user lost their money and to avoid such problems users avoid of using such mobile commerce related services.

PRIVACY:

Privacy is another issue related to the growth of m-commerce.For all kind of monetary transactions or other services one need to disclose his identity which many a times creates a huge problem for the customer. Hackers hack the security of wireless transmission and obtain all the information related to the customer, which may be related to the social or financial matter of a customer. GPS[Global Positioning System], on the one side giving benefits to the user by telling the directions and one can get the benefit during an emergency but in the other side a user is also send hislocation which may be used be someone else to track the current location of the user.

CONCLUSION:

The research reflects that M-commerce is adding significant value to the businesses in India. Key drivers of M-commerce include widespread adoption of mobile phones and smart phones, rising affluent middle class consumers. These factors have increased the appetite for M-Commerce in India it has lead to newer opportunities for the businesses to grow and for the M-consumers to obtain benefits in terms of convenience, freedom and speed of work. With the help of mobile commerce one can get the entire word knowledge on their smart phones, can access & manage their bank accounts, save time, avoid parking problem without going to bank; Entertainment, health care, education, traffic problems, ERP, inventory tracking & dispatching, traveling and ticketing are some of the area where mobile commerce is giving so many benefits in our lives. It is worth mentioning that M- commerce is facing teething problems and some of these are based on technical, regulatory, social and political issues. In times to come, the M-commerce is expected to become more secure as government and companies alike are investing on security etc to provide better services to safeguard interests of users of M-commerce.

Future seems promising with new 3G technology and soon with the advent of 4G technologies; a positive change in the way of m-commerce is also on the cards.

BIBLIOGRAPHY

1. *A meta-analysis of mobile commerce adoption and the moderating effect of culture2012Computers in Human Behavior 2851902-1911*
2. *A review for mobile commerce research and applications2007Decision Support System 3-15*
3. *An innovative electronic group-buying system for mobile commerce2013Electronic Commerce Research and Applications 1-13*
4. *Consumer-based m-commerce: exploring consumer perception of2005Computer Standards & Interfaces 271347–357*
5. *Determinants of Consumer Perceptions toward Mobile Advertising2012Journal of Interactive Marketing 26121-32*
6. *Determining the mobile commerce user requirements using an analytic approach2009Computer Standards & Interfaces 144-152*
7. *Evaluation of mobile services and substantial adoption factors with Analytic Hierarchy Process (AHP) Telecommunications Policy In press*
8. *Exploring convenience in mobile commerce: Moderating effects of gender Computers in Human Behavior In press*
9. *Factors influencing the adoption of M-commerce: An exploratory Analysis2011International Conference on Industrial Engineering and Operations Management Kuala Lumpur, Malaysia*
10. *From electronic to mobile commerce TECH MONITOR 38-45*
11. *From Electronic To Mobile Commerce: Technology Convergence Enables Innovative Business Services2008 1-19*
12. *Increasing trust in mobile commerce through design aesthetics Computers in Human Behavior 673–684*
13. *Key success factors for mobile platforms using the value grid model2012Journal of Business Research 6591335–1345*
14. *Mobile Commerce Beyond Electronic Commerce: Issue And ChallengeS Asian Journal of Business and Management Sciences 12119-129*
15. *Mobile Commerce market in India*

16. Mobile commerce product recommendations based on hybrid multiple channels Electronic Commerce Research and Applications 94-104

17. Mobile Electronic Commerce: Emerging Issues20001st International Conference on E- Commerce and Web Technologies477-486LondonSpringer

18. Mobile marketing research: The-state-of-the-art2010International Journal of Information Management 302144-151

19. Mobile-banking adoption by Iranian bank clients Telematics and Informatics In press

20. Predicting consumer decisions to adopt mobile commerce: Cross country empirical examination between China and Malaysia2012Decision Support Systems 134-43

21. Predicting m-commerce adoption determinants: A neural network approach Expert Systems with Applications 523-530

22. Research and markets2012

23. Security Issues in M-Commerce: A Usage-Based 264-282

24. Technological regimes in m-commerce: Convergence as a barrier to diffusion and entrepreneurship? 2009 Telecommunications Policy 19-28

25. The conceptualization and measurement of m-commerce user satisfaction2007Computers in Human Behavior 381-398

26. The effects of location personalization on individuals' intention to use mobile services2012Decision Support Systems 534802-812

27. 2012The Indian Telecom Services Performance Indicators Telecom Regulatory Authority of India New Delhi Mahanagar Doorsanchar Bhawan, Jawahar Lal Nehru Marg, New Delhi-110002

28. The market for wireless electricity: The case of India2010Energy Policy 3831537– 1547

29. Towards a Reference Model for M-Commerce Applications2004 1-14

30. Trading privacy with incentives in mobile commerce: A game theoretic approach Pervasive and Mobile Computing

31. Unique Features of Mobile Commerce Tokyo Tokyo Japan

Mining Interesting Pattern Set Through Data Driven Search

Arun Pratap Srivastava*, Dr. Mohd. Hussain**
*Ph.D. Student, NIMS University, Jaipur
**Director, MG Institute of Management & Technology, Lucknow

ABSTRACT

Mining association rules is a task of data mining, which extracts knowledge in the form of significant implication relation of useful items (objects) from a database. Mining multilevel association rules uses concept hierarchies, also called taxonomies and defined as relations of type 'is-a' between objects, to extract rules that items belong to different levels of abstraction. These rules are more useful, more refined and more interpretable by the user. Several algorithms have been proposed in the literature to discover the multilevel association rules. In this article, we are interested in the problem of discovering multi-level frequent itemsets under constraints, involving the user in the research process. We proposed a technique for modeling and interpretation of constraints in a context of use of concept hierarchies. Three approaches for discovering multi-level frequent itemsets under constraints were proposed and discussed: Basic approach, "Test and Generate" approach and Pruning based Approach.

Keywords: Knowledge Discovery; Data Mining; Association Rules; Itemsets; Concept Hierarchies

INTRODUCTION

The Knowledge Discovery from Database (KDD), means the non-trivial process of identifying, from the data, patterns or valid knowledge which is new, useful and understandable [1]. The KDD is motivated by the huge volumes of data collected around the world, and the more efficient and reliable environment of exchange of data provided by systems and networks. Data mining is the core step of KDD process, defined as the set of intelligent, complex and highly sophisticated data processing techniques, used to extract knowledge. Knowledge can take several forms depending on the purpose of the user and the data mining algorithm. Mining association rules is a data mining task which consists in extracting meaningful relationships of the form (X implies Y) between objects (Items) of a database, such as X and Y are subsets of items. The validity of an association rule is defined by two measures where the threshold is defined by user: the first measure is the support which means the scope of the rule, i.e. the frequency of the set (X UNION Y) in the database. The second measure is the confidence that means the accuracy of the rule, i.e. the conditional probability of occurrence of Y knowing X. This problem was proposed in [2] for the analysis of transactions of a sale database. Since then, mining association rules has become a very important task of data mining and has demonstrated efficacy in diverse application areas: telecommunications, medical diagnostics, space exploration ... This problem has been addressed in several articles in the literature [3, 4, 5, 6, 7], which allowed the development of several algorithms for discovering association rules.

Approaches mentioned above are aimed at discovering association rules at the terminal level of abstraction, i.e. the association rules containing only the items belonging to the transactions of database. However, there is a need in many applications to association rules at higher levels of abstraction, these are multi-level association rules [9] or generalized association rules [8]. Mining multi-level association rules is motivated by several reasons, such as:

- Association rules at the lowest level of abstraction may not satisfy the support constraint. Thus, one may omit several rules potentially useful.
- The multi-level association rules are more refined, give a global view and are more interpretable and more understandable to the user.
- The multi-level association rules can provide solutions to the problem of redundant or unnecessary rules, often encountered in real world applications.

To extract multi-level association rules, concept hierarchies or items taxonomies are needed. A concept hierarchy is modeled by a directed acyclic graph (DAG) whose nodes represent items and arcs represent 'is-a' relations between two items. Concept hierarchies represent the relationships of generalization and specification between the items, and classify them at several levels of abstraction. These concept hierarchies are available, or generated by experts in the field of application. Figure 1 illustrates an example of a concept hierarchy on food products. The problem of discovering multi-level association rules has been treated in several articles in the literature that suggested many methods for solving the problem. Many studies are focused on the problem of finding multi-level frequent itemsets, which represent the main and most complex stage in the process of extracting association rules.

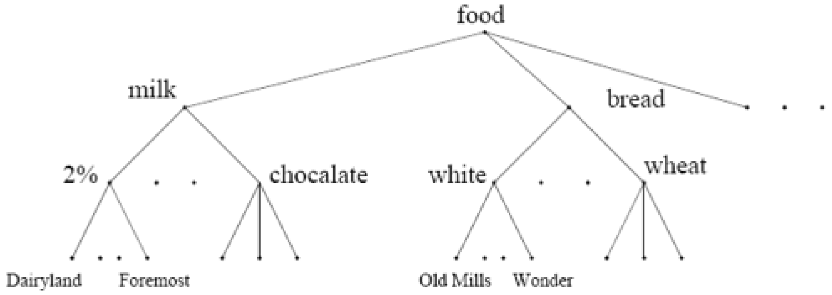


Figure 1. Example of a concept hierarchy on food products

This paper deals with the problem of finding frequent multi-level itemsets under constraints, given a deep belief of the importance of involving the user in the process of mining association rules. This process leads to developing more reliable and efficient solutions, especially for processing large volumes of data.

Our contribution is to propose, first, a technique of definition and interpretation of constraints in the context of use of concept hierarchies. Then, three approaches and algorithms for discovering frequent multi-level itemsets under constraints are proposed and discussed:

basic approach, approach 'test and generate' and pruning based approach. To develop the approach by pruning, some changes will be made to the technique of definitionand interpretation of the constraints.

2. MINING MULTI-LEVELASSOCIATION RULES

At this section, a specification of the problem and a brief description of the techniques of extracting multi-level association rules proposed in the literature, are presented.

2.1. PROBLEM SPECIFICATION

Let I = $\{i_1, i_2, \dots \dots ., i_m\}$, a set of m items, also called literals. Let T = $\{t_1, t_2, \dots ...., t_n\}$, a database of n transactions, each transaction t_i is composed of a unique identifier (TID) and a subset i of I, i is composed of k items and i is defined as a k-itemset. HC is a concept hierarchy on the items of I, HC is also called taxonomy. It is modeled by a directed acyclic graph. An arc of HC represents an “is-a” relationship between the source and the destination. A node refers to an item of I. Let p and c, two nodes of HC, and there is an arc from p to c, p is said parent and c is said son. An item is not the parent of itself since the graph is acyclic. Transactions T contain only the items belonging to the lowest level (Terminal level). In taxonomy, levels are numbered from 0, as the level 0 represents the level Root. Items belonging to a level l, are numbered with respect to their parent in an ascending order, this coding was proposed in [9] for reasons of simplification. In Figure 1, the item milk, for example, takes the code 1**, since it belongs to level 1, the Dairyland item (terminal item) takes the code 111, which gives clear information about its position in the hierarchy and its parents.

The problem of mining multi-level association rules is to find the association rules containing items belonging to the different levels of abstraction, meeting the minimum thresholds of support and confidence, knowing that a transaction t supports an item x if and only if, x belongs to t or x is a parent of an item belonging to t. Similarly to the methods of discovering single-level association rules, multi-level association rules algorithms are mainly based on the discovery of frequent itemsets.

2.2. ALGORITHMS FOR MINING MULTI-LEVELASSOCIATION RULES: AN OVERVIEW

As indicated earlier, the problem of mining multi-level association rules has been covered in several researches. In [9], the authors have proposed series of algorithms for discovering multi-level frequent itemsets: ML-T2, ML-T1, ML-TMax, ML-T2+…. All these algorithms implement a top-down deepening method that starts with the treatment of the highest level of abstraction and then the lowest levels. These algorithms use different minimumsupport thresholds for the different levels of abstraction, these thresholds values decrease in the hierarchy of concepts for the following reasons:

- Avoid the generation of unnecessary or obvious association rules at high abstraction levels.
- Avoid the omission of useful association rules at low abstraction levels. Algorithms proposed in [9] can generate frequent itemsets for each level independently.

In [8], a new approach to solve the problem has been proposed. This approach consists in generating, in a first step, an extended version of the database, so that each transaction gives rise to a new transaction which, in addition to the initial items, contains the ancestors of each item of the transaction. Then, all transactions will contain items from different levels of abstraction in the concept hierarchy. In a second step, algorithms for discovering frequent itemsets are applied on this new extended version of database. Indeed, this approach can generate frequent itemsets containing, simultaneously, items belonging to several levels of abstraction. Three algorithms have been proposed, implementing several methods of optimization and performance improvement: Basic, Cumulate, Stratification. In [10], the PRUTAX algorithm was proposed for mining multiple level frequent itemsets, implementing a hash tree based method in order to reduce the number of support calculations as it counts only the supports for candidate itemsets whose ancestors are all frequent.

In [11], the authors have reviewed the proposed algorithms in [9], and proposed new improved and optimized algorithms: ML-T2L1, ML-T1LA, ML-TML1, ML-TML1, ML- T2LA. In [12], a formal framework for generalized itemsets was defined based on two relationships: Superset-Subset and Parent-Child. Then, the SET algorithm was proposed to enumerate all generalized frequents itemsets, SET uses two constraints based on the defined relationships on itemsets in order to avoid support calculations for infrequent itemsets. In [13], a top-down progressive deepening method of mining cross level frequent itemsets has been proposed, i.e. in what appear simultaneously items from different levels of abstraction. Their method, based mainly on the work of Han and Fu [9,11], is to create a data structure that combines incrementally the 1-itemsets (items) for each level of abstraction. This structure is used to generate 2-itemsets candidates for all levels of abstraction, which are cross-level itemsets (containing items from several levels of abstraction and not just the level being processed). This type of frequent itemsets and association rules can reveal new correlations potentially more useful for the user.

3. ALGORITHMS FOR MINING FREQUENT MULTI-LEVEL ITEMSETS UNDER CONSTRAINTS

The objective of this paper is to develop a method of finding frequent multi-level itemsets under constraints. Our method is to consider the needs of the expert (user), and to give him the possibility to manage and personalize the research process. To achieve this goal, in the beginning the technique developed for modeling the constraints in a context of use of concept hierarchies on the items of the database is presented. Then, scenarios considered and studied to solve the problem will be presented in details.

3.1. MODELING THE CONSTRAINTS OF EXISTENCE ON ASSOCIATION RULES

The constraints on the association rules are the criteria defined by the user to customize and guide the search process to better achieve its objectives. The support and confidence are two fundamental constraints in the process of discovering association rules. An association rule is not accepted if it does not meet these two constraints. Particular interest in this work is restricted to the constraints of existence, which enables the user to filter the items, which may be included in the itemsets to discover. In [14], the authors proposed a technique for modeling constraints that can be integrated into the search process of frequent itemsets. This technique uses the principles of classic logic. It considers an existence constraint as a Boolean expression in disjunctive normal form: a disjunction of conjunctions, treating an item as a literal. To clarify this technique, we give the definitions of some concepts from classical logic:

- A literal: a literal is an atom (also called positive literal) or the negation of an atom. The atoms form clauses.

- The conjunction or AND logic: is a logical operator in the calculation of the proposals. The proposition obtained by linking two propositions by this operator is also called logical product. The conjunction of two propositions P and Q is true if both propositions are simultaneously true, otherwise it is false. The conjunction is: P AND Q.

- A disjunction or OR logic: is a logical operator in the calculation of the proposals. The proposition obtained by linking two propositions by this operator is also called logical sum. The disjunction of two propositions P and Q is true when one of them is true and is false when both are simultaneously false. The disjunction is: P OR Q.

- Disjunctive Normal Form: a disjunctive normal form (DNF) is a standardization of a logical expression which is a disjunction of conjunctive clauses.

SPECIFICATION OF THIS TECHNIQUE:

According to this technique and based on the definitions above, a constraint CT will be structured as follows:

$$CT = c_1 \text{ OR } c_2 \text{ OR } c_3 \text{ OR } \ldots\ldots.. \text{ OR } c_n$$

Each ci is a conjunction with the following structure:

$$C_i = e_{i1} \text{ AND } e_{i2} \text{ AND } e_{i3} \ldots\ldots... \text{ AND } e_{ini}$$

An element e_{ij} represents the elementary level; it must have valid logical value (True or False). It consists of a literal (Item, in our case) and, if necessary, a sign of negation. To be valid and satisfies a constraint, an itemset must have the logical value 'True' for at least one conjunction C_i of CT.

Example:

Given the following items: A, B, C, D, and E.

And a constraint Ct01:

Ct01 = (A AND B) OR ((NOT A) AND D) OR (D AND C).

To be valid for the constraint CT01, an itemset it01 must satisfy at least one of the following clauses:

- A and B, in it01. - Not A and D in it01. - D and C, in it01.

It01 may, for example, be one of the following:

- it01 = {A, B, C}   - it01= {D, C, A}

Relying on this technique of modeling constraints, several algorithms for discovering frequent itemsets satisfying the constraints of existence (Constraints controlling the appearance of items in itemsets), defined by the user, have been proposed in [14].

3.2. MODELING THE CONSTRAINTS OF EXISTENCE IN A CONTEXT OF USE OF CONCEPT HIERARCHIES

In this paper, the modeling technique of constraints proposed in [14] and presented in Section 3.1 is extended to make it applicable in the context of multi-level frequent itemsets. In a context of use of concepts hierarchies, a constraint CT keeps the same structure as:

$$CT = c_1 \text{ OR } c_2 \text{ OR } c_3 \text{ OR } \ldots\ldots\ldots \quad \text{OR } c_n$$

Each Ci is a conjunction with the following structure:

$$C_i = e_{i1} \text{ AND } e_{i2} \text{ AND } e_{i3} \ldots\ldots\ldots \text{ AND } e_{ini}$$

The difference compared to the technique proposed in [14], is that the element e_{ij} may be composed of an item belonging to different levels of the concept hierarchy, and not only to the terminal level. This influences the way of interpretation of the constraint itself. The interpretation of a constraint in the context of use of concept hierarchies is defined as follows:

Consider the structure of the constraint CT, illustrated above.

Let e_{ij}, a basic element in one of the conjunctions (C_i) of constraint CT. Two scenarios may arise:

1. e_{ij} = I01, as I01 is an item:

For an itemsets satisfies IT01 element e_{ij}, I01 must contain IT01 or IT01 contain at least one of the descendants of I01 in the concept hierarchy.

2. e_{ij} = (NOT I01), as I01 is an item:

For an itemsets satisfies IT01 element eij, IT01 mustn't contain I01, or any item from the descendants of I01.

3.2. ALGORITHMS FOR MINING FREQUENT MULTI - LEVEL ITEMSETS UNDER CONSTRAINTS

The existing algorithms for discovering multilevel frequent itemsets do not address the problem of constraints which can be defined by the user to customize the results. In this paper, constraints of existence are particularly treated. As part of this goal, first and foremost, a technique of modeling constraints in a context of use of concept hierarchies is developed, by extension of the technique proposed in [14]. This technique allows easier and deterministic integration of constraints in the algorithms. In this section, a detailed study of different scenarios for solving the problem is presented. These are based on the algorithms for discovering multi-level frequent itemsets proposed in [9] and [11]. An example of a concept hierarchy, with fictitious items for reasons of simplification and interpretation, is presented in Figure 2. An example of a database used for the illustration of the application of algorithms, is presented in Table 1. The concept hierarchy in Figure 2 consists of 3 levels of abstraction, codification of items related to their position in the hierarchy is used [9].

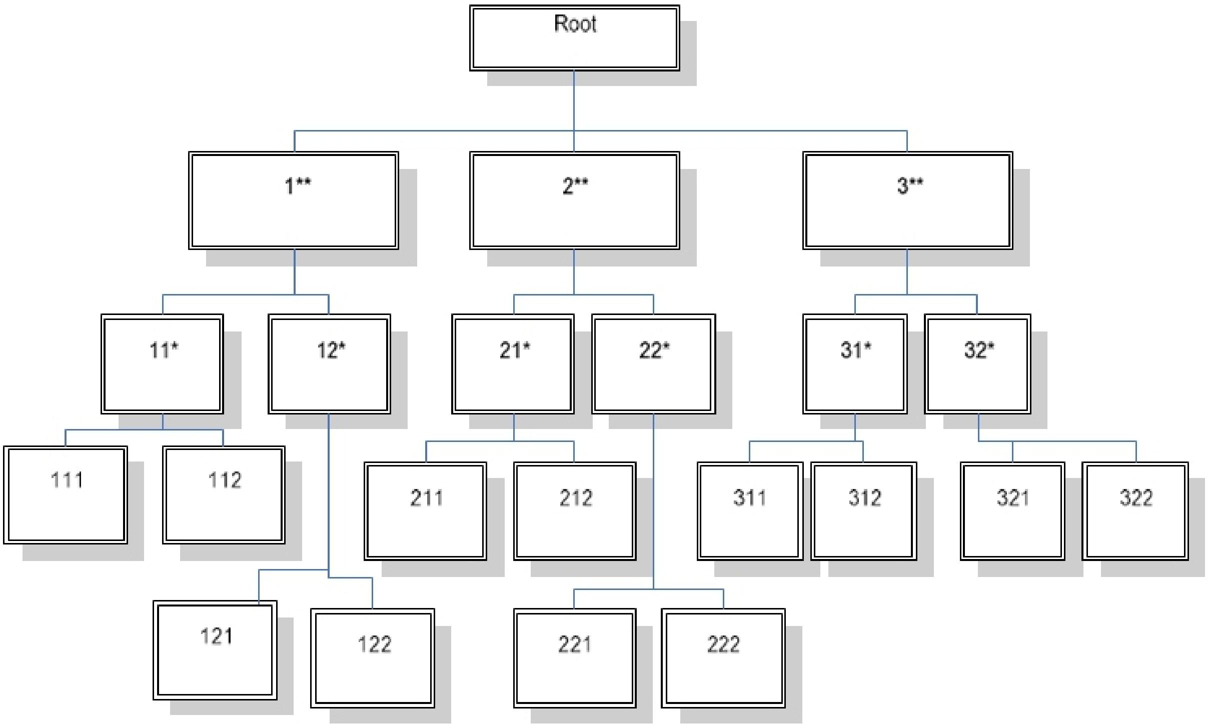
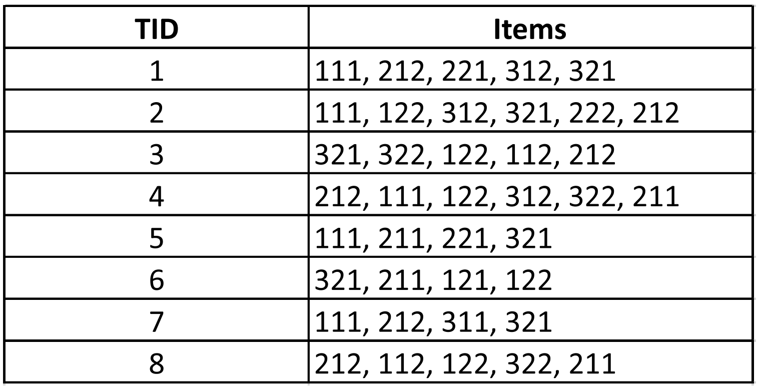


Figure 2. The Concept Hierarchy

Table 1: Database



TID	Items
1	111, 212, 221, 312, 321
2	111, 122, 312, 321, 222, 212
3	321, 322, 122, 112, 212
4	212, 111, 122, 312, 322, 211
5	111, 211, 221, 321
6	321, 211, 121, 122
7	111, 212, 311, 321
8	212, 112, 122, 322, 211

3.3.1. SCENARIO 1:

Basic Algorithm : The first scenario considered in the discovery of multi- level frequent itemsets under constraints proceeds as follows:

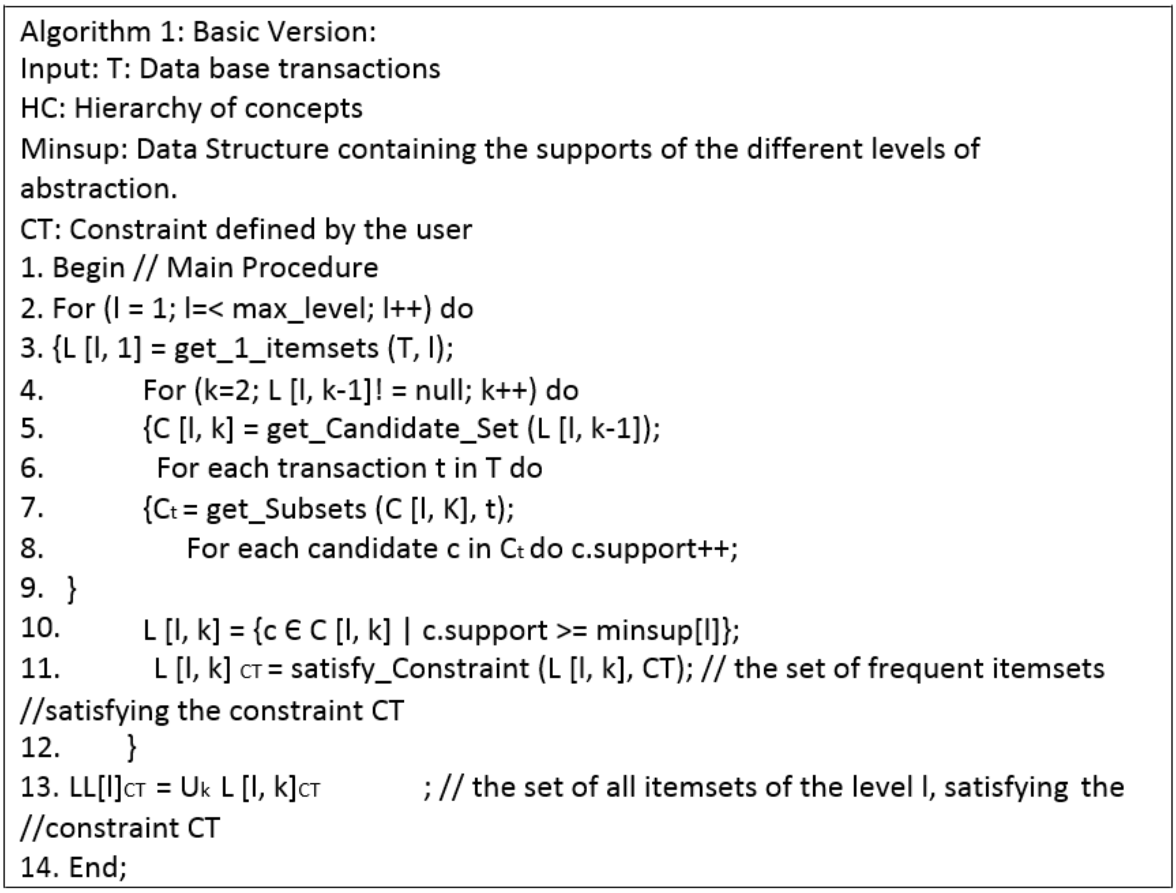
- Search for frequent itemsets for each level independently, based on the Apriori algorithm and using different values of the support: A minimum value of support for each level is defined.

- After finding the frequent itemsets of a level l, the validity of these itemsets against the constraint defined by the user is verified.

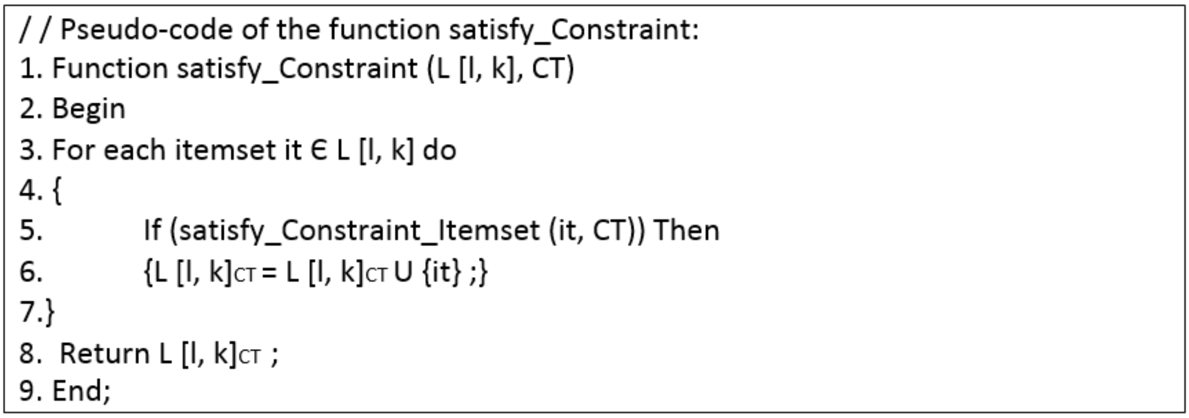
- Elimination of frequent itemsets which do not satisfy the constraint.

This approach is the solution "Generate and test". It proceeds to verify the satisfaction of constraints after the discovery of frequent itemsets. This approach is presented in the following algorithm in table 2:

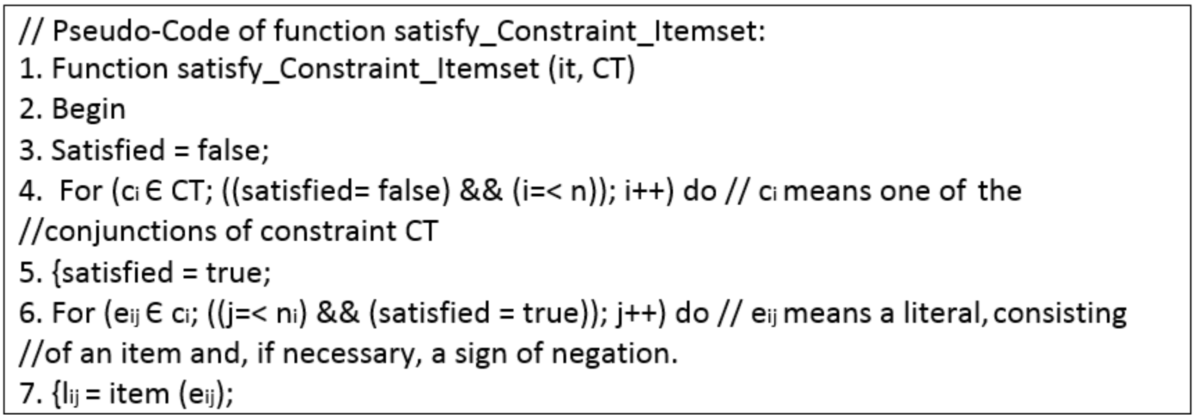
Table 2: Pseudo-code of the first algorithm of extraction of multi-level frequent itemsets under constraints: Scenario 1.



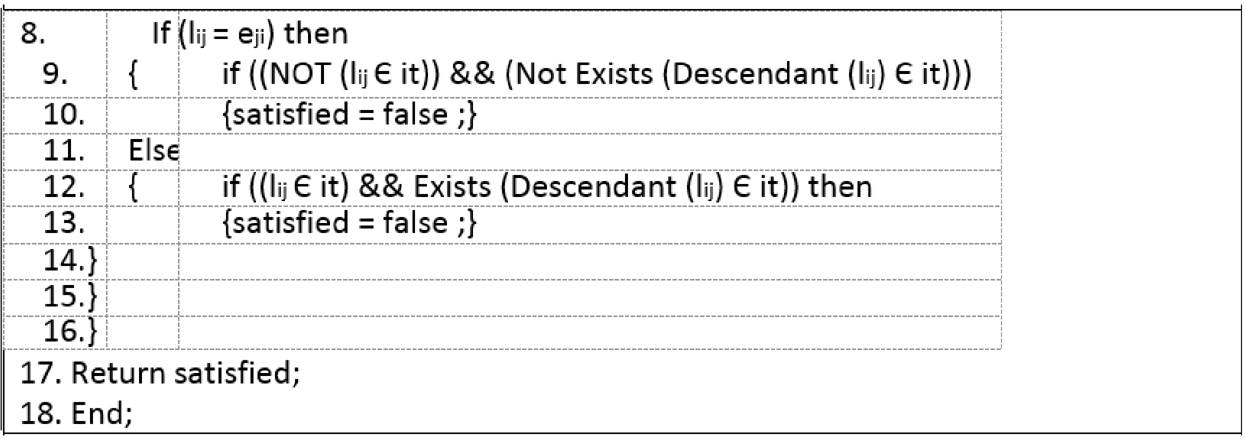
```
Algorithm 1: Basic Version:
Input: T: Data base transactions
HC: Hierarchy of concepts
Minsup: Data Structure containing the supports of the different levels of
abstraction.
CT: Constraint defined by the user
Begin // Main Procedure
For (l = 1; l=< max_level; l++) do
{L [l, 1] = get_1_itemsets (T, l);
        For (k=2; L [l, k-1]! = null; k++) do
        {C [l, k] = get_Candidate_Set (L [l, k-1]);
         For each transaction t in T do
        {$C_t$ = get_Subsets (C [l, K], t);
            For each candidate c in $C_t$ do c.support++;
 }
        L [l, k] = {c ∈ C [l, k] | c.support >= minsup[l]};
         L [l, k] $_{CT}$ = satisfy_Constraint (L [l, k], CT); // the set of frequent itemsets
//satisfying the constraint CT
     }
LL[l]$_{CT}$ = $U_k$ L [l, k]$_{CT}$        ; // the set of all itemsets of the level l, satisfying the
//constraint CT
End;
```



```
/ / Pseudo-code of the function satisfy_Constraint:
Function satisfy_Constraint (L [l, k], CT)
Begin
For each itemset it ∈ L [l, k] do
{
        If (satisfy_Constraint_Itemset (it, CT)) Then
        {L [l, k]$_{CT}$ = L [l, k]$_{CT}$ U {it} ;}
}
 Return L [l, k]$_{CT}$ ;
End;
```



```
// Pseudo-Code of function satisfy_Constraint_Itemset:
Function satisfy_Constraint_Itemset (it, CT)
Begin
Satisfied = false;
 For ($c_i$ ∈ CT; ((satisfied= false) && (i=< n)); i++) do // $c_i$ means one of the
//conjunctions of constraint CT
{satisfied = true;
For ($e_{ij}$ ∈ $c_i$; ((j=< $n_i$) && (satisfied = true)); j++) do // $e_{ij}$ means a literal, consisting
//of an item and, if necessary, a sign of negation.
{$I_{ij}$ = item ($e_{ij}$);
```



```
8.      If ($l_{ij}$ = $e_{ji}$) then
9.    {       if ((NOT ($l_{ij}$ ∈ it)) && (Not Exists (Descendant ($l_{ij}$) ∈ it)))
10.           {satisfied = false ;}
11.   Else
12.   {       if (($l_{ij}$ ∈ it) && Exists (Descendant ($l_{ij}$) ∈ it)) then
13.           {satisfied = false ;}
14.}
15.}
16.}
17. Return satisfied;
18. End;
```

In conclusion, here are some comments for better clarification of the previous algorithm:

- The function satisfy_Constraint, called at line 11 of the main procedure, filter a set of frequent k-itemsets at a level l (any l, k), to get out a subset noted L [l, k]CT whose itemsets satisfy the constraint CT.

- The function satisfy_Constraint uses another function that is named satisfy_Constraint_Item set (See line 5 of the function satisfy_Constraint). This function checks whether an itemset satisfies a constraint or not. It implements the principle of interpretation of constraints.

- The function satisfy_Constraint_Itemset itself uses a function called item (See line 7 of the satisfy_Constraint_Itemset function), with the parameter e_{ij}. This function returns the item involved in the element e_{ij}, after removal of the sign of negation.

- The function Descendant (See lines 9 and 12 of the satisfy_Constraint_Itemset function) returns all descendants of an item, given as input parameter.

ILLUSTRATION:

For reasons of simplification, only a subset of the whole running example of the scenario1 ispresented in what follows, based on the hierarchy of concepts and the database of Figures 2 and 3. CT is the constraint defined by the user:

CT = ((NON (3**)) AND (11*)) OR (2**)

A value of minimum support is assigned for each level, as the following table:

Table 3: Illustration of the first algorithm for extracting multi-level frequent itemsets under constraints: Scenario1.

Level	Support
1	5
2	4
3	3

Level 2: Minsup = 4

Itemsets	Support	Itemsets	Support
{11*, 12*}	4	~~{12*, 31*}~~	2
{11*, 21*}	7	{12*, 32*}	5
{11*, 31*}	4	{21*, 31*}	4
{11*, 32*}	7	{21*, 32*}	8
{12*, 21*}	5	{31*, 32*}	3

L [2, 2]

Level 2: Minsup = 4

Itemsets	Support	Itemsets	Support
{11*, 12*}	4	{21*, 31*}	4
{11*, 21*}	7	{21*, 32*}	8
{12*, 21*}	5		

L [2, 2] CT

Itemsets	Support	Itemsets	Support
{11*, 12*, 21*}	4	{21*, 31*, 32*}	4
~~{11*, 12*, 31*}~~	2	{12*, 21*, 32*}	5
{11*, 12*, 32*}	4	{31*, 21*, 11*}	4
~~{12*, 21*, 31*}~~	2	{32*, 21*, 11*}	7

L [2, 3]

Itemsets	Support	Itemsets	Support
{11*, 12*, 21*}	4	{21*, 31*, 32*}	4
{31*, 21*, 11*}	4	{12*, 21*, 32*}	5
{32*, 21*, 11*}	7		

L [2, 3] ^{CT}

An example illustrating a detailed implementation of scenario 1 is presented above, which helped generate the frequent itemsets satisfying the constraint CT and belonging to different levels of abstraction in the hierarchy of concepts in Table 1. Checking the validity compared to the constraint is done after the calculation of supports for all the itemsets. This induces the processing, for each pass, of the support of a large number of itemsets, which may not satisfy the constraint defined by the user. This operation consumes time and reduces the performance of the algorithm. The term pass is defined as the basic research stage of the k-frequent itemsets on a level of abstraction l (any l and k).

3.3.2. SECOND SCENARIO:

Approach "Test and Generate": The approach presented in the scenario 1 is to verify the validity of the itemsets against the constraint after finding all frequent itemsets noted L [l, k]. This involves the calculation of the supports of candidate itemsets noted C [l, k], at each pass. Knowing that a large number of frequent itemsets do not satisfy the constraint defined by the user, another approach that avoids this loss of time is presented in this section. This approach consists in creating a filter on all candidate itemsets in each pass. This filter is designed to eliminate the itemsets which do not satisfy the constraint before calculating their supports. This ensures that the calculation of the support is applied only for itemsets that satisfy the user constraint.

Some examples can be extracted from the illustration of the section 3.3.1 such as:

- The set L [2, 1] contains 5 frequent itemsets; only 2 among them satisfy the constraint CT.
- The set L [3, 1] contains 7 frequent itemsets; only 3 among them satisfy the constraint CT.

The difference between the number of frequent itemsets and the itemsets that satisfy the constraint in the same pass is clear and remarkable. This difference increases certainly when dealing with real life large databases.The application of the approach of scenario 2 improves the overall performance of the algorithm. However, it does not find all the frequent itemsets, but only a small part, because a k-itemset which does not satisfy a constraint, can participate to the generation of a (k +1)- Itemset that satisfies this constraint, based on A-priori.

The following examples are given to illustrate this approach:

- Consider all frequent 1-itemsets of level 2, L [2,1], the itemset {31*} is frequent but does not satisfy the constraint CT. Despite this, this itemset is used to generate the 2-itemset {21 *, 31 *} which is frequent and satisfies CT. Thus, if the itemset {31 *} has not been generated in L [2,1], we failed to find the itemset {21*, 31*)} in L [2,2] CT.

- Consider all the frequent 2-itemsets of level 3, L [3,2], the itemset {111,321} is frequent but does not satisfy the constraint CT. However, this itemset is used to generate the 3-Itemset {111, 212, 321} which is frequent and satisfies the constraint CT.

The conclusion is that a frequent itemset which does not satisfy the constraint in one pass can contribute to the generation of frequent itemsets in the next pass. Indeed, the approach of scenario 2 leads to the omission of the generation of several frequent itemsets satisfying the constraint. Then this algorithm is incomplete and does not solve the problem and achieve the objectives. Another approach that is supposed to draw advantage from the real needs of the user is presented in the following section.

3.3.3. THIRD SCENARIO:

Pruning based Approach: Algorithm MLC-Prune: This approach is based on a new method for introducing constraints by the user. This constraint is divided into two parts: the first is devoted to items that the user decides to remove from the mining process; the second is devoted to items that will be part of frequent itemsets.

Modeling constraints:

The constraint of the user is divided in two parts, called sub-constraints, the terminology of modelling of the constraints is defined in section 3.2:

- The first sub-constraint contains the literals or items, not covered by the user during the current search of frequent itemsets. This sub-constraint, noted CT_NEG (Negation), is modeled as follows:

$$CT\_NEG = (NON\ g_1)\ AND\ (NON\ g_2)\ AND........\ \ AND\ (NON\ g_n)$$

g_i designate items or literals.

- The second sub-constraint contains literals or items that the user wishes to have in the itemsets to discover. This sub-constraint, noted CT_AFF (affirmation), is modeled in the form of disjunction of conjunctions:

$$CT\_AFF = c_1\ OR\ c_2\ OR\ c_3\ OR......,\ OR\ c_n$$

c_i is combination of items, with the following structure:

$c_i = e_{i1}$ AND e_{i2} AND e_{i3} ....AND e_{ini}

e_{ij} is an item or literal. The specificity of e_{ij} in CT_AFF is that it can not contain a sign of negation. The use of negation sign is only done in the first sub-constraint CT_NEG.

Principle:

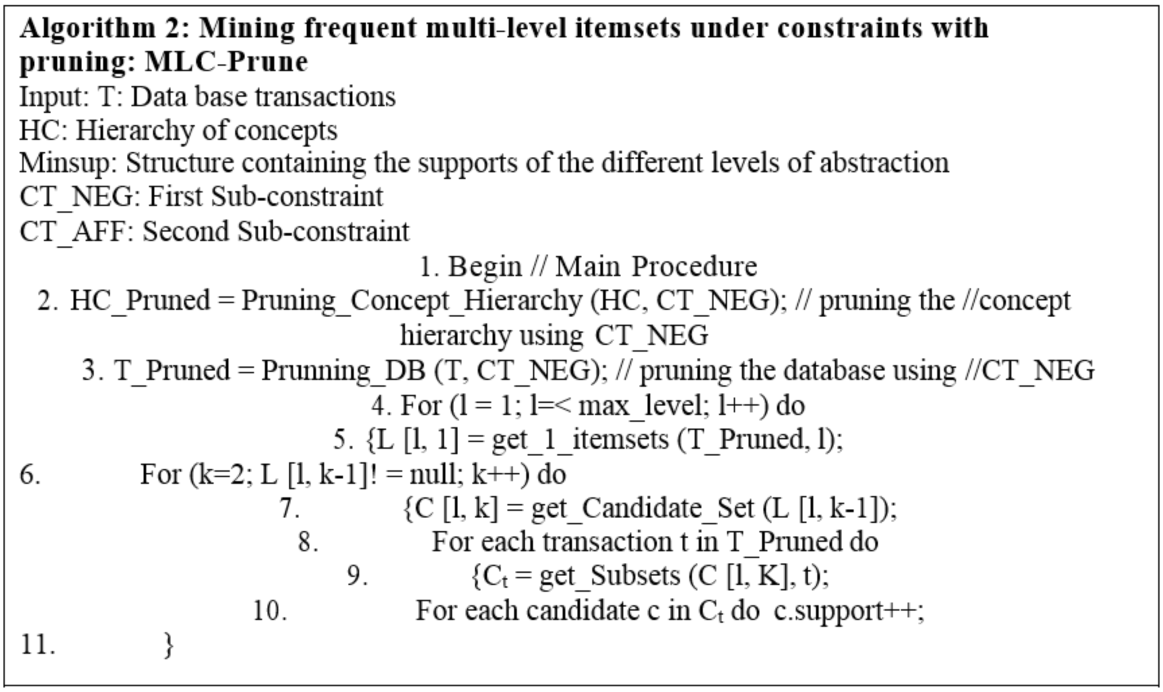
The search method of frequent multi-level itemsets under constraints with pre-pruning, presented in this scenario, proceed as follows:

- In a first step, it performs a pruning operation which consists in removing the items contained in the sub-constraint CT_NEG (Items removed by the user), from the database and the concept hierarchy. Recognizing that the elimination of one item of the concept hierarchy implies the elimination of all his descendants, i.e., a branch of the hierarchy, based on the principle of interpretation of the constraints presented in the section 3.2.

- In a second step, we proceed to searching frequent itemsets that satisfy the second sub-constraint CT_AFF, applying the principle of scenario 1, presented in the section 3.3.1.

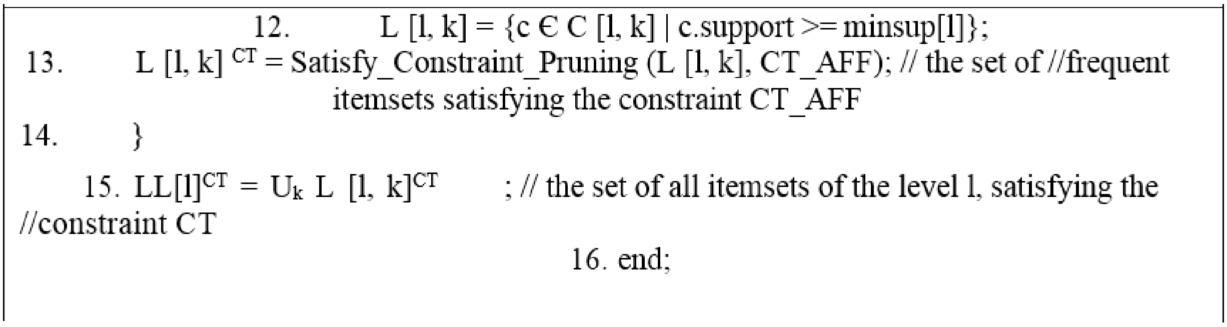
The main contribution of this method is the pruning of the database and the concept hierarchy, which precedes the operation of discovering frequent itemsets. This reduces the itemsets lattice's size to run through for each level of abstraction. In addition to that, we verify the validity of frequent itemsets over the sub-constraint CT_AFF which does not contain literals with a sign of negation. This method operates on the definition of the constraints by the user and obliged him to divide it into two sub-constraints and make choices on items to eliminate from the search process.

Table 4: Pseudo-code of the algorithm of mining frequent multi-level itemsets under constraints with pre-pruning: Scenario 3 : MLC_Prune

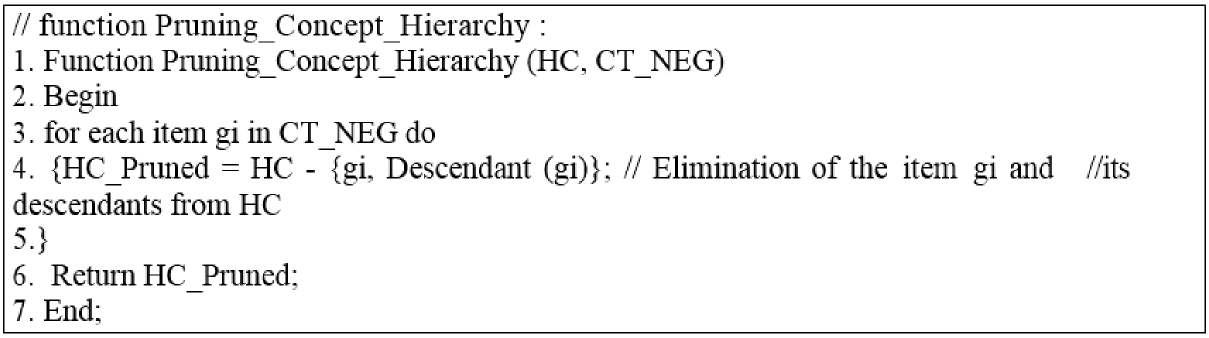


Algorithm 2: Mining frequent multi-level itemsets under constraints with pruning: MLC-Prune

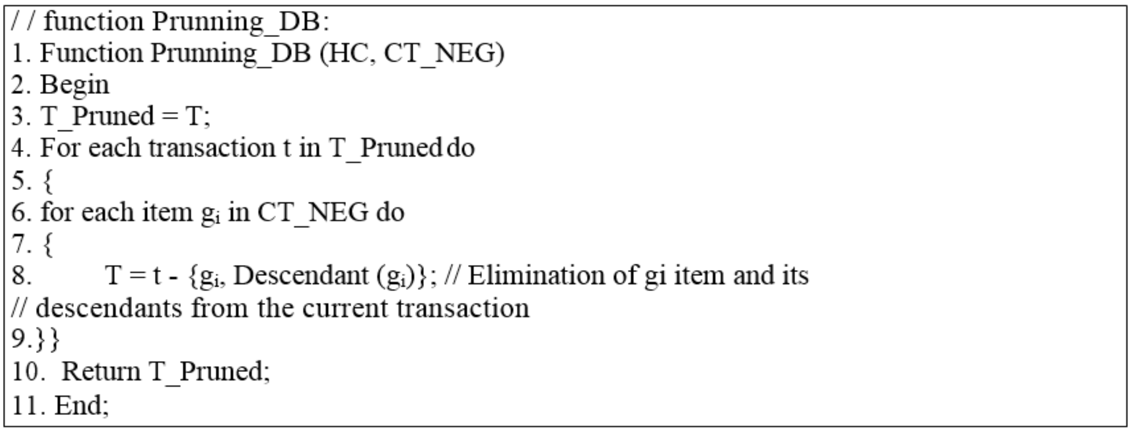
```
Input: T: Data base transactions
HC: Hierarchy of concepts
Minsup: Structure containing the supports of the different levels of abstraction
CT_NEG: First Sub-constraint
CT_AFF: Second Sub-constraint
Begin // Main Procedure
  HC_Pruned = Pruning_Concept_Hierarchy (HC, CT_NEG); // pruning the //concept hierarchy using CT_NEG
  T_Pruned = Prunning_DB (T, CT_NEG); // pruning the database using //CT_NEG
  For (l = 1; l=< max_level; l++) do
    {L [l, 1] = get_1_itemsets (T_Pruned, l);
    For (k=2; L [l, k-1]! = null; k++) do
      {C [l, k] = get_Candidate_Set (L [l, k-1]);
      For each transaction t in T_Pruned do
        {C_t = get_Subsets (C [l, K], t);
        For each candidate c in C_t do  c.support++;
        }
```



```
      L [l, k] = {c Є C [l, k] | c.support >= minsup[l]};
      L [l, k]^CT = Satisfy_Constraint_Pruning (L [l, k], CT_AFF); // the set of //frequent itemsets satisfying the constraint CT_AFF
    }
    LL[l]^CT = U_k L [l, k]^CT ; // the set of all itemsets of the level l, satisfying the //constraint CT
end;
```



```
// function Pruning_Concept_Hierarchy :
Function Pruning_Concept_Hierarchy (HC, CT_NEG)
Begin
  for each item gi in CT_NEG do
    {HC_Pruned = HC - {gi, Descendant (gi)}; // Elimination of the item gi and //its descendants from HC
    }
  Return HC_Pruned;
End;
```



```
/ / function Prunning_DB:
Function Prunning_DB (HC, CT_NEG)
Begin
  T_Pruned = T;
  For each transaction t in T_Pruned do
  {
    for each item g_i in CT_NEG do
    {
      T = t - {g_i, Descendant (g_i)}; // Elimination of gi item and its
      // descendants from the current transaction
    }}
  Return T_Pruned;
End;
```

```
/ / function Satisfy_Constraint_Pruning:
Function Satisfy_Constraint_Pruning (L [l, k], CT_AFF)
Begin
For each itemset it Є L [l, k] do
{
    If (Satisfy_Constraint_ Itemset_Pruning (it, CT_AFF)) Then
    {$L [l, k]^{CT} = L [l, k]^{CT}$ U {it} ;}
}
 Return $L [l, k]^{CT}$ ;
End;
```

```
// function Satisfy_Constraint_ Itemset_Pruning:
Function Satisfy_Constraint_ Itemset_Pruning (it, CT_AFF)
Begin
Satisfied = false;
For ($c_i$ Є CT_AFF; ((satisfied= false) && (i=< n)); i++) do // $c_i$ is one of the //conjunctions of the sub-constraint CT_AFF
    {satisfied = true;
    For ($e_{ij}$ Є $c_i$; ((j=< $n_i$) && (satisfied = true)); j++) do // $e_{ij}$ means a literal or an //item
    {
        If ((NOT ($e_{ij}$ Є it))&& (Not Exists ( Descendant ($e_{ij}$) Є it))) then
            {satisfied = false; }
}}}
Return satisfied;
End
```

The following observations are presented to better clarify the algorithm:

- The main procedure of this algorithm begins with the pruning of the concept hierarchy and the database using the sub-constraint CT_NEG. This is done using Pruning_Concept_Hierarchy and Prunning_DB functions.

- Line 13 of the main procedure, calls the function Satisfy_Constraint_Pruning to identify the frequent itemsets that satisfy the sub-constraint CT_AFF.

- The Satisfy_Constraint_Pruning function uses another function called Satisfy_Constraint_ Itemset_Pruning, which verifies the validity of an itemset in relation with the second sub-constraint CT_AFF.

Example

The following example illustrates the performance of our approach using the hierarchy of concepts of Figures 2 and 3. Given the constraint CT divided into two sub- constraints:

- CT_NEG = (NOT (3**))
- CT_AFF = ((11*) OR (2**)).

After the pruning of the hierarchy of concepts and the database, the following results in Figure 3 and Table 5 are obtained:

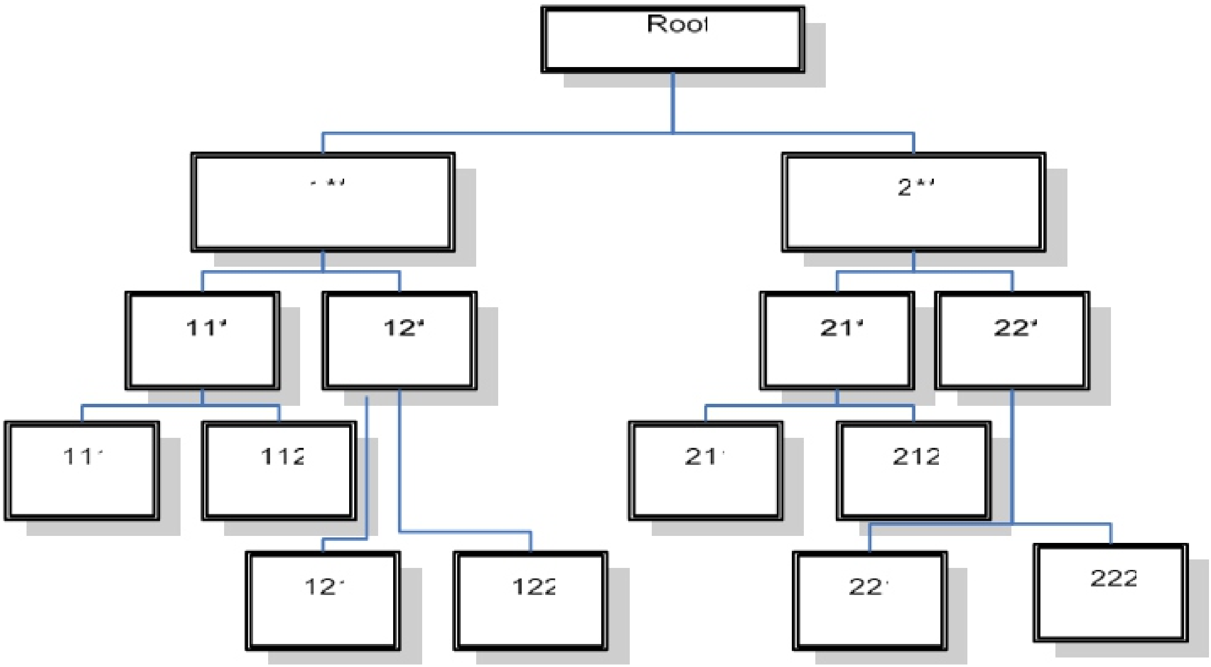


Figure 3: Pruned Concept Hierarchy

Table 5: Pruned Database

TID	Items
1	111, 212, 221
2	111, 122, 222, 212
3	122, 112, 212
4	212, 111, 122, 211
5	111, 211, 221
6	211, 121, 122
7	111, 212
8	212, 112, 122, 211

The reduced size of the concept hierarchy and the database after removal of the item (3**) and its descendants is noted. The following example details the execution illustration of this approach:

Table 6: Illustration of the execution of the algorithm of mining frequent multi- level itemsets under constraints with Pre-Pruning: Third Scenario: MLC-Prune

Level 1 :Minsup = 5

Itemsets	Support
{1**}	8
{2**}	8

L [1,1]

Itemsets	Support
{2**}	8

L [1,1]^{CT}

Itemsets	Support
{1**, 2**}	8

L [1,2]

Itemsets	Support
{1**, 2**}	8

L [1,2]^{CT}

Level 2 :Minsup = 4

Itemsets	Support
{11*}	7
{12*}	5
{21*}	8
{22*}	3

L [2, 1]

Itemsets	Support
{11*}	7
{12*}	5
{21*}	8

L [2, 1]^{CT}

Itemsets	Support
{11*, 12*}	4
{11*, 21*}	6
{12*, 21*}	5

L [2, 2]

Itemsets	Support
{11*, 12*}	4
{11*, 21*}	6
{12*, 21*}	5

L [2, 2]^{CT}

Itemsets	Support
{11*, 12*, 21*}	4

L [2, 3]

Itemsets	Support
{11*, 12*, 21*}	4

L [2, 3]^{CT}

Level 3 : Minsup = 3

Itemset	Support	Itemset	Support
{111}	5	{211}	4
{112}	2	{212}	5
{121}	1	{221}	1
{122}	4	{222}	1

L [3, 1]

Itemset	Support
{111}	5
{211}	4
{212}	5

L[3,1]^{CT}

Itemset	Support	Itemset	Support
{111, 122}	2	{122, 211}	2
{111, 211}	2	{122, 212}	5
{111, 212}	2	{211, 212}	1

L[3,2]

Itemsets	Support
{122, 212}	4

L[3,2]^{CT}

This running example shows clearly that the number of itemsets generated and analyzed was significantly reduced compared to the approach of the first scenario. This is due to the runing phase, which has eliminated the item (3**) and its descendants in the database and the concept hierarchy using the sub-constraint CT_NEG.

Rationale of the pruning based approach

The approach proposed in this scenario comes in the goal of optimizing mining process of multi-level frequent itemsets under constraints. This approach requires that the user divides his constraint into two sub-constraints: CT_NEG and CT_AFF. CT_NEG includes the items that the user wishes to eliminate from the search process. CT_NEG is used to achieve a pruning operation of the database and the concept hierarchy. This pruning reduces the size of the trellis of itemsets for each level of abstraction and then the time reserved for the calculation of supports. In addition to that, transactions in the pruned database are smaller which improves the performance of the database scan. Moreover, the reduction in the number of discovered itemsets can improve their interpretation by the user. The technique used for modeling constraints of this approach allows the user to define its objectives in terms of the content of the discovered patterns. The effectiveness of this algorithm is validated when treating real life large databases.

3.3.4. EXPERIMENTATIONS:

In order to study the effectiveness of the approaches suggested for the resolution of the problem of mining multi-level frequent itemsets under constraints, a series of experiments were carried out. The algorithms related to approaches of scenarios 1 and 3, respectively, proposed in sections 3.3.1 and 3.3.2 were implemented. A generation of a database (With several sizes: 3000, 4000, 5000 and 6000 transactionswith average of 8 items per transaction) and a concept hierarchy (With several sizes: 10, 30, 40 and 50 roots, e.g., items of level 1) on its items, was performed in order to experiment our algorithms. All experiments were performed under identical technical conditions. The implementation of the algorithms was carried out in following environments: Oracle JDeveloper to implement the algorithms, and an Oracle 10g server (Sun Sparc E450, 1 GB RAM, OS: Unix Solaris 10), for the database.

In a first experiment, several values of minsup (support threshold) were affected for the different levels (Level 1: 30%, Level 2: 20%, level 3: 10%). the size of the database was changed several times in order to study the impact of this change on the performance of scenarios 1 and 3. It should be noted that the constraints used for both scenarios are semantically equivalent. The results of this experiment are showed in Figure 4 below.

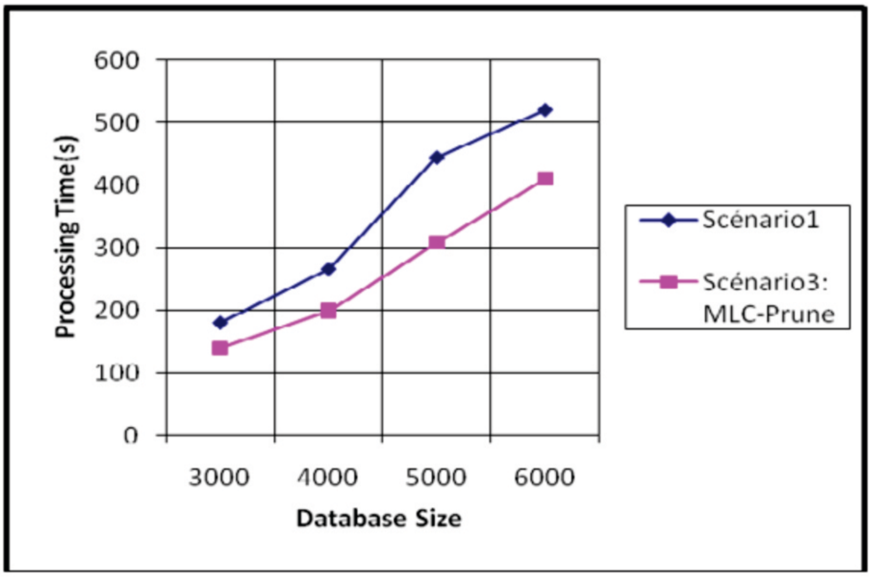


Figure 4: Experimentation 1: Comparison of the performances of first and third scenario, depending on the size of the database

The processing time of the third scenario is lower than the first scenario. This is due to the pruning step, in the third scenario, which reduces the number of itemsets analyzed and the complexity of the generation of candidates at each pass. The difference of execution time between the two algorithms increases with the increase in the size of the database.

In the second experimentation, a fixed size for the database has been set and we tried to study the impact of changes in the value minsup (support threshold) and to study the behavior of the algorithms of the first and third scenario. In this experiment, we assigned the same value of minsup for all levels of abstraction. The constraints are semantically equivalent. The results of this experiment are showed in Figure 5.

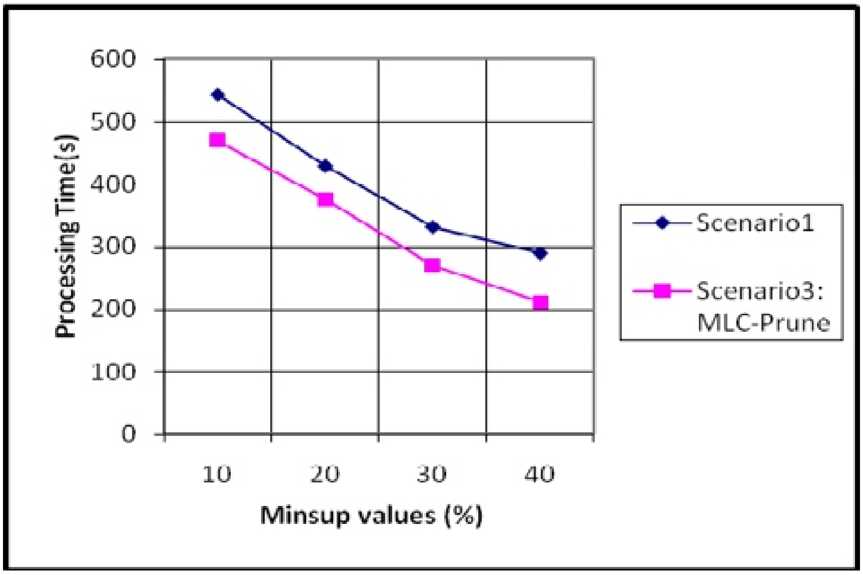


Figure 5: Experimentation 2: Comparison of the first and third scenario depending on the values of minimum support.

Similarly to the results of the first experimentation, the third scenario is more efficient than the first scenario. Performances of both algorithms better with higher support thresholds.

In the third experimentation, we studied the behavior of our algorithms, Scenario1: Basic and Scenario 3: MLC-Prune, under modification of the number of roots of the concept hierarchy, e.g., the number of items of level 1. We increased the number of roots from 10 to 50. As shown on figure 6, the processing time increases by increasing the number of roots. MLC-Prune is more efficient then the basic algorithm (Scenario1). The reason is that as the number of roots increases, the pruning step, implemented in MLC-Prune Algorithm, will have more interest and reduces significantly the itemsets lattice analyzed for each level of abstraction. Then, MLC-Prune treats always a smaller concept hierarchy and database. Furthermore, the constraints defined for algorithms processing handle with a high number of items, which harden the operation of checking itemsets validity and give more effectiveness to the pruning operation.

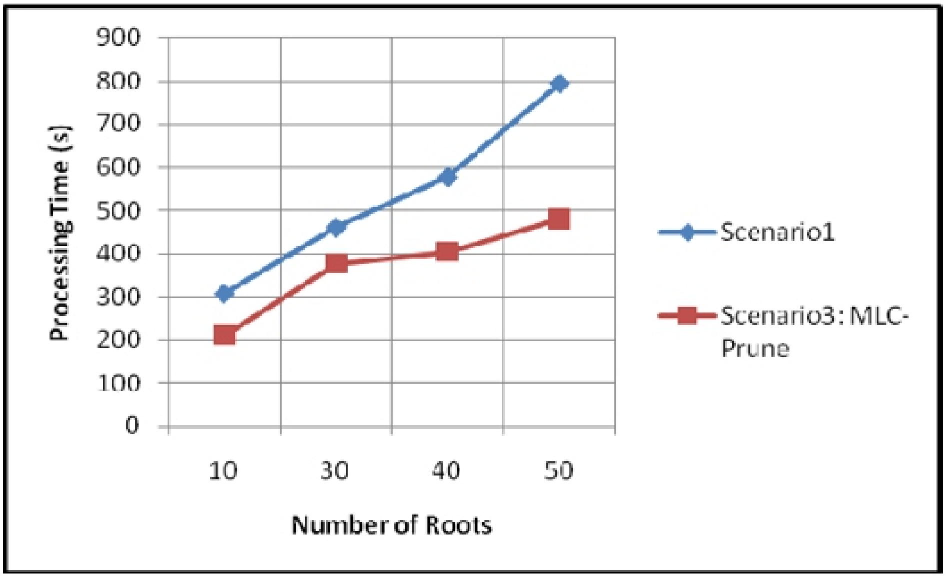


Figure 6: Experimentation 3: Comparison of the first and third scenario (MLC-Prune) Depending on the number of roots of the Concept Hierarchy

The fourth experimentation, whose results are shown in Figure7, presents a comparison between our algorithms and other algorithms of the literature, ML-T1 and ML-T2 proposed in [9]. ML-T2 and ML-T1 were implemented because they implement the same mining strategy with our algorithms. The number of database transactions was progressively increased and we executed all the algorithms in typically identical technical conditions. Results in Figure7 show that MLC-Prune Algorithm is the most efficient. This is heroically caused by the pruning step based on a very rich constraint, eliminating many branches of the concept hierarchy. The optimization technique implemented in ML-T2 algorithm which consists in pruning the database by eliminating all non frequent 1- itemsets of level 1 and their descendants wasn't very efficient as we assigned low support threshold for level 1 processing in ML-T2. In addition to that, this optimization technique may have more interest when handling more huge databases.

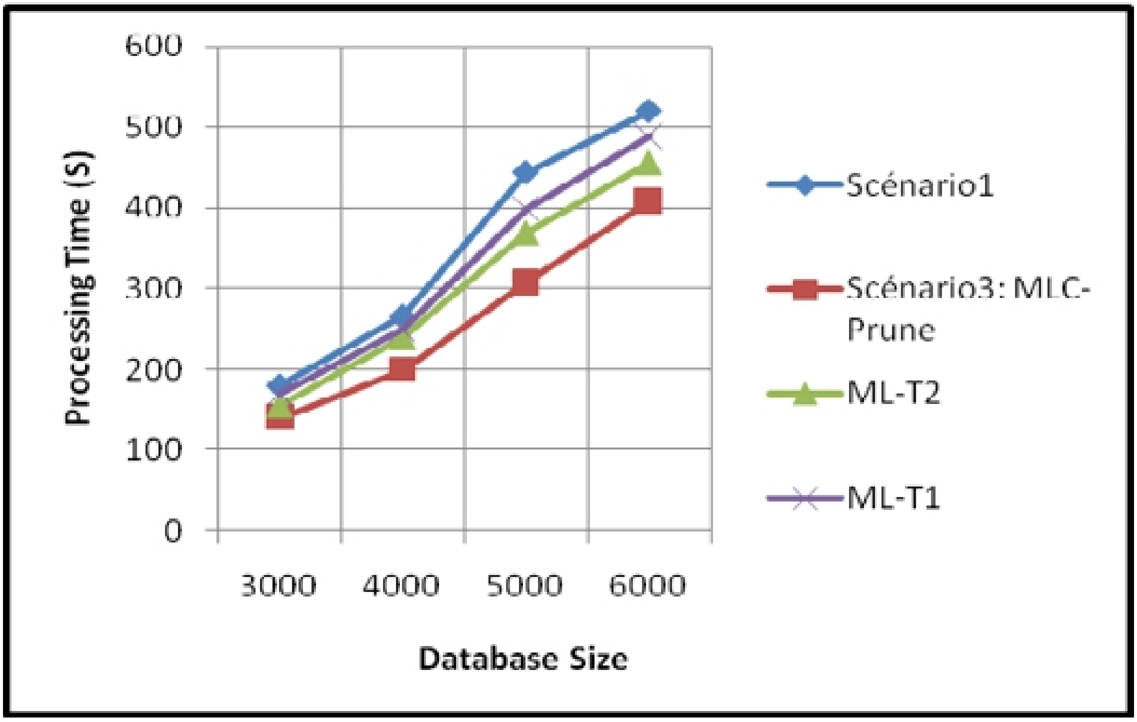


Figure 7: Experimentation 4: Comparison of the first and third scenario (MLC-Prune) with ML-T2 and ML-T1 algorithms

The results of the experimentations have confirmed our expectations on the theoretical level and have demonstrated the feasibility of our approaches.

4. CONCLUSION

In this paper, we introduced the problem of mining multiple level frequent itemsets under constraints, which allow the user to control the mining process and especially the existence of items into itemsets. We proposed a technique for modeling existence constraints in the context of use of concept hierarchies. Then, three algorithms were developed and studied to resolve this problem: The algorithm Basic (Scenario 1), the Test and Generate algorithm (Scenario 2) and the pruning based algorithm (Scenario 3). It is to note that it was proved that the algorithm of the scenario 2 is not complete and leads to the omission of a high number of frequent itemsets. Several Experimentations were performed in order to validate the algorithms we proposed in this paper and to study their behavior depending on some parameters such as database size and minimum support value. We have also compared our algorithms to other algorithms of the literature.

This work will be completed in our research group, by the design and implementation of a SQL like language that allows the expert to specify the minimum support for each level of the concept hierarchy and specify constraints; in addition to the introduction of other quality measures: confidence, lift, Loevinger, etc.

REFERENCES

[1] Fayyad, U., Piatetsky-Shapiro, G., et Smyth, P. From Data Mining to Knowledge Discovery: An Overview, in Fayyad, U., Piatetsky-Shapiro, G.,Amith, Smyth, P., and Uthurnsamy, R. (eds.), Advances in Knowledge Discovery and Data Mining, MIT Press, 1-36, Cambridge, 1996.

[2] Agrawal, R., Imielinski, T., Swami, A. Mining Association Rules Between Sets of Items in Large Databases, in Proceedings ACM SIGMOD International Conference on Management of Data, P. 207, Washington DC, Mai 1993.

[3] Agrawal, R., Srikant, R. Fast Algorithms for Mining Association Rules, in Proceedings of the 20th International Conference on Very Large Data Bases (VLDB'94), pp 487- 499, Santiago, Chile, September 1994.

[4] Savasere, A., Omiecinski, E., Navathe, S., An Efficient Algorithm for Mining Association Rules in Large Databases, in Proceedings of the 21th conference onVLDB (VLDB'95), Zurich, Switzerland, September 1995.

[5] Zaki, M.J., Parthasarathy, S., Ogihara, M., Li, W., New Algorithms for fast discovery of Association Rules, in Proceedings of the 3rd International Conference on KDD and data mining (KDD'97), Newport Beach, California, August 1997.

[6] Pasquier, N., Bastide, Y., Taouil, R., Lakhal, L., Pruning Closed Itemset Lattices for Association Rules, in Actes des 14ème journées Bases de Données Avancées, P. 177- 196, 2005.

[7] Han, J., Pei, J., Yin, Y., Mining Frequent Patterns without Candidate Generation, in Proceedings of the 2000 ACM-SIGMOD Int'l Conf. On Management of Data, Dallas, Texas, USA, May 2007.

[8] Srikant, R., Agrawal, R., Mining generalized association rules, In Proceedings of the 21st VLDB Conference, Zurich, Switzerland, 1995.

[9] Han, J., Fu, Y., Discovery of Multiple-Level Association Rules from Large Databases, in Proceedings of the 21st Very Large Data Bases Conference, Morgan Kaufmann, P. 420-431, 1995.

[10] Hipp, J., Myka, A., Wirth, R., Güntzer, U., A new algorithm for faster mining of generalized association rules, in 2nd PKKD, 1998.

[11] Han, J., Fu, Y., Mining Multiple-Level Association Rules in Large Databases, in IEEE Transactions on Knowledge and Data Engineering, Vol. 11, No. 5, Septembre/Octobre 1999.

[12] Sriphaew, K., Theeramunkong, T., A New Method for Finding Generalized Frequent Itemsets in Generalized Association Rule Mining, in Proceedings of the VIIth International Symposium on Computers and Communications, P. 421-431, 2002.

[13] Thakur, R. S., Jain, R. C., Pardasani, K. R., Mining Level-Crossing Assosiation Rules from Large Databases, in the Journal of Computer Science 2(1), P. 76-81, 2006 .

[14] Srikant, R., Vu, Q., Agrawal, R., Mining Association Rules with Item Constraints, in Proceedings of the 3rd International Conference on Knowledge Discovery and Data Mining (KDD'97), P. 67-73, AAAI Press, 1997.

Engineering Reach To Globalization: Prime Movers To USA, UK, China And India

Prem Prakash Satpathy*, S. Nibedita*, S. Roy*, Sakshi Kumari* Binod kumar*
*Department of Electronics and Communication Engineering, Cambridge Institute of Technology, Ranchi

Today world is changing very fast and around the world most highly sophisticated electronics gadgets are used. In Japan and China the revolution is very high and it is affecting world around USA, UK, Russia, Korea, India, Middle East, Gulf countries and UAE. The emerging rends in Mobile communication, internet, sericulture, fisheries, mechanization, chemical and missile aviation, aeronautics, antibiotics, medical engineering, polymer engineering, textile engineering and pharmaceutical engineering and application is speeding the present life style. The people and Associates are to maximum reach and energise with food, water, cosmetics, utilities and engineering application.

The software industries in UK and America are making maximum use of soft technology in day today use, speeding on power utilization, power transmission and power management. The Power Industries and distributors are to reform the world on Global interaction and exchange of communication ideas in finance, technology, power, civilization and up gradation for software use and utilities.

Stratified Antenna

Satellites are placed on the orbit to understand geo-stationary movement, earth and territorial position on communication, technology transfer and other planetary motion.

Satellite

Revolving satellite is used for online picture on Mars, Moon, Neptune and Uranus. It makes revolving around sun and earth orbit to investigate on soil, water and longevity on other planets and biological and technological MIMO stability.

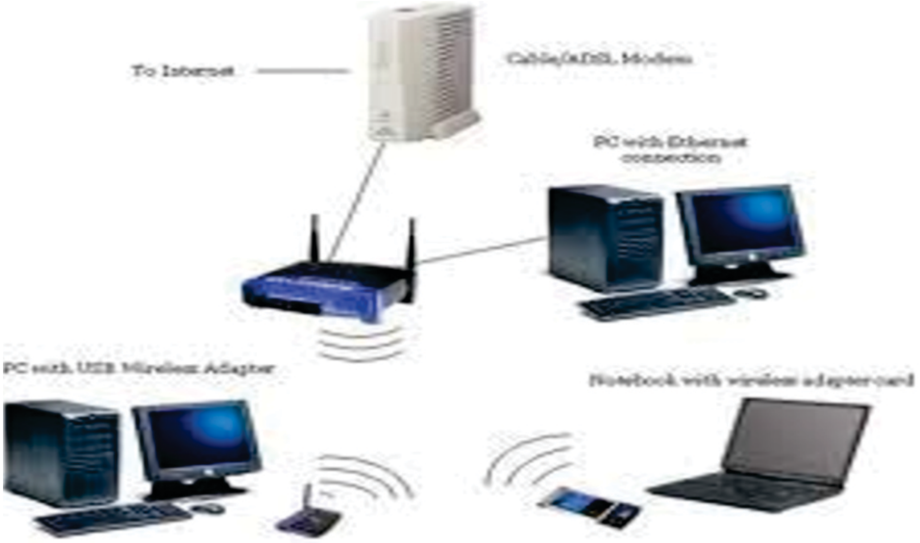
Revolving Satellite

Around 55 million of population of world, the major resource application are based on Engineering design; software and hardware reach to users by telecommunication, navigation, aerospace engineering, satellite and mobile communication. Present era is more intensive in upgrade, reach to technology and utilization. Even, pharmaceutical engineering and products are making major recovery from fatal diseases, cancer and immune deficiency. USA and UK are major resource provider world wide on engineering reach to offenders.

Telecommunication

India and India Space programme, telecommunicating Satellite, channel based software makes high integrity and application on user friendliness, uses, and Reach on engineering application. India is innovative on software and Hardware installation, commissioning and distribution of services on Mobile, 3G, wireless communication, satellite radio, aerodynamics, thermal application, sensors, broadcasting application, technology update and reach.

The wireless communication in India is emerging with 4G and 4.5 G Technology. It is flexible, digital and makes congestion control on communicating with remote. The user is free to access easy link band using Ethernet, communication protocol 804.2, 804.3, 804.6 etc and wireless operated on broadcasting and downloading application. The software is aggressive and makes usage control on communication and reduces congestion control and heavy traffic load. It is systematic to recipient and minimizes loading effect on heavy traffic. The data transmitted and received is used to cognitive on software based radio for high propagation of range 100GHZ -180 GHZ. The wireless link is as shown in figure:


To Internet
Cable/xDSL Modem
PC with Ethernet connection
PC with USB Wireless Adapter
Notebook with wireless adapter card

Wireless Communication

Robot is more aggressive in China, Japan, US, and UK. Many high sophisticated robots are used in technological measures and effective due to maximum utility. India is also intensive for high quality robot for industrial measures, production and software access on automation. The Robot are programmable and used for technological diversity, games, web multimedia application, graphical and 3D topological application.

Robot

FINDINGS AND RESULTS

There is great scope to engineering application to human beings and future technology is web based industrial Automation. It is supported by Robot and communicating Technologies in India, USA, UK, Japan, China, Malaysia, Singapore, Russia, Korea, Taipei, etc.

REFERENCES

1. Planning Commission (2004), Report of Committee on India Vision 2020, Government of India.

2. Planning Commission (2005), Mid-term Appraisal of 10th Five Year Plan. Government of India.

3. Srinivasan, T. N. and Suresh Tendulkar (2003), reintegrating India with the World Economy, Institute of international Economics, Washington DC.

4. The Financial Express (2006), Future Fuels, May 14, 2006 pages 6-7.

5. CMIE(2005), Energy –India, Economic Intelligence Service, Centre for Monitoring Indian Economy, April 2005.

Issues And Challenges In Web Services

Sarvesh Tanwar*
*Asstt. Prof. in Mody Institute of Science & Technology, Laxmangarh

ABSTRACT

Web Services Security (WS-Security) is the emerging security standard designed to address these issues. Web services are a widely touted technology that aims to provide tangible benefits to both business and IT. Their increasing use in the enterprise sector for the integration of distributed systems and business critical functions dictates the need for security assurance yet there is currently no security testing methodology specifically adapted to applications that implement web services. Web Service Enhancement (WSE) allows you to implement message level security solutions including authentication, encryption and digital signatures. In this paper we analyzes the threats and security issues that can be related to the use of web services technology in a web application.

Keywords: Ws-Security,WSE,Digital signatures, authentication.

1. INTRODUCTION

Web services are used by an increasing number of companies as they expose products and services to customers and business partners through the Internet and corporate extranets. Microsoft has released Web Services Enhancements (WSE) 2.0 for Microsoft .NET 1.1 and WSE 3.0 for .NET 2.0, which supports WS-Security and a related family of emerging standards. The security requirements for these service providers are of paramount importance. In some cases, primarily intranet or extranet scenarios where you have a degree of control over both endpoints, the platform-based security services provided by the operating system and Internet Information Services (IIS) can be used to provide point-to- point security solutions.

However, the message based architecture of Web services and the heterogeneous environments that span trust boundaries in which they are increasingly being used pose new challenges. These scenarios require security to be addressed at the message level to support cross-platform interoperability and routing through multiple intermediary nodes.

2. ISSUES IN WEB SERVICES

Quality of service (QoS) is a combination of several qualities or properties of a service, such as:

Availability: is the percentage of time that a service is operating.

Security: properties include the existence and type of authentication mechanisms the service offers, confidentiality and data integrity of messages exchanged, no repudiation of requests or messages, and resilience to denial-of service attacks.

Response time: is the time a service takes to respond to various types of requests. Response time is a function of load intensity, which can be measured in terms of arrival rates (such as requests per second) or number of concurrent requests. QoS takes into account not only the average response time, but also the percentile (95th percentile, for example) of the response time.

Throughput: is the rate at which a service can process requests. QoS measures can include the maximum throughput or a function that describes how throughput varies with load intensity.

3. MAIN WEB SERVICES THREATS

Web services are a more and more common building block in modern web applications. Threat analysis of a web application can lead to a wide variety of identified threats. Some of these threats will be very specific to the application; others will be more related to the underlying infrastructural software, such as the web or application servers, the database, the directory server and so forth.

A web service is essentially an XML-messaging based interface to some computing resource. The web services protocol stack consists of:

- Some transport layer protocol, typically HTTP.
- An XML-based messaging layer protocol, typically SOAP [9]
- A service description layer protocol, typically WSDL [10]
- A service discovery layer protocol, typically UDDI [11]

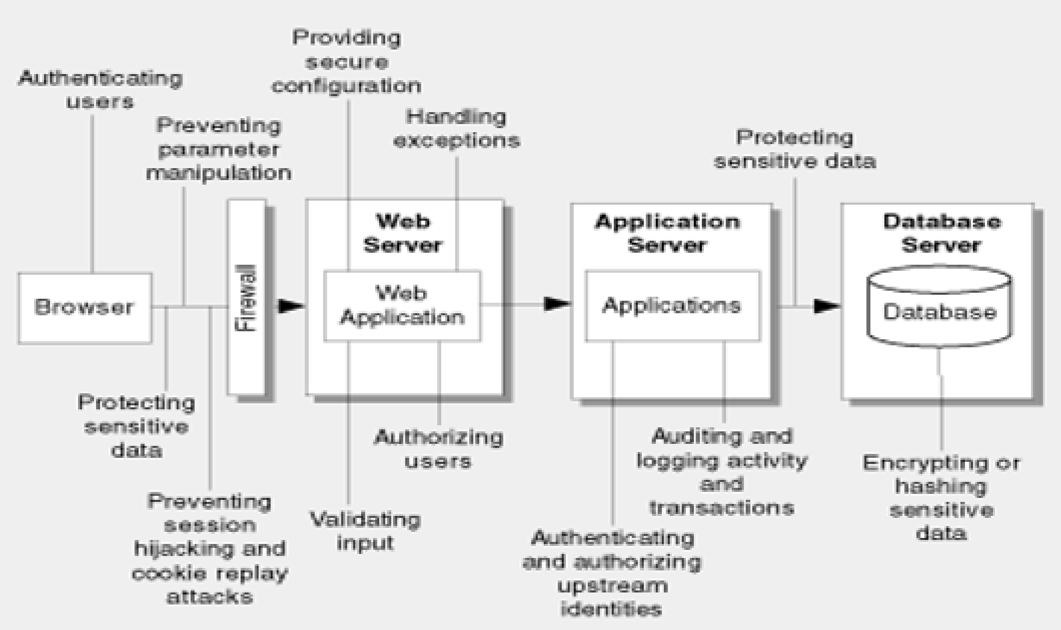

Authenticating users
Providing secure configuration
Preventing parameter manipulation
Handling exceptions
Protecting sensitive data
Web Server
Application Server
Database Server
Browser
Firewall
Web Application
Applications
Database
Protecting sensitive data
Authorizing users
Auditing and logging activity and transactions
Encrypting or hashing sensitive data
Preventing session hijacking and cookie replay attacks
Validating input
Authenticating and authorizing upstream identities

Figure 3.1: Issues in web applications[1]

I. UNAUTHORIZED ACCESS

Web services that provide sensitive or restricted information should authenticate and authorize their callers. Unauthorized Access is when a person who does not have permission to connect to or use a system gains entry in a manner unintended by the system owner. The popular term for this is “hacking”.

VULNERABILITIES

Vulnerabilities that can lead to unauthorized access through a Web service include:

- No authentication used
- Passwords passed in plaintext
- Basic authentication used over an unencrypted communication channel

COUNTERMEASURES

You can use the following countermeasures to prevent unauthorized access:

- Use password digests
- Use Kerberos tickets
- Use X.509 certificates

- Use Windows authentication.
- Use Digital Certificates

PARAMETER MANIPULATION

Manipulating the data sent between the browser and the web application to an attacker's advantage has long been a simple but effective way to make applications do things in a way the user often shouldn't be able to. In a badly designed and developed web application, malicious users can modify things like prices in web carts, session tokens or values stored in cookies and even HTTP headers.

No data sent to the browser can be relied upon to stay the same unless cryptographically protected at the application layer. Cryptographic protection in the transport layer (SSL) in no way protects one from attacks like parameter manipulation in which data is mangled before it hits the wire.

Parameter tampering can often be done with:

- Cookies
- Form Fields
- URL Query Strings
- HTTP Headers

Example of Cookies manipulation from a real world example on a travel web site modified to protect the innocent (or stupid).

```
Cookie: lang=en-us; ADMIN=no;
y=1 ; time=10:30GMT ;
The attacker can simply modify the cookie to;
 Cookie: lang=en-us; ADMIN=yes;
y=1 ; time=12:30GMT ;
```

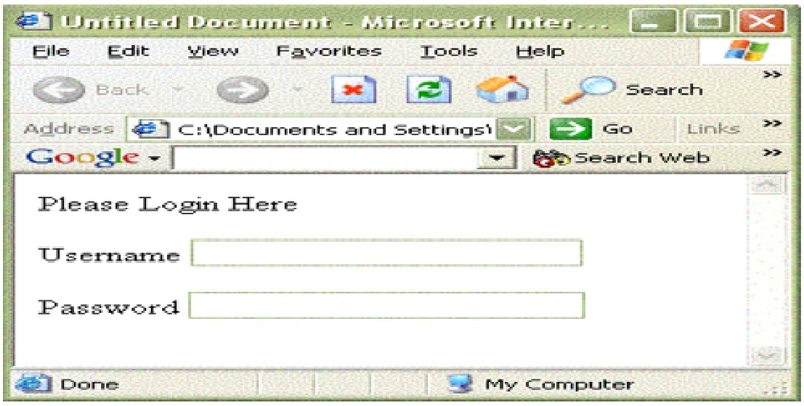
II. HTTP HEADER MANIPULATION

HTTP headers are control information passed from web clients to web servers on HTTP requests, and from web servers to web clients on HTTP responses. Each header normally consists of a single line of ASCII text with a name and a value. Sample headers from a POST request follow [5].

```
Host: www.someplace.org
Pragma: no-cache
Cache-Control: no-cache
User-Agent:Lynx/2.8.4dev.9
Content-type: application/x-www-form- urlencoded
Content-length: 49
```

Often HTTP headers are used by the browser and the web server software only. Most web applications pay no attention to them. However some web developers choose to inspect incoming headers, and in those cases it is important to realize that request headers originate at the client side, and they may thus be altered by an attacker.

As an example an application uses a simple form to submit a username and password to a CGI for authentication using HTTP over SSL. The username and password form fields look like this.



Please Login Here

Username

Password

Some developers try to prevent the user from entering long usernames and passwords by setting a form field value maxlength=(an integer) in the belief they will prevent the malicious user attempting to inject buffer overflows of overly long parameters. However the malicious user can simply save the page, remove the maxlength tag and reload the page in his browser. Other interesting form fields include disabled, readonly and value. As discussed earlier, data (and code) sent to clients must not be relied upon until in responses until it isvetted for sanity and correctness. Code sent to browsers is merely a set of suggestions and has no security value.

COUNTERMEASURES

You can use the following countermeasures to prevent parameter manipulation:

- Digital Signatures can be used to verify the users so that parameters are not tempered in transit.

- Encrypt the message payload to provide privacy.

III. NETWORK EAVESDROPPING[3][4]

Network Eavesdropping or network sniffing is a network layer attack consisting of capturing packets from the network transmitted by others' computers and reading the data content in search of sensitive information like passwords, session tokens, or any kind of confidential information.

The attack could be done using tools called network sniffers. These tools collect packets on the network and, depending on the quality of the tool, analyze the collected data like protocol decoders or stream reassembling.

Depending on the network context, for the sniffing to be the effective, some conditions must be met:

- **LAN ENVIRONMENT WITH HUBS**

This is the ideal case because the hub is a network repeater that duplicates every network frame received to all ports, so the attack is very simple to implement because no other condition must be met.

- **LAN ENVIRONMENT WITH SWITCHES**

To be effective for eavesdropping, a preliminary condition must be met. Because a switch by default only transmits a frame to the port, a mechanism that will duplicate or will redirect the network packets to an evil system is necessary. For example, to duplicate traffic from one port to another port, a special configuration on the switch is necessary. To redirect the traffic from one port to another, there must be a preliminary exploitation like the arp spoof attack. In this attack, the evil system acts like a router between the victim's communication, making it possible to sniff the exchanged packets.

- **WAN ENVIRONMENT**

In this case, to make a network sniff it's necessary that the evil system becomes a router between the client server communications. One way to implement this exploit is with a DNS spoof attack to the client system.

Network Eavesdropping is a passive attack which is very difficult to discover. It could be identified by the effect of the preliminary condition or, in some cases, by inducing the evil system to respond a fake request directed to the evil system IP but with the MAC address of a different system.

EXAMPLES

When a network device called a HUB is used on the Local Area Network topology, the Network Eavesdropping become easier because the device repeats all traffic received on one port to all other ports. Using a protocol analyzer, the attacker can capture all traffic on the LAN discovering sensitive information.

With network eavesdropping, an attacker is able to view Web service messages as they flow across the network. For example, an attacker can use network monitoring software to retrieve sensitive data contained in a SOAP message. This might include sensitive application level data or credential information.

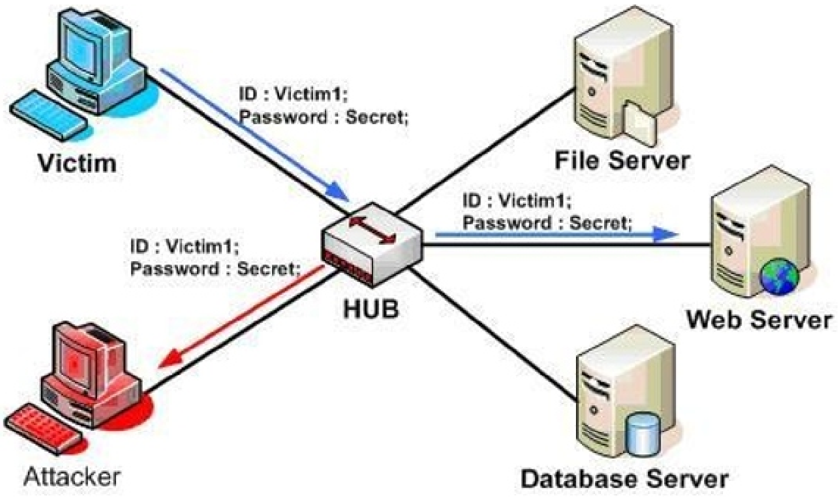


Figure 3.2: Local Eavesdropping attack.

VULNERABILITIES

Vulnerabilities that can enable successful network eavesdropping include:

- Credentials passed in plaintext
- No message level encryption used
- No transport level encryption used

CountermeasuresYou can use the following countermeasures to protect sensitive messages as they flow across the network:

- Use transport level encryption such as SSL or IPSec. This is applicable only if you control both endpoints.

- Encrypt the message payload to provide privacy. This approach works in scenarios where your message travels through intermediary nodes route to the final destination.

IV. DISCLOSURE OF CONFIGURATION DATA[1]

There are two main ways in which a Web service can disclose configuration data. First, the Web service may support the dynamic generation of Web Service Description Language (WSDL) or it may provide WSDL information in downloadable files that are available on the Web server. This may not be desirable depending on your scenario.

VULNERABILITIES

Vulnerabilities that can lead to the disclosure of configuration data include:

Unrestricted WSDL files available for download from the Web server

A restricted Web service supports the dynamic generation of WSDL and allows unauthorized consumers to obtain Web service characteristics Weak exception handling.

COUNTERMEASURES

You can use the following countermeasures to prevent the unwanted disclosure of configuration data: Authorize access to WSDL files using NTFS permissions.

- ✓ Remove WSDL files from Web server.
- ✓ Disable the documentation protocols to prevent the dynamic generation of WSDL.
- ✓ Capture exceptions and throw a Soap Exception or Soap Header Exception that returns only minimal and harmless information — back to the client.

V. MESSAGE REPLAY

Replay attack is a common kind of attack, the hackers are using to break the security of a web service. Web service messages can potentially travel through multiple intermediate servers. With a message replay attack, an attacker captures and copies a message and replays it to the Web service impersonating the client. The message may or may not be modified.

Vulnerabilities

Vulnerabilities that can enable message replay include:

- ✓ Messages are not encrypted
- ✓ Messages are not digitally signed to prevent tampering
- ✓ Duplicate messages are not detected because no unique message ID is used.

The most common types of message replay attacks include:

Basic replay attack: The attacker captures and copies a message, and then replays the same message and impersonates the client. This replay attack does not require the malicious user to know the contents of the message.

Man in the middle attack: The attacker captures the message and then changes some of its contents, for example, a shipping address, and then replays it to the Web service.

Countermeasures

In Web Sphere Application Server Versions 6 and later, when you enable integrity, confidentiality, and the associated tokens within a SOAP message, security is not guaranteed. This list of security concerns is not complete. You must conduct your own security analysis for your environment.

Ensuring the message freshness

Message freshness involves protecting resources from a replay attack in which a message is captured and resent. Digital signatures, by themselves, cannot prevent a replay attack because a signed message can be captured and resent. It is recommended that you allow message recipients to detect message replay attacks when messages are exchanged through an open network.

You can use the following elements, which are described in the Web services security specifications, for this purpose:

- Timestamp
- Using XML digital signature and XML encryption properly to avoid a potential security hole
- Protecting the integrity of security tokens
- Verifying the certificate to leverage the certificate path verification and the certificate revocation list
- Protecting the username token with a password

VI. TAMPERING[2]

The highest risk for tampering exists at the client side. An attacker can tamper with all assets residing on the client machine or traveling over the HTTP channel. This leads to the following threats that are considered most relevant in this category.

- ✓ A SOAP (Simple Object Access Protocol) message is replayed, leading to the unintended duplication of a server action or to inconsistencies on the server.
- ✓ A SOAP message is tampered with or maliciously constructed, leading to a whole variety of problems on the server side, such as information

VII. DENIAL OF SERVICE

In addition, sending a client a malicious assembly in a rich client scenario could do denial of service on that client. Also communication overload could be a threat. DoS attacks have been used as tools to make political statements [7] and extortions [8]. The latest high-profile DoS attacks against MasterCard, Visa, and other organizations linked to the late-2010 WikiLeaks incident [9] only highlight the vulnerability and susceptibility of many organizations to DoS attacks. The increased use of web services technologies to deliver major governmental services (such as the Australian Standard Business Reporting (SBR) system1) and to enable cloud computing (including Amazon clouds2) only highlights the urgency of addressing the DoS problem in web services. Recent work [6] shows that flooding attacks are still an effective way to exhaust a web service provider's CPU resources. Most existing work has not addressed the resource imbalance issue that is the key to successful flooding-based DoS attacks.

DoS attacks on web services

A) Flooding Attack: This attack attempts to exhaust a server's resources by sending a large amount of legitimate requests. The request messages in this case are well-formed and valid without any malicious XML structure or content. Consequently, such an attack cannot be detected by relying on a signature based XML firewall. Normally, such an attack is mitigated through some forms of lower network layer packet analysis, such as IP address analysis.

B) Semantic Attack: Heavy Cryptographic Processing Attack: A well-known type of a web services semantic attack is the heavy cryptographic processing attack in which an attacker sends a payload with an oversized WS-Security header containing many cryptographic elements (such as nested encryption or a large number of digital signatures). The goal is tooverload the server's resources, either through parsing a large security header or by forcing the server to process the numerous cryptographic directives.

CONCLUSION

Securing Web Services is a major concern while using the Web applications and Services. To provide security to Web application different Encryption techniques to encrypt the passwords and messages and Digital Signatures to authenticate the users so that unauthorised persons can't access the web services.

REFERENCES:

[1] msdn.microsoft.com/en- us/library/ff649028.aspx

[2] Microsoft Patterns and Practices: Building Secure ASP. NET Applications, Microsoft Press, January 2003

[3] W3C Note, Web Services Description Language (WSDL) 1.1, 15 March 2001, http://www.w3.org /TR/2001/NOTE-wsdl-20010315/

[4]Web services security provides message integrity, confidentiality, and authentication

[5]http://www.someplace.org/login.php

[6] S. Suriadi, A. Clark, and D. Schmidt, "Validating denial of service vulnerabilities in web services," in Network and System Security, International Conference on Network and System Security. IEEE Computer Society, 2010, pp. 175–182.

[7] J. Nazario, "Political DDoS: Estonia and beyond," in USENIX Security '08. USENIX, July 2008,http://streaming.linux- magazin.de/events/usec08/tech/archive/jnazario/.

[8] J. Leyden, "Techwatch weathers DDoS extortion attack," The Register, 2009, http://www.theregister .co.uk/2009/01/30/ techwatch ddos/.

[9] J. Vijayan, "MasterCard SecureCode service impacted in attacks over WikiLeaks," Computer World, 2010, http://www.computerworld.com/s/article/9200541/MasterCard SecureCode service impacted in attacks over WikiLeaks.

Vulnerabilities in Web Pages and Web Sites

Subhash Chander*, Ashwani Kush**

*Department of Computer Sc. Govt. P.G. College, Sec-14, Karnal (Haryana)

**Department of Computer Science, University College, Kurukshetra University, Kurukshetra

ABSTRACT

The number of online resources is increasing day by day in the public and private sectors in all departments. Even small shopkeepers, vendors are trying to get themselves online because of various advantages. One can find each and every shopping Mall and even office (Government or Private) is either online or is in the process of becoming online. But while doing so certain security precautions/flaws exist in all such sites and that may be dangerous for their growth in the competitive market as well in the government sectors. Certain security related metrics are mandatory and are minimum for the smooth working of such websites and web portals. Also many e-governance sites at national, state and district level exist in India. Acuentix Vulnerability measurement tool has been used to check certain security flaws in two websites related with educational department. Two websites taken into account are gckarnal.org and uckkr.org.

Keywords: Web Page, website analysis, vulnerability, scanning, e-governance.

INTRODUCTION

Web applications have been highly popular since 2000 as they allow users to have an interactive experience on the Internet. Various Topologies of Networking has provided great convenience to the Government and private organizations. According to the latest figures published in the Global Information Technology Report 2009-2010 only 4.4% of the Indian population has access to the internet. At the same time, the southern Indian state of Andhra Pradesh has invested some $5.5m in their Smart GOV initiative. This is intended to put all local government services online. The two main objectives are again to cut 'red tape' and reduce costs for the taxpayers [13]. With the help of Internet one can view static web pages, rather create personal accounts, add content, query databases and complete transactions. In this way web applications frequently collect, store and use sensitive personal data to deliver services to citizens. Customers are getting lot of benefits from these applications and ideas of e-government, e-commerce and e-learning have emerged. But there is always a risk of loss of private information stored in web applications that can be easily compromised through non ethical ways. To protect their critical IT assets, most organizations use various technical protective and detective solutions. Properly placing infrastructure security solutions can increase the effectiveness of an overall enterprise security profile, but technical point solutions alone won't provide a comprehensive security strategy. For an organisation to identify susceptibility to attacks before their IT systems are exploited, it must also perform regularly scheduled vulnerability assessment and remediation [14]. E-government is one of the most important aspects of the Internet. E- Government reflects the real vision for modernizing public administration and making it more effective and efficient. In this sense, it implies a holistic view on the whole administration and government system, i.e. processes, communication and information resources, cultural and social issues, organizational strategies, technical solutions, security issues etc. [1]. Organization networks often are victims of their own success. The networks that deliver ubiquitous computing to every desktop and client also bring the vulnerabilities of impatient users to their clients [2]. Those impatient users may connect themselves to the wired network without permission, resulting in a breach of perimeter defenses that leaves the wired users wide open to compromise. In the age of ICT, citizens also have become so much aware about their rights to get information from the government offices. Also many state governments have started giving services to its citizens in time bound manner. State governments in Punjab, Haryana, Himachal Pradesh and Rajasthan have started giving their services within the framework of Right to service act. Development of secure e-government systems requires a comprehensive model for security that businesses will have to be ready to meet the increased demand of effective and secure online services. Providing such secure online services in e-Government requires consideration at different levels and for the distinct domains of e-Government. To achieve this various technical aspects need to be taken care of. Many concepts and tools have been developed to provide secure transactions, to protect against hacker attacks. Successfully implementing e-government requires a level of trust on the part of all transaction can by implemented during the life cycle of the project [3]. Vulnerability means one can penetrate into websites or portals in an unauthorized way. There are certain Rogue access points through which hackers can penetrate into the portal and may do they like. The problems that may be faced in this situation of breach of security include anonymous access by authorized network users; denial of service attacks (intentional or unintentional); unintended release or compromise of sensitive information. Hacker also takes care of the fact that network performance is not degraded to avoid attention of system administrators. A web application security scanner is a program that communicates with a web application to identify potential security vulnerabilities in the web application and architectural weaknesses. Unlike source code scanners, web application scanners don't have access to the source code and therefore detect vulnerabilities by actually performing attacks. According to the Privacy Rights Clearinghouse, more than 18 million customer records have been compromised in 2012 due to insufficient security controls on corporate data and web application [8]. In a copyrighted report published in March 2012 by security vendor Cenzic, the most common vulnerability in recently tested applications are cross site scripting (37%) and SQL Injection (16%). One of the weaknesses is that such tools can not cover 100 % of the source code of the application [8]. There is need of developing secure code and its proper testing for various vulnerabilities claimed or unclaimed. But merely developing secure code without attesting to its assurance capabilities is akin to operating an automobile without checking to ensure that the brakes work as expected. With such an outlook, a crash becomes not just possible but inevitable [7]. Also logical & technical flaws can not be found with such tools. Section 2 gives details major attacks Cross site scripting and SQL injection, section 3 gives detail about Vulnerability assessment and penetration testing, section 4 gives details about Working of Acunetix Web Vulnerability Scanner (WVS), section 5 gives certain results of two educational sites and their Vulnerability scan reports and section 6 gives conclusion of the paper.

2. CROSS SITE SCRIPTING AND SQL INJECTION VULNERABILITIES

By having access control, hackers are able to penetrate and are able to deface or edit the web pages. The base of web portal is web page. By combining various web pages a website is created and by combining various websites a portal, to be utilized by many people, is created. Ultimately if one can check vulnerability of web page then ultimately vulnerabilities of websites and web portals can be checked. The hierarchical base of web portal is shown here in fig 1.

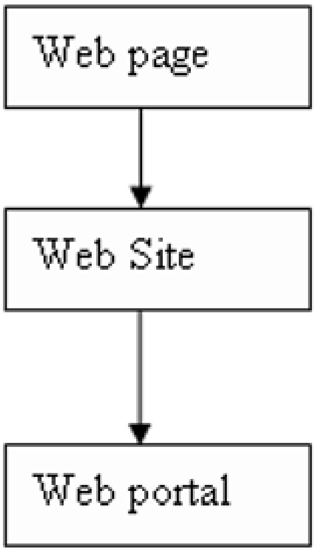


Fig. 1 Hierarchical base of a web portal

Every web page has certain security related flaws or weaknesses as SQL Injection, Privilege escalation, authentication, authorization, data loss, access control, error handling/ information leakage, command execution, session management, client side attacks, information disclosure, denial of services, audit logs, etc. For checking the vulnerability of websites and various attacks thereon, there are various soft wares available in the market. Cross–site scripting (XSS) vulnerabilities have been reported and exploited since the 1990s. The most affected sites due to XSS vulnerabilities are social networking sites. Cross-site scripting (XSS) is a type of security vulnerability that is found in web applications, such as web browsers through breaches of browser security that enables attackers to inject client-side script into web pages viewed by other users. A cross-site scripting vulnerability may be used by hackers to bypass access controls. Cross–site scripting is also one of the special cases of code injection. Cross-site scripting uses well known vulnerabilities that are available in web-based applications, servers, or plug-in systems they depend upon. While injecting malicious scripts into web pages, an attacker can gain elevated access-privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user. Exploiting one of these known vulnerabilities, certain malicious content is mixed into the original content being delivered from the compromised site. This whole activity operates under the permissions granted to that system from the user side. Major classifications of the types of XSS are non-persistent and persistent. Non- persistent XSS vulnerability is the most common type of vulnerability being exploited. Google could allow malicious sites to attack its users who visit them while logged in. The persistent XSS vulnerability is a more devastating variant of a cross-site scripting flaw. It occurs when the data provided by the attacker is saved by the server, and then permanently displayed on normal pages returned to other users in the course of regular browsing, without proper HTML escaping. Here hacker's script is rendered automatically to third party websites rather than individual targets. SQL injection is a technique for targeting databases through a website. It is done by including small parts of SQL statements in a web form. SQL injection utilizes code injection technique to exploit vulnerability in a website's software. It happens when user input is incorrectly filtered for various special characters embedded in SQL statements. SQL commands are injected from the web form into the database and change the database content or dump the database information like credit card or passwords to the attacker. SQL injection is known for attacks on websites but it can also be used to attack any type of SQL database [11]. Such type of attacks can be used by the hackers to acquire and edit the information stored in Government databases. It is very critical to think about the loss if information regarding the owners of land is displayed to anti social elements in the society. Getting information about the bank accounts of a bank can be risky job for banks and its customers. Hence majority of the attacks on databases and e-governance are of the type SQL injection.

3. VULNERABILITY ASSESSMENT AND PENETRATION TESTING

Our vulnerability is increasing daily as our use of and dependence on electronics continues to grow. The current vulnerability of our critical infrastructures can both invite and reward attack if not corrected [12] Vulnerability scanner is a computer program that is used to assess computers, computer systems, networks or applications for weaknesses. There are a number of types of vulnerability scanners available today, depending on particular targets. While functionality varies between different types of vulnerability scanners, they share a common, core purpose of enumerating the vulnerabilities present in one or more targets [5]. These two terms namely Vulnerability assessment and penetration testing are normally used in the same situation. Although there are certain phases that seem to similar in both the tools yet there is a lot of difference between the two terms.

(1) Vulnerability Analysis is used to identify the vulnerabilities (weak points) on a network, whereas a Penetration Testing is used to access systems in an unauthorized way.

(2) Vulnerability Analysis deals with potential risks, whereas Penetration Testing is actual proof of concept. Vulnerability Analysis is a process of identifying and quantifying the security Vulnerabilities in a system. Vulnerability Analysis doesn't provide validation of Security Vulnerabilities. Validation can be only done by Penetration testing [4].

(3) A Vulnerability Analysis provides list of the flaws that exist on the system while a Penetration Testing provide an impact analysis of the flaws on the underlying network, operating system, database etc.

(4) Through vulnerability analysis one can know about the logical flaws whereas penetration testing is used to exploit those flaws identified through vulnerability assessment. As example through vulnerability analysis one can know the status of open ports or non availability of antivirus on a particular machine and then with the help of that Penetrating testing what resources of the machine can be accessed and used, manipulate by the hackers.

(5) Vulnerability Analysis is a passive process whereas penetrating testing is an active process where ethical hackers simulate an attack and test network and system tolerance power.

(6) A Vulnerability Analysis explains about Vulnerabilities present and used to improve security posture whereas penetration testing can be used to break-in vulnerable systems and gives only a snapshot of the effectiveness of your security programs.

4. WORKING OF ACUNETIX WEB VULNERABILITY SCANNER (WVS)

Acunetix Web Vulnerability Scanner (WVS) is an automated web application security testing tool that audits your web applications by checking for vulnerabilities like SQL Injections, Cross site scripting and other exploitable hacking vulnerabilities [10]. Acunetix WVS scans any website or web application that is accessible via a web browser. It also offers a strong and unique solution for analyzing off-the-shelf and custom web applications including those relying on client scripts such as JavaScript, AJAX and Web 2.0 web applications. It is suitable for any small, medium sized and large organizations with intranets, extranets, and websites aimed at exchanging and/or delivering information with/to customers, vendors, employees and other stakeholders. Acunetix WVS works in the following manner:

1. The Crawler analyzes the entire website by following all the links on the site and in the robots.txt file and sitemap.xml (if available). WVS will then map out the website structure and display detailed information about every file. It also analyses hidden application files, such as web.config.

2. After the crawling process, It launches a series of vulnerability attacks on each page found, in essence emulating a hacker. Also, WVS analyses each page for places where it can input data, and subsequently attempts all the different input combinations. This is the Automated Scan Stage.

3. During the scan process, a port scan is also launched against the web server hosting the website. If open ports are found, Acunetix WVS will perform a range of network security checks against the network service running on that port.

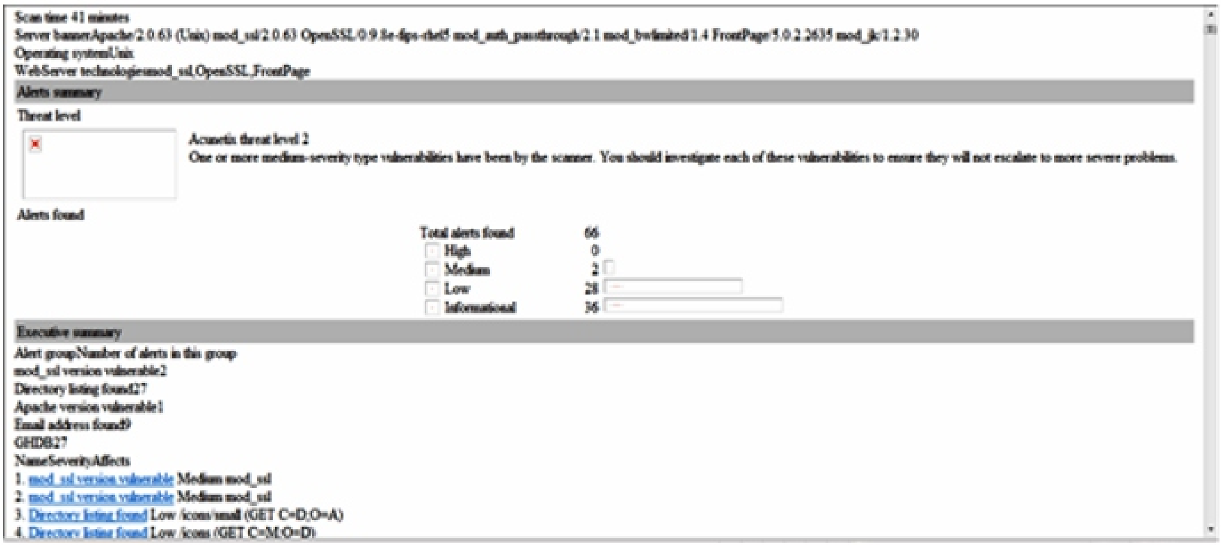
4. As vulnerabilities are found, Acunetix WVS reports these in the 'Alerts' node. Each alert contains information about the vulnerability such as POST variable name, affected item, http response of the server

5. If open ports are found, they will be reported in the 'Knowledge Base' node. The list of open ports contains information such as the banner returned from the port and if a security test failed.

6. After a scan has been completed, it can be saved to file for later analysis and for comparison to previous scans. Using the Acunetix reporter a professional report can be created summarizing the scan [10].

5. FINDINGS AND RESUTS

Acunetix WVS has been applied to two educational institute websites namely gckarnal.com and uckkr.org. Results of the scanner are shown here in fig. 2 and fig. 3. Two websites have been checked for the existing vulnerabilities.



Scan time 41 minutes
Server bannerApache/2.0.63 (Unix) mod_ssl/2.0.63 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 mod_jk/1.2.30
Operating systemUnix
WebServer technologiesmod_ssl,OpenSSL,FrontPage

Alerts summary

Threat level

Acunetix threat level 2
One or more medium-severity type vulnerabilities have been by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

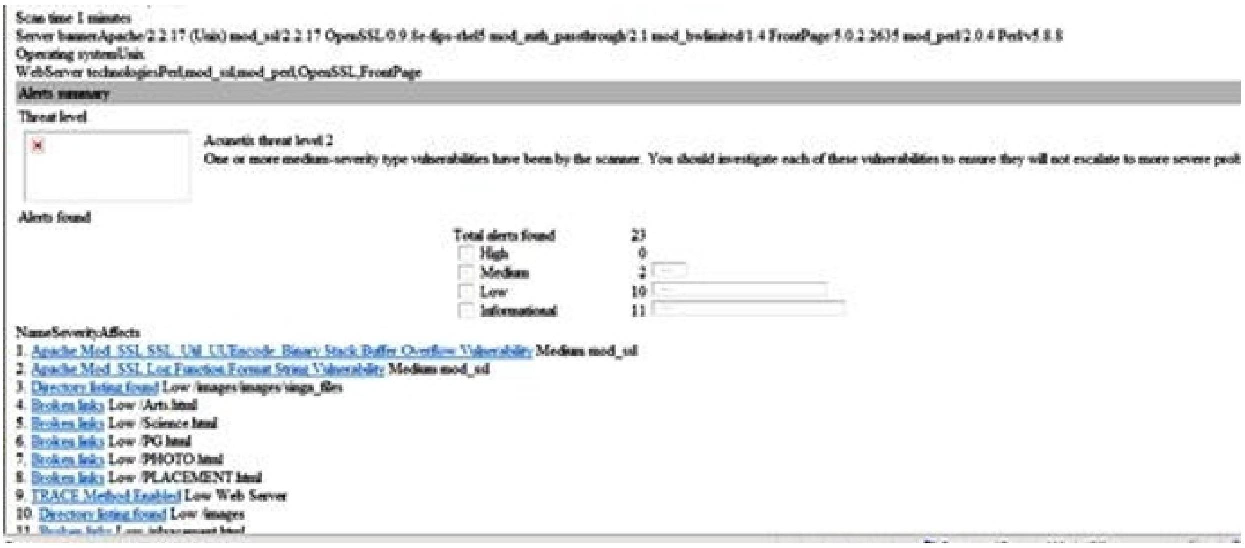
Alerts found

Total alerts found	66
High	0
Medium	2
Low	28
Informational	36

Executive summary

Alert groupNumber of alerts in this group
mod_ssl version vulnerable2
Directory listing found27
Apache version vulnerable1
Email address found9
GHDB27
NameSeverityAffects
1. mod_ssl version vulnerable Medium mod_ssl
2. mod_ssl version vulnerable Medium mod_ssl
3. Directory listing found Low /icons/small (GET C=D;O=A)
4. Directory listing found Low /icons (GET C=M;O=D)

Figure 2 summary of gckarnal.com



Scan time 1 minutes
Server bannerApache/2.2.17 (Unix) mod_ssl/2.2.17 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 mod_perl/2.0.4 Perl/v5.8.8
Operating systemUnix
WebServer technologiesPerl,mod_ssl,mod_perl,OpenSSL,FrontPage

Alerts summary

Threat level

Acunetix threat level 2
One or more medium-severity type vulnerabilities have been by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe prob

Alerts found

Total alerts found	23
□ High	0
□ Medium	2
□ Low	10
□ Informational	11

NameSeverityAffects
1. Apache Mod_SSL SSL_Util_UUEncode_Binary Stack Buffer Overflow Vulnerability Medium mod_ssl
2. Apache Mod_SSL Log Function Format String Vulnerability Medium mod_ssl
3. Directory listing found Low /images/images/singa_files
4. Broken links Low /Arts.html
5. Broken links Low /Science.html
6. Broken links Low /PG.html
7. Broken links Low /PHOTO.html
8. Broken links Low /PLACEMENT.html
9. TRACE Method Enabled Low Web Server
10. Directory listing found Low /images
11. Broken links Low /infrastructure.html

Figure 3. Summary of uckkr.org

Both the results show that gckarnal.com has more security alerts as compared to uckkr.org. Majority of the alerts are informational or low category. Number of medium and high alerts is same for both the sites. Details of various alerts shown in results are here as under. Mod_ssl alerts are the medium level alerts found in the both the results. Mod_ssl is an optional module for the Apache HTTP Server. This Mod_ssl alert would most likely result in a denial of service attack if triggered, but could theoretically allow for execution of arbitrarycode. It is also clear that these alerts may be false positive. It is one of the limitations of the Vulnerability scanners that it requires human intervention for analyzing the data after scanning process. Scanners can only report vulnerabilities as per plug-ins installed in the scan database. They cannot determine whether the response is a false negative or a false positive. Hence after medium alerts, there is one message like it can be a false positive. Regarding vulnerability scanning, "false negative" is the failure to recognize an existence of a flaw in the system or the network under assessment, whereas "false positive" is the incorrect determination of the presence of vulnerability. The former might be due to missing plug-ins in a scanner database while the latter requires human judgment to confirm [6]. It is possible to provide HTTP and HTTPS with a single server machine, because HTTP and HTTPS use different server ports. The number of low level alerts is 28 and 10 for gckarnal.com and uckkr.org respectively. Low level alerts include directory listing and broken links mainly. In gckarnal.com majority of the alerts in low level category are directory listings, whereas in case of uckkr.org majority of the alerts in low level category are broken links. A link that does not work any more is called a broken link or dead link. A link may become broken for several reasons. The simplest and most common reason is that the website concerned doesn't exist anymore. Many times one gets a message like error 404-page not found, that is because of dead link and means that web server responded, but the specific page could not be found. There may be several other reasons of the broken link. A link might also be broken because of some content filters or firewalls and on the part of the authoring side. On an Apache HTTP Server, directory listing refers to a directory on the server that does not have a default index file. The file is usually called index.html, index.htm, index.php, etc. Hence make it sure that directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. In informational alerts category majority of the alerts are based on the e-mail address found and related with icons and pictures. Other informational alerts are related with Google hacking database (GHDB) or icons and Jpg files available on these sites. While implementing e-governance projects, there is a gap between those making concepts and those who have to implement them. Action has to be taken to improve the conditions for successfully implementing e-Government projects [9].

6. CONCLUSION

Acunetix Web Vulnerability Scanner is used for website security scanning that checks for SQL injection, Cross site scripting and other vulnerabilities. It checks password strength on authentication pages and automatically audits shopping carts, forms, dynamic content and other web applications. Both the websites taken in consideration are educational institute websites. After completion of the scan a detailed report is provided and reports those pinpoints where vulnerabilities exist. By looking at the report it is clear that majority of the security alerts are informational type and are not counted in high level of alerts. Overall uckkr.org is having fewer alerts and is more secure as compared to gckarnal.com. Also there is a lot of difference in the scan time of both the portals. Interestingly website having more vulnerability takes more time for vulnerability scanning. Hence e-governance portals must also be tested against such vulnerabilities before rolling out, otherwise sensitive information related with the citizen's database including private information may be compromised and utilized wrongly by the hackers.

7. REFERENCES

[1] Wimmer Maria and Bredow Bianca Von," E-Government: Aspects of Security on Different Layers", 12th IEEE International workshop on Database and Expert Systems Applications "On the Way to Electronic Government, Pp 350-355, Munich, Germany, 2001

[2] Henning Ronda R., "Vulnerability Assessment in Wireless Networks," pp.358, Symposium on Applications and the Internet Workshops (SAINT Workshops), 2003

[3] Al-Ahmad,W. and Al-Kaabi, R. ,"An Extended Security Framework for e- Government", Pp 294-295 ,Intelligence and security informatics (ISI), IEEE International Conference 17-20, June, Taipei, Taiwan, E-ISBN: 978-1-4244-2415-3, Print ISBN: 978-1-4244-2414-6 (2008)

[4] "Penetration testing Vs Vulnerability Assessment", available at www.primeinfoserv.com/pdf /consulting/VAvsPT-Prime.pdf

[5] Available at www.en.wikipedia.org

[6] "An Overview of Vulnerability Scanners", February (2008), Available at www.infosec.gov.hk/ english/technical/fil es/vulnerability.pdf

[7] Paul Mano ," Assuring software security through testing , White ,Black and somewhere in between" , A whitepaper available on www.isc2.org

[8] Available at www.rtbot.net/Web_application_security_scanner

[9] Lenk Klaus and Traunmüller Roland," Electronic Government: Where Are We Heading?", EGOV, LNCS 2456, pp. 1–9, Springer-Verlag Berlin Heidelberg ,2002.

[10] User manual of Acunetix Web Vulnerability Scanner V8, v.1 (2012) and available at www.acunetix.com

[11] Mathur Peeyush et al. ," Sql-injection security evolution analysis in asp.net", International Journal Of Engineering Science & Advanced Technology (IJESAT), Volume-2, Issue-3,Pp 657 – 663, ISSN: 2250–3676 (2012)

[12] Caelli W.J. et al.," Policy and Law: Denial of Service Threat", An Investigation into the Detection and Mitigation of Denial of Service (DoS) Attacks: Critical Information Infrastructure Protection, Pp 41-114, Chapter 3, © Springer India Pvt. Ltd. 2011

[13] Johnson Christopher W. and Raue Stefan ," On the Safety Implications of E- Governance: Assessing the Hazards of Enterprise Information Architectures in Safety-Critical Applications", SAFECOMP 2010, LNCS 6351, pp. 402–417, Springer- Verlag Berlin Heidelberg 2010

[14] Liu Simon, Holt Larry, and Cheng Bruce ,"A Practical Vulnerability Assessment Program", Vulnerability Assessment, Pp 36-42, IT PRO , Published by the IEEE Computer Society, 2007

Instructions for Authors

Essentials for Publishing in this Journal

1 Submitted articles should not have been previously published or be currently under consideration for publication elsewhere.

2 Conference papers may only be submitted if the paper has been completely re-written (taken to mean more than 50%) and the author has cleared any necessary permission with the copyright owner if it has been previously copyrighted.

3 All our articles are refereed through a double-blind process.

4 All authors must declare they have read and agreed to the content of the submitted article and must sign a declaration correspond to the originality of the article.

Submission Process

All articles for this journal must be submitted using our online submissions system. http://enrichedpub.com/ . Please use the Submit Your Article link in the Author Service area.

Manuscript Guidelines

The instructions to authors about the article preparation for publication in the Manuscripts are submitted online, through the e-Ur (Electronic editing) system, developed by **Enriched Publications Pvt. Ltd**. The article should contain the abstract with keywords, introduction, body, conclusion, references and the summary in English language (without heading and subheading enumeration). The article length should not exceed 16 pages of A4 paper format.

Title

The title should be informative. It is in both Journal's and author's best interest to use terms suitable. For indexing and word search. If there are no such terms in the title, the author is strongly advised to add a subtitle. The title should be given in English as well. The titles precede the abstract and the summary in an appropriate language.

Letterhead Title

The letterhead title is given at a top of each page for easier identification of article copies in an Electronic form in particular. It contains the author's surname and first name initial .article title, journal title and collation (year, volume, and issue, first and last page). The journal and article titles can be given in a shortened form.

Author's Name

Full name(s) of author(s) should be used. It is advisable to give the middle initial. Names are given in their original form.

Contact Details

The postal address or the e-mail address of the author (usually of the first one if there are more Authors) is given in the footnote at the bottom of the first page.

Type of Articles

Classification of articles is a duty of the editorial staff and is of special importance. Referees and the members of the editorial staff, or section editors, can propose a category, but the editor-in-chief has the sole responsibility for their classification. Journal articles are classified as follows:

Scientific articles:

1. Original scientific paper (giving the previously unpublished results of the author's own research based on management methods).

2. Survey paper (giving an original, detailed and critical view of a research problem or an area to which the author has made a contribution visible through his self-citation);

3. Short or preliminary communication (original management paper of full format but of a smaller extent or of a preliminary character);

4. Scientific critique or forum (discussion on a particular scientific topic, based exclusively on management argumentation) and commentaries. Exceptionally, in particular areas, a scientific paper in the Journal can be in a form of a monograph or a critical edition of scientific data (historical, archival, lexicographic, bibliographic, data survey, etc.) which were unknown or hardly accessible for scientific research.

Professional articles:

1. Professional paper (contribution offering experience useful for improvement of professional practice but not necessarily based on scientific methods);
2. Informative contribution (editorial, commentary, etc.);
3. Review (of a book, software, case study, scientific event, etc.)

Language

The article should be in English. The grammar and style of the article should be of good quality. The systematized text should be without abbreviations (except standard ones). All measurements must be in SI units. The sequence of formulae is denoted in Arabic numerals in parentheses on the right-hand side.

Abstract and Summary

An abstract is a concise informative presentation of the article content for fast and accurate Evaluation of its relevance. It is both in the Editorial Office's and the author's best interest for an abstract to contain terms often used for indexing and article search. The abstract describes the purpose of the study and the methods, outlines the findings and state the conclusions. A 100- to 250-Word abstract should be placed between the title and the keywords with the body text to follow. Besides an abstract are advised to have a summary in English, at the end of the article, after the Reference list. The summary should be structured and long up to 1/10 of the article length (it is more extensive than the abstract).

Keywords

Keywords are terms or phrases showing adequately the article content for indexing and search purposes. They should be allocated heaving in mind widely accepted international sources (index, dictionary or thesaurus), such as the Web of Science keyword list for science in general. The higher their usage frequency is the better. Up to 10 keywords immediately follow the abstract and the summary, in respective languages.

Acknowledgements

The name and the number of the project or programmed within which the article was realized is given in a separate note at the bottom of the first page together with the name of the institution which financially supported the project or programmed.

Tables and Illustrations

All the captions should be in the original language as well as in English, together with the texts in illustrations if possible. Tables are typed in the same style as the text and are denoted by numerals at the top. Photographs and drawings, placed appropriately in the text, should be clear, precise and suitable for reproduction. Drawings should be created in Word or Corel.

Citation in the Text

Citation in the text must be uniform. When citing references in the text, use the reference number set in square brackets from the Reference list at the end of the article.

Footnotes

Footnotes are given at the bottom of the page with the text they refer to. They can contain less relevant details, additional explanations or used sources (e.g. scientific material, manuals). They cannot replace the cited literature.

The article should be accompanied with a cover letter with the information about the author(s): surname, middle initial, first name, and citizen personal number, rank, title, e-mail address, and affiliation address, home address including municipality, phone number in the office and at home (or a mobile phone number). The cover letter should state the type of the article and tell which illustrations are original and which are not.