July - December, 2010 Vol. 2 No. 2 ISSN 0973-5658

BVICAM's IJIT

BVICAM's International Journal of Information Technology

CONTENTS

BHARATI VIDYAPEETH PUNE BHARATI VIDYAPEETH POONA

Bharati Vidyapeeth's
Institute of Computer Applications and Management
A-4, Paschim Vihar, Rohtak Road, New Delhi-63

Email : bijit@bvicam.ac.in, Website : http://www.bvicam.ac.in

Volume 2, Number 2

July – December, 2010

BVICAM's International Journal of Information Technology (BIJIT) is a bi-annual publication of Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), A-4, Paschim Vihar, Rohtak Road, New Delhi – 110063.

ISSN 0973 – 5658

Address for Correspondence:

Prof. M. N. Hoda
Chief Editor – BIJIT
Director, Bharati Vidyapeeth's
Institute of Computer Applications and Management,
A-4, Paschim Vihar, Rohtak Road, New Delhi – 110063 (INDIA).
Tel.: 91 – 11 – 25275055 Fax: 91 – 11 – 25255056 E-Mail: bijit@bvicam.ac.in
Visit us at www.bvicam.ac.in

Published and printed by Prof. M. N. Hoda, Chief Editor – BIJIT and Director, Bharati Vidyapeeth's Institute of Computer Applications and Management, A-4, Paschim Vihar, New Delhi – 63 (INDIA).
Tel.: 91 – 11 – 25275055, Fax: 91 – 11 – 25255056 E-Mail: bijit@bvicam.ac.in
Visit us at www.bvicam.ac.in

BVICAM's
International Journal of Information Technology (BIJIT)

BIJIT is a bi-annual publication of
Bharati Vidyapeeth's
Institute of Computer Applications and Management
A-4, Paschim Vihar, Rohtak Road, New Delhi – 110063 (INDIA)
Tel.: 91 – 11 – 25275055 Fax: 91 – 11 – 25255056 E-Mail: bijit@bvicam.ac.in
Visit us at www.bvicam.ac.in

Editorial

It is a matter of both honor and pleasure for us to put forth the fourth issue of BIJIT; the BVICAM's International Journal of Information Technology. This issue of the journal presents a compilation of ten papers that span a broad variety of research topics in various emerging areas of Information Technology and Computer Science. Some application oriented papers, having novelty in application, have also been included in this issue, hoping that usage of these would enrich the knowledge base and facilitate the overall economic growth. This issue shows our commitment in realizing our vision "*to achieve a standard comparable to the best in the field and finally become a symbol of quality"*.

As a matter of policy of the Journal, all the manuscripts received and considered for the Journal by the editorial board are double blind peer reviewed independently by at-least two referees. Our panel of expert referees posses a sound academic background and have a rich publication record in various prestigious journals representing Universities, Research Laboratories and other institutions of repute, which, we intend to further augment from time to time. Finalizing the constitution of the panel of referees, for double blind peer review(s) of the considered manuscripts, was a painstaking process, but it helped us to ensure that the best of the considered manuscripts are showcased and that too after undergoing multiple cycles of review, as required.

The ten papers that were finally published were chosen out of more than ninety papers that we received from all over the world for this issue. We understand that the confirmation of final acceptance, to the authors / contributors, is delayed, but we also hope that you concur with us in the fact that quality review is a time taking process and is further delayed if the reviewers are senior researchers in their respective fields and hence, are hard pressed for time.

We wish to express our sincere gratitude to our panel of experts in steering the considered manuscripts through multiple cycles of review and bringing out the best from the contributing authors. We thank our esteemed authors for having shown confidence in BIJIT and considering it a platform to showcase and share their original research work. We would also wish to thank the authors whose papers were not published in this issue of the Journal, probably because of the minor shortcomings. However, we would like to encourage them to actively contribute for the forthcoming issues.

The undertaken Quality Assurance Process involved a series of well defined activities that, we hope, went a long way in ensuring the quality of the publication. Still, there is always a scope for improvement, and so we request the contributors and readers to kindly mail us their criticism, suggestions and feedback at bijit@bvicam.ac.in and help us in further enhancing the quality of forthcoming issues.

Editors

C O N T E N T S

A Comparative Study of Software Requirements Tools for Secure Software Development

Mohammad Ubaidullah Bokhari[1] and **Shams Tabrez Siddiqui**[2]

Abstract - Requirement is the foundation of the entire software development life cycle. With proper requirement management a project can deliver the right solution on time and within budget. Requirement elicitation, requirement specification, and requirement validation are important to assure the quality of requirement documentations. All these three activities can be better analyzed by the software requirement tools. There are a number of software requirement tools available both commercially and freely downloadable, which provide a variety and quality of software requirement documentation. In addition, as the vulnerabilities of software increases, system needs an additional requirement for the security aspects which protect the software from vulnerabilities and makes software more reliable. This paper provides a comparative study of requirement tools showing trends in the use of methodology for gathering, analyzing, specifying and validating the software requirements and the result presented in the tables will help the developer to develop an appropriate requirement tool.

Index Terms -Software Security, Software Security Requirement, Requirements Tools, Ontology and Glossary, Software Requirements Specification

1. INTRODUCTION

The history of requirement engineering is not very outdated [2]. In earlier days the requirement phase was not taken seriously which caused many problems for software industry in later phases. Recently the importance of the requirement engineering has been recognized and a lot of research has commenced to generate quality requirements. The process of requirement generation consists of various activities, which includes requirement elicitation which captures the requirement by means of development teams, extending the requirement specification, and finally validates each requirement specification to corresponding user's needs. The requirement engineering is an iterative and co-operative process with an objective to analyze the problem, to document the results in a variety of formats and evaluate precision of the results produced [1]. The specification of requirement should be: complete, correct, consistent, unambiguous, verifiable and traceable.

[1]*Chairman, Department of Computer Science, Aligarh Muslim University, Aligarh*
[2]*Research Scholar, Department of Computer Science, Aligarh Muslim University, Aligarh.*
E-mail: [1]mubokhari2004@yahoo.co.in, mubokhari@rediffmail.com, [2]ksamtab@rediffmail.com and [2]kk_siddiqui@yahoomail.com

The non functional requirements, that are separate from procedural requirements includes : maintainability, portability, reusability, reliability, security and others does neither have any exact specification nor are there any metrics for specifying objectives of requirements [2]. In addition the functionality and its associated functional requirement widely varies between applications, especially between different application domains [3]. However, the same cannot be illustrated in the case of non functional requirements. The security criteria (authentication, privacy, authorization, integrity etc.) of some applications exhibit to less variation.

The system in our dictionary is concerned with an entity that interacts with the environment (hardware, software, human, and physical world with its natural phenomena). Its fundamental characteristics are computation and communication which may be characterized by fundamental properties like: performance, behavior, dependability, and security. Performance means up to what extent the system satisfies the user needs. Behavior includes what the system does to implement its function and is described by a sequence of states. Dependability means to avoid service failures that are more frequent and more severe than is acceptable. It is an integrating concept that encompasses the following attributes [4]:

1. Availability: readiness for correct service.
2. Reliability: continuity of correct service.
3. Safety: absence of catastrophic consequences on the user(s) and the environment.
4. Integrity: absence of improper system alterations.
5. Maintainability: ability to undergo modifications and repairs.

Security is very similar to dependability except additional attribute confidentiality (absence of unauthorized disclosure of information) which has an edge over the dependability attributes. Security comprises attributes of confidentiality, integrity and availability (CIA).

In the software development processes both designers, and requirement engineers play an important role to develop quality software. Many techniques have been proposed. There are specific requirement elicitation techniques, such as interviewing, questionnaire, or storyboarding techniques, for the specification of the requirements, such as scenarios or use case modeling, and for the validation of the elicited requirements, such as prototyping.

The objective of this work is to show the advantages and disadvantages of the current requirements tools, present a palette of requirements engineering techniques which could aid requirement engineer in their work. In addition, the comparison presented should help in the continuous process of improvement of the existing software requirement tools in order to focus more on requirements engineering, and therefore

contribute to improve the quality of the requirement capturing that are built with these methodologies. The present work gives a survey and a comparative study of the current approaches available in the requirement tools that use different methodologies and model to handle requirements engineering. For that reason, we outline the requirements engineering process and an overview of classic requirements engineering techniques in § 2. The brief description includes the most commonly used techniques to capture, define and validate the requirements of a system. In § 3, the main requirement engineering methodologies are described including requirements specification, that in different degree of detail include requirements specification. This section also includes a classification of requirements. In § 4, these approaches are compared from different points of view. Finally § 5 presents some conclusions and suggestions for future.

2. SOFTWARE REQUIREMENT ENGINEERING

Software requirement is defined as a condition or capability that must be met or fulfilled by a system to satisfy a contract, standard, specification, or other formally imposed documents (IEEE standard 610.12-1990). The requirement engineer shall address the following things (IEEE standard):

1. Functionality: What the software supposed to do?
2. Performance: How does the software perform the user needs?
3. Attributes: What are the portability, maintainability, correctness, and security considerations.
4. External Interface: How does the system interact with the environment?
5. Design constraints: Are there any required standards in effect, policies of database, resource limit, operating environments etc.?

Although, there are a number of techniques available to perform the task of requirement engineering, but a standardized process supporting the requirement engineering and guaranteeing the quality of the software requirement is still lacking. The process of requirement engineering consists of mainly three activities which are described as follows:

2.1 Requirement Elicitation

The process of requirement gathering is by asking stakeholders to describe their views. This is a complex procedure because it requires several groups of participants with different backgrounds. The most widely used techniques for requirement elicitation are:

1. **Interview.** Frequently used to understand the problem domain and objectives of the application to be developed. Interview is not easy to perform. It requires an experienced interviewer who needs to have the ability to choose the most appropriate interviewees [5].
2. **Joint Application Development (JAD).** An alternate method of interview in which a group of participants of all stakeholders project i.e. analysts, designers, users, system administrator, and customers are involved [6]. It has several advantages over the interview technique as it saves time.
3. **Brainstorming.** A type of group meeting similar to JAD which consists of collection of non evaluated ideas and information of stakeholders of the projects [7]. Brainstorming is easier as compared to JAD because it requires less work in the group and provides a better overview of the software requirement.
4. **Questionnaire and Checklist.** A technique in which a well prepared question has a limited choice of options and a concrete answer is possible. The main drawback of this technique is that an analyst should have certain knowledge about the problem domain and the application to be built in order to prepare the questionnaire and checklist.
5. **Case Modeling.** A technique was developed to define requirements more than for capturing them [8]. It is used to define actors, use cases and relationship between them.
6. **Scalability** is a method used by designer to provide an option to increase the requirement of an end user of a system if the business expands.

2.2 Requirement Specification

To improve accuracy and relevancy of the software requirement, the most widely used techniques are:

1. **Use Case Modeling** is a technique to define requirement although it is also used in elicitation of requirement. The main disadvantage of this method is that it is an ambiguous technique when defining complex requirements [9, 10].
2. **(TRS) Tradition Requirement Specification** is an ambiguous technique to define requirement in natural language without any kind of rule.
3. **Templates** are used to describe the requirements in natural language but in structured format. Templates are a table whose fields have a predefined structure and are filled by the development team using the user's terminology.
4. **Glossary and Ontology** are used to define the terminology related to the terminology used in the software project. Ontology is the method used to define the relationship of the concepts used in the project.
5. **Prototype** is a method to provide a context within which users are better able to understand the system they want to be built.

2.3 Requirement Validation

To improve accuracy and completeness of the software requirement. The following are the techniques used for requirement validation process:

1. **Audit** checks the results presented in the review documentation and compares it to the available checklist. It provides only a partial review of the information and results.
2. **Walkthrough** consists of reading and correcting the documentation and validates only the good interpretation of the information.
3. **Prototyping** is a technique used to validate the requirement using an existing software requirement tool.

3. SECURITY REQUIREMENT ENGINEERING

Security policy means to protect the software system by capturing secure software requirement of the system. Jan Jurjens [11] suggested some security requirements which are discussed below:

3.1 Fair Exchange

Fair Exchange requirement postulates that the trade performed by e-commerce is fairly treated and prevented by cheating from either side. (e. g. the buyer or supplier should be able to prove the payment is made or goods supplied and to reclaim the money if the payment or goods are not delivered.

3.2 Non-repudiation

Non-repudiation security requirement supports the fair exchange, which means that action cannot be subsequently denied.

3.3 Role-based Access Control (RBAC)

Role-based access control security requirement play an important mechanism for controlling access to protect assets. It keeps permission manageable, with a large or frequently changing user-based software system

.

3.4 Secrecy and Integrity

The two most important security aspects are Secrecy (Confidentiality) and Integrity. Secrecy means the resources can be used only by legitimate party. Integrity of data means that it should be modified only by an authorized person.

3.5 Authenticity

The third main security requirement is authenticity. Authenticity can have two types, *Message authenticity* and *entity authenticity*. Message authenticity means that one can trace the data back to what its original source was, at some point in the past. Entity authenticity means it ensures the party who can identify participants in a protocol, and in particular make sure that the party has actually actively participated in the protocol at the time.

3.6 Freshness

A message can be treated fresh if it has been created during the current execution round of the system under consideration and therefore, cannot be a replay of an older message by the adversary.

3.7 Secure Information Flow

Security level can have different rules. One usually considers two security levels: high and low. High means highly sensitive or highly trusted whereas low means less sensitive or less trusted. Where trusted parts of a system interact with untrusted parts, one has to ensure that there is no exchange of data from trusted parts to untrusted parts. To ensure this no down flow policy, low data may influence high data, but not vise versa. The opposite of the condition no up-flow, enforces that parts of a system not trusted may not directly influence high data. High data may influence low data, but not for the opposite case.

3.8 Guarded Access

One of the principal security requirements is access control, which means that only a trusted user can have an access to a security based system.

4. SOFTWARE REQUIREMENTS TOOLS

The requirement specification obtained after requirement analysis used throughout the software development lifecycle, must be verified because the quality of the requirements is of utmost importance to deliver the right product. A number of software requirement tools which verify the qualities of the software requirements are given below:.

4.1. RequisitePro

The IBM Rational RequisitePro solution is a widely used and familiar Microsoft word tool to ease requirements based on use case model for software development project teams who want to improve the goals, enhance collaborative development, reduce project risk and increase the quality of applications before deployment [12].

Features:

1. The requirement in word documents are dynamically linked to supplementary requirements information stored in a database. They contain live requirements and allow remaining in a familiar Microsoft word environment to modify requirements.
2. From views into the database, it can be prioritizing link requirements and track changes and show requirements that can be affected by upstream and downstream change.
3. Enables detailed attribute customization and filtering to maximize informative value of each requirement
4. Connect requirements to use case model, enabling instantaneous access to use case specification from use-case diagram as well as visibility into requirements information.
5. Performs project-to-project comparisons using exportable XML-based project baselines.
6. Integrates with multiple tools and teams in the IBM Software Development Platform to improve accessibility and communication of requirements.

Disadvantages:

1. Since it connects requirements to use case model only and does not consider a misuse case. There may be some hole of intrusion present and the system may be considered as insecure.
2. Since a checklist can provide a better and tested requirements and RequisitePro does not have a checklist to ensure the criteria of the requirements.

3. Scalability is also an important non-functional requirement of software. RequisitePro has no provision for scalability according to project size.
4. Ontology and Glossary are the best practices to support the software development team throughout the software development life cycle. RequisitePro does not have any online glossary/ontology to define industry terms project references, corporative languages etc.
5. The key to understanding the problem are the process and project management requirements that reliability and maintainability which provide the ability to consider the different perspectives of the various contributors to the system development effort and to capture and relate the entire requirement. These facilities are not available.

4.2 CaseComplete

CaseComplete is a tool developed by Serlio Software to manage, share use cases and requirements based on Microsoft Word, CaseComplete helps to write use cases and requirements faster and easier that have excellent compliance with use case standards for a novice or an expert user whether working on solo system or a part of diverse team [13].

Features:

1. The requirement reports generated in word documents are dynamically linked with other requirements documented and stored in other place.
2. The requirement report is integrated with other phases of software development life cycle.
3. The report is generated in Microsoft Word and HTML formats of individual and complete requirement of the system
4. Generates the test plans, project plans and UML models directly from use case model.
5. Provides an index of glossary items which help to understand the terminology used in the system.
6. Covers the non-functional requirement specification.

Disadvantages:

1. There might be a need to increase the project team size. CaseComplete does not include scalability.
2. A checklist nowadays provides a better, tested requirement and CaseComplete does not contain any checklist. Therefore one cannot say that the gathered requirements have to be testified and have quality.
3. Since it has an export/import feature and can be hyperlinked with other application, an unauthorized user might be send or capture data. This tool is considered as a weak tool by means of security.
4. Since a wizard is considered as an easy method to just guide the requirement engineer to do their specific goal, CaseComplete can not be customized using any GUI or by using any wizard.

4.3 Analyst Pro

Analyst Pro is a tool for requirements management, tracing and analysis developed by Goda Software Inc. With Analyst Pro, requirements can be traced with any lifecycle software model e.g. waterfall, RUP, spiral. It also provides integrated configuration management to simplify the development process. It can be easily installed and deployed to geographically dispersed teams to collaborate on specification, analysis and project management [14].

Features:

1. Requirements Specification and Tracking – AnalystPro quickly establishes multidimensional traceability links with all project artifacts.
2. Scalable from 1 to 250 users.
3. Repository (for Non-Functional Requirements Objects) – Analyst Pro provides a repository for non-functional requirements objects. UML and other models created by external tools can be saved to the repository for sharing, collaboration, and configuration management, and for linking them to requirements and specifications.
4. Configuration Management – Analyst Pro simplifies the development process by providing integrated configuration management for project artifacts. Analyst Pro allows to baseline and lock project artifacts.
5. Other features include: Reusability of project settings and specification templates using project templates, control of access by creating user groups with different privileges; ability to assign a requirement or other task to team members and review their progress; built-in diagramming editors for creating project diagrams; easy generation of system documentation and change history reports, baseline comparison, traceability reports and status reports etc.

Disadvantages:

1. As it has an export/import facility, it can be interfaced with other applications. There might be a chance that the data may be accessed by other user.
2. As it is concerned with use case model requirements only and does not consider a misuse case, there are some holes of intrusion and system may be considered insecure.
3. The glossaries are the best practices and support the software development team throughout the software development life cycle. AnalystPro does not have any online glossary to define any industry term, project references, corporative languages etc.
4. It does not have any checklist to verify the criteria of requirements and a checklist is always facilitates to deliver quality and tested requirements.
5. Models and simulation are key components to understand all the relevant issues, early identification of risk areas and finding out alternate solutions produce quality system at lower cost. These facilities are not available with this tool.

4.4 Optimal Trace

The Optimal Trace developed by SteelTrace products provides a pragmatic approach for organizations to quickly and easily capture business and system requirements with a 40% per project ROI with little training or deployment expenditure necessary. Unlike traditional RM tools, Optimal Trace takes a

more structured view of requirements breaking them into Functional (in the form of a use case like storyboard structure of main flow, alternative flows etc.) and Non-functional requirements (qualities and constraints). Optimal Trace automatically generates graphical flows directly form text and maintains text and graphics in lockstep. Optimal Trace Professional is a single user version while Optimal Trace Enterprise is a multi-user variant [15].

Features:

1. Optimal Trace offers native integrations from Optimal Trace into UML modeling tools Rational Rose and Borland Together Solo and Control Center. The integrations are bi-directional with UML Use Case and Activity diagrams are automatically generated.
2. Optimal Trace Enterprise is designed for teams who are collaborating on requirement gathering and capture by updating and sharing a project.
3. It is tightly integrated with tools from the following leading vendors in the UML/MDA modeling space; Compuware (Optima1J Integration), IBM (Rational Rose Integration) and Borland (Together Integration).
4. Communication is easy with Optimal Trace's automated document generation and a selection of pre-canned templates that are fully customizable to company–specific standards and processes to ensure a high-quality requirement.

Disadvantages:

1. It does not contain any checklists to verify the criteria of requirements. Therefore, the requirements captured by the tools are not considered to be quality requirements as the requirements are not tested.
2. Since the requirement is concerned with use case model only a misuse case model is completely ignored. The requirements are not secured.
3. As it has an interface facility with other applications, there might be a chance that the data may be accessed by other unauthorized users. Therefore, it may be considered as a weak tool with regard to security aspects.
4. There might be a chance to increase the project team size and Optimal Trace has no feature of scalability according to team size which may create problem.
5. The glossaries are the best practices and support the software development team throughout the software development life cycle and it does not have any online glossary to define any industry term, project references, corporative languages etc.

4.5 DOORS

DOORS (Dynamic Object Oriented Requirements System) is an Information Management and Traceability (IMT) tool developed by Telelogic Inc.. Requirements are handled within DOORS as discrete objects. Each requirement can be tagged with an unlimited number of attributes allowing easy selection of subsets of requirements for specialist tasks. DOORS includes an on-line change proposal and review system that lets users submit proposed changes to requirements, including a justification. DOORS offer unlimited links between all objects in a project for full multi-level traceability. Verification matrices can be produced directly or output in any of the supported formats including RTF for MS-Word, Interleaf and Frame Maker. The DOORS Extension Language (DXL) is a high level language that provides access to virtually all DOORS functions for user extensions and customization [16].

Features:

1. A comprehensive support for recording, structuring, managing and analyzing requirement information.
2. User friendly Interface.
3. Import and export facility with other documents.
4. Complete two ways traceability across the development life cycle.
5. Unparallel integration with third party tools like Mercury and Matrixone.
6. Improved security control through the use of passwords, and timeouts which "lock up" DOORS after a specified period of inactivity.
7. Scalability for any size project with any number of users in any location.
8. New templates to make document generation easier have been added to the DOORS template library. New templates include ISO 12207, ISO 6592 and IEEE software standards.

Disadvantages:

1. Ontology and glossary are the best practices and support the software development team throughout the software development life cycle but it does not have any online glossary.
2. Since it has an export/import facility and can be interfaced with other applications, there might be a chance that the confidential data may be accessed by other users.
3. A checklist provides a better quality and tested requirements. However, DOORS does not contain any checklist.

4.6 GMARC (Generic Model Approach to Requirements Capture)

This tool developed by Computer System Architects Ltd. incorporates a fully developed Requirements Engineering Methodology and provides rapid elicitation of requirements using a generic approach to enhance re-usability and encourage standardization across projects [17].

Features:

1. The requirements can be directly elicited from the minds of the expert.
2. Traceability of requirements hierarchically, historically and inter-task as well as inter-document.
3. Identification and correction of subjective requirements.
4. The goals and constraints are separated.
5. Generic approach enhances re-usability and encourages standardization across projects.
6. Ease of modifiability of requirements documents with automatic adjustment of knock-on consequences.
7. Automatically generate data flow diagram models of functional aspects.

8. Ability to verify dynamic viability of system being specified via animation.
9. Automatic interchange of requirements information between models and specifications.
10. Ability to confine text output to any viewpoint for any application aspect for any layer of support at any level of detail or any combination.
11. Generate a powerful documentation structuring and filtering facilities.
12. Standard generic text interface simplifies linking to any other package.
13. User friendly Human Computer Interface.

Disadvantages:

1. The size of the project may increase and GMARC does not have any feature of scalability according to team size which may create a problem.
2. A checklist is nowadays provides a better quality and tested requirements and GMARC does not contain any checklist therefore one can not say that the gathered requirements have quantity and quality.
3. As the requirement is not concerned with use case model and a misuse case model. Therefore, we may say that the requirements are not perfect regards with secured aspects.
4. The glossaries are the best practices and support the software development team throughout the software development life cycle and it does not have any online glossary to define any industry term, project references, corporative languages etc.
5. There might be a chance to increase the project team size and GMARC does not have any feature of scalability according to team size which may create a problem.

4.7 Objective

Objectiver has been developed by Cediti and designed by RE practitioners to enable real requirements engineering. The tool relies on Kaos, a goal driven methodology and enables users to have a global overview on the system and a systematic link between all the models representing the system. Analysts have the possibility to draw diagrams and to define concepts (like goals, requirements, agent, entities, events, relationships, actions,) and relationships over those concepts (like refinement, conflict, operationalisation, responsibility, capability, performance, specialization, causes and so on). Diagrams can be explained with text documents including references to concepts elicited in the diagrams. All these pieces of information can then be put together to generate a requirements document compliant with predefined standards [18].

Features:

1. It builds a requirement model to describe the problem by defining and manipulating the relevant concept including queries.
2. It justifies the requirements by linking them to higher-level goals.
3. Provides a consistent and complete glossary of all the problems related terms.
4. It produces well structured, self-contained, motivated, easily understandable, standard requirements automatics generated documents.
5. It provides highly effective way to communicate about the requirements through multiple views on documents with easy navigation.
6. It ensures traceability from requirements to goals and checks the completeness and consistency of the requirements.

Disadvantages:

1. The size of the project may increase according to need of the stakeholders and Objectiver has no scalability feature which may create problem.
2. It does not have any export/import features to other software tools. Therefore, it may create problem if someone has to capture the requirement written in other tools.
3. It is not base on either use case or misuse case, therefore, from the security point of views it is hard to identify the vulnerability holes and attackers ideas.

4.8 RDT (Requirements Design & Traceability)

RDT is a software requirement, design, and traceability tool is developed by Igatech System Pvt. Ltd. It supports several mechanisms to aid the user in requirements analysis and identification. It can be used to formulate and generate specification before the specification is issued as a contract or request for tender. These include a parser that imports text documents then identifies requirements by key words and structure. The tool provides functionality for deriving, allocating and assigning requirements and acceptance test procedures. Requirements can be traced from top level requirements down to the lowest level requirements. The tool is able to classify/categorize requirements during identification using requirements attributes. It can also be used to show the design and traceability of requirements throughout the development of cycle of the contract. RDT is able to generate documentation directly into MS Word, including requirements and test specifications, requirement allocation matrices, parent-child relationships and design documents [19].

Features:

1. Revision tracking and baseline allocation including proposals for changes.
2. Workgroup access privileges to control user access down to individual records.
3. Comprehensive online context sensitive help.
4. Network accessible for multi user database access-up to 255 concurrent users.
5. Change Proposal Management, which enables a change proposal to be identified, and any data which will be added, changed, or deleted as a result of it being accepted.
6. Revised Import/Export, allowing sections of the database to be exported, including relationships with other requirements, tests and derivations.

7. Check-In Check-Out, enabling the sharing of data between different sites, and the ability to collate this data back to the master database.
8. User Defined Attributes gives users the ability to name their own unique attributes.
9. Document View Editing, providing a word processor style view of document data.
10. Automated requirements capture and syntax parsing directly from existing documents.
11. Improved User Interface. All data viewing windows are now available with multiple instances, enabling concurrent views of different data

Disadvantages:

1. A checklist always provides a quality, better and tested requirements. RDT does not contain any checklist therefore the gathered requirements have not to be quantified and have a better quality.
2. As the requirement is not concerned with use case model and a misuse case model. Therefore, we may say that the requirements are not perfect as concerned with secured aspects.
3. Since it has an export/import facility and be interfaced with other application. There might be a chance that the confidentiality of the data may be access by other user

4.9 RDD-100

RDD-100 is a Requirements Driven Development (RDD) software suite developed by Holagent Corporation. The RDD-100 uses several mechanisms to aid the user in analyzing and identifying requirements. These include a parser tool that can be defined and developed to help the user identify single or compound requirements. RDD captures and trace the requirement using its Element Relationship Attributes (ERA) and categorize them in a specific manner, where each source document, and the text for each requirement, is stored as a separate element. Graphical hierarchies show how individual pieces of data relate to each other and trace back to their sources [20].

Features:

1. RDD-100 provides the user the capability to interactively manipulate and data through a variety of diagrams including Behavior Diagrams, Hierarchical Views, Functional Flow Diagrams, N2 charts, IDEF0 and Data Flow Diagrams.
2. The report writers available in RDD-100 provide the users to manually create and identify requirements through several types of views.
3. Access Control to the data stored within the system design database can be managed within RDD-100 and can be determined by the rules of the user's process.
4. Data stored in RDD-100 can be shared with tools such as UML, hardware tools, scheduling tools, word processing tools, project management tools etc.
5. RDD-100 has online documentation that includes a user's guide and on-line help.
6. **Disadvantages:**
7. The size of the project may be increase and RDD-100, has not any feature of scalability according to team size which may create problem.
8. A checklist ensures the quality of requirements. RDD_100 does not have any provision of checklist therefore one can not say that the gathered requirements have to be tested.
9. As the requirement is not concerned with use case model and a misuse case model. Therefore, we may say that the requirements are not perfect as concerned with secured aspects.
10. As it has an interface facility with other application. There might be a chance that the data may be access by other unauthorized user. Therefore, it may be considered as a weak tool as concerned with the security aspects.

4.10 Requirements Traceability Management (RTM)

RTM developed by Serena Software Inc. supports multiple users working on the same requirements at the same time by implementing locking control on a requirement-by-requirement basis. Serena RTM is the only tool that supports the critical capabilities, at the object level on UNIX and PC platform using a standard database. RTM's toolset supports the ability to capture graphical information as traceable requirements objects. A class definition tool is included that allows the user to model any type of hierarchical project data (requirement document, hierarchies, system element structure and WBS). Once the hierarchy is defined generic relationships can also be established to allow cross-reference link information to be established between any active data item. Serena RTM is the only Oracle-based tool designed to manage all of the data for the development. It is also called as Engineering Information Management (EIM) tool, or Development Data Management (DDM) Tool, RTM allows you to organize and manage Critical Development-related data [21].

Features:

1. RTM has ability to intuitively organize and manage the information such as requirements, design, test, schedules changes, defects etc.
2. RTM provides online collaboration by all stakeholders, regardless of location.
3. Ability to remotely edit an MSWord document, which allows user to work on the documents offline.
4. Visibility into the state of each phase of development
5. RTM manages change at all levels of development through email notification of changes to other users.
6. RTM is a user interface both word and web, that are industry standards and commonly used in everywhere.
7. RTM is build on Oracle and therefore it offers Oracle advantages such as role base access control, guarded access, authenticity etc.

Disadvantages:

1. The size of the project may be increase and RTM, has not any feature of scalability according to team size, which may create problem.
2. A checklist always provides a quality, better and tested requirements. RTM does not contain any checklist

therefore the gathered requirements have not to be quantified and have a better quality.
3. Since it has an interface facility with other application. There might be a chance that the confidentiality of the data may be access by other user.
4. The Glossary are the best practices and support the software development team throughout the software development life cycle and it does not have any online glossary to define any industry term, project references, corporative languages etc.
5. It does not base on either use case or misuse case, therefore, from the security point of views it is hard to identify the vulnerability holes and attackers ideas

4.11 Reqtify

Reqtify is a requirement-monitoring tool developed by TNI-Software. It is the most effective solution for project teams to capture requirements from any source and easy to use for traceability and impact analysis, enabling quality development in both hardware and software projects [22].

Features:
1. Detection of requirement changes.
2. Graphical view: zoom, moves and resizing of documents.
3. Capture of requirements attributes, references, links, etc. at any level (High-level, Low-level)
4. Reports Generation & Customization capabilities
5. Interface with other tools like Processing tools, requirement tools, UML tools, verification tools etc.
6. Filter creation for more accurate analysis.

Disadvantages:
1. Glossary and Ontology are the best practices and support the software development team throughout the software development life cycle and it does not have any online glossary to define any industry term, project references, corporative languages etc.
2. It has the provision of interface with other software; therefore, the data of the software requirement can be accessed by some malicious user. Thus there is a chance of information disclosure.
3. The size of the project may be increase and Reqtify has not any feature of scalability according to team size which may create problem
4. Since a checklist can provide a better and tested requirements and Rectify does not have a checklist to ensure the criteria of the requirements.

4.12 IRqA

IRqA is not a specific requirement-engineering tool, but also it focused on information exploitation, which provides support to the entire requirement engineering cycle [28].

Features:
1. Requirement can be captured by manual and automatic from MS Word documents.
2. Graphical representation of concept models: class diagram (UML) and ER diagrams.
3. Classification criteria defined by the user, specification is being consistently checked.
4. Validation of requirements implementation in service.
5. Multiple specifications in domain and/or blocks.
6. Full end-to-end traceability from user requirements to the detailed design, implementation and test.
7. Integration with Object Oriented design tools with XML/UML export/import facility.
8. Reports defined by user in order to create documents based on industrial standards or existing templates in each organization.

Disadvantages:
1. The size of the project may be increase and IRqA has not any feature of scalability according to team size.
2. Glossary help and support the software development team throughout the software development life cycle and it does not have any online glossary to define any industry term, project references, corporative languages etc.
3. It has the provision of interface with other software; therefore, the data of the software requirement can be accessed by some malicious user. Thus there is a chance of information disclosure.

4.13 TcSE (Teamcenter Systems Engineering)

TcSE is a requirements management tool developed by UGS Inc. includes both Requirements Management and System Architect licenses. The Systems Architect solution gives the people responsible for planning the integrated mechanical, electrical and software product design a powerful tool to create and communicate requirements. The Requirements Management solution delivers product requirements to all of the entitled users who participate in your product lifecycle. Teamcenter brings your customers directly into your extended enterprise and reflects their concerns from the start of your product lifecycle to its conclusion [23].

Features:
1. An intuitive user interface that looks and acts a lot like Windows Explorer and Outlook.
2. Microsoft Office integrations allow users to interact with requirements information directly from their desktop
3. Document importing and exporting for requirements capture and generation.
4. Multi-user group environment that enables users to view and work on requirement concurrently in a controlled way.
5. Linking and tracing mechanisms like a summary requirement to a specific paragraph in the source document from which is was extracted
6. Security protections allow administrators to control user access, information access, and modification privileges.

Disadvantages:
1. Ontology and Glossary are the best practices and support the software development team throughout the software development life cycle and it does not have any online glossary to define any development terminology, project references, corporative languages etc.

2. The size of the project may be increase and TcSEe, has not any feature of scalability according to team size, which may create problem.
3. It has the provision of interface with other software; therefore, the data of the software requirement can be accessed by some malicious user. Thus there is a chance of information disclosure.
4. A user always wants the tools which are easy to use. A graphical representation always considered a better option for any requirement tools. TcSE does not has such feature

4.14 Code Assure

Code Assure Solo is the industry's first enterprise-class application security tool designed specifically to meet the needs and cost requirements of individual developers, project managers and security architects. It is the only tool that provides a comprehensive, process-oriented solution for identifying, assessing and remediation of software vulnerabilities throughout the development lifecycle [25].

Though CodeAssure Solo is purpose-built to meet the needs of individuals, it offers the same comprehensive security analysis capabilities that support entire development and security teams. With CodeAssure Solo, anyone – regardless of company size or budget – can benefit from the industry's most accurate analysis tool.

Features:

1. CodeAssure identifies and remediate the software vulnerabilities early in SDLC.
2. Deploy in an Eclipse environment and on existing projects
3. Achieve high acceptance rate for code without security flaws
4. Integrates into existing processes and systems.
5. Reduces the time and costs associated with analysis, remediation, and deployment of secure application.
6. Stakeholders are continuously informed of the current status of application security and policy violation.

Disadvantages:

1. A checklist ensures the quality of requirements. CodeAssure does not have any provision of checklist therefore one can not say that the gathered requirements have to be tested.
2. Ontology and Glossary are the best practices and support the software development team throughout the software development life cycle and it does not have any online glossary to define any development terminology, project references, corporative languages etc.
3. The size of the project may be increase and CodeAssure, has not any feature of scalability according to team size which may create problem.
4. A graphical user interface is very handy to use for a novice requirements engineer. CodeAssure has not such feature.

5. COMPARATIVE STUDY

The comparative study of the above requirements tools are based on two factors. The first one is analysis of the requirements simply gathered for the functional requirement, and second one is analysis of the requirements gathered for the security point of view as shown in the Table-1 and Table-2. The first one is said to be product oriented where as the second one may be regarded as security oriented.

All above requirement tools are compared with the parameters discussed in Software Requirement Engineering and Security Requirement Engineering sections earlier. In both section there are eight parameters and each parameter have been assigned (100/8) 12.5 points. The right ticks (√) show that the tools fulfill the parameters in which it exists. The total number of (√) are counted and multiplied by 12.5 and its total value is presented in Table-3. The tool having maximum points is considered as best one.

5.1 Product Oriented

Product oriented is the approach to describe the steps to be followed in order to perform the capture the requirements specification, elicitation and validation.

4.3 Security Oriented

Security oriented describes the techniques to be applied during the process of requirement gathering in order to satisfy the user non functional needs with respect to security aspects

6. POSSIBLE SHORTCOMINGS

There are possible shortcomings to our study. First, we want to stress that we do not have any right to compare the qualities of software products. Therefore, we cannot know if certain areas have been left out because of deliberate decision or lack of information or knowledge. As a consequence we do not judge the requirements tool as good or bad, but rather analyze the functionality of these tools. Second, the research work is based on the software freely downloaded or the documents available in the websites. The trial version of the software has some restricted privileges; therefore, it is hard to judge the quality of that tool.

7.0 CONCLUSION

In this paper we have presented the state of the art of requirements engineering both functional and non security and discuss their usability according to process and product. According to Table-3, we can conclude that DOORS are the one of the best requ

irement tool satisfying the both functional and non-functional requirements, whereas for the security point of view CodeAssure is the best among all the tools. We also advise to add checklist and glossary features and make CodeAssure the best security requirements tool.

As a result of our study, we still advise that there are a great potential in the field of the requirement engineering to gather, elicit and validate the requirements with respect to the functional and security aspects. We hope that the result presented in the tables will help developer to develop an appropriate requirement tools to overcome all the drawbacks as we mentioned in this

particular work and which will be beneficial for the functional and security point of views.

REFERENCES

[1]. Lowe D. Hali, W Hypermedia and the Web application Engineering Approach, John Wiley & Sons. 1999.

[2]. Adam Sachitano, Richard O. Chapman, "Security in Software Architecture: Case Study", Proceedings of 2004 IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY 10-11 June, 2004.

[3]. Donald Firesmith: "Specifying Reusable Security Requirements", *Journal of Object Technology*, vol. 3, no. 1, January-February 2004.

[4]. Algirdas Avi_zienis, Fellow, IEEE, Jean-Claude Laprie, Brian Randell, and Carl Landwehr, "Basic Concept and Taxonomy of Dependable and Secure Computing", IEEE Transactions on Dependable and Secure Computing, Vol. 1, No. 1, January-March 2004.

[5]. Pan, D., Zhu, D., Johnson, K. Requirements Engineering Techniques. Internal Report. Department of Computer Science. University of Calgary. Canada., 2001

[6]. Livesey D., Guinane T, "Developing Object-Oriented Software, An Experience-Based Approach (IBM's OOTC)", Prentice Hall, 1997.

[7]. Raghavan, S., Zelesnik, Ford, G. Lectures Notes of Requirements Elicitation. Educational Materials CMU/SEI-94-EM-10., 1994.

[8]. Jacobson, I. "Modeling with Use Cases: Formalizing Use Case Modelling". Journal of Object-Oriented Programming, 1995.

[9]. Insfrán, E., Pastor, O., Wieringa, R "Requirements Engineering-Based Conceptual Modeling". Requirements Engineering Journal, Vol 7 (1)., 2002.

[10]. Vilain, P., Schwabe, D., Sieckenius, C. "A diagrammatic Tool for Representing User Interaction in UML". Lecture Notes in Computer Science. Proc. UML'2000. York, England., 2000.

[11]. Jan Jurjens, "Secure Systems Development with UML", Springer-Verlog, 2005.

[12]. www-306.ibm.com/software/awdtools/reqpro.

[13]. http://www.serlio.com/casecomplete

[14]. http://www.analysttool.com

[15]. www.compuware.com/products/optimaltrace

[16]. http://www.telelogic.com/corp/products/doors

[17]. http://myweb.tiscali.co.uk/gmarc/general%20features.htm

[18]. http://www.objectiver.com

[19]. http://www.igatech.com/rdt

[20]. http://www.holagent.com

[21]. http://www.serena.com/Products/rtm/home.asp

[22]. http://users.reqtify.tni-software.com/?p=home

[23]. www.ugs.com/products/teamcentre

[24]. http://sesa.dit.unitn.it/sttool/

[25]. http://www.securesoftware.com/products

Tools	Product	Security
RequisitePro	62.5	25.0
Case Complete	72.5	25.0
Analyst Pro	50.0	37.5
Optimal Trace	62.5	12.5
DOORS	72.5	62.5
GMARC	50.0	12.5
Objectiver	62.5	12.5
RDT	62.5	12.5
RDD-100	50.0	25.0
RTM	37.5	50.0
Reqtify	50.0	25.0
TcSE	37.5	62.5
Code Assure	25.0	87.5
IRqA	50.0	12.5

Table 3: Details of Product and Security Technique

Application of Fuzzy Relations in Convalescing Link Structure

Raj Gaurang Tiwari[1], Mohd. Husain[2] and **Raees Ahmad Khan[3]**

Abstract - The link structure of website allows us to spread the link power of home page to the individual pages of the site. In this paper we define the content and web pages as two important and prominent factors in website navigation and restate the enhancement in the website navigation as making some useful changes in the link structure of the website based on the aforementioned factors. Then we suggest a new method for proposing the changes using fuzzy approach to optimize the website architecture. Applying the proposed method to a real case of Azad Institute of Engineering & Technology (AIET) Lucknow website, we discuss the results of the novel approach at the final section.

Index Terms - Web content, Web navigation, Website system, Web usage mining, Website Link Structure

1. INTRODUCTION

In current scenario website plays a significant role in success of an e-business and giving more intelligence to e-commerce sites is popularly recognized as one of the effective strategies that increases customer satisfaction because they react intelligently and can give a personalized response to each customer [3]. It is, then, no small wonder that most companies feel that they need at least some level of web presence today.

Moreover, web pages are hard to design in a systematic way. Web architecture, routine path, and page contents are often intuitively decided. These are some of the reasons that lead users to errors or inconvenient access when browsing a website, thereby bringing a negative impression to individuals or companies. In order to deal with this problem, identification of user intention and behavior becomes necessary and the concept of website usability is defined as "How well and how easily a user, without formal training, can interact with a website?" Better structure of web links takes visitors easier and sooner to their targets in a website and also it enhances website navigation. Many previous researches applied web mining techniques to analyze web logs to evaluate website link structure and usability. While some researchers analyze past user access patterns to discover common user access behavior in order to improve website structure, others may employ it to redesign websites or to discover user access patterns and to develop adaptive websites. To analyze and capture visitors' opinions about website usability, different methods and metrics are proposed.

[1,2]*Azad Institute of Engineering & Technology, Lucknow (UP), INDIA*
[3]*Babasaheb Bhimrao Ambedkar University, Lucknow (UP), INDIA*
E-mail: [1]rajgaurang@gmail.com, [2]mohd.husain90@gmail.com and [3]khanraees@yahoo.com

While in some cases, web designs are measured according to their formatting, composition and different web topic categorization and also some scales focus on customer evaluations and different customer groups, many studies use operation research methods to evaluate website usability and enjoy OR potentials in formulating website link structure as mathematic relations. Also, the graph theory has recently attracted many attentions in website usability evaluation. On the other hand, recent developments in data and web mining technology can help enterprises determine problems in communication, and improve their tactics in response to customers. Some of the useful knowledge captured from customers, can be the information regarding the website structure and design, these groups of information from clients and their usage behavior are described as web usage mining which is a sub set of web mining literature. This kind of information about the website layout can help the designers to find the clients preferences and draw backs of his/her design based up on and so to improve the website structure in order to simplify the navigation for the clients. This paper presents the website as a link structure between some nodes of information which are the web pages and illustrates them using the notion of directed graphs. By using such a description about the website, improving the navigation in website can be paraphrased as making some useful changes in the link structure of the website in order to enhance the navigation possibilities for clients.

Web mining taxonomy [2] can be presented as:

1. Web Content Mining (WCM): is consisted of mining the multimedia documents, involving text, hypertext, images, audio and video information. This deals with the extraction of concept hierarchies/relations from the web and their automatic categorization.
2. Web Structure Mining (WSM): is composed of mining the inter-document links, provided as a graph of links in a site or between sites. For example, in Google a page is important if important pages point to it. WSM pertains to mining the structure of hyperlinks within the web itself.

Web Usage Mining (WUM): is made of mining the data generated by the users' interactions with the web. This includes trend analysis, and web access association/sequential pattern analysis. While the previous techniques utilize the real or primary data on the web, usage mining mines secondary data generated by the users' interaction with the web. This category of web mining is the most recent method in personalizing web page.

During the next section we will state the research problem precisely. The third section goes to the characteristics of the utilized fuzzy method and its relative concepts. The fourth part of the paper will discuss a real case of website of Azad Institute of Engineering & Technology (AIET), Lucknow in order to

illustrate the functionality of the proposed fuzzy method and finally, the last section brings up some conclusions on the novel contribution of the paper.

2. PROBLEM STATEMENT

Website structure plays an integral role in the success of the firms' marketing strategies and is exactly the problem we are going to deal with through this paper discussing a case study of website of Azad Institute of Engineering & Technology (AIET), Lucknow. "How can the website navigation be enhanced mostly using the data gathered from visitors?" states the research question in this paper. As the visitors are the best ones who can judge the navigation process of a website, we have applied visitors' surveys as the instruments for gathering data about the navigation status of the AIET website. What mostly complicate the research problem are the factors to survey the visitors on along with the necessary methodology for analyzing the data. Finding appropriate solutions for these complexities about the AIET website shapes the main and novel contribution of this paper.

3. WEB CONTENT, WEB PAGES AND THEIR PROPOSED FUZZY RELATIONS

A. Web Contents and Web Pages

Each web site is designed in order to present some highlighted content through its web pages. The website content topics are the ingredients which shape the discussed subjects through its web pages [14] and upon which the designers decide about the number of web pages and the link structure which shape the web site architecture. So, the strength of relations between the website content topics and also the intensity of dependency between each web page and each content topic are the main building blocks of the website architecture [1]. It can be paraphrased that each existing link between two distinct web pages is the result of two web pages covering the same content or two web pages covering different content topics which are largely related and dependent to each other. Based on such reasoning, the link structure of any website can be enhanced based on the existing relations between the content topics presented through the website and also the intensity of the relations between each content topic and each web page. This paper proposes a system which can enhance the website architecture based on two types of mentioned relations. Dealing with this problem, understanding the visitor intentions and preferences becomes highly necessary. Web users have different purposes and intentions when browsing a website. By recognizing the visitor preferences, the system can help designers understand visitors' usage behavior and can suggest ways to build more effective websites.

Each designer can extract the main content topics which have been covered through the web site. The intensity and strength of aforementioned relations in a website based on the user opinion can guide the designers in how to construct the link structure inside a web site system and can be used as a criterion in order to classify the web pages in to categories of: authoritative and hub web pages. While authoritative web pages usually contain the most reliable and detailed contents about a specific topic, hub documents contain many links to authoritative documents without going in to details of any special topic[14], presenting the agenda of web site contents, the home page can be a good example of hub web pages. On the other hand the final web pages which present intended information and services for each content, can be categorized as authoritative pages. The authoritative web pages usually have at least one strong relation to the content topics while the hub pages usually don't have any special strong relation with any content.

B. Proposed Fuzzy Relations between the Content Topics and the Web Pages

Presenting mathematically, the strength of discussed relations between the content topics and similarly the intensity of relations between the content topics and the web pages are not instinctively crisp. That's why we have used fuzzy theory in order to model such relations mathematically. Any two content topics can have different strength of relation which can be expressed linguistically as "weak", "medium" or "strong". On the other hand the intensity of relation between a content topic and a web page follows the same rule and can not be expressed in terms of crisp values, this intensity can be described similarly through the linguistic values of "weak", "medium" or "strong", too. This brings up the notion of membership value for each relation, which determines the existence intensity of each relation. The fuzzy relations can be illustrated as below:

$$\begin{cases} C_i \xrightarrow{\mu_{ij}} C_j \\ W_k \xrightarrow{\mu'_{ij}} C_j \end{cases} (i \neq j)$$

Where C_i stands for the i^{th} content and Wk represents the k^{th} web page in the website structure, also μ_{ij} shows the membership degree for the relation between the content topics and presents the degree of dependency between them. Similarly the μ'_{lj} represents the membership value of the relation between the web page W_k and the content C_i , which is the degree of dependency between the content topic and the web page. The higher the membership degree, the more the web page covers the content through its subjects.

4. EXPERIMENTAL EVALUATION

A. Experimental Data

For the experimental evaluation we considered the website of Azad Institute of Engineering and Technology (AIET), Lucknow. One of the main responsibilities of AIET is imparting quality education and training to the students in the chosen field of study, to enhance the knowledge, infuse confidence and sharpen their skills preparing to compete in today's globalization age and changing scenario. Having the hits rate of more than 100-150 person/day, AIET web site is playing the integral role of a portal for engineering and management students. Thus, large number of new web pages are designed and added to/substituted by the previous web pages in the web site structure on a monthly basis aiming to

simplify the users' access to the intended information as much as possible. Having such a gigantic size, providing an effective way of navigation for such a link structure is a real woe for the team of web designers these days. During previous months, the website of AIET (http://www.aiet.ac.in) has been frequently changed to have better face to users. During this period of time, different homepages were developed. The homepage and link structure were dramatically changed again and again and imposed a considerable amount of cost on the department monetarily and time wise. But after changing the structure of the website, there was no "the best design" and so they just agreed on the current layout. In order to present a real example for the proposed fuzzy inference system, we consider the link structure of the AIET website which covers almost 5 content topics through 16 web pages. Figure-1 illustrates the link structure as a directed graph. The web page number 1 on top of the graph illustrates the current homepage.

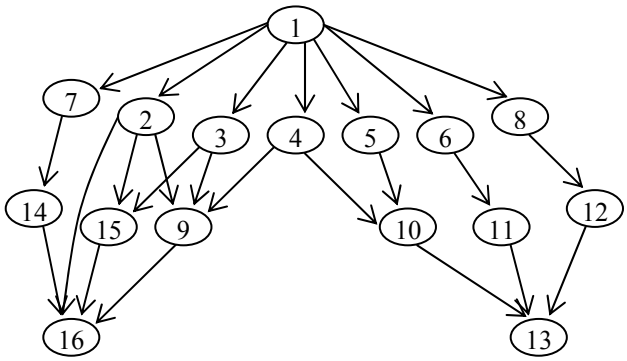


Figure1: The directed graph of initial AIET website structure

In order to reach a performance measure for the navigation process in the AIET website, browser cookies were used to record the needed data. Since the content of cookies depends on the programmer, we wrote a cookie program to obtain the necessary information from visitors such as user IP, stay time at each page, browsing sequence, and so on. Then applying the time threshold of 10 seconds, which was the least time of stay for each user in any target page, we could distinguish the passing (hub) web pages from the target ones. This helped us measuring the average navigation time for a user since its entrance to the website till he/she reaches his/her first target page. This duration was 29 seconds on average before applying the fuzzy method to the website. Measuring this KPI after applying the new link structure reached by the use of fuzzy method would help us to understand the degree of improvement in the website navigation. Two types of questionnaires needed to be applied in order to gather the necessary data about the AIET website. The first questionnaire which asked the visitor to comment on the strength of relation between each couple of content topics was presented to the user at his/her entrance to the web site. On the other hand, the second questionnaire which sought the visitor comments on the intensity of relation between each web page with each single content topic was presented to him/her during his/her visit from related web page. Through this process two types of questionnaires were filled by the visitors during his/her visit from the web site.

The visitors' qualitative answers were quantified using some defined fuzzy linguistic rules, so as to enable us to run the inferring process over the collected data. Figure 2 illustrates these fuzzy linguistic rules.

Running two visitors' surveys for 8 days, the surveys were responded by 60 visitors and based on the results we could reach to two different matrices of content topics relations and also the web pages and the content topics relations, denoting the inputs for the fuzzy minimal inference system [15]. Tables I and II present those matrices along with their membership values having used the linguistic rules (C_k stands for the k^{th} content topic and W_i for the i^{th} web page).

B. Analyzing Effectiveness of Proposed Fuzzy Technique

Using proposed linguistic rules and applying the minimal fuzzy inference engine, we calculated the membership value for each pair of web pages as the degree of intensity for their relation. Table III presents the resulted membership degree for each pair of web pages.

	C1		C2		C3		C4		C5	
C1	S	μ ≥ 6	S	μ ≥ 6	M	3 > μ > 6	W	μ ≤ 3	W	μ ≤ 3
C2	S	μ ≥ 6	S	μ ≥ 6	S	μ ≥ 6	W	μ ≤ 3	W	μ ≤ 3
C3	M	3 > μ > 6	S	μ ≥ 6	S	μ ≥ 6	M	3 > μ > 6	W	μ ≤ 3
C4	W	μ ≤ 3	W	μ ≤ 3	M	3 > μ > 6	S	μ ≥ 6	S	μ ≥ 6
C5	W	μ ≤ 3	W	μ ≤ 3	W	μ ≤ 3	S	μ ≥ 6	S	μ ≥ 6

Table 1: The relations' strength between the content topics with their fuzzy membership values

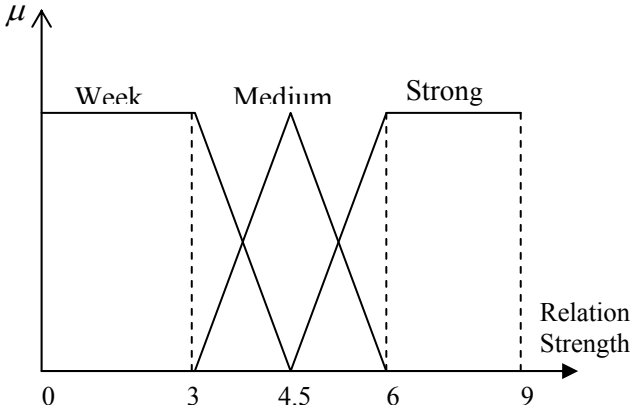


Figure2: Illustration of the linguistic rules as fuzzy variables

Applying the linguistic rules presented before, the content of Table III can be changed to the linguistic variables demonstrated in Table IV.

The directed graph of Fig. 3 illustrates the link structure of AIET website in addition with the strength of its links, having

resulted from the utilization of the proposed fuzzy method.

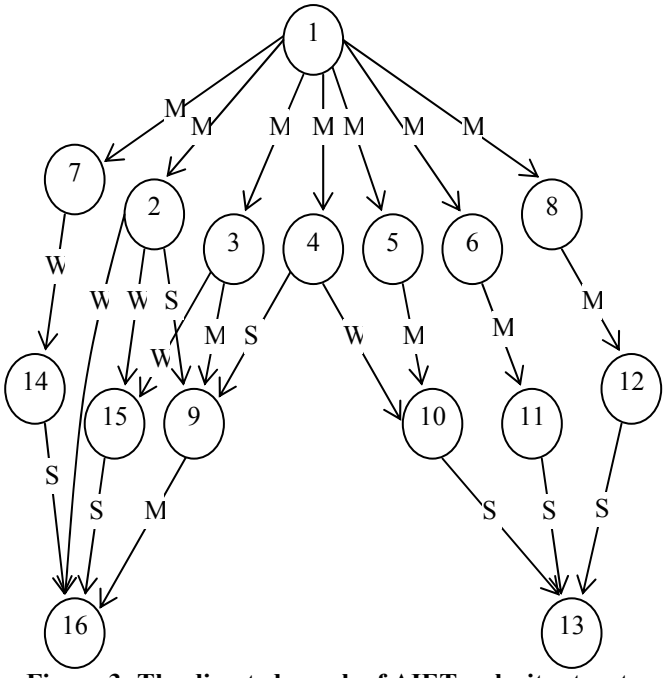


Figure 3: The directed graph of AIET web site structure along with its links' strength

As illustrated in Figure 3, it's obvious that some of the links which were considered in the AIET website structure are so weak that we could omit them from the architecture of the web site. In contrast, as presented in Table IV, there are some important links which can be added to the website link structure in order to better facilitate the navigation process through the web site and make the web site architecture more effective.

In order to observe the efficiency of the proposed procedure we substituted all 5 weak-ranked links in the AIET website structure (Fig. 3) by 5 strong-ranked links from the Table IV which were not included in the structure. After seven days of trial for the new structure, the average navigation time for the visitors decreased to 20 seconds which demonstrates an enhancement of more than 30 percent in AIET website system.

5. CONCLUSIONS

Contents are the building blocks of the web pages in a website system and the degree of relation between pairs of content topics in addition to the intensity of relation between the content topics and each web page provide a sensible basis for deciding about the existence of a link between each pair of web pages. Using such a basis, a fuzzy method, applying minimal inference engine, was proposed to analyze the data gathered through two surveys from website visitors. The surveys collected the visitors' comments on the intensity of relationship and dependency between the pairs of content topics in a website and also between each content topic and each webpage. In order to observe the proposed fuzzy method, a case study of AIET website was analyzed. Through the case study two aforesaid surveys were run and the gathered data were utilized by the proposed fuzzy method, the resulting link structure for the AIET website showed that our proposed method has an improvement of more than 30% in website structure efficacy, decreasing the time of navigation for website visitors from 29 seconds to 20 seconds on average.

	C 1		C 2		C 3		C 4		C 5	
W1	M	3 > μ > 6	M	3 > μ > 6	M	3 > μ > 6	M	3 > μ > 6	M	3 > μ > 6
W2	S	μ ≥ 6	S	μ ≥ 6	W	μ ≤ 3	W	μ ≤ 3	W	μ ≤ 3
W3	S	μ ≥ 6	W	μ ≤ 3	W	μ ≤ 3	W	μ ≤ 3	W	μ ≤ 3
W4	M	3 > μ > 6	S	μ ≥ 6	W	μ ≤ 3	W	μ ≤ 3	W	μ ≤ 3
W5	W	μ ≤ 3	S	μ ≥ 6	M	3 > μ > 6	W	μ ≤ 3	W	μ ≤ 3
W6	W	μ ≤ 3	S	μ ≥ 6	M	3 > μ > 6	W	μ ≤ 3	W	μ ≤ 3
W7	W	μ ≤ 3	M	3 > μ > 6	S	μ ≥ 6	W	μ ≤ 3	W	μ ≤ 3
W8	W	μ ≤ 3	M	3 > μ > 6	S	μ ≥ 6	W	μ ≤ 3	W	μ ≤ 3
W9	W	μ ≤ 3	W	μ ≤ 3	S	μ ≥ 6	W	μ ≤ 3	W	μ ≤ 3
W10	W	μ ≤ 3	W	μ ≤ 3	W	μ ≤ 3	S	μ ≥ 6	M	3 > μ > 6
W11	W	μ ≤ 3	W	μ ≤ 3	W	μ ≤ 3	S	μ ≥ 6	W	μ ≤ 3
W12	W	μ ≤ 3	W	μ ≤ 3	W	μ ≤ 3	S	μ ≥ 6	M	3 > μ > 6
W13	W	μ ≤ 3	W	μ ≤ 3	W	μ ≤ 3	M	3 > μ > 6	S	μ ≥ 6
W14	W	μ ≤ 3	W	μ ≤ 3	W	μ ≤ 3	W	μ ≤ 3	S	μ ≥ 6
W15	W	μ ≤ 3	W	μ ≤ 3	W	μ ≤ 3	S	μ ≥ 6	S	μ ≥ 6
W16	W	μ ≤ 3	W	μ ≤ 3	W	μ ≤ 3	M	3 > μ > 6	S	μ ≥ 6

Table 2: The relations between the content topics and the web pages with fuzzy membership value

In the majority cases, adding links increases the efficiency and efficacy of the website. However what determines which links to be added or substituted in a website structure can be confusing to the designers. Our proposed fuzzy approach can provide the designers with an appropriate method for ranking the links in a website which can excessively help designers to decide about which links to be omitted and which ones to be added to the website structure in order to enhance the visitor's navigation effectiveness. It is obvious that applying such a fuzzy approach doesn't autonomously enhance the structure of the website, instead it can operate as a decision support system assisting the website designers to classify and rank the different

links in their website architecture which can help them to take better decisions considering the existence and also the number of links in the website composition.

Fig. 4 illustrates the graph of the new structure for AIET site.

REFERENCES

[1]. Tiwari Raj Gaurang, et. al. "Significance of State Cloning Concept in clustering click stream" in the Proceedings of National Conference on Emerging Technologies in Computer Science (ETCS-2007) MIET, Meerut, India, Sep 23, 2007, pp – 227-233.

[2]. Tiwari Raj Gaurang, et. at. "Mining Interesting Knowledge and Pattern Discovery from Weblogs" in National Seminar Held at IIET, Bareilly, August 2007.

[3]. Kim, W., Y.U. Song, and J.S. Hong, Web enabled expert systems using hyperlink-based inference. Expert Systems with Applications, 2004: pp. 1-13.

[4]. E.Rosen, D. and E. Purinton, Website design: Viewing the web as a cognitive landscape. Journal of Business Research, 2004(57): pp. 787.

[5]. Lee, J.-H. and W.-K. Shiu, An adaptive website system to improve efficiency with web mining techniques. Advanced Engineering Informatics, 2004. 18: pp. 129-142.

[6]. Benbunan-Fich, R., Using protocol analysis to evaluate the usability of a commercial web site. Information & Management, 2001(39): pp. 151- 156.

[7]. Saudi, A. and M.H.A. Hijazi. Using similarity measures and association rule for web personalization. in M2USIC. October 2004. Malaysia. pp. 16-19.

[8]. Nakayama, T., H. Kato, and Y. Yamane. Discovering the gap between web site designers' expectations and users' behavior. in The 9th Int'l World Wide Web Conference on Computer Networks. May 2000. Amsterdam, Holland. pp. 811-822.

[9]. Arotaritei, D. and S. Mitra, Web mining: a survey in the fuzzy framework. Fuzzy Sets and Systems, 2004. 148: pp. 5-19.

[10]. Mitra, S. and H.L. Larsen, Special issue on web mining using soft computing. Fuzzy Sets and Systems, 2004. 148: pp. 1-3.

[11]. Vrazalic, L. Website usability in context: an activity theory based usability testing method. in The national conference on Transformational Tools for 21st Century Minds. 2003. pp. 41-47.

[12]. Blackmon, M.H., M. Kitajima, and P.G. Polson. Repairing usability problems identified by the cognitive walkthrough for the web. in SIGCHI conference on Human factors in computing systems. 2003. Florida, USA. pp. 497-504.

[13]. Huang, M.-H., Web performance scale, Information & Management, 2004.

[14]. Kim, K.-J. and S.-B. Cho, Personalized mining of web documents using link structures and fuzzy concept networks. Applied Soft Computing, 2005.

[15]. Gorzalczany, M.B., Computational intelligence systems and applications: neuro-fuzzy and fuzzy neural synergisms. 2002: Springer.

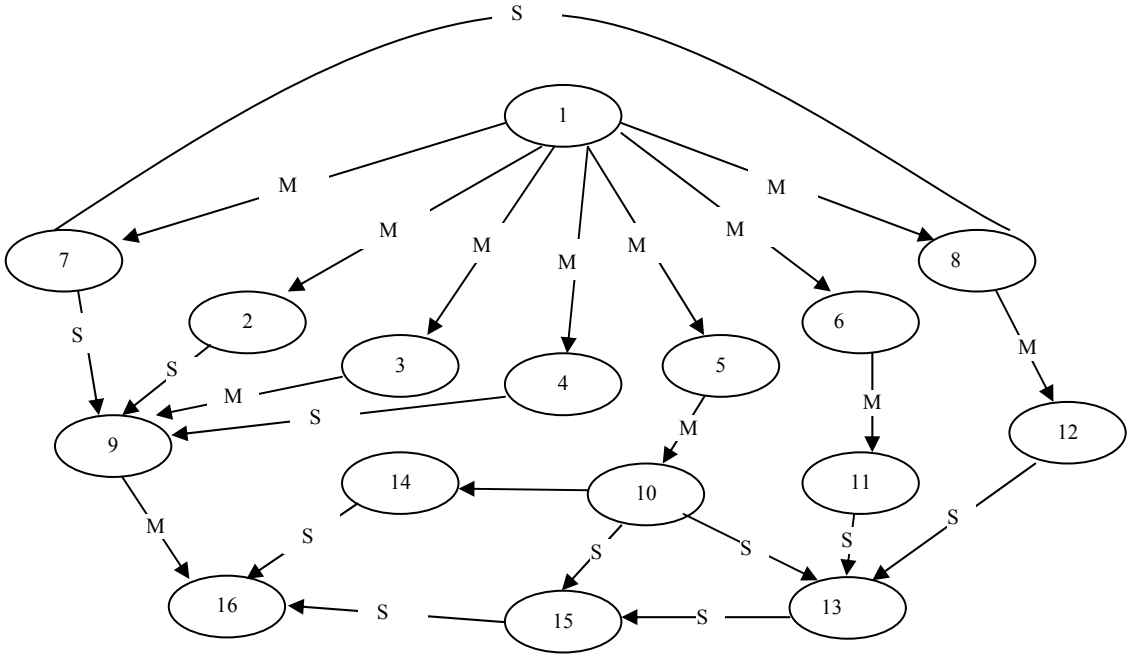


Figure 4: The directed graph of secondary AIET website architecture along with its links' strength

W1	W2	W3	W4	W5	W6	W7	W8	W9	W10	W11	W12	W13	W14	W15	W16

W1		3 > μ > 6	3 > μ > 6	3 > μ > 6	3 > μ > 6	3 > μ > 6	3 > μ > 6	3 > μ > 6	3 > μ > 6	3 > μ > 6	3 > μ > 6	3 > μ > 6	3 > μ > 6	3 > μ > 6	3 > μ > 6	3 > μ > 6
W2			μ ≥ 6	μ ≥ 6	μ ≥ 6	μ ≥ 6	μ≥6	μ≥6	μ≥6	μ ≤ 3	μ ≤ 3	μ ≤ 3	μ ≤ 3	μ ≤ 3	μ ≤ 3	μ ≤ 3
W3				μ ≥ 6	μ ≥ 6	μ ≥ 6	3>μ>6	3>μ>6	3>μ>6	μ ≤ 3	μ ≤ 3	μ ≤ 3	μ ≤ 3	μ ≤ 3	μ ≤ 3	μ ≤ 3
W4					μ ≥ 6	μ ≥ 6	μ ≥ 6	μ ≥ 6	μ ≥ 6	μ ≤ 3	μ ≤ 3	μ ≤ 3	μ ≤ 3	μ ≤ 3	μ ≤ 3	μ ≤ 3
W5						μ ≥ 6	μ≥6	μ ≥ 6	μ ≥ 6	3 > μ > 6	3 > μ > 6	3 > μ > 6	3 > μ > 6	μ ≤ 3	3 > μ > 6	3 > μ > 6
W6							μ≥6	μ ≥ 6	μ ≥ 6	3 > μ > 6	3 > μ > 6	3 > μ > 6	3 > μ > 6	μ ≤ 3	3 > μ > 6	3 > μ > 6
W7								μ ≥ 6	μ ≥ 6	3 > μ > 6	3 > μ > 6	3 > μ > 6	3 > μ > 6	μ ≤ 3	3 > μ > 6	3 > μ > 6
W8									μ ≥ 6	3 > μ > 6	3 > μ > 6	3 > μ > 6	3 > μ > 6	μ ≤ 3	3 > μ > 6	3 > μ > 6
W9										3 > μ > 6	3 > μ > 6	3 > μ > 6	3 > μ > 6	μ ≤ 3	3 > μ > 6	3 > μ > 6
W10											μ ≥ 6	μ ≥ 6	μ ≥ 6	μ ≥ 6	μ ≥ 6	μ ≥ 6
W11												μ ≥ 6	μ ≥ 6	μ ≥ 6	μ ≥ 6	μ ≥ 6
W12													μ ≥ 6	μ ≥ 6	μ ≥ 6	μ ≥ 6
W13														μ ≥ 6	μ ≥ 6	μ ≥ 6
W14															μ ≥ 6	μ ≥ 6
W15																μ≥6
W16																

Table 3: The fuzzy membership values for the relations between web pages

	W1	W2	W3	W4	W5	W6	W7	W8	W9	W10	W11	W12	W13	W14	W15	W16
W1		M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
W2			S	S	S	S	S	S	S	W	W	W	W	W	W	W
W3				S	S	S	M	M	M	W	W	W	W	W	W	W
W4					S	S	S	S	S	W	W	W	W	W	W	W
W5						S	S	S	S	M	M	M	M	W	M	M
W6							S	S	S	M	M	M	M	W	M	M
W7								S	S	M	M	M	M	W	M	M
W8									S	M	M	M	M	W	M	M
W9										M	M	M	M	W	M	M
W10											S	S	S	S	S	S
W11												S	S	S	S	S
W12													S	S	S	S
W13														S	S	S
W14															S	S
W15																S
W16																

Table 4: The strength of relations between web pages

System versus Process Perspectives of Enterprise Resource Planning Implementations

Vikram Tiwari

Abstract - This paper reviews literature concerning implementation of Enterprise Resource Planning (ERP), its successful and unsuccessful cases, and the critical success factors of its implementation, in order to identify gaps in academic thinking and propose future research opportunities. ERP implementation research often takes only a systems-oriented view of the implementation process and not a process-oriented view. This narrow technological perspective of the implementation process feeds into limiting the measuring of the success of ERP implementation to standard project-based assessment performance measures. Since the process of ERP implementation consists of many phases, only one of which is the actual ERP system installation, and since each phase can have quantifiable success measures feeding the subsequent stage, it is feasible to take a broader approach to ERP implementation process and its success measurement. This paper categorizes and maps the extant research to this proposed ideology.

1. INTRODUCTION

Most organizations, irrespective of the nature of their business, are today involved in some kind of enterprise level Information Technology (IT) initiative. These initiatives, credited with improving operating efficiencies include Enterprise Resource Planning systems (ERP). While some organizations are evaluating purchase/upgrade of such systems, others are in various phases of the implementation process. Irrespective of the nature of the ERP initiative and the stage of adoption it is in, a perpetual issue faced by IT managers is the ability to measure the impact of such systems on the improvement in performance, and therefore validating the need for more of these costly initiatives.

Traditionally, the success of ERP implementation projects has been measured by checking its compliance against targeted time, optimal resource utilization and the budgeted cost. While this is desirable from a tactical perspective, it nonetheless is a restrictive performance criterion. Successful implementations are those where one can map the usefulness of the implemented IT system against verifiable and quantifiable enhancements in working performance. While a direct cause-effect relationship is generally challenging to establish, it is usually possible to keep track of the key indicators, which have the greatest potential to influence improvements in performance. The timely reporting of such indicators by IT project managers solidifies a company's commitment to continued IT initiatives, lays down benchmarked data for future implementations, and makes buy-in easier from work force.

Information and Logistics Technology, 312 Technology II, College of Technology, University of Houston, Houston, TX 77204-4023,
E-mail: vtiwari@uh.edu

2. ERP: SYSTEM vs. PROCESS VIEWS

ERP as a concept may be defined as "seamless integration of processes across functional areas with improved workflow, standardization of various business practices, improved order management, accurate accounting of inventory and better supply chain management" (Mabert et al. 2000); whereas ERP Systems are merely the vehicles through which this is accomplished (Jacobs 2003). The concept of ERP is fundamentally tied to the integration, standardization, extension and assurance of future flexibility for corporate processes, whereas the system represents the technical manifestation of these goals and the changes required to attain and maintain them (Jacobs 2003, Ng et al. 1999).

Research dealing with ERP as a concept deals with issues like success factors, measures of success, ERP systems' integration into the business strategy, and impacts of ERP implementation on overall business objectives. Research in ERP systems deals with system intricacies and process design to meet the conceptual objectives of the ERP. As is evident from the definitions above, ERP as a concept goes above and beyond ERP Systems. ERP Systems are a means to an end; the end being a seamless information flow across functional areas. Permille Kræmmergaard et al. (2000) define ERP implementation as "an ongoing process of integration and transformation of business using an ERP System." According to Jacobs (2003) and our survey of ERP implementation literature, academic research deals predominantly with the ERP systems. Consequently, the boundary demarcating a successful ERP deployment and a successful ERP Implementation is very blurred, and ERP System Implementation success measures are used as a substitute for measuring the ERP success.

Davenport (1998) indicates that there is an important difference between enterprise and enterprise systems. Many companies fail in their implementation efforts because of failure to "reconcile the technological imperatives of the enterprise system with the business needs of the enterprise itself."

Several authors have made the point that ERP deployments are in-fact sequential phase-by-phase activities. Markus and Tanis (2000) develop a framework for ERP Implementation and measuring its success using the Emergent Process Theory of Soh and Markus (Soh et al. 1995). This model describes IT Implementation as a series of three phases – system development, implementation and on-going operations. The outcomes of one phase become starting conditions for the next. Therefore, decisions and actions made in a phase may increase or decrease the potential for success subsequently. We thus feel that it is critical that ERP Implementation studies necessarily evaluate the performance based on comprehensive success measures and not on standalone success measures. Also, since a typical ERP project extends over several years and has profit and operational ramifications extending over several years (Mabert et. al, 2001), static and one-time success measures are

of little value and only capture one small aspect of the big picture.

Mabert et al. (2002) state that "many different factors ranging from pre-implementation planning to system configuration influence performance, which managers should be sensitive about when implementing major systems like ERP". There is an extensive body of knowledge concerning IT System Implementations and their successes, and in some aspects ERP System Implementations can be thought of as extension of IT Systems. ERP research relating to purely system or package implementation can ideally make use of the fundamentals already developed in IT research (Jacobs et al. 2003).

Markus and Tanis (2000) indicate that "there is a fundamental gap in both practical and academic thinking about information systems and a lack of consensus and clarity about the meaning of success". Upon review of literature concerning ERP implementation, ERP success and failure cases, ERP implementation critical success factors, etc. we noticed that the same problem applies to ERP: success is rarely explicitly defined, and if it is defined, the explanations often differ.

We feel that the academic community should take a holistic view of the ERP Implementation process and its success measurement. This would mean measuring the success or failure of an ERP Implementation not just from a technological perspective but from a multi-dimensional business perspective. With this in mind, we surveyed the most cited research done in ERP Implementation and tried to categorize where that research lies within our proposed ideology. In this paper, we make an attempt to collect most popular definitions of success, to cite some common performance measures used in the industries and in academic research, and to see how these measures can be used efficiently in correspondence with the phase-by-phase ERP implementation approach.

3. SURVEY OF LITERATURE

Understanding success of an ERP implementation project and being able to appropriately measure success is very important for numerous reasons. First of all, ERP implementation efforts are very expensive and usually cost companies several million dollars. Therefore, managers would be interested in evaluating the result of the implementation project, in understanding benefits that the company received from the project. Secondly, having a common understanding of ERP implementation success would make it easier for academics to conduct empirical studies and to compare and differentiate ERP implementations across industries and across different organizations. Lastly, Umble et al. (2003) list existence of focused performance measures as one of the very important factors that lead to successful implementation. Often in business, you get what you measure. So, existence of good success metrics creates a strong motivation for employees involved in the implementation project and the company may achieve desired outcomes. If we measure only the ERP Systems Implementation success then we may get a good system that may not necessarily benefit the business. If we measure positive business outcomes after the implementation, then we may get a system that actually benefits the business in the long run.

In this section we review the most cited ERP research against our proposed ideology - that ERP Implementation is a phase-by-phase process where each phase should have its own success measures (Figure 1); and, for a meaningful evaluation of an ERP Implementation (not just an ERP System Implementation) comprehensive success measures would be more appropriate than stand-alone metrics. With this in mind we searched for published research, using the keywords "ERP", "ERP Implementation" and "ERP success", in our university's academic databases. Some areas of research like - research concerning human-behavior/ change management during ERP Implementations were avoided. Our focus was on ERP Implementation research within the gambit of Operations Management.

"A model of ERP project implementation" by Parr et al. 2000, proposes a Project Phased Model (PPM) of ERP implementation which consists of three phases: planning, project, and enhancement. The main focus is on the project (system implementation) phase. In this paper the authors link the critical success factors (and not success measures) with implementation stages. The paper cites three other process models of ERP Implementations:

1. The five phase model of Bancroft et. al (1998) – the focus phase, as is phase, to be phase, construction and testing phase and the actual implementation phase
2. The five phase model of Ross (1998) – design, implementation, stabilization, continuous improvement and transformation
3. The four phase model of Markus and Tanis (1999) – chartering, project, shake-down and onwards and upwards.

Except for Markus and Tanis, none of the models relates success measures to the phases of implementation.

"Enterprise Resource Planning: Managing the implementation process" by Mabert et. al (2002) empirically investigates and identifies key differences in the approaches used by companies that managed their implementation on-time and/or on-budget versus the ones that did not, using data collected through a survey of US manufacturing companies that have implemented ERP systems. The paper implicitly uses the systems perspective for the ERP Implementation process and uses 'on-time and on-budget' as the performance measures for measuring success. Though they do report in their findings that pre-implementation issues play a major role in the overall system performance.

"A research framework for studying the implementation of Enterprise Resource Planning Systems", by Kaemmergaard et. al, 2000, presents three different perspectives of ERP implementation – the organizational, business and technological. Their definition of implementation includes – IT/IS strategy formulation, decision process, development of implementation plans, the technical set-up, the use and profitability of the systems and the further development of the systems and the organization. The paper mentions the need to have performance measures which more accurately reflect the

true performance and capture all perspectives, but does not state any such measures.

"Towards the unification of critical success factors for ERP implementations", by Sousa et.al (2000), implicitly refers to ERP System Implementation when in fact it is describing a full ERP Implementation. The paper develops a unified framework for analyzing critical success factors – strategic, tactical, organizational and technological. The critical success factors that they mention capture many business aspects and not just the technological implementation side of the project: business process reengineering, sustained management support, organizational change etc.

"Enterprise Resource Planning: Common Myths Versus Evolving Reality" Mabert et al. (2001) provides state of the art overview of the market for ERP Systems and alludes to the implementation of ERP as an IT/software implementation. The paper also hints at using ROI (return on investment as a measure of success for ERP Implementation).

"Enterprise Resource Planning: Measuring Value" by Mabert et al. (2001) – presents an attempt to capture, through a user survey, respondent's and firm's characteristics, the pre-implementation planning process and management, the implementation process, subjective measures of ERP success, and objective measure of ERP success. The authors point out that the environment in which businesses operate is continuously changing, a company which set out today to implement an ERP will be faced with a very different competitive environment by the time the implementation is over, which may be several years. Hence it may not always be possible (and perhaps advisable) to compare operational measures of success across different time-periods.

"ERP Implementation: Chief Information Officers' perceptions of Critical Success factors" by Fiona Fui-Hoon Nah, Kathryn M.Zuckweiler, Janet Lee-Shang Lau (2003) reports the results of a survey of chief information officers' perceptions of critical success factors in ERP Implementation. The questionnaire, (provided at the end of the paper) asks the respondents to rate factors which are critical for an ERP Package Implementation. However, the paper does define what success measures the respondents should consider while answering questions on critical success factors. Moreover, the questions vacillate between ERP System related questions to ERP Concept related questions and hence the validity of what is being measured becomes a little fuzzy.

"Enterprise resource planning: Implementation procedures and critical success factors", by Elisabeth J. Umble, Ronald R.Haft, M.Michael Umble (2003) state that "successful ERP implementations require that organizations engage in excellent project management. This includes a clear definition of objectives, developments of both work plan and resource plan, and careful tracking of project progress." This definition is probably more apt for defining an ERP System implementation as its focus is on the "project" aspect of the Implementation. The paper does point out that managers need to understand that ERP is more of a business issue than just a technological challenge.

"Enterprise resource planning: a taxonomy of critical factors" by Majed Al-Mashari, Abdullah Al-Mudimigh, Mohamed Zairi (2003) provide a framework for analyzing critical success factors. They segregate the ERP Implementation process into – setting up stage, implementation stage and evaluation stage. They also provide general parameters for classifying ERP benefits. The authors cite various studies to make the point that the logic of an ERP System may conflict with the logic of the business, and this may result in an implementation failure. The authors also state that "well-defined strategic targets help to keep the project team on track throughout the entire implementation process". This reasoning (which may be attributed to Davenport, 1998) is being used by more and more researchers. Our basic proposition is that researchers should view an ERP Implementation in its entirety with measurable successes along the way (Figure 1).

"Vicious and virtuous cycle in ERP Implementation: a case study of interrelations between critical success factors", H. Akkermans and K van Helden (2002) is based on a case study used to analyze and explain poor project performance in one ERP implementation in the aviation industry. The paper depicts a timeline of the ERP Package Implementation which is inadvertently referred to as a timeline for the ERP Implementation. A look at the critical success factors proposed in the paper makes it apparently clear that what they are capturing clearly goes beyond just a software implementation. For example, some of the success factors identified include architecture choices, management support, business process re-engineering and user training. Each of these factors will be relevant in a different phase of the implementation of the ERP Concept and referring to them as factors of success for implementation of the ERP Package is taking a myopic view of the situation. Moreover, the paper does not define the measures of success used to rank and classify the success factors.

The most common way for looking at ERP success is to treat it as a regular IT implementation and to apply the most popular performance metrics used in IT to ERP implementation. According to Mabert et al. (2003), various companies commonly cite the following measures of ERP success: the project was completed on time and within budget. Although these metrics have been among the most popular success measure in IT implementation area, lately the IT success was redefined by various researchers.

M. Al-Mashari et al. extend the definition of IT success based on the Lyytinen and Hirschheim's definition of IT project failure. In addition to existing dimension of completing the project on time and within budget that they call "process success", they define three new dimensions: correspondence success (does the system meet the specific objectives?), interaction success (do the users have positive attitudes towards the system?), and expectation success (does the system match the expectations?) (Al-Mashari 2003). We feel that adopting this success measurement framework to the definition of ERP success would lead to better understanding of the actual performance of the ERP system.

Moreover, ERP implementation is not only about installing a new IT system; it also has significant strategic, organizational, and even cultural implications (Davenport). Therefore, its success should not be measured solely on the same metrics as the success of any IT implementation. For this reason, Markus and Tanis suggest two major approaches for defining success of enterprise systems: from the implementation project perspective and from the business results perspective. The first approach may utilize IT implementation metrics, but the second approach should take into account whether the company has achieved its strategic goals and whether the business performance has improved in any way as a result of the implementation.

Sedera et al. outlay a research proposal that aims to develop a system for measuring performance of enterprise systems based on the Balance Scorecard framework created by Norton and Kaplan (1992). The Balance Scorecard helps organizations to convert their corporate mission and strategy into a set of performance metrics. This framework emphasizes use of financial performance indicators but also includes various operational drivers of financial objectives, in other words, this approach includes both quantitative and qualitative factors. The authors argue that ERP implementation projects may benefit from adoption of this measurement framework, because the ERP systems bring in many intangible benefits that cannot be measured quantitatively (Sedera 2003). Bartholomew (1999) argues that actually 80% of the ERP benefits in a typical business organization are intangible. The Balance Scorecard framework was created to measure performance of the whole organization, and, certainly, it will need some alterations to be applicable to the ERP implementation projects. For example, instead of translating corporate mission, companies would have to translate their implementation objectives into performance metrics.

A very rich stream of literature in ERP implementation concerns ranking and classification of critical success factors. Umble et al. (2003) list existence of focused performance measures as one of the very important factors. Some business performance measures proposed in the paper are as following: on time deliveries, gross profit margin, customer order-to-ship time, inventory turns, vendor performance. They suggest considering ERP implementation successful if "it achieves a substantial proportion of potential benefits," where potential benefits of ERP implementation include personnel reductions, decrease in operating and IT costs, improved demand forecasts, increased speed of production cycle, improved customer service, reduction of inventory and better inventory control.

Another success measurement is proposed by Ptak and Schragenheim and cited by Umble (2003) in one of the critical success factors studies. They define success as achievement of the desired level of ROI, as it was identified during the planning phase. Hitt, Wu and Zhou use the following performance metrics in their empirical study of relationship between companies' success and ERP adoption: labor productivity, return on assets, inventory turnover, return on equity, profit margin, asset turnover, account receivable turnover, debt to equity ratio, and Tobin's q (market value over book value).

We believe that in some cases measuring achievement solely based on the above stated indicators may lead to fallacious conclusions about the success or failure of ERP. Mabert et al. (2001) raise an important issue of business dynamics as it is related to the measurement of success. Since most implementation projects take a few years to complete, a lot can happen in business during these years and the business performance indicators may change significantly due to various intervening factors that are absolutely not related to the ERP implementation. We feel this is a very valid and important point and fits nicely with our thinking that ERP Implementations should be considered as a phased activity with each phase feeding into the other, hence the implementation should be studied as a whole and its success measured in terms of improvements in the operational parameters on a longitudinal time-phased basis over each phase of the implementation life-cycle.

4. CONCLUSIONS AND FUTURE RESEARCH SUGGESTIONS

A review of ERP Implementation literature reveals misalignment in understanding between academics on what aspect of the implementation and success of the implementation is actually being measured. This gap also highlights the potential opportunity for future research (Figure 2).

Throughout the years of research in ERP field, academic researchers have suggested numerous definitions of ERP implementation and practitioners have approached it in different ways. Based on our literature review and common understanding of business, we believe that the most comprehensive approach to defining ERP implementation is in terms of phases. Defining ERP implementation in terms of phases captures different stages of ERP implementation starting from planning period and ending with the long term business outcomes achieved as a result of the implementation. We identified four major phases models proposed in the academic literature:

1. The Project Phased Model (PPM) of Parr et al. (2000) The limitation of this model is that it focuses mainly on the project phase, therefore it deals mostly with the ERP Systems implementation;
2. The five phase model of Bancroft et al. (1998). In our opinion, a limitation of this model is that it ends with the implementation phase and does not consider the business performance after the ERP implementation;
3. The five phase model of Ross (1998) – This model starts with the design phase, which refers to the determination of critical guidelines and decision making for the implementation. In our view, this is a limitation of this model: it does not consider the very early phase where the business determines the need for the ERP implementation. We feel that the seeds of success or failure of an ERP Implementation are planted in this very first stage.

4. The four phase model of Markus and Tanis (1999) – This model is the most comprehensive in our view. It starts with the creation of the ERP business case and ends with the long term outcomes of the ERP implementation.

If the company adopts a phased framework for the ERP implementation (Figure 1), the success should also be measured by stages. Companies have a choice of numerous operational and business metrics proposed by different researchers and practitioners. IT success metrics are applicable only during the actual system implementation stage. The metrics to be used at each stage will vary according to the nature of the business and specific business objectives. In any case, these metrics should be defined during the planning stage of the implementation, so that the implementers know what to strive for in the implementation process. Developing such phase-wise success measures can be a very fruitful area of research. Such research, in our opinion, could have a profound impact on ERP Implementations.

This analyses and conclusions are based solely on our literature review and personal judgment. We believe that another opportunity for further research in this area is to conduct a survey of companies that have implemented ERP and of ERP implementation consultants to test our proposition that approaching implementation in terms of phases, where each phase has its own set of success metrics, leads to a better and smoother implementation process; and using the same survey to see whether the outcome of one phase affects the success or failure of the subsequent phase.

Research and Development in the field of ERP implementation is an evolving and developing area. Conducting analytically studies that address and quantify the ERP Implementation success and factors will greatly benefit the entire Information Technology industry.

Another research opportunity in this field is creating a pool of success metrics and identifying what circumstances should make businesses choose certain metrics and not use the others. A research tool that may be applicable to such analysis is an empirical based longitudinal study of companies that have implemented ERP couple of years ago to see what changes did they notice in the long term business outcomes, what quantitative and qualitative benefits did they encompass, and also to collect information about their business characteristics, business objectives, and motivation for ERP implementation. Once this information is obtained, it would be interesting to match certain business benefits achieved with the business and ERP implementation objectives. Once there is a pool of such success metrics created, another interesting research study could be to go back to the famous ERP implementation cases that describe either success or failure of the implementation (von Helens et. al 2004) and check whether the use of proposed metrics would actually give a truer picture of the success of the case.

REFERENCES

[1]. Akkermans, H.; van Helden, K. Vicious and virtuous cycles in ERP implementation: a case study of interrelations between critical success factors. European Journal of Information Systems, Mar 2002, Vol. 11 Issue 1, p35.

[2]. Al-Mashari, Majed; Al-Mudimigh, Abdullah; Zairi, Mohamed. Enterprise resource planning: A taxonomy of critical factors. European Journal of Operational Research, 4/16/2003, Vol. 146 Issue 2, p352.

[3]. Bancroft, N., Seip, H., and Sprengel, A. Implementing SAP R/3, 2nd edition, Manning Publications, Greenwich, 1998.

[4]. Carr, Nicholas. G. 2003. IT Doesn't Matter. Harvard Business Review.

[5]. Davenport, Thomas H. Putting the Enterprise into the Enterprise System. Harvard Business Review, Jul/Aug 98, Vol. 76 Issue 4, p121.

[6]. Fui-Hoon Nah, Fiona; Zuckweiler, Kathryn M.; Lee-Shang Lau, Janet. "ERP Implementation: Chief Information Officers' Perceptions of Critical Success Factors. International Journal of Human-Computer Interaction, Aug 2003, Vol. 16 Issue 1, p5.

[7]. Hitt, Lorin M.; Wu, D.J.; Xiaoge Zhou. Investment in Enterprise Resource Planning: Business Impact and Productivity Measures. Journal of Management Information Systems, Summer 2002, Vol. 19 Issue 1, p71.

[8]. Jacobs, F. Robert; Bendoly, Elliot. Enterprise resource planning: Developments and directions for operations management research. European Journal of Operational Research, 4/16/2003, Vol. 146 Issue 2, p233.

[9]. Kraemmergaard, P., and Moeller, C. (2000). "A Research Framework for Studying the Implementation of Enterprise Resource Planning Systems," Proceedings of IRIS, Uddevalla.

[10]. Mabert, Vincent A.; Soni, Ashok; Venkataramanan, M. A. Enterprise resource planning: Managing the implementation process. European Journal of Operational Research, 4/16/2003, Vol. 146 Issue 2, p302.

[11]. Mabert, Vincent A.; Soni, Ashok; Venkataramanan, M. A. Enterprise Resource Planning: Common Myths Versus Evolving Reality. Business Horizons, May/Jun2001, Vol. 44 Issue 3, p69.

[12]. Mabert, Vincent A.; Soni, Ashok; Venkataramanan, M. A. Enterprise Resource Planning: Measuring Value. Production & Inventory Management Journal, 2001 3rd/4th Quarters, Vol. 42 Issue 3/4, p46.

[13]. Mabert, Vincent A.; Soni, Ashok. Enterprise Resource Planning Survey of U.S. Manufacturing Firms. Production & Inventory Management Journal, 2000 2nd Quarter, Vol. 41 Issue 2, p52.

[14]. Ng, J. K. C.; Ip, W. H.; Lee, T. C. A paradigm for ERP and BPR integration. International Journal of Production Research, 06/15/99, Vol. 37 Issue 9, p2093.

[15]. Markus M., Tanis C. 2000. "The Enterprise Systems Experience- From Adoption to Success", in Framing the Domains of IT Research Glimpsing the Future Through the Past, R. W. Zmud (Ed.), Pinnaflex Educational Resources, Cincinnati, OH.

[16]. Parr, A.; Shanks G.; A model of ERP project implementation. Journal of Information Technology, 2000, Vol.15, 289-303.
[17]. Ross, J.W., Vitale M.R.; The ERP Revolution: Surviving versus Thriving; Center for Information Systems Research; Sloan School of Management, 1998.
[18]. Sedera, D., Gable, G., and Rosemann, M. A Balanced Scorecard Approach to Enterprise Systems Performance Measurement, Proceedings of the Twelfth Australasian Conference on Information Systems, 2001
[19]. Sousa, J. E., Collado J.P.,Towards the unification of critical success factors for ERP implementations, 10th Annual Business Information Technology 2000 Conference, Manchester.
[20]. Umble, Elisabeth J.; Haft, Ronald R.; Umble, M. Michael. Enterprise resource planning: Implementation procedures and critical success factors. European Journal of Operational Research, 4/16/2003, Vol. 146 Issue 2, p241.
[21]. Von Hellens, Liisa, Neilsen, S., Beekhuyzen, J. Qualitative Case Studies on Implementation of Enterprise Wide Systems. 2005. Idea Group Publishing, Hershey PA.

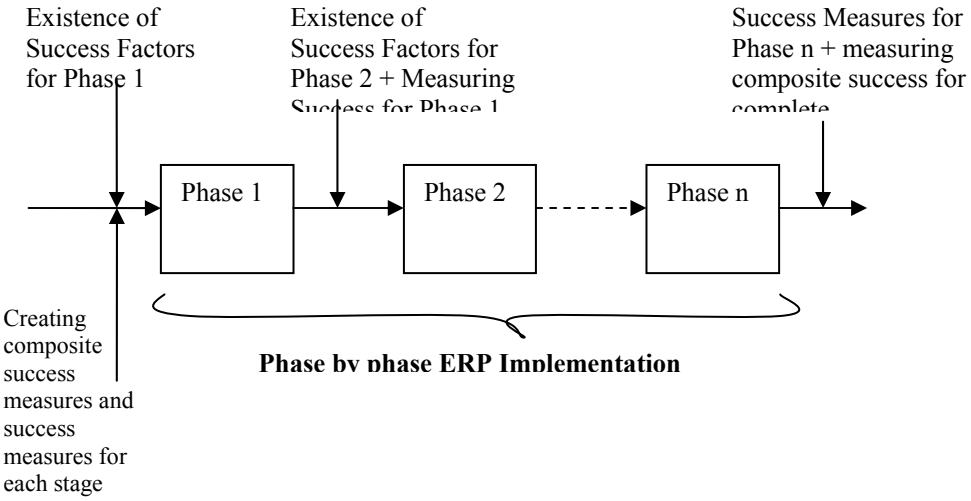


Figure 1: Proposed Framework for Measuring Composite Success of ERP Implementation

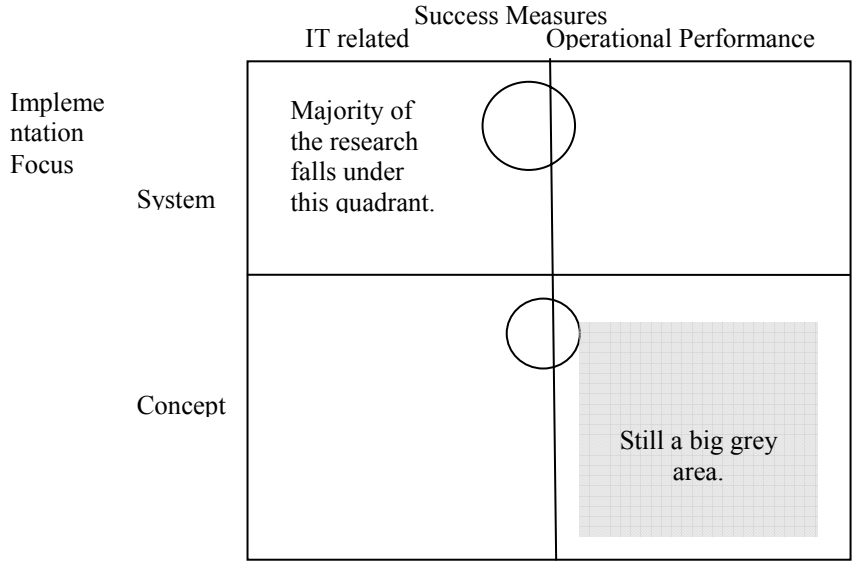


Figure 2: Identify Potential Research Areas in ERP Implementations and Success Measurement

Restricted Backtracked Algorithm for Hamiltonian Circuit in Undirected Graph

Vinay Kumar

Abstract - While determining whether a graph is Hamiltonian, it is enough to show existence of a Hamiltonian cycle in it. An algorithm based on restricted backtracking is presented in the paper that uses tie breaking rules to reduce the possible number of backtrackings. If x is any intermediate node in HC then once its neighbour y has been visited from x, x is no longer required so drop it and process is continued on the remaining subgraph. Each node is visited exactly once in a HC except the start node. Adjacency matrix is used to encode the graph. Prevention of backtracking is achieved up to next node from start node. From third node onward, wherever it is not possible to break tie uniquely, a provision for backtracking is kept only for tied nodes. Time complexity of algorithm is $O(n^4)*B(n)$ in the worst case where B(n) is a factor due to possible backtracking. It returns $O(n^2)$ in the best case and $O(n^3)*B(n)$ on the average.

Index Terms - articulation point; complexity class; P; NP; Hamiltonian graph; connected graph; line sweeping; restricted backtracking

1. INTRODUCTION

The Icosian game [4], introduced by Sir William Hamilton is known as Hamiltonian Circuit (HC) problem [7]. The objective of the game is to visit all nodes of the graph exactly once before returning to the initial node. In graph theoretic world, a Hamiltonian circuit is defined as a simple cycle that contains every vertex of graph exactly once except the first one which is visited again at the end to complete the cycle [8]. A graph is said to be Hamiltonian if it contains a HC else it is nonhamiltonian. Although many graphs can be trivially determined as Hamiltonian or nonhamiltonian even then the problem is very complex in general. The problem of finding a Hamiltonian cycle in an undirected graph is studied for over a hundred years [36]. The problem "Does a graph G have a Hamiltonian cycle?" can be defined in formal language as

HAM_CYCLE = {<G>: G is a Hamiltonian graph}

Showing existence of one Hamiltonian cycle in G is sufficient to conclude that the graph is Hamiltonian. However, it is expected to test all possible n! permutations of vertices before concluding that G is nonhamiltonian. Basic properties of graph [5, 16, 38] are used in the introduced algorithm to restrict backtracking to the maximum possible extent and to avoid it if it can be. It is, therefore, not always required to explore all possible n! arrangements of vertices before concluding that a graph is nonhamiltonian. The following facts are taken into consideration while developing the algorithm.

1. One edge is sufficient to cross over from one node to its adjacent node [11]
2. Once a node is visited, it is no longer required (except the initial node), so drop it [1].
3. A node **y** to visit from **x** can be selected using some tie breaking rules in such a way that possibility of backtracking to explore other possible path from **x**. is drastically reduced [18, 19].
4. At any stage, if dropping of node **x** yields more that one dangle node [38], and if it is not avoidable (backtracking not possible), the graph can be concluded as nonhamiltonian.
5. If at the end only initial node is left then graph is Hamiltonian otherwise it is nonhamiltonian [22].

The core of the algorithm development process lies in the point 3 above. The detailed steps are outlined in section 2 of this paper. Section 3 contains proof for the correctness of the algorithm followed by two illustrative examples in section 4. Section 5 deals with computational analysis of the algorithm. Before stepping into section 2 let us see a basic concept that if graph contains an articulation point then graph is nonhamiltonian [24].

Let G = (V, E) be a connected undirected simple graph with $|V| = n \geq 3$, and $|E| = m$ where $m \geq n$. A graph is simple if it contains neither loop nor multi edge [3, 26]. A graph is connected if there is a path between every pair of nodes in it [3]. To maintain flow of presentation, few terms like node and vertex, edge and arc are used synonymously. In this paper, a graph implies a simple connected graph with no articulation point, unless otherwise stated. DFS (depth first traversal) algorithm is used to test connectivity and non-existence of articulation point in graph. DFS algorithm executes in polynomial time [2, 6, 27]. An articulation point in a graph G is a node **x** that, when removed from G, partitions set V into two (or more) non empty subsets U and W such that

- U and W are disjoined, and
- No node in U is adjacent to any node in W [28].

Theorem 1: A graph G = (V, E) with an articulation point has no Hamiltonian Circuit.

Proof: Let v be the articulation point and U and W be the two non empty subsets of V such that

- $V = U \cup W \cup \{v\}$,
- $v \notin U$, $v \notin W$ and
- $U \cap W \neq \phi$

Let us proof it by contradiction. Suppose G has a HC. Three possibilities about starting node x of HC in G are (a) x = v or (b) $x \in U$ or (c) $x \in W$.

Case (a) when x =v

Scientist 'D', NIC, Block A, C.G.O Complex, Lodhi Road New Delhi 110 003, India
E-mail: vinay.kumar@nic.in and vinay5861@gmail.com

Since G is connected, v has adjacent nodes in both U and W. Once a node in U is visited from v, there is no way to come to any node in W without visiting v. Similar case is faced when a node in W is visited first. Therefore there is no HC in G [10].

Case (b) when $x \in U$

Starting from x visit all nodes in U first, in the best case. Then visit v then a node in W. Once in W, there is no way to return to x because v is removed. Therefore there is no HC in G

Case (c) when $x \in W$

It can be proved in the same way as in the case (b). ♦

Corollary 1: A graph G containing a node of degree ≤ 1 is nonhamiltonian.

Proof: Any node y adjacent to the node x of degree one is an articulation point in G. A node of degree zero is unreachable. ♦

Converse of the theorem that "a graph having no articulation point is Hamiltonian" is not true. Many graphs can be presented in the support [13, 21]. However this theorem helps in early conclusion on the nonhamiltonian graph. Presence of an articulation point indicates that as and when it is dropped from the graph while traversing to find HC, it ensures that at least two nodes are left in the current subgraph when algorithm terminates its execution.

2. ALGORITHM

The step by step algorithm determines existence of one cycle out of possible n! to conclude that G is Hamiltonian. Current node **x**, other than initial node, is dropped when its neighbour **y** is visited. While dropping **x** it is ensured that no backtracking to the node **x**, in due course can yield otherwise result. It is achieved by applying tie breaking rule whenever ∃ more than one options from **x**. If it is not possible to break a tie, the possible options available at that point is stored in array BACKTRACK []. The array BACKTRACK [] is indexed on the nodes as visited in the graph. List of currently visited nodes is denoted by π. And nodes are referred as $v_1, v_2, v_3, \ldots, v_n$ in the sequence they are visited. Before applying the algorithm, line-sweeping [37] algorithm is executed on the graph to merge all nodes in one linear component because all nodes in a line are visited one after other in a sequence as per this algorithm. For example if nodes from j to k are merged (visited) in sequence then merged (visited) nodes are referred as $<v_j, v_{j+1}, \ldots, v_{j+k}>$. List of articulation points is updated in the current subgraph when a node is dropped from graph. The list of current articulation point is referred as ARTPNT.

When a node v_2 or later visited node v_k is dropped from current subgraph, start node v_1 may become dangle. While counting number of dangle nodes at any stage in the algorithm, only intermediate nodes are taken into account but not node v_1.

Let G = (V, E) be a simple graph with |V| = n, |E| = m, m ≥ n. Initialize adjacency matrix M[n, n] as per adjacency in G. The degree spectrum [8, 9, 12] of G is stored in one dimensional array Degree[n].

Step 1: Select a node $\mathbf{v_1}$ from G such that $\mathbf{v_1}$ is of minimum degree. Resolve a tie by taking node from earliest row (or column) of matrix M. For example if nodes in rows 5 and 10 have same minimum degree then select node from row 5. Initialize path π to $\mathbf{v_1}$ and Start_node to $\mathbf{v_1}$.

Start_node ← $\mathbf{v_1}$; π: $\mathbf{v_1}$

Step 2: Find a node to be visited next from start node.

Step 2.1 Create a set of all nodes adjacent to $\mathbf{v_1}$ and call it NGBR – set of neighbours of Start_node.

Step 2.2 Select a node $\mathbf{v_2}$ from NGBR to visit next in the following way. Resolve any tie as in Step 1.

Step 2.2.1 Pick up a node of degree two. If such node is found then go to step 2.3 else continue to next step 2.2.2

Step 2.2.2 Find a node that does not yield any dangle node when dropped from graph G. If such node is found then go to step 2.3 else continue to next step 2.2.3.

Step 2.2.3 Find a node that yields only one dangle node when dropped from G. If such node is found then go to step 2.3 else skip to step 5.

Step 2.3 Initialize Current_node to $\mathbf{v_2}$ and extend path π up to $\mathbf{v_2}$.

Current_node ← $\mathbf{v_2}$; π: $\mathbf{v_1}$ $\mathbf{v_2}$

Update NGBR = NGBR – {$\mathbf{v_2}$}

Update set ARTPNT treating Current_node as dropped.

Step 3: Select a node $\mathbf{v_{j+1}}$ from adjacent nodes of Current_node $\mathbf{v_j}$ to visit next in the following way. Resolve a tie by ignoring the node that is in ARTPNT. Even then if there is tie then resolve as in Step 1, keep list of other candidate nodes at BACKTRACK [$\mathbf{v_j}$] and set flag BACKTRAK_possible as true.

Step 3.1 If number of adjacent node is one then return the node and go to step 3.6 else remove the Start_node from list of adjacent node, if it is in the list, and continue to step 3.2.

Step 3.2 If there are more than one adjacent node of degree two then go to step 5 else pick up the node of degree two. If such node is found then go to step 3.6 else continue to step 3.3.

Step 3.3 Find a node that is neither in NGBR nor equal to Start_node and that does not yield any dangle node when dropped from graph G. In case of tie resolve it. If such node is found then go to step 3.6 else continue to next step 3.4.

Step 3.4 Find a node that is neither in NGBR nor equal to Start_node and that yields only one dangle node

when dropped from G. In case of tie resolve it. If such node is found then go to step 3.6 else continue to step 3.5.

Step 3.5 Find a node from nodes not considered in step 3.3, 3.4 as below:

Step 3.5.1 Find a node that does not yield any dangle node when dropped from G. If such node is found then go to step 3.6 else go to step 3.5.2

Step 3.5.2 Select a node that yields one dangle node when dropped. If such node is found then go to step 3.6 else continue to step 5.

Step 3.6 Initialize
Prev_Cuurent_node←Current_node
Current_node← $\mathbf{v_{j+1}}$
Extend path π up to $\mathbf{v_{j+1}}$.
Drop Prev_Cuurent_node from graph and update the degree of all affected nodes accordingly in G
Update set ARTPNT for the current subgraph treating current node as dropped
Update NGBR, if required.

Step 4: Repeat Step 3 as long as visit to a neighbor is possible else go to step 5.

Step 5: **If** only Start_node is left at this stage, after successive removal of intermediate nodes, then G is Hamiltonian

Else If back track is possible (i.e. BACKTRAK_possible is true) **then**
Restore the matrix by adding nodes one by one from last visited node in $\boldsymbol{\pi}$ up to last index node $\mathbf{v_k}$ in array BACKTRACK. Then pick up first node from list of options available in BACKTRACK [$\mathbf{v_k}$] and initialize
Current_node← $\mathbf{v_k}$
Update set ARTPNT, NGBR and BACKTRAK_possible flag as applicable for the latest subgraph and Repeat Step 3 as long as visit to a neighbour is possible.

Else Graph G is nonhamiltonian.

The algorithm in steps 1 through 5 ensures two things: (1) it restricts backtracking by dropping the visited intermediate nodes, and (2) while dropping a node it ensures that no other path from that node shall yield different result in most of the circumstances by using tie breaking rules. While iterating in step 3, only remaining sub graph is taken. Algorithm terminates when no more visit is possible i.e. even backtracking is not feasible. A visit is not possible if there is no adjacent node to Current_node and BACKTRAK_possible falg is false. This case arises when there is only one node (i.e. Start_node) is left at the end or graph is detected as nonhamiltonian at an early stage. Two illustrations of the algorithm are given in the following section that deals with the situation (1) when no backtracking is required and (2) when it is really required.

3. ILLUSTRATIVE EXAMPLES

A primitive idea about working of the algorithm is shown using a visually very simple graph in figure1. This is the case when no backtracking is required. Represent the graph as adjacency matrix [15, 20]. Start from a node of minimum degree. All nodes in this graph are of equal degree 3. Without loss of generality, let A be in the earliest row (column) and select node A to start with. Here,

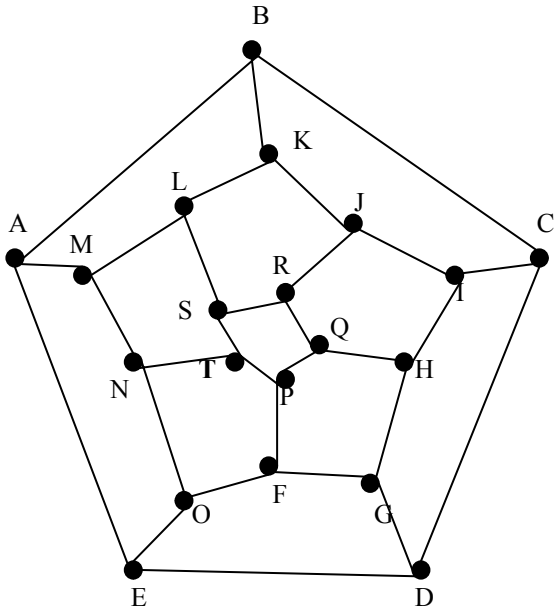


Figure 1

Start_node ← **A;**
π: **A**

A has three adjacent nodes B, E and M and all are of degree 3. None of them yields any dangle node when dropped from G, thus using step 2.2.2, we may select node B using tie breaking rule to proceed further. Here,

Current_node ← **B;**
π: **A B**
NGBR = {B, E, M} – {B} = {E, M}
ARTPNT = {}

Now node B has two adjacent nodes C and K. Using step 3.3 select node C to proceed and following updating is done.

Prev_Cuurent_node← **B**
Current_node← **C**
π: **A B C**.

Drop node **B** from graph and update the degree of all affected nodes accordingly in G. The set ARTPNT = {} for the current subgraph. There is no need to update NGBR. The step by step execution of algorithm is outlined in the table 1 below.

Algorithm steps	Node Selected	Current Path π:	Articulation Set ARTPNT	BACKTRACK [iteration]
1	A	A		
2.2.2	B	A B	{}	
3.3	C	AB C	{}	{K}
3.3	D	ABC D	{}	{I}
3.3*	G	ABCD G	{}	
3.3	F	ABCDG F		
3.3	P	ABCDGF P		
3.3	T	ABCDGFP T	{L}	
3.3	S	ABCDGFPT S	{L K, J}	
3.4*	R	ABCDGFPTS R	{L, K, J}	
3.2	Q	ABCDGFPTSR Q	{L, K, J}	
3.1	…	ABCDGFPTSR QHIJKL	{}	
3.1	M	ABCDGFPTSRQHIJKL M		
3.2	N	ABCDGFPTSRQHIJKLM N	{E}	
3.1	…A	ABCDGFPTSRQHIJKLMN OEA		

Table 1: Indicates that a tie was resolved between nodes G and E using NGBR

.At the end only one node A is left in the subgraph and hence G is Hamiltonian. Here numbering of node has no effect on the requirement of backtracking as long as tie is resolved as per the algorithm. The graph in figure 2 is Hamiltonian. Backtracking may be required in one case. Node A in this graph is of minimum degree 2. Select node A to start with. Here,

Start_node ← **A;**

π: **A**

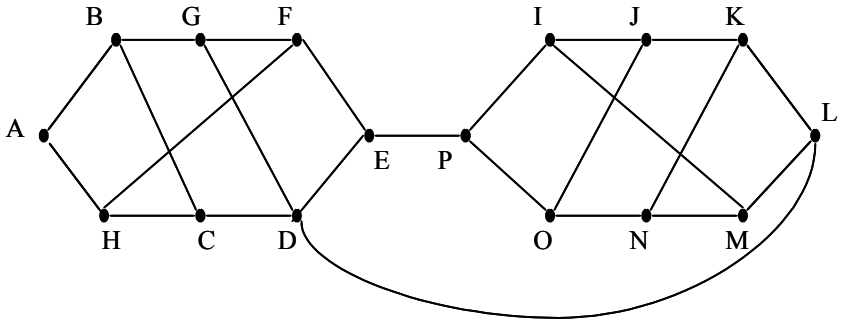


Figure 2

Node A has two adjacent nodes B and H and both are of degree 3. None of them yields any dangle node when dropped from G, thus using step 2.2.2, we may select node B using tie breaking rule to proceed further. Here,

Current_node ← **B;**

π: **A B**

NGBR = {B, H} – {B} = {H}

ARTPNT = {H}

Now node B has two adjacent nodes C and G. Using step 3.3, node C is selected to proceed further with following updating.

Prev_Cuurent_node← **B**

Current_node← **C**

π: **A B C**.

ARTPNT = {H, F}

Drop node **B** from graph and update the degree of all affected nodes accordingly in G. The set ARTPNT = {} for the current subgraph. There is no need to update NGBR. The step by step execution of algorithm is outlined in the table 2 below.

Algorithm steps	Node Selected	Current Path π:	Articulation Set ARTPNT	BACKTRACK [iteration]
1	A	A		
2.2.2	B	A B	{H}	
3.3	C	AB C	{H, F}	{G}
3.3	D	ABC D	{H, F, E, P}	
3.2	G	ABCD G	{H, F, E, P}	

Algorithm steps	Node Selected	Current Path π:	Articulation Set ARTPNT	BACKTRACK [iteration]
3.1	F*	ABCDG F	*	*
℘5	G	AB G	{H}	
3.3	F	ABG F	{H, C, D}	
3.3	E	ABGF E	{H, C, D, L}	
3.3	P	ABGFE P	{H, C, D, L}	
3.3	I	ABGFEP I	{H, C, D, L}	{O}
3.3	J	ABGFEPI J	{H, C, D, L}	
3.4	K	ABGFEPIJ K	{H, C, D, L, M, N}	{M}
3.2	O	ABGFEPIJ K	{H, C, D, L, M, N}	
3.1	…A	ABGGFEPIJK ONMLDCHA		

Table 2

* Dropping of the node F yields two dangle nodes E and H (other than start node).

℘ By step 5 backtracking is initiated up to node C and replacing C by G (available option at that level).

Examples demonstrate the working of the algorithm. At the end only one node A is left in the subgraph and hence G is Hamiltonian. The following graph in figure 3 is a nonhamiltonian. To show this there is no need to explore possibly all 9! permutations of 9 nodes. Just two runs are enough to say that the graph is nonhamiltonian.

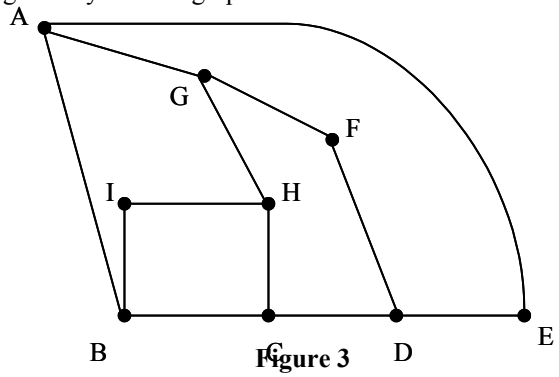


Figure 3

Algorithm correctness is proved in the following section. Related theorems, lemma, propositions and definitions are described as and when required. Obvious results are taken as axioms without any proof.

4. PROOF OF CORRECTNESS

An adjacent node y is visited from x in such a way that a cycle of length less than |V| does not form in the graph. The algorithm takes a biconnected graph (connected graph without articulation point) [14, 17] G = (V, E) as input (precondition) and outputs (post condition) a Hamiltonian (or nonhamiltonian path) π and a subgraph H of G with following properties:

If G is Hamiltonian

then $H = (V_H, E_H)$ with $|V_H| = 1$ and $|E_H| = 0$

Else $H = (V_H, E_H)$ with $|V_H| \geq 2$ and $|E_H| \geq 0$

Here V_H is set of nodes in H and E_H is set of edges in H. The proof of correctness has two parts:

(i) Partial correctness: If the algorithm will terminate then it will give the right result i.e. the result will satisfy the post condition.

(ii) Termination: Proof that the algorithm terminates [24].

To prove the correctness of the algorithm, it is required to prove the following postulates:

(a) Algorithm always finds a ***correct*** start node,

(b) It always finds a node adjacent to start node in correct way, if available, to initiate the process of finding HC in G,

(c) In every iteration, next node from the current node is found, if a visit is possible otherwise program terminates,

(d) Tie breaking rules restrict (in fact reduces number of possible) backtracking i.e. if G is found to be nonhamiltonian at k^{th} node, then backtracking to any of the previously ignored node does not yield any otherwise result.

(e) If only Start_node is left at the end then graph is hamiltonian else it is nonhamiltonian, and

(f) Finally algorithm terminates.

In general, if G is Hamiltonian then a HC may start from any node [35] and if G is nonhamiltonian then a cycle cannot be completed starting from any nodes in G. There is no loss of generality in selecting a start node based on some criteria. Thus the proposition,

"In a Hamiltonian graph a HC begins from a node x of minimum degree"

is true. And step 1 of algorithm selects a node of minimum degree from G to start with. Further, a start node has at least two adjacent nodes.

Lemma 1: $\forall x \deg(x) \geq 2$, where x is a node in the input graph G.

Proof: Let y be any node in G. The graph G is biconnected so there are at least two node disjoint paths between x and y. It implies that ∃ distinct nodes u, v adjacent to x such that one path from x to y goes through u and another through v.

$\therefore \deg(x) \geq 2$. ♦

Corollary: The start node $\mathbf{v_1}$ has $m \geq 2$ adjacent nodes.

Let L(x) denote the set of all adjacent nodes of x then $L(\mathbf{v_1})$ = {y | y is adjacent to $\mathbf{v_1}$}. We refer $L(\mathbf{v_1})$ as NGBR. Among m (≥ 2) adjacent nodes to start node $\mathbf{v_1}$, the different possibilities are:

(i) all are of degree two, or
(ii) some are of degree two and other are of degree > 2, or
(iii) all are of degree > 2.

One node from NGBR is taken to leave the start node and one other will be required to complete HC if G is Hamiltonian. In the case of (i) and (ii), it is STEP 2.2.1 that picks up a node $\mathbf{v_2}$ of degree 2 to start with. However in case of (iii), the algorithm looks one step further to make sure that once the node (to be selected) is removed from graph, it yields not more than one dangle node (excluding start node). The algorithm prefers in step 2.2.2 over 2.2.3, to select a node that does not yield any dangle node. Thus in order of precedence of steps 2.2.1, 2.2.2 and 2.2.3 (from left to right) the algorithm finds a node next to start node yielding the post condition as below:

π : $\mathbf{v_1v_2}$
H = G
NGBR = $L(\mathbf{v_1}) - \{\mathbf{v_2}\}$
ARTPNT = As determined.

It is obvious that algorithm finds a node next to start node. It resolves a tie as per the criteria described in the algorithm as and when it arises. Backtracking is restricted at this stage. It is proved in the lemma 2 that no backtracking is required at this level. Correctness of this step is implied from the lemma 2 and theorem2.

Lemma 2: If G is Hamiltonian then $\forall \mathbf{x} \in L(\mathbf{v_1})$ pre Hamiltonian $\mathbf{v_1x}$ leads to a Hamiltonian cycle. ***Proof:*** Let us prove it using mathematical induction on the degree m of start node $\mathbf{v_1}$. It is to be noted that start node is of minimum degree in G.

Basis Step: For m = 2, the result is obviously true.

Inductive Step: Let the result be true for m = k i.e. $\forall \mathbf{x} \in L(\mathbf{v_1})$ pre Hamiltonian $\mathbf{v_1x}$ leads to a Hamiltonian cycle. Let one of the Hamiltonian cycle be

$$\mathbf{v_1}x\ldots z\ldots y\ \mathbf{v_1}$$

where $\mathbf{x}, \mathbf{y} \in L(\mathbf{v_1})$. See the figure 4(a) for conceptual visualization of Hamiltonian cycle from graph shown in figure 5(a). It is in no way to trivialize the general proof of the lemma.

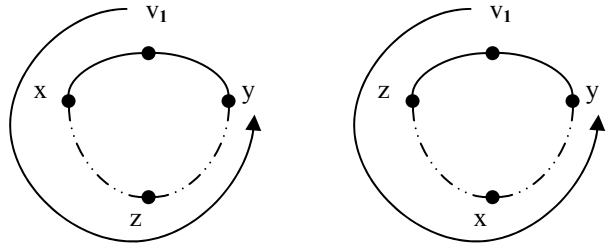


Figure 4

Let us add an edge from $\mathbf{v_1}$ to a node z in G in such a way that degree ($\mathbf{v_1}$) remains minimum in G and $\mathbf{v_1}$ remains the start node. Also $\forall x \in L(\mathbf{v_1})$ degree(x) > k otherwise $\mathbf{v_1}$ can no longer remain minimum degree node if an edge is added from $\mathbf{v_1}$ to any other node $z \notin L(\mathbf{v_1})$ in G. Further, addition of an edge in graph may make a nonhamiltonian graph Hamiltonian but not the reverse.

Let us now remove the edge between $\mathbf{v_1}$ and x. Even then $\mathbf{v_1}$ remains one of the minimum degree node and hence the start node. For conceptual visualization see figure 5(b).

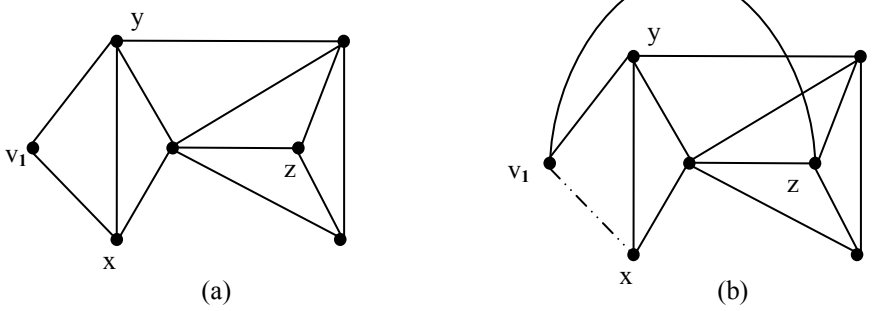


Figure 5

Now again m = k and hence the result is true from the assumption. See figure 4(b) for Hamiltonian cycle from graph 5(b). Presence of edge ($\mathbf{v_1}$, x) does not alter the result but only increases the number of possible Hamiltonian cycles in G. ♦

Theorem 2: If G is found to be nonhamiltonian at k^{th} node, then backtracking to any node x in NGBR = $L(\mathbf{v_1}) - \{\mathbf{v_2}\}$ does not yield any otherwise result.

Proof: Let $\deg(\mathbf{v_1})$ = m (≥ 2). When m = 2, $\mathbf{v_1}$ has two adjacent nodes i.e. $|L(\mathbf{v_1})|$ = 2 and any of the three cases outlined above may be applicable.

When m > 2, only case (iii) is applicable. Algorithmic step 2.2.2 or 2.2.3 finds a node $\mathbf{v_2}$ because step 2.2.1 is not relevant.

Case 1: When m = 2. Let the two adjacent nodes be **x** and **y** and rest of the graph be **H**. If both x and y are of degree two then any one can be used to leave the start node and other is

used to arrive at. No backtracking to y (in case x is selected) or to x (if y is selected) can yield otherwise result.

Suppose, without loss of generality, that deg(x) = 2 and deg(y) > 2. Instead of selecting x, refer figure 6, let node y be selected to start with and at the k^{th} stage it is found that x is an adjacent node of $\mathbf{v_k}$ then it leaves no alternative but to backtrack to the earliest available option from $\mathbf{v_{k-1}}$ otherwise the visit to x shall form a cycle of length < n. On the other hand if x is selected then y can always be ignored as it is in NGBR and alternative node to move ahead is available. Dotted lines in the figure 4 indicate the adjacency to y from k^{th} node (current subgraph H).

When deg(x) > 2 and deg(y) > 2 and both yield no dangle node when dropped then any one can be selected to leave the start node and other to arrive at. Same is true when both yield single dangle node when dropped from G. When one yields no dangle and other yields one dangle node then the first is selected to keep wider option available at the next step and hence reducing the number of possible backtracking later on to nodes $\mathbf{v_3}$ or any node visited thereafter. It is in no way contradictory to previous one when a node with degree 2 is preferred over other one.

Case 2: when m > 2. Because $\mathbf{v_1}$ is of minimum degree therefore $\forall x \in L(\mathbf{v_1})$, deg(x) > 2 and algorithmic step 2.2.2 is applicable to select a node $\mathbf{v_2}$. Obviously at this stage no node x can yield any dangle node. Tie is broken as per the coding of adjacency matrix M for G. Correctness follows from lemma 2.♦

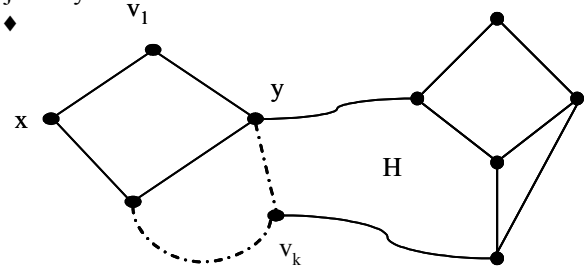


Figure 6

After proving the correctness of step 2, it is turn to show the correctness of step 3 and 4 of algorithm. Let $\mathbf{v_k}$ be the current node visited at the K^{th} iteration. It is essential to establish that in a Hamiltonian graph ∃ no valid current node $\mathbf{v_k}$ such that it is adjacent to more than one node of degree 2, and, backtracking from it is not possible. This excludes the start node. A current node is taken in context of the present subgraph H of G after successive removal of the visited nodes. A current node is said to be valid if and only if it either leads to a Hamiltonian cycle (possibly with backtracking) or helps in concluding that graph is nonhamiltonian at that stage itself. The hypothesis is proved in Lemma 3 and the hypothesis that a valid current node has at least one adjacent node in a Hamiltonian graph is proved in Lemma 4.

Lemma 3: In a Hamiltonian graph a valid current node cannot be adjacent to n > 1 nodes of degree 2, excluding start node.

Proof: Let the current node be $\mathbf{v_k}$ and y and z be two adjacent nodes of $\mathbf{v_k}$ such that both are of degree 2 none is equal to $\mathbf{v_1}$. Node $\mathbf{v_k}$ is dropped once its neighbour is visited. It causes the degree of y and z reduced to one. While arriving at $\mathbf{v_1}$ in order to complete the HC either y or z is left out. This is contradiction to the assumption that graph is Hamiltonian.♦

Lemma 4: A valid current node has at least one adjacent node in the current sub graph in a Hamiltonian graph.

Proof: Let $\mathbf{v_k}$ be the current node in the current subgraph H of G. Lemma 1 and lemma 3 imply that every node is of minimum degree two. Let y and z be two such adjacent nodes to $\mathbf{v_k}$. If $\mathbf{v_k}$ is visited before visiting both y and z, or $\mathbf{v_k}$ is visited after y but before z or vice versa then the result is obvious. In the case when $\mathbf{v_k}$ is visited possibly after visiting y and z both, then in order to complete HC in G, there must be another arc as exit route from $\mathbf{v_k}$ and hence an adjacent node.♦

Let $L(\mathbf{v_k}) = \{y \mid y \text{ is adjacent to current node } \mathbf{v_k}\}$. A node $y = \mathbf{v_{k+1}} \in L(\mathbf{v_k})$ is taken to visit next using step 3 and step 4 of the algorithm. Step 3.1 does not leave any option whereas step 3.2 is preferred because of reason proved in case 1 of theorem 2. Backtracking at 3.2 is restricted because selection of any node

$$x \in L(\mathbf{v_k}) - \{y \mid y \in L(\mathbf{v_k}) \text{ and degree}(y) = 2\}$$

would make y dangle. Correctness of the step 3.1 and 3.2 is implied from lemma 3. Again from second part of case 1 of theorem 2, step 3.3 is preferred over 3.4. Since current node may not satisfy the condition of minimum degree node of original graph G, a provision of possible backtracking is kept wherever tie breaking is not possible. Precedence and correctness of the steps is implied from lemma 2 and 3.

Step 3.5 finds node from NGBR which are possibly available and not considered in step 3.3 and 3.4 in order to ensure that a cycle of length < n is not formed prematurely. This step is executed if it is not possible to find a node in 3.3 or 3.4. Correctness of precedence of steps in order of 3.1, 3.2, 3.3, 3.4, 3.5.1 and 3.5.2 is derived from Lemma 2, 3 and theorem 2. After selection of a node in step 3, the post condition is:

$\pi : \mathbf{v_1 v_2 v_3} \ldots \mathbf{v_{k+1}}$
$H = H - \{\mathbf{v_k}\}$
$NGBR = L(\mathbf{v_1}) - \{\mathbf{v_{k+1}}\}$
ARTPNT = As determined.
BACKTRACK $[\mathbf{v_{k+1}}]$ = {x | x ∈ $L(\mathbf{v_k})$ and x satisfies criteria of 3.3 or 3.4 based on which $\mathbf{v_{k+1}}$ has been selected to move on.}

A node **y** selected in step 3.5 is from NGBR only. It implies that current node $\mathbf{v_k}$ has more than one adjacent nodes and degree(y) > 2 otherwise it would have been selected in either step 3.1 or step 3.2. It further implies that there is no non NGBR node adjacent to $\mathbf{v_k}$ that satisfies 3.3 and 3.4. If there exists more than one nodes satisfying 3.5.1 or 3.5.2 then a node is selected without noting the tied node for backtracking later on. It is implied from lemma 2 that backtracking to any

node latter on does not yield any otherwise result. This provides the proof for postulate (d). The proof of the next postulate (e) is given in theorem 3.

Theorem 3: A graph G is Hamiltonian, if and only if only start node is left at the end of the execution of the algorithm.

Proof: *If only start node* $\mathbf{v_1}$ *is left at the end of the execution of the algorithm then G is Hamiltonian:*

If the algorithm terminates with one node $\mathbf{v_1}$ left subgraph H, it ensures that all intermediate nodes have been visited and subsequently removed. It proves that all nodes starting from the start node have been visited exactly once before finally arriving at start node, therefore forming a HC.

If G is Hamiltonian then only start node is left at the end of the execution of the algorithm:

From lemmas 3 and 4, it is always possible to find an adjacent node to currently visited node in a Hamiltonian graph using the algorithm. Thus at the end only start node $\mathbf{v_1}$ is left when algorithm successfully terminates.♦

Corollary: If more than one node is left when algorithm terminates then G is nonhamiltonian.

Proof: This can be proved by method of contra positive. The 'only if' part of theorem 3 may be stated contra positively as "If not 'only start node is left at the end of the execution of algorithm' then graph is not Hamiltonian'". It can be further stated in simplified language as "if more than one node is left when algorithm terminates then G is nonhamiltonian". Proof is obvious from second part of theorem 3.♦

The important thing for any algorithm is not only to find a correct solution when it exists but to terminate after a finite number of steps in every case. The loop due to step 4 terminates when either or both of the following conditions are met.

i) Number of nodes in the leftover current sub graph is reduced to 1, or/and
ii) No suitable node is found to visit next.

In case (ii) the loop due to step 4 is possibly restarted subject to availability of a node to backtrack. Now it remains to prove that the algorithm terminates in all cases. It is implied from lemma 3 and 4 that the algorithm always returns a node to visit next from the current node if a graph is Hamiltonian. Whenever a valid node is returned to visit next, the number of nodes in the graph is reduced by 1. At the end, the subgraph contains start node only. The step 4 terminates and algorithm goes to step 5. 'If' part of this step ensures the termination.

On the other hand, if a graph is nonhamiltonian then the algorithm goes to step 5 either from 2.2.3 or from 3.5.2. In case of step 2.2.3 there is no possibility of backtracking and hence number of nodes left at that time is > 2. Whereas if control is transferred to step 5 from 3.5.2 then either backtracking is possible to step 3 or it is not possible. In former case, the loop at step 3 and 4 is restarted from a node stored at step 3.3 or 3.4. The node considered once is not considered again for backtracking and therefore ultimately ensures termination of algorithm. This is ensured by step 5. In the latter case the algorithm terminates there.

5. ANALYSIS OF THE ALGORITHM

Determining time complexity of an algorithm requires derivation of an expression that finds number of steps needed to complete the task as a function of the problem size **n** and is to be considered modulo a multiplicative constant [25, 29]. Objective of this section is to compute time complexity of the algorithm in best, worst and average cases [32, 33, 34]. The computation takes into consideration possibility of backtracking in case of tie breaking rules become insufficient.

The algorithm consists of the following major components.

(i) Step 1 and Step 2 are executed once and in sequence.
(ii) Step 3 and step 4 are repeated (n – 2) times.
(iii) Step 5 may force back tracking.

Time complexity of algorithm depends upon number of nodes **n** and edges **e** in G [30, 31]. Step 1 finds start node and it executes in $O(n^2)$ times. Step 2 is executed once and in sequence with step 1. Let time complexity of the step 2 be f(n) to be computed later. Next step 3 and 4 are repeated n times. Let its time complexity be h(n) to be computed later. Hence, the time complexity H(n), of the algorithm is

$$H(n) = O(n^2) + f(n) + O(n * (h(n)) * B(n) \quad \text{.....(1)}$$

Here B(n) is a time complexity function due to possible backtrack. There are three sub steps within step 2. Step 2.1 computes set NGBR. The set union operation is of O(1) as it simply appends a node adjacent to Start node to set NGBR. Append operations may be executed at the most (n – 1) times when all other nodes are adjacent to start node i.e. when graph is complete. Matrix encoding of the graph ensures that no checking of prior presence of a node is required before putting the node in NGBR. Thus step 2.1 if of O(n).

Within step 2.2, 2.2.1 is of O(n). Step 2.2.2 and 2.2.3 can be put within a loop that executes in $O(n^2)$ time complexity. Thus step 2.2 is of $O(n^2)$. In step 2.3, set difference operation

NGBR = NGBR – {Current_node}

is performed in O(n) times. Existence of an articulation point in a graph is determined by applying depth first traversal (DFS) algorithm, which of order of number of edges in the graph i.e. $O(n^2)$ in the worst case. Therefore,

$$f(n) = O(n) + O(n^2) + O(n^2)$$

$$= O(n^2) \quad \text{.....(2)}$$

Turning to step 3, it is repeated n, in fact (n – 1) times due to step 4. It contains six sub steps. In order to initiate the task a list of adjacent nodes is constructed which is of O(n). Then from 3.1 to 3.6 steps are executed in sequence. Step 3.1 and 3.2 are of O(1) and O(n) respectively. Step 3.3 and 3.4 are of $O(n^3)$. Tie, if any, is broken in O(n) and BACKTRACK list is updated in O(1) and that too in sequence, therefore step 3.3 and 3.4 remains of $O(n^3)$.

Next Step 3.5 is of O(n) average case as number of such node shall be minimum. However in worst case it may be of $O(n^2)$. Step 3.6 performs all tasks that step 2.3 performs. In addition to that step 3.6 drops the node just previously visited. The task is performed in O(n) time. Thus, step 3.6 is of $O(n^2)$. Time complexity h(n) of step 3 and 4 therefore can be written as

$$h(n) = O(n) + O(n^3) + O(n^2)$$

$$= O(n^3) \quad \text{.....(3)}$$

Substituting values (2) and (3) in equation (1), the complexity **H(n) is O(n^4 *B(n))**. The B(n) factor is applicable when backtracking is unavoidable from third node onward. Though backtracking is required to a few (one or two) nodes in a few graphs, statistically, even then it can not be overlooked in the worst case.

In the best case, if every node is adjacent to a few nodes e.g. two or three, then f(n) and h(n) are of order n and hence H(n) is of O(n^2). In general, number of adjacent nodes decreases as the algorithm progresses. This happens because of removal of intermediate nodes. In a complete graph, it will be (n – 1), then (n – 2), then (n – 3) and so on. And towards the end, it will be 4, 3, 2 and finally left with one. Therefore while computing f(n) and h(n), steps 3.3 and 3.4 are considered for (n – 1)(n – 2) then for (n – 2)(n – 3) and so on up to 3*2, 2*1 times. The average number of time then steps 3.3 and 3.4 are executed is

$$= \frac{(n-1)(n-2) + (n-2)(n-3) + ... + 3*2 + 2*1}{n}$$

$$= \frac{1}{n}\left(\sum_{i=2}^{n-1} i^2 + \sum_{i=2}^{n-1} i \right) = O(n^2)$$

Considering call to set membership function, h(n) shall return a complexity of O(n^3) and f(n) of O(n^2). If gradual removal of nodes are taken into consideration then algorithm may not enter into nested loop like construct of 3.3 and 3.4 all the times. In this case h(n) and f(n) shall return complexity of O(n) for some node. If about 50% call enter into nested loop and remaining return without entering into it then amortized analysis yields time complexity of O(n^2) for h(n). It means H(n), the complexity of the algorithm, is of O(n^3*B(n)) from equation (1) in average case.

6. CONCLUSION

The algorithm presented in the paper has been tested on large number of graphs varying from simple to very complex up to the tune of 300 nodes. The algorithm is programmed in C language and adjacency matrix is used as data structure to store graph. A graph is pre-processed using line-sweeping [37] algorithm, to merge all nodes in a linear component. It is found that the algorithm executes in polynomial time in most of the time. Number of backtracking required is almost negligible. But unless the algorithm is improved to completely prevent the backtracking from third node onward, it can not be claimed of the polynomial time.

The gist of algorithm is to visit next node, prune the graph by dropping the visited intermediate node as and when its neighbour is visited. While selecting the neighbour to visit next, it is ensured that no backtracking to the current node will be needed in many cases to confirm the result. Wherever there is absolutely no way to break the tie, provision to keep the option open for backtracking is made. Number of nodes to be explored, next, is reduced at every step due to pruning. This reduces the complexity of the algorithm from n! to polynomial of degree 3. In worst case, when backtracking is required, the complexity calculation is generalized to non polynomial.

The presented algorithm may be further improved to evolve tie breaking rule(s) to prevent backtracking in steps 3.3 and 3.4. If it so happens, it might be a breakthrough in the field of graph algorithm and theory of algorithmic complexity. The algorithm presented may find its application in many areas. The author of this paper is using it in steganographic technique using graph theoretic approach.

7. ACKNOWLEDGEMENT

I am thankful to my friends and students who occasionally come to me for guidance in Discrete Mathematics, Theory of Computation and Analysis & Design of Algorithms. I am grateful to all those who constantly encouraged me to go for such academic work besides the work which I am doing in NIC. I remain indebted to my teachers and colleagues who have supported in many ways in completing the work. At the last but not the least, I place my sincere thanks to all anonymous referees/reviewers who gave very critical judgement and suggestions to improve upon algorithm and overall presentation of the paper.

REFERENCES

[1]. A. M. Frieze, "Limit Distribution for the Existence of Hamiltonian Cycles in a Random Bipartite Graph", European Journal of Combinatorics (1985) 6, 327-334.

[2]. Akiyama, Takanori, Nishizeki, Takao and Saito, Nobuji, NP-completeness of the Hamiltonian cycle problem for bipartite graphs. J. Inf. Process. v3 i2. 73-76.

[3]. Alfred V. Aho, John E. Hopcroft, and Jeffrey D. Ullman, 1974, The Design and Analysis of Computer Algorithm, Addison-Wesley.

[4]. Berge C. 1962, Theory of Graphs and its Application, Methuen Press.

[5]. Berge, Graphs and Hypergraphs, Elsevier Science Ltd, 1985.

[6]. Bertossi, Alan A., Finding Hamiltonian circuits in proper interval graphs. Inform. Process. Lett. v17 i2. 97-101.

[7]. Bertossi, Alan A., The edge Hamiltonian path problem is NP-complete. Inform. Process. Lett. v13 i4-5. 157-159.

[8]. Bollob~s, 'Almost all regular graphs are Hamiltonian', European Journal of Combinatorics 4 (1983) 311-316.

[9]. Chvátal, V., Hamiltonian cycles. In: Wiley-Intersci. Ser. Discrete Math, Wiley, Chichester. pp. 403-429.

[10]. Corneil, D.G., Lerchs, H. and Stewart Burlingham, L., Complement reducible graphs. Discrete Appl. Math. v3. 163-174.

[11]. E. Shamir, 'How many edges are needed to make a random graph Hamiltonian?' Combinatorica (1983).

[12]. G. A. Dirac, 1952, Some theorems on abstract graphs, Proc. London. Math. Soc.2.

[13]. Garey, M.R., Johnson, D.S. and Endre Tarjan, R., The planar Hamiltonian circuit problem is NP-complete. SIAM J. Comput. v5 i4. 704-714.
[14]. Haiko Müller, Hamiltonian circuits in chordal bipartite graphs, Discrete Mathematics, v.156 n.1-3, p.291-298, Sept. 1, 1996
[15]. Itai, Alon, Papadimitriou, Christos H. and Szwarcfiter, Jayme Luiz, Hamilton paths in grid graphs. SIAM J. Comput. v11 i4. 676-686.
[16]. J. A. Bondy and U.S.R. Murty, 1976, Graph Theory with Applications, North-Holland.
[17]. J. Blazewicz , A. Hertz , D. Kobler , D. de Werra, On some properties of DNA graphs, Discrete Applied Mathematics, v.98 n.1-2, p.1-19, Nov. 15, 1999.
[18]. Jacek Błazewicz , Marta Kasprzak, Complexity of DNA sequencing by hybridization, Theoretical Computer Science, v.290 n.3, p.1459-1473, 3 January 2003.
[19]. Jacek Blazewicz , Marta Kasprzak, Computational complexity of isothermic DNA sequencing by hybridization, Discrete Applied Mathematics, v.154 n.5, p.718-729, 1 April 2006.
[20]. Jan van Leeuwen, 1990, Handbook of theoretical computer science, MIT Press.
[21]. Jitender S. Deogun , George Steiner, Polynomial Algorithms for Hamiltonian Cycle in Cocomparability Graphs, SIAM Journal on Computing, v.23 n.3, p.520-552, June 1994 [doi>10.1137/S0097539791200375].
[22]. Karp, Richard M., Reducibility among combinatorial problems. In: Complexity of Computer Computations (Proc. Sympos., IBM Thomas J. Watson Res. Center, Yorktown Heights, N.Y, 1972), Plenum, New York. pp. 85-103.
[23]. Knuth, D. E., 1973, The art of Computer Programming, vol 1, Fundamental algorithm, Addison-Wesley Publishing Company.
[24]. Lawler, Eugene L., Combinatorial Optimization: Networks and Matroids. 1976. Holt, Rinehart and Winston, New York.
[25]. Lewis, Harry and Christos Papadimitriou, 1978, "The efficiency of algorithms, Scientific American", 238:96-109.
[26]. M. Held and R. M. Karp, ' A dynamic programming approach to sequencing problems', SIAM Journal on Applied Mathematics 10 (1962) 196-210.
[27]. M. R. Garey, D. S. Johnson, and L. Stockmeyer. Some simplified NP-complete problems. Proceedings of the sixth annual ACM symposium on Theory of computing, p.47-63. 1974.
[28]. Mark Keil, J., Finding Hamiltonian circuits in interval graphs. Inform. Process. Lett. v20 i4. 201-206.
[29]. Michael R. Garey and David S. Johnson (1979). Computers and Intractability: A Guide to the Theory of NP-Completeness. W.H. Freeman. ISBN 0-7167-1045-5. A1.3: GT37–39, pp.199–200.
[30]. Karp, R. M., & Steele, J. M. (1985). Probabilistic analysis of heuristics. In The Traveling Salesman Problem, pp. 181-205. John Wiley & Sons, Essex, England.
[31]. Rubin, Frank, "A Search Procedure for Hamilton Paths and Circuits'". Journal of the ACM, Volume 21, Issue 4. October 1974.
[32]. Selmer Bringsjord & Joshua Taylor, P = NP, Department of Cognitive Science, Department of Computer Science, RAIR Lab, RPI, Troy, NY
[33]. Sipser, M. 1992, The history and status of the P verses NP question, in Proceedings of the 24th Annual ACM Symposium on the Theory of Computing, pp 603-618.
[34]. Stephen Cook, 2000, The P versus NP Problem, Official Problem Description, Millennium Problems, Clay Mathematics Institute.
[35]. T.I. Fenner and A.M. Frieze, 'on the Existence of Hamiltonian Cycles in a Class of Random Graphs', Discrete Mathematics 45(1983) 301-305.
[36]. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, 1998, Introduction to Algorithms, PHI.
[37]. Vinay Kumar, and Sharma, V. (2006) 'Overcoming 64kb data size limit in handling large spatial data in GISNIC while cleaning and building topology', Int. J. Information Technology and Management, Vol. 5, No. 1, pp.77–86.
[38]. Vinay Kumar, 2002, Graph Theory, Chapter 7, Discrete Mathematics, Ed 1, BPB Publication, New Delhi, India.

Traffic Generation Model For Delhi Urban Area Using Artificial Neural Network

Shivendra Goel[1], J. B. Singh[2] and **Ashok Kumar Sinha[3]**

Abstract - Transport facility and socio-economic structure for a city are interdependent resulting into improved transport infrastructure, which in turn influences socio-economic growth. As the society evolves it generates transport demand. The classical transportation planning methods are based on simple extrapolation of trends. Some mathematical models like linear regression models have also been used by researchers for estimating traffic generation for future period, however, these models do not account for nonlinearly in the model. In the present paper Artificial Neural Network Model has been used in modal Traffic Generation in Delhi Urban Area .ANN models account for nonlinear relationship between independent variables and the dependent variables. Future estimates of percentage of traffic generation by cars, buses and smaller vehicles in the inner, middle and outer areas of urban Delhi have been derived using the ANN. The model is implemented on MATLAB and the error in the training phase of ANN is quite low.

Index Terms - ANN - Artificial Neural Network

1. NTRODUCTION

1. 1 Different Phases of urban Transportation Planning

Trip generation is the first step in the conventional four-step urban transportation Planning process, widely used for forecasting travel demands. It predicts the number of trips originating in or destined for a particular traffic analysis zone. Urban area is divided into several traffic zones which are the clusters of households and socio-economic activities.

Trip distribution (or **destination choice** or **zonal interchange analysis**), is the second component (after trip generation, but before mode choice and route assignment) in the traditional four-step urban transportation planning process. This step matches trip makers' origins and destinations to develop a "trip table" a matrix that displays the number of trips going from each origin to each destination. Gravity model, entropy maximization models are widely used for trip distribution analysis [3].

Mode choice analysis is the third step in the conventional four-step urban transportation Planning process. Trip distribution's zonal interchange analysis yields a set of origin destination tables followed by; mode choice analysis allows the modeler to determine which mode of transport will be used.

Traffic assignment concerns the selection of routes (alternative called paths) between origins and destinations in transportation networks. It is the fourth step in the conventional urban transportation planning process. The zonal interchange analysis of trip distribution provides origin-destination trip tables. Mode choice analysis tells which travelers will use which mode. To determine infrastructure requirement, its cost and benefit, we need to know the number of travelers on each route and link of the network (a route is simply a chain of links between an origin and destination). We need to undertake traffic (or trip) assignment exercise.

The Paper on "Planning for unpredictable future: Transport in Great Britain in 2030" by Kiron Chatterjee & Andrew Gordon [1], explores alternative future scenarios for Great Britain in the year 2030 and the Implications these have for travel demand and transport provision. In this paper author made a National transport model to forecasts the national road traffics. In this work no mathematical model has been developed where income could be a parameter for estimating trip generation. In Indian context wide income disparity which plays a dominant role in trip generation and modal choice behavior.

This paper attempts to model the traffic generation percentage in Delhi urban area by different modes such as car, buses and two wheelers in Delhi. Delhi urban area has been divided in the following Categories i.e. Delhi inner areas, Delhi middle areas and Delhi outer areas.

Delhi Inner Area consists of the following areas of Delhi region, it includes Dhola Kuan, Raja Garden, Azadpur, ISBT, B.S. Gurudwara, AIIMS.

Delhi Middle Area consists of the following areas of Delhi region, it includes Ashoka Road, Bara Khamba Road, Janpath, ourter circle (CP), Sansad Marg, K.G. Marg, Inner Circle CP, Punckuin Road, Tolstoy marg, Rajpath Road.

Delhi Outer Area consists of the following areas of Delhi region, it includes Singu Border (NH1), Badarpur Border (NH1), Rojokari Boarder (NH8), Shahadra(NH24), Kalindi Kunj, M.G. Road (Aaya Nagar), Old Gurgaon Road, Tikri Border (NH10), Gazipur (NH24 ByPass) Mohan Nagar Border, Loni Border, Noida Link Road.

Artificial Neural Network has been used as a model for the above analysis.

2. ETHODOLOGY

2.1 Artificial Neural Network Model:

The architecture of the ANN consists of three layers namely input layer, hidden layer and output layer [3]. The input layer having input matrix denoted by **IW**11 having a source 1(2nd index) and a destination 1(1st index). The vector input 'P' is transmitted through a connection that multiplies its strength by the scalar weight W to form the product w*p. The neuron has a scalar bias 'b'. The bias 'b' is being added to the product w*p at summing junction by shifting the function 'f' to the left by an amount 'b'. The bias is much like a weight, except that it has a constant input of 1. The activation function net input 'n', is the sum of the weighted input w*p and the bias 'b'. This sum

[1]*Research Scholar, Shobhit University, Meerut*
[2]*Director, Shobhit University, Meerut*
[3]*Dean (Computer Science), ABES Engineering College, Ghaziabad*
E-mail: [1]shivendragoel@gmail.com,
[2]jbs.tomar@shobhituniversity.ac.in and
[3]aksinha@computer.org

is the argument of the activation function f_1. Here f_1 is activation function typically a sigmoid function, which takes the argument 'n' and produces the output 'a', weight 'w' and bias 'b' both are adjustable scalar parameters of the neuron. The central idea of neural networks is that such parameters can be adjusted so that the network exhibits the desired behavior. Thus we can train the network to do a particular job by adjusting weight or bias parameters or the network itself will adjust these parameters to achieve some desired end. The next section will be layer weight (LW).

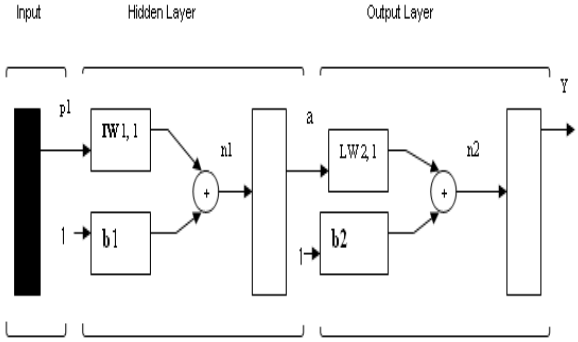


Figure 1a: Lay out of the multi-input multi-layer feed forward ANN.

In the present paper the ANN applied to traffic modeling is implemented in two phases viz training of the network based on part data and then estimating the output i.e. the traffic generated by socio-economic activities in Delhi urban area in percentage by cars, buses and two wheelers in the year 2021

Proposed Model

Percentage of Vehicle type C is Dependent on the Population (P) of Delhi and Per Capital Income (PCI) of Delhi.

C=f (P, PCI). Fig 1b shows the ANN Model for Proposed Model.

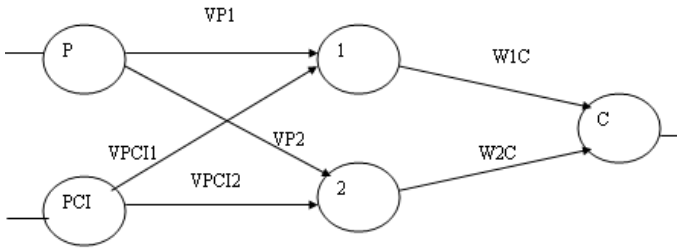


Figure 1b: ANN Model for Proposed Model

3. HYPOTHESIS OF THE MODEL

The proposed model Calibrated for different vehicle types like cars, buses and two wheelers for various zones in Delhi Urban areas

(i) Zone: Inner area

Vehicle type: cars

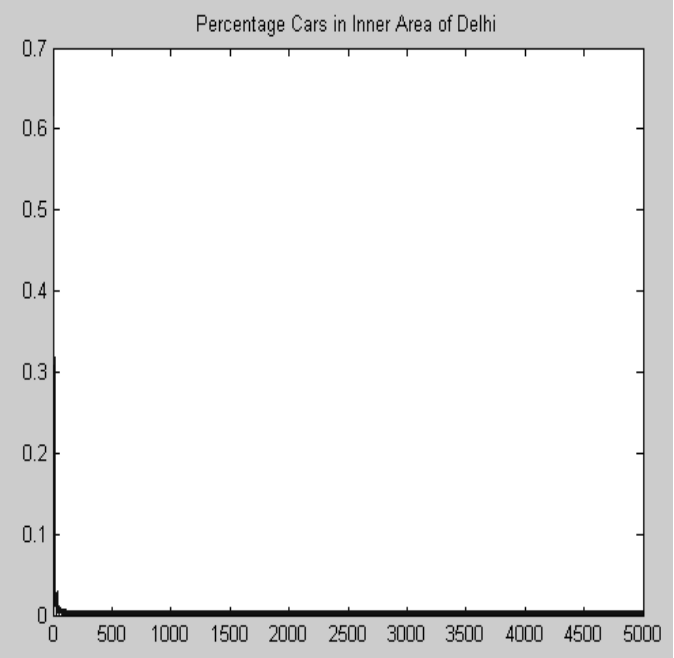
Data on the input variables are given in tables-1 and 2 and the error plot after training of ANN is given in errorgraph-1.

Year	Population of Delhi(P)	Per Capita Income of Delhi in Rupee.(PCI)
1991	9421000	12500
1994	10700000	17355
1997	12000000	25500
2000	13500000	29623
2002	14526000	31500

Table 1: Source [6&7]

Year	Percentage of Car in Inner Area (CI).
1991	27
1994	30
1997	33
2000	36
2002	38

Table-2: Source [6&7]



Error Graph 1

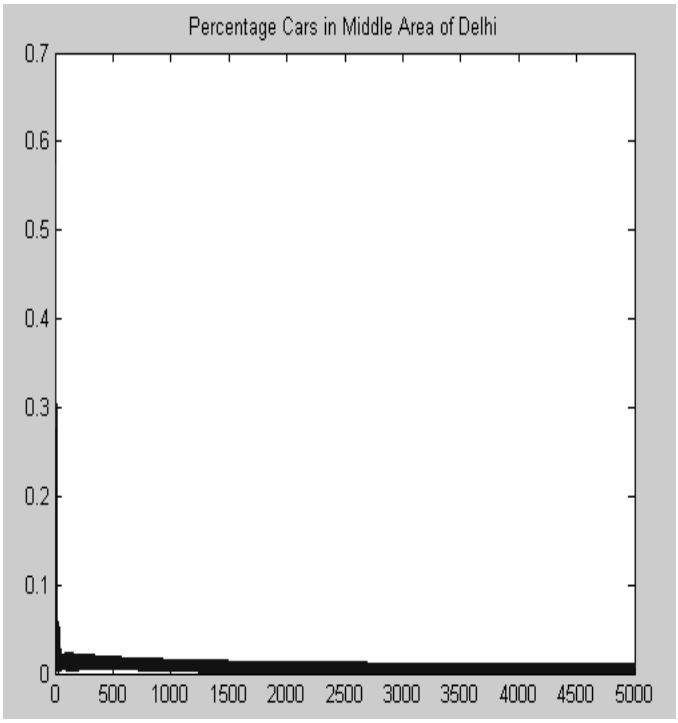
(ii) Zone: Middle area

Vehicle type: Cars

Data on the input variables are given in table1 and 3 and the error plot after training of ANN is given in errorgraphs2.

Year	Percentage of Car in Middle Area (CM).
1991	31
1994	34.5
1997	38.2
2000	41.5
2002	44

Table 3: Source [6&7]

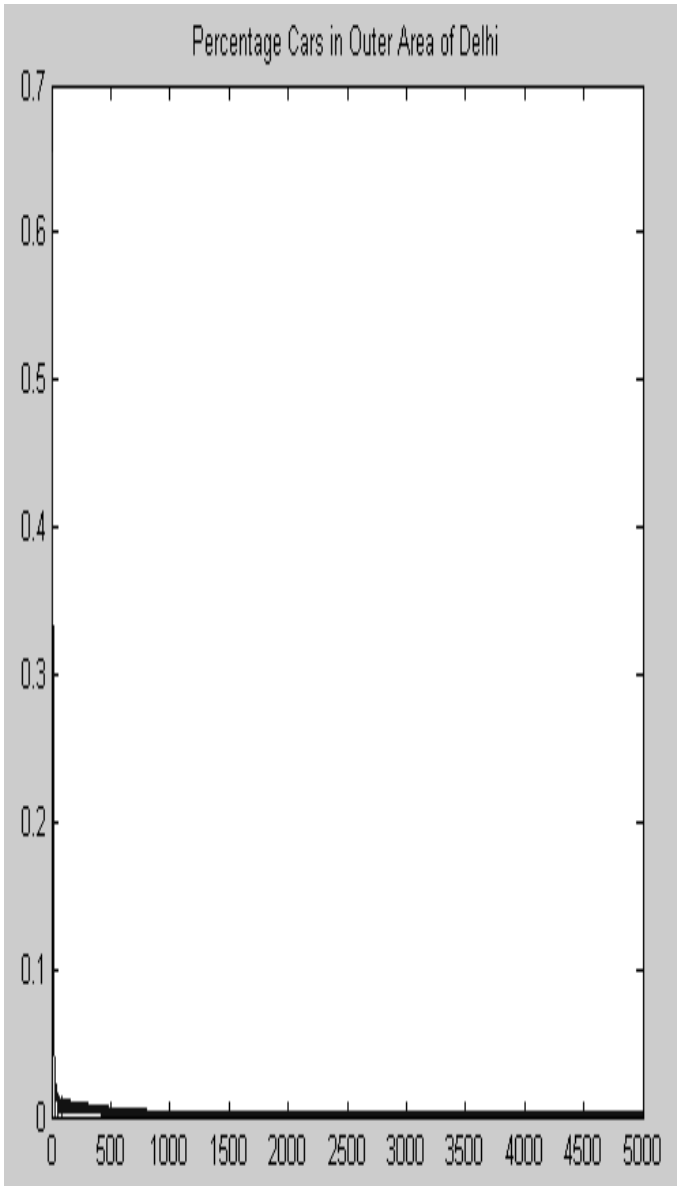


Error Graph 2

(iii) Zone: Outer area
Vehicle type: Cars
Data on the input variables are given in table-1 and 4 and the error plot after training of ANN is given in error graphs-3.

Year	Percentage of Car in Outer Area (CO).
1991	23
1994	25.5
1997	27.9
2000	30.3
2002	32

Table 4: Source [6&7]

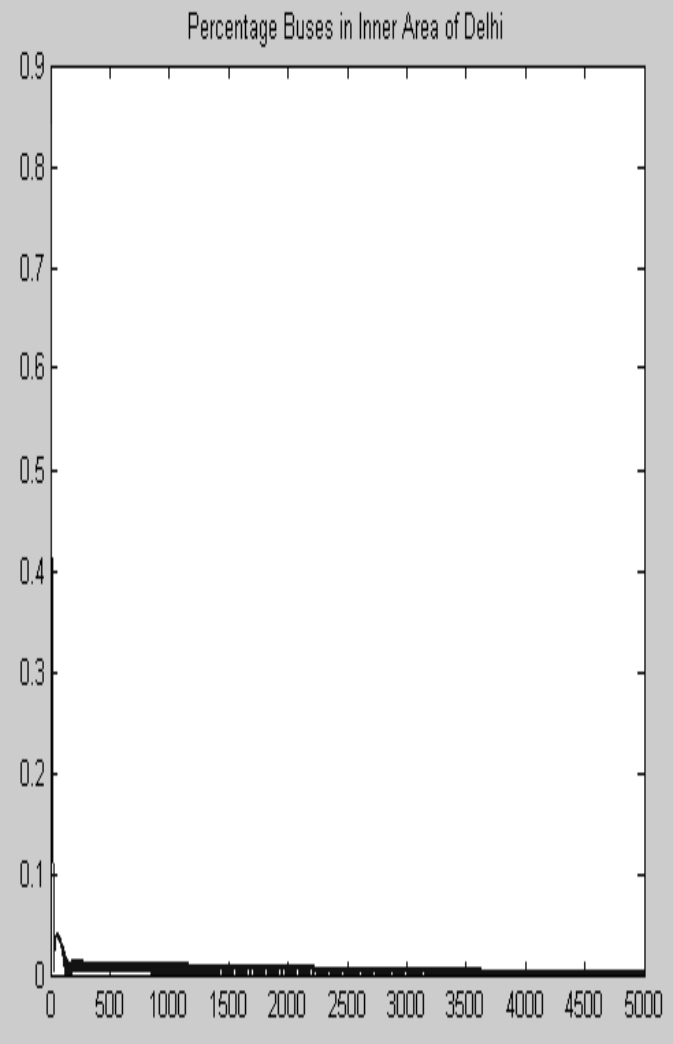


Error Graph 3

(iv) Zone: inner area
Vehicle type: Buses
Data on the input variables are given in table 1 and 5 and the error plot after training of ANN is given in error graphs -4

Year	Percentage of Buses in Inner Area (BI).
1991	6
1994	5.7
1997	5.5
2000	5.3
2002	5

Table 5: Source [6&7]

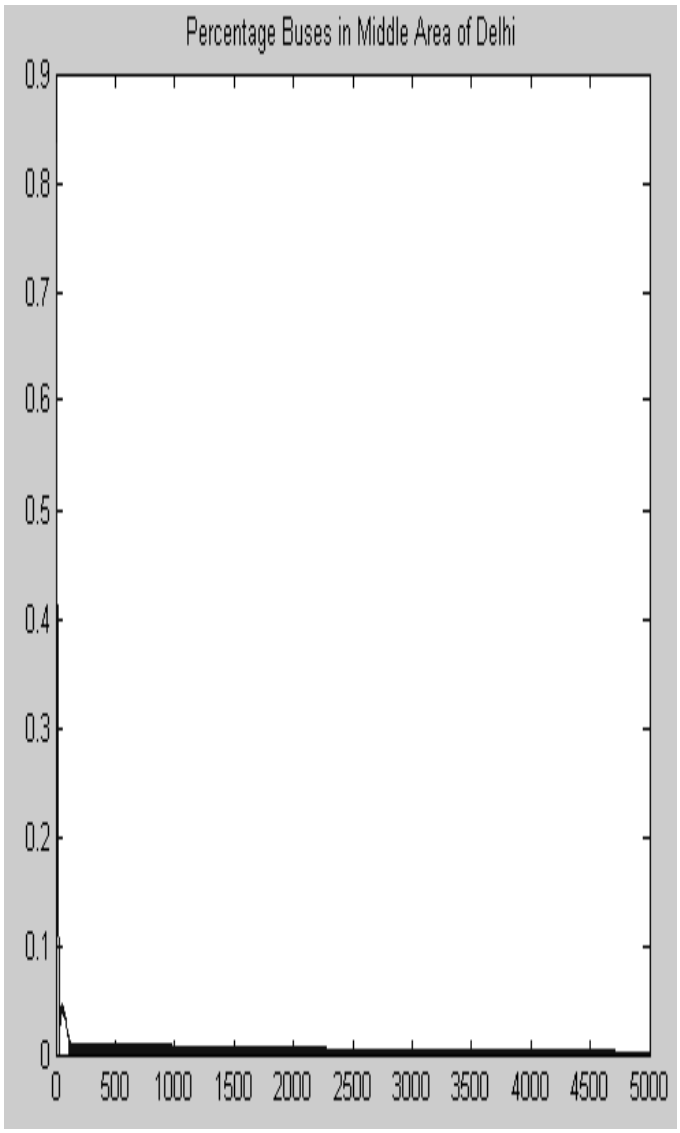


Error Graph 4

(v) Zone: Middle area
Vehicle type: Buses
Data on the input variables are given in table 1 and 6 and the error plot after training of ANN is given in error graph-5.

Year	Percentage of Buses in Middle Area (BM).
1991	6
1994	6
1997	6
2000	6
2002	6

Table 6: Source [6&7]

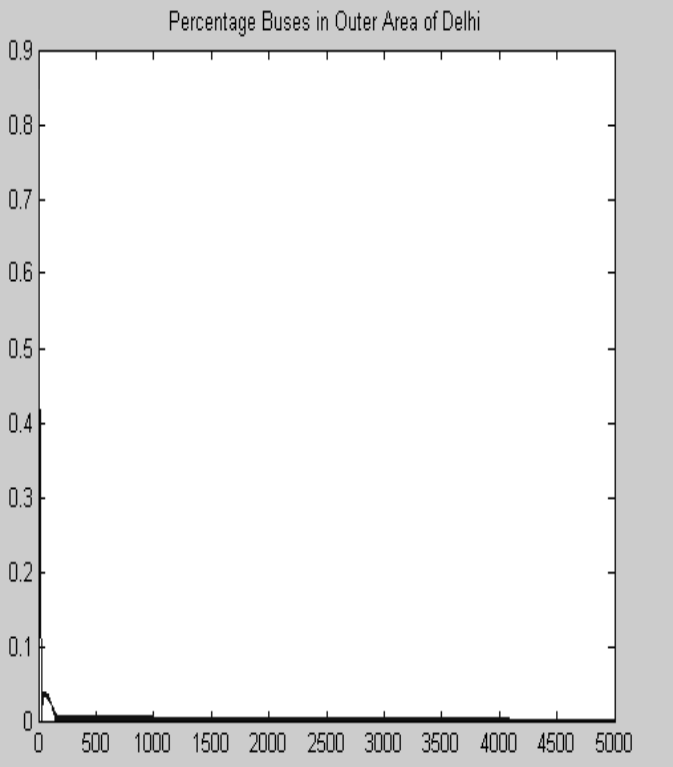


Error Graph 5

(vi) Zone: Outer area
Vehicle type: Buses
Data on the input variables are given in table 1 and 7 and the error plot after training of ANN is given in error graph -6.

Year	Percentage of Buses in Outer Area (BO).
1991	5
1994	5
1997	5
2000	5
2002	5

Table 7: Source [6&7]



Error Graph 6

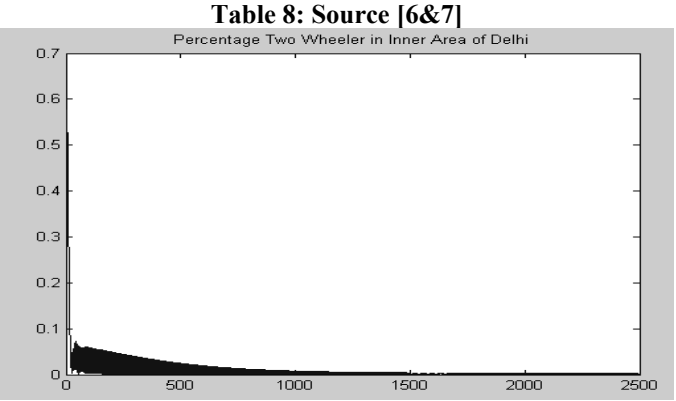
(vii) Zone: inner area

Vehicle type: Two wheelers

Data on the input variables are given in table 1 and 8 and the error plot after training of ANN is given in error graph 7.

Year	Percentage of Two Wheelers in Inner Area (TI).
1991	33
1994	32.7
1997	32.5
2000	32.2
2002	32

Table 8: Source [6&7]



Error Graph 7

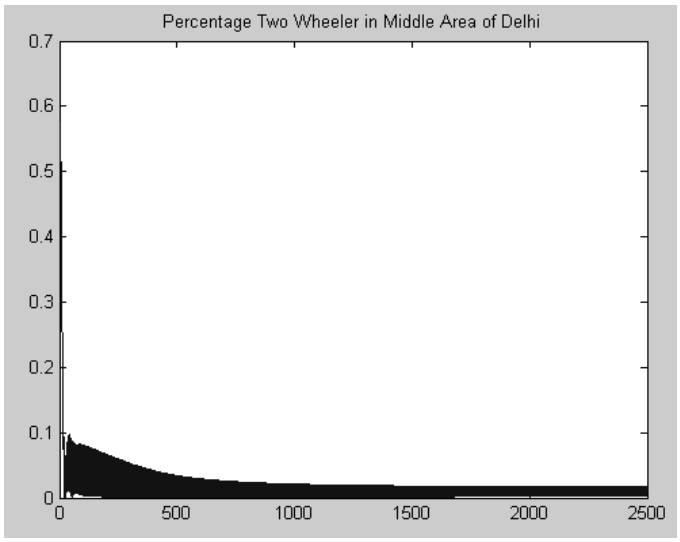
(viii) Zone: Middle area

Vehicle type: Two Wheelers

Data on the input variables are given in table 1 and 9 and the error plot after training of ANN is given in error graph 8.

Year	Percentage of Two Wheelers in Middle Area(TM).
1991	37
1994	35.4
1997	33.7
2000	32.2
2002	31

Table 9: Source [6&7]



Error Graph 8

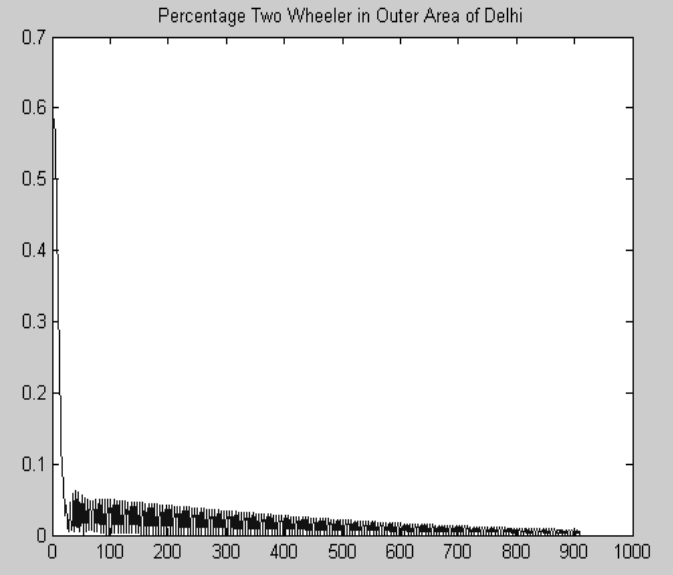
(ix) Zone: Outer area

Vehicle type: Two Wheelers

Data on the input variables are given in table 1 and 10 and the error plot after training of ANN is given in error graph 9.

Year	Percentage of Two Wheelers in Outer Area(TO).
1991	31
1994	31.3
1997	31.6
2000	31.8
2002	32

Table 10: Source [6&7]



Error Graph 9

Note: Data for 1991 and 2002 were directly available. Data for the other years have been interpolated accordingly.

4. RESULTS

As per the master plan of Delhi for 2021

Based on the trend analysis of past population we are assuming approximation 20% growth in population (P) and percapita income (PCI) for next 20 years, the estimates of modewise traffic in different zone are given in the pie chart.

Inner Area

Figure 1 shows the number of cars will be 50 % and number of buses will be 0.2348 % and number of two wheelers will be 18.7436 %.

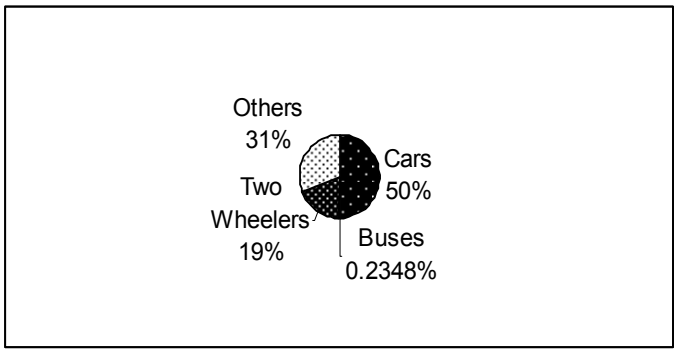


Figure 1: Mode wise traffic in inner area of Delhi in 2021

Middle Area

Figure 2 shows the number of cars will be 50 % and number of buses will be 0.1844 % and number of two wheelers will be 27.2394 %.

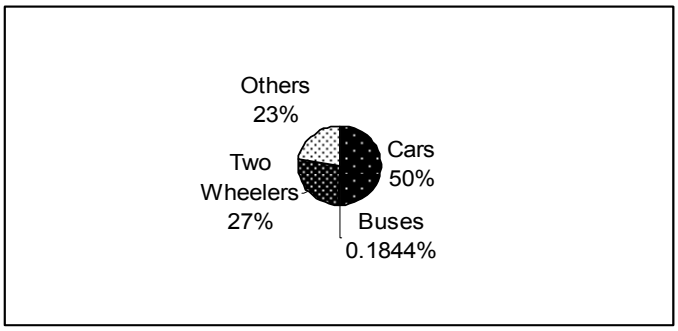


Figure 2: Mode wise traffic in middle area of Delhi in 2021

Outer Area

Figure 2 shows the number of cars will be 50 % and number of buses will be 0.1166 % and number of two wheelers will be 36.5493 %. And of the percentage is share by other mode of Communications.

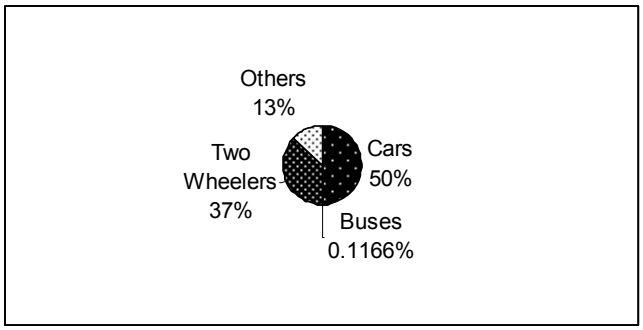


Figure 2: Mode wise traffic in outer area of Delhi in 2021

5. CONCLUSION

The present paper has successfully demonstrated the application of Artificial Neural Network for modeling traffic generation in Delhi Urban Area. The data on socio-economic variables have been collected from Economic Survey of Delhi, Delhi Planning Dept. and C.R.R.I Study 2002.Error generated in training phase is quite low; it is approximately 0.33% on Inner Car Percentage the calculation of error is based on the method of Steepest Descent [8]. The application demonstrates that the relationship between socio-economic variable and transport variable is non-linear which is taken care by ANN.

REFERENCES

[1]. Kiron Chatterjee & Andrew Gordon, "Transport in Great Britain in 2030," ELSEVIER Transport Policy Journal 2006. pp. 254-264.

[2]. Shivendra Goel and Ashok K. Sinha, "Trip Generation Modeling using Artificial Neural Network," 2nd National Conference; INDIACom-2008, at BVICAM, New Delhi. pp. 495-498.

[3]. B. G. Hutchinson – *Principles of urban Transport systems planning;* Mc Graw Hill.

Continued on page no. 250

Design Patterns for Successful Service Oriented Architecture Implementation

G. M. Tere[1] and B. T. Jadhav[2]

Abstract - The successful implementation of Service Oriented Architecture (SOA) relies on a careful and holistic approach to business planning. One of the most important tools in the evaluation, purchase, and ongoing use of SOA is the best practices that vendors, consultants, and customers have developed and used. The promise of business agility, improved customer service, and competitive advantage with SOA is real. What varies most is the time, cost, and ease of SOA implementation. By learning from the experiences of those organizations that have been through the process and looking at the standard best practices of large-scale technology implementations, success can come at earlier stage. The Patterns for e-business are a group of proven, reusable assets that can be used to increase the speed of developing and deploying Web applications. This paper focuses how the Self-Service and Extended Enterprise business patterns, and the Application Integration pattern, can be used to start implementing solutions using the service-oriented architecture approach. Although the model of Web service interoperability is straightforward, it introduces new development practices and methodologies that can be difficult to learn. However, it can be successfully implemented if we recognize certain patterns to design issues.

Index Terms - Adapter, Controller, Design Patterns, Façade, Proxy, SOA.

1. INTRODUCTION

The role of architect is to evaluate business problems and build solutions to solve them. Architect begins by gathering input of the problem, outline of the desired solution, and any special considerations or requirements that need to be factored into that solution[1,2]. The architect then takes this input and designs the solution. This solution can include one or more computer applications that address the business problems by supplying the necessary business functions.

In the real world, web apps are complicated. A popular web site gets thousands of hits per day. To handle this kind of volume, most big web sites create complex hardware architectures in which the software and data is distributed across many machines. A common architecture is configuring the hardware in layers or tiers of functionality. Adding more computers to a tier is known as horizontal scaling and is considered one of the best ways to increase throughput. Most of the software for a big web application lives in either the web-tier or the business-tier. The web-tier frequently contains HTML pages, JSPs, servlets, controllers, model components, images and so on[13,23]. The business-tier contains EJBs, legacy applications, lookup registers, database drivers and databases. Many developers use J2EE containers to solve same problems. They found recurring themes in the nature of the problems they were dealing with, and they come up with the reusable solutions to these problems[4]. These design patterns have been used, tested and refined by other developers. A software design pattern is a repeatable solution for a commonly-occurring software problem.

[1]Department of Computer Science, Shivaji University, Kolhapur 416 004, India
[2]Department of Computer Science Y .C. Institute of Science, Shivaji University Satara - 415 001, India
E-mail: [1]girish.tere@gmail.com and
[2]btj21875@indiatimes.com

2. OVERVIEW OF SOA

SOAs provide modular services that can be easily integrated throughout an enterprise. They are flexible and adaptable to the current information technology (IT) infrastructure and investments. SOA implementations continue their emergence in business as a mechanism for integrating organizational operations in new and different ways and for promoting reuse while leveraging the existing value of legacy systems. In any business, the bottom line is the essential test of any technology. SOA can provide a significant return on investment (ROI) by integrating legacy and mixed technologies and maximizing the value of existing investments while minimizing risk. Promoting reuse through SOA also helps reduce overall development costs. If services and their data are generic enough, they can be accessed through a variety of interfaces. Decoupling services from their presentation reduces expenses and decreases the overall development time. Further, SOA makes IT consider the dynamic operations of an organization, not just a set of static requirements, thereby exposing information and data sharing across the organization and focusing development on the best ways to improve overall operations[3,7,9].

Although SOA brings significant business benefits, there are challenges to their implementation. As SOA services are typically coarse-grained and loosely coupled, their operations exhibit more latency than more tightly coupled implementations. This can be a challenge when implementing with real time requirements. SOA is designed to bring together legacy systems in heterogeneous IT environments. Standardization of naming, definitions, and identification can present implementation challenges. However, these challenges can be resolved by the implementation of identity and naming services. Finally, SOA is designed to cut through an organization horizontally and vertically, which presents many cultural, cooperation, ownership, and budget issues. Strong leadership must be in place, and executive support must be clear and evident in order for any SOA implementation to be a success[21].

Best practices suggest that there is an overall commitment to increase organizational efficiency. These practices must be

considered from the specific context of your organization. Although the notion of best practices is constantly evolving, it's clear that the following areas are critical:

a) Vision and leadership
b) Strategy and roadmap
c) Policies and security
d) Governance and acquisition
e) Operations and implementation

A key benefit of SOA is reuse of services. It's often tempting to build something from scratch instead of reusing what's already available. This can often happen for two reasons. First, developers may not be aware that a similar service already exists. Therefore, it's important to maintain a directory of available services that is readily accessible and uses the common vocabulary adopted across the organization.

Second, when designing and implementing services, their use outside traditional boundaries must be considered. Creating coarse□grained, modular services helps to promote their reuse in the organization. Organizations should not cringe from updating services that have already been deployed when there are additional needs demanding extension of functionality. For example, eventually, all the requirements should be factored into a single 'get Customer' service rather than having multiple services that get different subsets of customer information.

3. BRIEF OVERVIEW OF DESIGN PATTERNS

Patterns are defined as "an idea that has been useful in one practical context and will probably be useful in others"[19]. Patterns are good constructs for designing Web services. Design patterns are reusable solutions to common software design problems. Design patterns speed up the development process through the implementation of tried and tested solutions. They can play an important role in SOA implementation, especially in the standardization of service design. Since their introduction in the late 1980s, numerous patterns have been recognized and documented. Many SOA implementations use Web services[16]. It is important for architects of SOA implementations to have an understanding of the four primary design patterns for Web services:

1. Adapter: Promotes the reuse of existing technologies through wrappers, extending your existing investments
2. Façade: Used to reduce the coupling between the client and the server components—an essential technique for creating the appropriate level of granularity
3. Proxy: Provides an object surrogate, used to simplify the interaction between Web services components
4. Controller: A key component of the Model-View-Controller (MVC) architecture, used as an intermediary between the user interface (UI) and the data[5,7].

[A] Adapter

As previously discussed, promoting the reuse of existing technologies is essential for a successful—and profitable—SOA implementation. The Adapter design pattern, shown in Figure 1, allows compatible classes to work together by converting the interface of an existing class into an interface that clients expect. JCA is Java Connector Adapter[8,9].

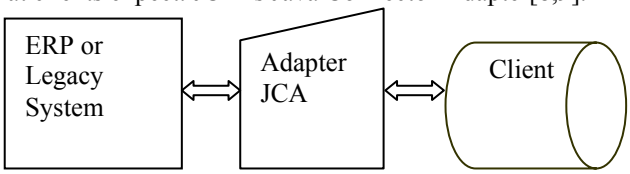


Figure 1: The Adapter design pattern

Organizations will look to reuse existing technologies in their SOA implementations; this is where the Adapter pattern is implemented. Typically, existing technologies provide interfaces that are incompatible with Web services. The Adapter pattern provides a bridge to the existing technology. You don't have to start from scratch when designing Web services: The Adapter pattern can leverage your existing investment and quickly get you started on the road to service implementation. However, it's important to realize that not every application may be a useful service. It's important to be judicious in your design.

Adapter or Wrapper: Used to expose internal application functionality with a different interface. In computer programming, the adapter design pattern (often referred to as the wrapper pattern or simply a wrapper) translates one interface for a class into a compatible interface. An adapter allows classes to work together that normally could not because of incompatible interfaces, by providing its interface to clients while using the original interface. The adapter translates calls to its interface into calls to the original interface, and the amount of code necessary to do this is typically small. The adapter is also responsible for transforming data into appropriate forms. For instance, if multiple boolean values are stored as a single integer but your consumer requires a 'true'/'false', the adapter would be responsible for extracting the appropriate values from the integer value. The Adapter pattern is used to convert the programming interface of one class into that of another. We use adapters whenever we want unrelated classes to work together in a single program.

[B] Façade

Providing the appropriate level of granularity is essential to service design. Services that are too fine grained can increase the overall network traffic as many service requests are made to perform an operation. More coarse-grained services can increase overall latency, but they help expose services that expose a business function. The façade pattern is a software engineering design pattern commonly used with Object-oriented programming. (The name is by analogy to an architectural facade.) Façade: Used to encapsulate complexity and provide coarse-grained services[26].

A façade is an object that provides a simplified interface to a larger body of code, such as a class library. A facade can make a software library easier to use and understand, since the facade

has convenient methods for common tasks; make code that uses the library more readable, for the same reason; reduce dependencies of outside code on the inner workings of a library, since most code uses the facade, thus allowing more flexibility in developing the system; wrap a poorly-designed collection of APIs with a single well-designed API (as per task needs).

An Adapter is used when the wrapper must respect a particular interface and must support a polymorphic behavior. On the other hand, a façade is used when one wants an easier or simpler interface to work with.

Façade defines a higher-level interface that makes the subsystem easier to use. The Façade pattern, shown in Figure 2, is often used to expose coarse-grained services. Instead of exposing the direct, one-to-one functionality of an existing software component or business function, the Façade pattern promotes encapsulation of these lower-level services to provide a single higher-level function

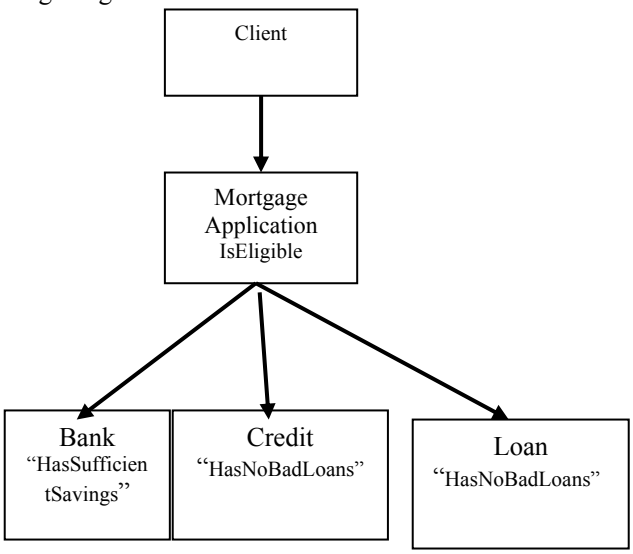


Figure 2: The Façade design pattern

The Façade pattern promotes consistent interfaces, abstracting clients from the implementation details of a service. Further, the pattern facilitates control and management of a service, providing a single entry point that simplifies elements such as security and transaction management. The Façade pattern is a familiar approach to building coarse-grained services. In J2EE, the Façade was represented by a session bean, while the fine-grained components were typically entity beans. For Web services, the same approach can be leveraged. The idea is to take existing components that are already exposed and encapsulate some of the complexity into high-level, coarse-grained services that meet the specific needs of the client. In using this approach, you can enhance overall performance of the Web services interactions and centralize infrastructure services such as security and transactions. Figure 3 shows the relationships between an application's presentation and business tiers using the Façade pattern.

The Façade pattern here is used between presentation and business tiers as a method of encapsulating application logic to address the specific needs of particular clients[3,16].

[C] Proxy

The Proxy design pattern, shown in Figure 4, provides a surrogate or placeholder for another object. It can be used to simplify the interactions among services. The proxy can serve as a

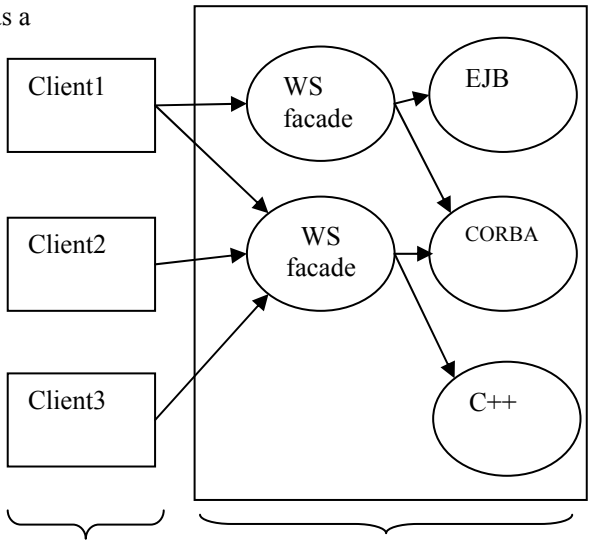


Figure 3: The Façade Pattern.

standardized interface for a collection of legacy back end services. In other words, instead of providing a service for each individual back end service, you can use the proxy to consolidate the messages into a single service, and then dispatch the request to the appropriate back end service, which simplifies the interaction with a collection of services. In computer programming, the proxy pattern is a software design pattern. A proxy, in its most general form, is a class functioning as an interface to something else. The proxy could interface to anything: a network connection, a large object in memory, a file, or some other resource that is expensive or impossible to duplicate. A well-known example of the proxy pattern is a reference counting pointer object.

In situations where multiple copies of a complex object must exist the proxy pattern can be adapted to incorporate the flyweight pattern in order to reduce the application's memory usage. Typically one instance of the complex object is created, and multiple proxy objects are created, all of which contain a reference to the single original complex object. Any operations performed on the proxies are forwarded to the original object. Once all instances of the proxy are out of scope, the complex object's memory may be deallocated.

A proxy is a stand-in for something or someone else. As an actor, you might hire a proxy to attend an autograph signing session. Your proxy is providing a layer between you and your fans, but can forward relevant messages as necessary. You want your proxy to behave as much like you do as possible, so

that the fans believe they are interacting with you directly. Proxy is used as a surrogate for another object or service.

The Wrapper pattern leverages the popular Adapter pattern. The basic idea is to convert a component's interface into another interface that the client expects. This would typically be used to provide some compatibility with the client. The adapter pattern can be used to expose existing technologies as Web services. For example, if you are running on a J2EE platform and have a need to interact with a C++ component, you may wrap the C++ component with JNI code, and then expose that Java interface as a Web service using the available Web services tools.

Proxies in software are similar to proxies in real life. You might create a distributed object proxy. Such a proxy is designed to make its clients think that they are directly interacting with the object, when in reality the object lives in a process on a remote machine. The proxy manages the intricacies of communicating with the distributed object while ensuring that the client remains blissfully ignorant of these details.

The Proxy design pattern can also be used for testing, especially when you are communicating with a third-party object that you do not control. The proxy would implement the same interface as the third party service and can stand in its place during the testing process. Again, this simplifies the testing process.

In the Proxy pattern one object can be used as a surrogate for another, often to offload processing from one component to another. This pattern has been frequently used to hide complexity of the SOAP messaging constructs. It can also be used in the development of mock objects, which have been around for quite some time.

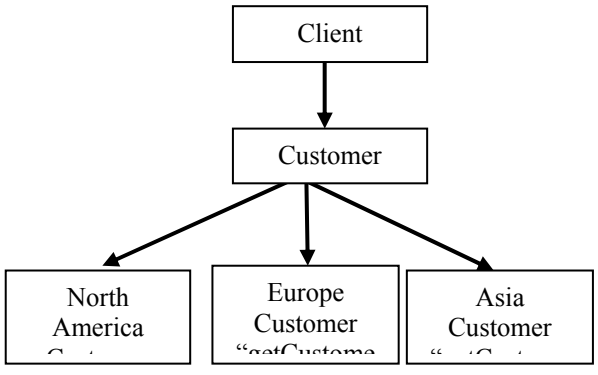


Figure 4: The Proxy design pattern

These are just a few of the design patterns that can readily be applied to Web service development. As you become more comfortable with Web service paradigms, you will find these patterns can guide you just as they do with other types of object-oriented design.

[D] Controller

The Controller design pattern, shown in Figure 5, is probably best known from the MVC application architecture. In the MVC architecture, the model contains the data that the application requires; the view manages the user UIs; and the controller provides the logic and serves as the interface between the model and the view. The Controller design pattern is used to separate the presentation and data layers[5].

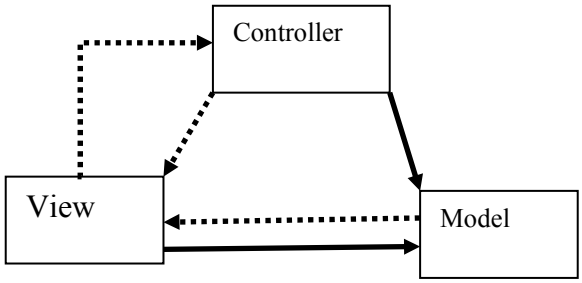


Figure 5: The Controller design pattern

The Controller design pattern can be used in SOA architectures to leverage existing application MVC design architectures and encapsulate the business logic of the service.

4. CONCLUSIONS

SOA best practices are constantly evolving. However, efforts must be made in each of the areas discussed: vision and leadership, strategy and roadmap, policies and security, governance and acquisition, and operations and implementation. Having a skilled professional who has a good understanding of SOA and can communicate that vision to all the stakeholders is essential to a successful implementation.

Look for the easy and achievable goals as you begin your SOA implementation. Establish success with a project; learn from your mistakes as well as from your success. An incremental and agile approach will be essential.

Whether design patterns are a familiar tool or a new concept, an understanding of the four key design patterns—Adapter, Façade, Proxy, and Controller—will be essential to SOA implementation. Begin with indentifying the services you need to implement, and then look to see how they fit into one of these patterns.

REFERENCES

[1]. Booch, Gary, SOA Best Practices, Software architecture, software engineering, and Renaissance Jazz blog www-03.ibm.com/developerworks/blogs/page/gradybooch.

[2]. Craig Larman, Applying UML and Patterns - An Introduction to Object-Oriented Analysis and Design, 2nd Ed, Prentice Hall, 2001.

[3]. Dirk Krafzig, Karl Banke, Dirk Slama, Enterprise SOA: Service-Oriented Architecture Best Practices, Prentice Hall PTR, Nov 2004.

[4]. Deepak Alur, John Crupi, Dan Malks, Core J2EE Patterns: Best Practices and Design Strategies, 2nd Ed., Prentice Hall / Sun Microsystems Press, 2003.

[5]. Eric Freeman, Elisabeth Freeman, Kathy Sierra, Bert Bates, Head First Design Patterns, O'reilly, 2008.
[6]. Erich Gamma, Richard Helm, Ralph Johnson, John M. Vlissides, Design Patterns: Elements of Reusable Object-Oriented Software, Addison Wesley, 1995.
[7]. Erl, Thomas, SOA: Principles of Service Design, Upper Saddle River, Prentice Hall, 2007.
[8]. Evdemon, John, ''Principles of service design: Service patterns and antipatterns.'' MSDN, August 2005. http://msdn2.microsoft.com/en-us/library/ms954638.aspx.
[9]. Fitts, Sean. ''When exceptions are the rule: Achieving reliable and traceable service oriented architectures.'' SOA/WebServices Journal, September 2005. http://webservices.sys-con.com/read/121945.htm.
[10]. Herr, Michael and Uwe Bath, Paper: The business-oriented background of Service Backbone. http://www.servicebackbone.org/, January 2004.
[11]. Herr, Michael and Ursula Sannemann, Paper: The Architecture of Service Backbone. http://www.servicebackbone.org/. October 2003.
[12]. Hohpe, Gregor, and Bobby Woolf. Enterprise Integration Patterns:Designing, Building, and Deploying Messaging Solutions. Boston: Addison-Wesley, 2004.
[13]. IBM Patterns for e-business http://www.ibm.com/developerWorks/patterns/.
[14]. Ivar Jacobson, Object-oriented Software Engineering – Approach, Addison Wesley, 1992.
[15]. Jonathan Adams, Srinivas Koushik, Guru Vasudeva, George Galambos, Patterns for e-business: A Strategy for Reuse, IBM Press, 2001.
[16]. Kanthi Hanumanth, and Alasdair Nottingham. ''Patterns: Implementing an SOA using an Enterprise Service Bus in WebSphere Application Server V6.'' IBM Redbooks, 2005.
[17]. Keith Levi, Ali Arsanjani, A goal-driven approach to enterprise component identification and specification, Communications of the ACM Volume 45 Issue 10, 2002.
[18]. Krafzig, Dirk, Karl Ganke, and Dirk Slama. Enterprise SOA: Service Oriented Best Practices, Prentice Hall, 2005.
[19]. Martin Fowler, Analysis Patterns, Addison-Wesley, 2004.
[20]. Mark Endrei, Jenny Ang, Ali Arsanjani, Sook Chua, Philippe Comte, Pål Krogdahl, Min Luo, Tony Newling, Patterns: Service-Oriented Architecture and Web Services, IBM, April 2004.
[21]. Mike Rosen, Boris Lublinsky, Kevin T. Smith, Marc J. Balcer, Applied SOA: Service-Oriented Architecture and Design Strategies, Wiley Publishing, Inc., 2008.
[22]. Olaf Zimmermann, Mark R Tomlinson, Stefan Peuser, Perspectives on Web Services; Applying SOAP, WSDL and UDDI to Real-World Projects, Springer, 2003.
[23]. Oracle's SOA Resource Center at http://www.oracle.com/technologies/soa/center.html.
[24]. Paul C. Brown, Implementing SOA: Total Architecture in Practice, Addison Wesley Professional, April 2008.
[25]. Towards a Pattern Language for Service-Oriented Architecture and Integration, Part 2: Service Composition.'' IBM developerWorks, December 2005. www128.ibm.com/developerworks/webservices/library/ws-soa-soi2.
[26]. Web Service Façade for Legacy Applications, Microsoft patterns & practices Developer Center, June 2003. http://msdn.microsoft.com/en-us/library/ms979218.aspx.

Continued from page no. 244

[4]. Peter Guller, "Integration of Transport and Land- use planning in Japan: Relevant finding from Europe," Workshop on Implementing sustainable Urban Travel Policies in Japan and other Asia-Pacific Countries, Tokyo, 2-3, March 2005. http://www.internationaltransportforum.org/europe/ecmt/urban/Tokyo05/Gueller.pdf
[5]. Mukti Advani & Geetam Tiwari, "Does high capacity means high demand?," Conference Proceeding- Future Urban Transport-2006, held at Gotenburg, Swedan. http://web.iitd.ac.in/~tripp/publications/paper/planning/mukti_FUT06.pdf
[6]. Data from Economic Survey of Delhi, Delhi Planning Dept., Delhi.
[7]. Results of C.R.R.I Study 2002.
[8]. S. Rajasekaran – *Neural Networks, Fuzzy Logic, and Genetic Algorithms*; Prentice Hall of India, 2003.

Continued From page no. 216

Tools/Attributes	Glossary & Ontology	Checklist	Templates	Use Case Modeling	Prototyping & Audit	TRS	Scalability	External Interface
RequisitePro	X	X	√	√	√	√	X	√
CaseComplete	√	X	√	√	√	√	X	√
Analyst Pro	X	X	X	√	X	√	√	√
Optimal Trace	X	X	√	√	√	√	X	√
DOORS	X	X	√	√	√	√	√	√
GMARC	X	X	√	X	√	√	X	√
Objectiver	√	√	√	X	√	√	X	√
RDT	√	X	√	X	√	√	√	√
RDD-100	√	X	√	X	X	√	X	√
RTM	X	X	√	X	X	√	X	√
Reqtify	X	X	X	√	√	√	X	√
TcSE	X	**X**	X	√	X	√	X	√
Code Assure	X	X	X	X	X	√	X	√
IRqA	X	√	X	√	X	√	X	√

Table 1: Software Functional Requirements

Tools/Attributes	Fair Exchange	Non-repudiation	Rbac	Secrecy & Integrity	Authenticity	Secure Information Flow	Guarded Access	Freshness
RequisitePro	√	X	X	X	X	X	X	√
CaseComplete	√	X	X	X	X	X	X	√
Analyst Pro	√	X	√	X	√	X	X	X
Optimal Trace	√	X	X	X	X	X	X	X
DOORS	√	X	√	X	√	X	√	√
GMARC	X	X	X	X	X	X	X	√
Objectiver	X	X	X	X	X	X	X	√
RDT	X	X	X	X	X	X	X	√
RDD-100	√	X	X	X	X	X	X	√
RTM	X	X	√	√	√	X	√	√
Reqtify	√	X	X	X	X	X	X	√
TcSE	X	√	√	√	√	√	√	√
Code Assure	X	√	√	√	√	√	√	√
IRqA	X	X	√	X	X	X	X	X

Table 2: Software Security Requirements

Note: √: Means satisfies the criterion
X: Means does not satisfy the criterion

A Secure Private Key Encryption Technique for Data Security in Modern Cryptosystem

Dilbag Singh[1] and **Ajit Singh**[2]

Abstract - ***The present paper provides a conceptual framework on the proposed private key encryption technique that can be used for data security in modern cryptosystem. This encryption technique uses the concept of arithmetic coding and can be used as an independent system as well as can be clubbed with any of the encryption system that works on floating point numbers. It provides you with a 256 character key (length of the key can be increased or decreased on the basic of the character set required) that can be used as a one time resident key or a key for every message depending on the level of security required. The proposed technique converts a word of text into a floating-point number that lie in between 0 and 1. This floating point no. is obtained on the basis of the probability of characters contained within the word of text and the one time key which has been provided .The security level can be further increased by generating different floating point number every time when a word repeat and increasing the length of the key.***

Index Terms - Arithmetic Coding, Encryption, Decryption, Floating point number, Resident and Regular key.

1. INTRODUCTION

During this time when the Internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce, security becomes a tremendously important issue to deal with. To provides the security cryptography come into the existence [1].Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet. Within the context of any application-to-application communication, there are some specific security requirements, including:

a) Authentication: The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
b) Privacy/confidentiality*:* Ensuring that no one can read the message except the intended receiver.
c) Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
d) Non-repudiation*:* A mechanism to prove that the sender really sent this message.

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, two types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, and public-key (or asymmetric) cryptography, each of which is described below. In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into ciphertext, which will in turn (usually) be decrypted into usable plaintext [2].

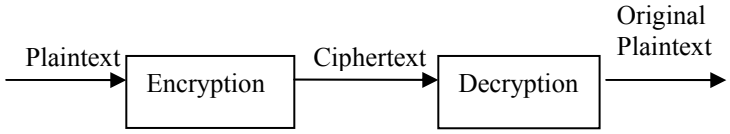


Figure 1: Basic Operation of Cryptography

1.1 Symmetric Encryption [2]

Symmetric Encryption (also known as symmetric-key encryption, single-key encryption, one-key encryption and private key encryption) is a type of encryption where the same secret key is used to encrypt and decrypt information or there is a simple transform between the two keys as shown in fig.2.

A secret key can be a number, a word, or just a string of random letters. Secret key is applied to the information to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. Symmetric algorithms require that both the sender and the receiver know the secret key, so they can encrypt and decrypt all information.

There are two types of symmetric algorithms: Stream algorithms (Stream ciphers) and Block algorithms (Block ciphers).

[1]*Department of Computer Science & Engineering, Choudhary Devi Lal University, Sirsa, Haryana (India)*
[2]*Department of Computer Science & Engineering, BPS Mahila Vishwavidyalaya, Khanpur Kalan, Sonepat, Haryana (India)*
E-mail: [1]*dbs_beniwal@rediffmail.com and*
[2]*ghanghas_ajit@rediffmail*.com

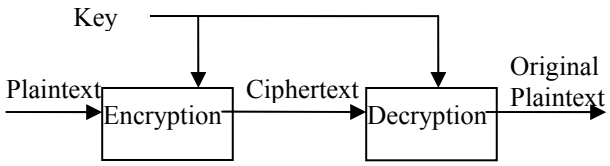


Figure 2: Symmetric Cryptosystem: KE= KD (KE Encryption Key and KD: Decryption Key

1.1.1 Types of Symmetric algorithms

Symmetric algorithms (Symmetric-key algorithms) use the same key for encryption and decryption. Symmetric-key algorithms can be divided into Stream algorithms (Stream ciphers) and Block algorithms (Block ciphers).

1.1.1.1StreamCiphers

Stream ciphers as shown in fig.3 encrypt the bits of information one at a time - operate on 1 bit (or sometimes 1 byte) of data at a time (encrypt data bit-by-bit). Stream ciphers are faster and smaller to implement than block ciphers, however, they have an important security gap. If the same key stream is used, certain types of attacks may cause the information to be revealed.

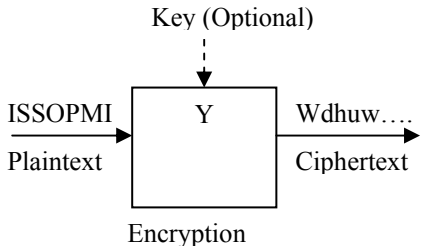


Figure 3: Stream Cipher-Convert one symbol of plaintext immediately into a symbol of ciphertext

1.1.12BlockCiphers

Block cipher (method for encrypting data in blocks as shown in fig.4) is a symmetric cipher which encrypts information by breaking it down into blocks and encrypting data in each block. A block cipher encrypts data in fixed sized blocks (commonly of 64 bits). The most used block ciphers are Triple DES and AES.

Some examples of symmetric encryption algorithms:

AES/Rijndael
Blowfish
CAST5
DES
IDEA
RC2
RC4
RC6
Serpent
Triple DES

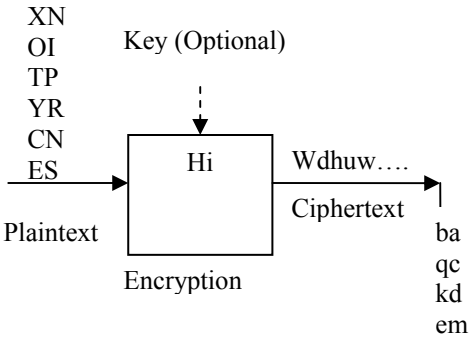


Figure 4: Block Cipher- Convert a group of plaintext symbols as one block

1.2 Asymmetric Encryption [8]

Asymmetric encryption (Also called Public Key Encryption) uses different keys for encryption and decryption. The decryption key is very hard to derive from the encryption key. The encryption key is public so that anyone can encrypt a message. However, the decryption key is private, so that only the receiver is able to decrypt the message. It is common to set up "key-pairs" within a network so that each user has a public and private key. The public key is made available to everyone so that they can send messages, but the private key is only made available to the person it belongs to.

1.2.1 Working of Asymmetric Encryption System[8]:

The sender and the recipient must have the same software. The recipient makes a pair of keys - public key and private key (both keys can be unlocked with a single password). Public key can be used by anyone with the same software to encrypt a message. Public keys can be freely distributed without worrying since it is only used to scramble (encrypt) the data. The sender does not need the recipient's password to use his or her public key to encrypt data. The recipient's other key is a private key that only he or she can use when decrypting the message. Private key should never be distributed since the private key assures that only the intended recipient can unscramble (decrypt) data intended for him or her.

To understand asymmetric encryption better consider an example, Jack makes public key A and private key A, and Jill makes public key B and private key B. Jack and Jill exchange their public keys. Once they have exchanged keys, Jack can send an encrypted message to Jill by using Jill's public key B to scramble the message. Jill uses her private key B to unscramble it. If Jill wants to send an encrypted message to Jack, she uses Jack's public key A to scramble her message, which Jack can then unscramble with his private key A. Asymmetric cryptography is typically slower to execute electronically than symmetric cryptography.

Some Asymmetric Algorithms (public key algorithms) such as RSA allow the process to work in the opposite direction as well: a message can be encrypted with a private key and decrypted with the corresponding public key. If the recipient wants to decrypt a message with Bob's public key he/she must know that the message has come from Bob because no one else has sender's private key.

Digital signatures work this way.

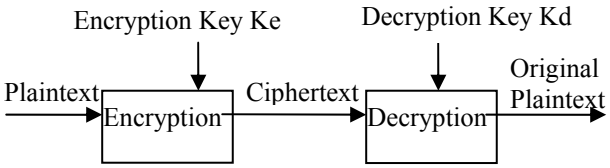


Figure 5: Asymmetric Cryptosystem: KE≠KD (KE Encryption Key and KD: Decryption Key)

Some examples of popular asymmetric encryption algorithms:
RSA
DSA
PGP

2. ARITHMETIC CODING

In arithmetic coding, a message is encoded as a real number in an interval from one to zero. The idea behind arithmetic coding is to have a probability line, 0-1, and assign to every symbol a range in this line based on its probability [6], the higher the probability, the higher range which assigns to it. Once we have defined the ranges and the probability line, start to encode symbols, every symbol defines where the output floating point number lands.

The coding algorithm is symbol wise recursive; i.e., it operates upon and encodes (decodes) one data symbol per iteration or recursion. On each recursion, the algorithm successively partitions an interval of the number line between 0 and 1, and retains one of the partitions as the new interval. Thus, the algorithm successively deals with smaller intervals, and the code string, viewed as a magnitude, lies in each of the nested intervals. The data string is recovered by using magnitude comparisons on the code string to recreate how the encoder must have successively partitioned and retained each nested subinterval. Arithmetic coding differs considerably from the more familiar compression coding techniques, such as prefix (Huffman) codes [4].

Arithmetic coding typically has a better compression ratio than Huffman coding, as it produces a single symbol rather than several separate codeword and can be use in compression based encryption system [12]. There are a few disadvantages of arithmetic coding. One is that the whole codeword must be received to start decoding the symbols, and if there is a corrupt bit in the codeword, the entire message could become corrupt. Another is that there is a limit to the precision of the number which can be encoded, thus limiting the number of symbols to encode within a codeword. [7]

3. SHANNON CHARACTERISTICS OF A GOOD ENCRYPTION SYSTEM [5]

1. The amount of security needed should determine the amount of labor appropriate for the encryption and decryption.
2. The set of keys and enciphering algorithm should be free from complexity.
3. The implementation of the process should be as simple as possible.
4. Errors in ciphering should not propagate and cause corruption of further information in the message.
5. The size of the enciphered text should be no larger than the text of the original message.

4. PERPOSED PRIVATE KEY ENCRYPTION TECHINQUE

The proposed technique is based on the concept of arithmetic coding [9] in which a word of text is converted into a floating-point number that lie in the range between 0 and 1. Private Key encryption system based on this technique can be used as an independent system as well as can be clubbed with any of the encryption system that works on floating point numbers [7]. The probability table can also be set according to the user requirement and the combination of two keys working one over the other makes it extremely difficult to break as the total no of exhaustive cases shoot up tremendously.

4.1 Requirements

A. Two Keys

The system is implemented using two keys: -

1. Resident key: - It's a one-time key provided by the user when the software is installed or initiated.
2. Regular key: -This key is subjected to change as and when the user thinks that the previous keys have been disclosed. Length varies with security requirements.

Note: Regular key used when the system work in independent mode.

B. A Table

A table containing all symbols along with probability of occurrence [3,9].

Symbol	Probability of Occurrence	Symbol	Probability of Occurrence
^	0.0001	N	0.0380
A	0.0500	O	0.0320
B	0.0500	P	0.0300
C	0.0450	Q	0.0380
D	0.0455	R	0.0400
E	0.0380	S	0.0400
F	0.0360	T	0.0320
G	0.0400	U	0.0300
H	0.0360	V	0.0350
I	0.0380	W	0.0300
J	0.0320	X	0.0300
K	0.0400	Y	0.0250
L	0.0360	Z	0.0779
M	0.0360		

4.2 Implementation

In the Add on to the Existing Encryption System mode of implementation the technique converts a word of text into a floating-point number. This floating point no. is obtained on the basis of the probability of characters contained within the word of text and the one time key which has been provided[10, 11].

Explanation

Encryption: - Each character in the 256-character key is associated with its corresponding probability of occurrence using the table. The sequence of these characters along with their probabilities acts as the basis for Algorithm [9] of the technique to work.

Algorithm

In order to implement the algorithm array data structure can be use for the resident key, priority table and message. To encrypt the message, algorithm includes the following steps:

Step 1:- On the basis of the resident key and priority table derive another table (Range table)

a)Initialize range_from=0, range_to=probability [first element of the key], counter=1

b) Repeat steps for all the characters in the one time key
range_from [counter] =range_to[counter-1]
range_to[count]=range_from[count]+ probability[count]
Count=count + 1;

Step2:- Read the word to be encrypted. 2.1

Step3:-Initialize Low_value=0, High_value=1 2.2
difference=1, count=1

Step4:- Repeat for every character of the word
Temp=Low_value[count-1]
Low_value[count]=low_value[count–1]+ difference[count-1] * range_from[symbol]
High value[count]=temp + difference[count –1]* range_to[symbol]
Difference[count]=high_value[count]- low_value[count]
Count=count+1

Step5:- float_code=low_value

Step6:- Repeat process for every word in the file

Output: Output is a floating point no. that is corresponding to the inputted word. It can be provided further to any other encryption algorithm that works on floating point numbers

Decryption: - Getting the floating points its time now that we convert it into original text.

Algorithm

To deecrypt the message, algorithm include the following steps:

Step 1:- while flote_code ! = 0.0 repeat step 3 to 5

Step 2:- initialize count=1

Step3:- find range[symbol] where float_code lies and set count accordingly.

Step4:-float_code
=(float_code - range_from[count])/prob[count]

Step5:- store symbol in a character string

Srep6:- count=count+1

Step7:- repeat process for every word in the file

Output: Output is the original text.

Example:

Encryption:

The resident key used is

a b c d e f g h i j k l m n o p q r s t u v w x y z

Enter the word to be encrypted

anil

Symbol	Low_value	High_value	Difference
a	0.0001	0.0501	0.05
n	0.026205	0.028105	0.0019
i	0.026851	0.026923	7.22e-05
l	0.026884	0.026886	2.5992e-06

Equivalent floating point number is 0.026884

Decryption:

Symbol	Range_From	Range_To	Prob.	Flot_Code
a	0.0001	0.0501	0.05	0.535674
n	0.5221	0.5601	0.038	0.357204
i	0.3401	0.3781	0.038	0.4501
l	0.4501	0.4861	0.36	6.53798e-13

The word is anil

5. KEY FEATURES

1. It's a Private Key Encryption system.
2. Make the system that can operates in different modes Add on to the existing encryption system Independent system
3. Flexibility: - The system is extremely flexible as allows the length of both the keys to be changed, the length of the resident key depends on the character set required. The probability table can also be set according to the user requirement.
4. Extremely difficult to break the code by brute force attack: - The combination of two keys working one over the other makes it extremely difficult to break as the total no of exhaustive cases shoot up tremendously.

6. EFFICIENCY

The proposed technique satisfies all the Shannon Characteristics of a Good Encryption System as shown in the table given below. It makes the system faster, portable and requires memory space of less than 15kb and also provides an efficient data security during communications.

Sr. No.	Shannon Characteristics of a Good Encryption System	Proposed Technique
1	The amount of security needed should determine the amount of labor appropriate for the encryption and decryption.	√
2	The set of keys and enciphering algorithm should be free from complexity.	√

Continued on page no. 270

Minor Irrigation Census Computerization: A Step towards ICT for Micro Level Planning in Water Resources Management and Planning to Achieve Rural Prosperity

Ajay Kumar Gupta[1], Kishore Kumar[2] and **Madaswamy Moni[3]**

Abstract - ***India's achievements in development of Water Resources have been remarkable, since independence. The National Water Policy 2002 has addressed the issues related to develop, conserve, utilize and manage these important natural resources in this Millennium. There are approximately 20 million Minor Irrigation structures in the country, which are classified as: Dugwell, Shallow Tube well, Deep Tube well, Surface Flow Irrigation Scheme, and Surface Lift Irrigation Scheme.***

The Ministry of Water Resources (MoWR) has already conducted three Censuses with the reference Year: 1986-87, 1993-94 and 2000-01, and currently Census with the reference Year 2006-07 is in progress. National Informatics Centre (NIC) is involved in computerizing the census data and subsequent data analysis as per the business logic given by MoWR.

This Paper draws a roadmap for using this database for formulating various Schemes to improve the socio-economic condition of small and marginal farmer, and also its immense need for grassroots level development and planning for Water Resources Management and Planning. This paper also shows as to how this database is useful to the national initiatives such as "DISNIC-Plan: IT for Micro Level Planning", a Central Sector Schemes of NIC and recommended by Planning Commission (http://www.disnic.gov.in) and "Agriculture Resources Information Systems (AgRIS)", a Central Sector Scheme of the Department of Agriculture & Cooperation in Pilot Districts (http://www.agris.nic.in). This becomes a major component of the proposed "National Water Portal" of the MOWR.

Index Terms
AgRIS - Agriculture Resources Information Systems
BI - Business Intelligence
CCA - Culturable Command Area
DISNIC - District Information System NIC
DSS - Decision support System
GW - Ground Water
GIS - Geographical Information System
IT - Information Technology
Mha - Million Hactare
MoWR - Ministry of Water Resources
MI - Minor Irrigation
NIC - National Informatics Centre
NABARD- National Bank for Agriculture & Rural Development
PC - Potential Created
PU - Potential Utilised
SW - Surface Water
WRID - Water Resources Informatics Division

[1,2,3]Water Resources Informatics Division, National Informatics Centre, New Delhi – 110 003
E-Mail: [1]ajaykgupta@nic.in, [2]kkumar@nic.in and [3]moni@nic.in

1.0 INTRODUCTION

For effective implementation of irrigation policy and planning, sound database regarding Minor Irrigation Sector is a must. The inadequacy of data has been considered as a serious constraint at various forums of irrigation planning. The National Commission on Agriculture had recommended that "Census of irrigation sources should be undertaken alongwith the agricultural census once in 5 years, Special irrigation surveys on the number of wells and their utilisation may be undertaken by the States". Planning Commission also recommended for a detailed census of minor irrigation works in 1970. A meeting of the Technical Committee for agriculture census 1980-81 considered the inclusion of list of items relating to minor irrigation in the primary enumeration schedules, but it could not be agreed. The main reason for non-inclusion of items relating to minor irrigation was that the agriculture census data was to be compiled from the existing data of land records of various States. The data do not have the information relating to minor irrigation works as desired.

1.1 Definition of Minor Irrigation Schemes

The criteria for classification of minor irrigation schemes have been changing from time to time. Since April 1993 all ground water schemes and surface water schemes (both flow schemes and lift schemes) having culturable command area upto 2000 hectares individually are considered as minor irrigation schemes.

1.2 TYPES OF MINOR IRRIGATION WORKS

1.2.1 Ground Water (GW) Schemes

1. Dugwell
2. Shallow Tubewell
3. Deep Tubewell

1.2.2 Surface Water (SW) Schemes

1. Surface Flow Schemes
2. Surface Lift Schemes

1.3 NEED FOR COMPUTERISATION

1.3.1 High volume of data :

The minor Irrigation schemes are very large in number and data generated at field level has to pass through various levels of functionaries. The delay is imperative. This delay could be attributed to either the complicated procedures

involved at each level or the deteriorating condition of the basic documents. The errors like to creep in during transitions at different levels. It is proposed to store the data from the field level itself in the computer.

1.3.2 Importance of data

After collecting the error free data from all the States, Minor Irrigation Wing of the Ministry of Water Resources (MoWR) publish a report related to census statistics. This publication is useful not only to the professionals, planners and researchers in irrigation and agriculture sectors but also to all others who are directly or indirectly connected with the development of irrigation and water resources management in India.

The objective of this project is to gather the correct and validated data of Minor Irrigation Census from all the concerned states. These data to be compiled at headquarter and will be used for decision support. These data with appropriate software will be distributed to all the concerned states with their data.

1.3.3 Information called for by different departments

Agriculture being the most important economic activity in our country, all planning and other related activity depend on the information collected from Irrigation schemes. Effective compilation, classification and timely availability of this information are essential. Computerization of Minor Irrigation Census will facilitate accurate compilation and timely dissemination of desired information.

1.3.4 How the computerisation system can improve upon the Manual system:

Keeping in the view of computerisation's vast scope for compilation of census data, the following are the advantages of the computerised system vis-à-vis traditional system:

1. Duplication of data can be eliminated.
2. Data integrity and timeliness is ensured.
3. Data can be kept safely in electronic media like Hard disks, CD-ROM, Pen drives, Cartridges etc, thereby making the census data more secure.

2.0 COMPUTERISATION OF CENSUS DATA

The National Informatics Centre (NIC), was requested to develop necessary software for computerising the Census data. Such software's in CDROM were provided to Minor Irrigation Census Commissioners for computerising the Census data. Wherever necessary, private consultants/agencies were hired by the Minor Irrigation Census Commissioners to do the data entry of the primary enumeration schedules, using data entry software provided by NIC. The work was taken up at the district headquarters to avoid transportation difficulty and misplacement of enumeration schedules. It also minimised the delays in computerisation. The validated CDROM having data, collected during the census on primary enumeration schedules were prepared and after duly ascertaining the correctness of data two copies were passed on to the Minor Irrigation Census Commissioner at the state level. A copy of the data media was sent to the centre by the State Minor Irrigation Census Commissioners. Based on the primary data at the State headquarters, a State Minor Irrigation Census Report was brought out for which a tabulation plan was supplied by the NIC, New Delhi. The census data received from the States at the Centre in floppies were utilised for compiling a National Level Minor Irrigation Census Report. The processing of the report was taken up with the help of National Informatics Centre (NIC).

2.1 Methodology

The Census data was collected through canvassing six different enumeration schedules. One of the schedules is the village schedule which was canvassed by the enumerators through enquiries from patwaries/village level workers/gram pradhans, and the revenue or land records maintained in the government records. The other five schedules were to be canvassed by enumerators through enquiries from the owners of the schemes. These five schedules relate to five different types of minor irrigation schemes. The various schedules alongwith instructions for filling up were given to state governments. The fieldwork of the census was either undertaken by the nodal department itself or entrusted to some other agency which the State/UT government considered fit in respect of infrastructures available with it. However, for the entire census operation, Minor Irrigation Census Commissioner, was the pivotal point. The primary work of collection of data was carried out by the enumerators. They were village level workers or village accountants or lekhpals or patwaries or a combination of these as the case may be. The work of supervision was entrusted to the next superior officer of the field agency by the State/UT. They were Block Level Officers or Sub-Divisional Officers who in order to ensure the correctness of data recorded by an enumerator conducted frequent site visits of the schemes.

In order to increase the reliability of data a sample check was conducted in addition to the enumeration and supervision of data collection as mentioned above. Systematic sampling technique was adopted for 5 percent sample check at the district level. It helped in detecting under enumeration/over enumeration and hence a correction factor, wherever necessary, was applied to the main census results. The following methodology was adopted for drawing the sample.

2.2 Salient Features of the Software

The software developed has the following salient features

1. The screens are user friendly
2. Wherever there is codification, only codes can be entered and corresponding name is displayed automatically. All care has been taken in case of incorrect codes wherein a help screen pops out to list the valid codes available to view and select accordingly.
3. Validation checks have been incorporated in the software at the appropriate fields

The software has been developed in a modular fashion and has the following main modules:

a) Data Entry module
b) Report generation module
c) Decision Support System
d) Query Module
e) Business Intelligent Module
f) GIS presentation

2.3 Application Architecture and Technologies

The overall objective of this project is to gather the correct data and process for different purpose. The database collected from all States/ UTs have been merged for making a National level database and a number of reports have been generated.
The application has been divided into three modules based on their requirement i.e. Data Entry Module, Abstract Creation and Decision Support System (DSS). The objective of Data Entry Module is to gather the validated base/ enumerated data. Abstract Creation Module will process these data (base/ enumerated data) for generating a database that will be used by Decision Support System. DSS Module will generate all types of reports, queries and provide useful information.

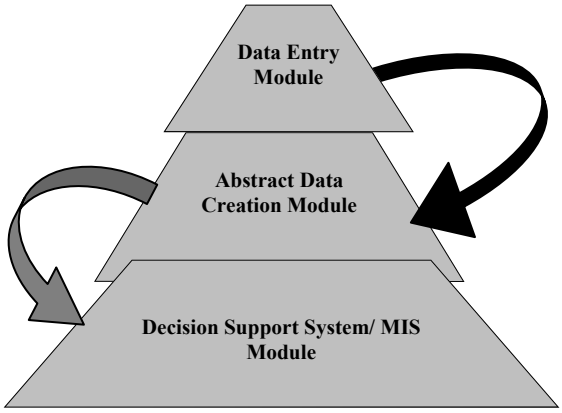


Figure 1

Project Architecture

(i) **Situation before the initiative**: Before this initiative, the data was compiled manually. Reliability of data was not guaranteed. Processing and compilation took lot of time. Publication of reports took around seven years.
(ii) **Strategy Adopted**: Data was collected by the State Government through Five different schedules of enquiry. Data entry was done by the State Government through private vendors at State/District level. Processing and tabulation was done in the Ministry of Water Resources at New Delhi.
(iii) **Result Achieved/ Value Delivered to beneficiary of the project**:

1. Strengthen the decision-making in the management of water Resources
3. Access of information based on pre-defined queriesImproved Management Information SystemOnline Analytical Processing System and Data Visualization
6. Data dissemination through web site
8. Models for discovery of pattern among data **Other distinctive features/ accomplishments of the project**:
10. Decision Support System with Query Module
11. Portal – disseminating information/reports up to village level
12. Business Intelligent functionality

3.0 TRAINING PROGRAMME FOR DATA COLLECTION

Training cum workshops were organised by the Minor Irrigation Census Commissioners at the State Headquarters in which the District Level Officers participated. A representative from the Centre was invariably an Observer in such workshops. The details of the methodology adopted for the census, its procedure, concepts and definitions were discussed thoroughly and necessary clarifications were given. The instructions for filling up the primary enumeration schedules were also discussed during the workshops. In turn, the District Level Officers organised training programmers' at district headquarters where the primary enumerators participated. They were explained thoroughly the instructions for filling up the primary enumeration schedules.
A National Level Workshop was conducted by NIC at New Delhi for all the State Government officers entrusted with the MI Census data collection and computerisation work. The live software demo was carried out and feedback were collected and addressed in the software. The CDROM containing the software along with Users' Manual was distributed among all the participants.

4.0 PROCEDURE FOR CONDUCTING CENSUS OPERATION:

The Primary enumerators while negotiating the schedules were to visit the owner of the minor irrigation scheme or its next neighbour and collect information on the basis of personal enquiry from him. The physical verification of the schemes was also to be done by the enumerators. The purpose of the census was to be explained to the farmers to win over their confidence in revealing the specific information in respect of minor irrigation works. Assurance that the data furnished by them would be kept confidential needed to be given to the farmers. Certain information relating to the schemes were to be collected by the enumerators by physical examination of the scheme.
After filling up the schedules, the enumerators were required to deposit all completed schedules with the Block Development Officer/Officer in-charge at the block level. The block level officer supplied all the schedules to the district level officer concerned who computerised the data contained in the prescribed schedules and passed on the floppy containing data as well as the schedules, to the Minor Irrigation Census Commissioner of the State/UT.

5.0 RELIABILITY OF DATA

The Census of Minor Irrigation Works has been completed by the States/UTs on various dates in a span of about five years. A number of difficulties were encountered by the States in its completion. Depending on the gap between the reference year and the date of census, the reliability of data varies. Smaller the gap, more reliable the data collected. Despite best efforts by the Minor Irrigation Census Commissioners in the States, certain limitations remain in this report to be looked into in future census operation. Broadly these limitations are elaborated in the following paragraphs.

5.1 Features

1. Strengthen the decision-making in the management of water resources
2. Access of information based on pre-defined queries
3. Improved Management Information System
4. Online Analytical Processing System and Data Visualization
5. Data dissemination through web site
6. Models for discovery of pattern among data

5.2 Impact

1. Efficient planning and decision making for development of Water Resources through consistent and consolidated information.
2. Empower end users to perform in-depth Analysis.
3. Prediction of irrigation potential/utilization and segmentation of areas through OLAP models.

5.3 Hardware & software used for Census computerization

5.3.1 For Development Purpose

For MIS Software

Hardware

One Server –PIII Xeon, OS: 2000 Server
Two Client- PIV, OS: 98 SE, RAM: 128 MB

Software

Microsoft Visual Basic 6.0, Microsoft VB.NET, Seagate Crystal Repot, SQL Server 2000, MS-ACCESS 2000

For Business Intelligence/ GIS Software

Hardware

One Server –PIII Xeon, OS: 2000 Server, Brand: HCL, RAM:1.0 GB

Software

COGNOS and ARCINFO, SQL Server 2000

5.3.2 For Deployment Purpose

For MIS Software

Hardware

Client having 128MB RAM and loaded with OS 98 SE or higher.

Software

No specific software is needed.

For Business Intelligence/ GIS Software

Hardware

NIC have specific Server installed at NICHQ for BI & GIS respectively, no specific hardware was purchased for this project

Software

Any Internet browser is required at client side

5.4 Minor Irrigation Census portal

http://mowr.gov.in/micensus/mi3census/index.htm

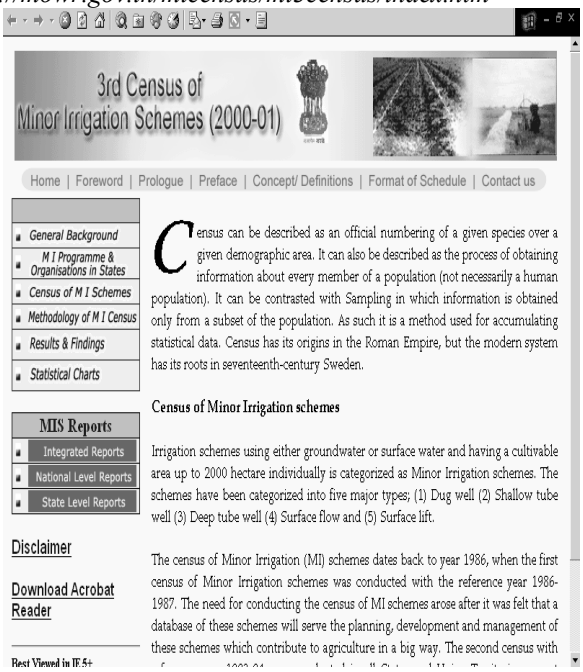


Figure 3

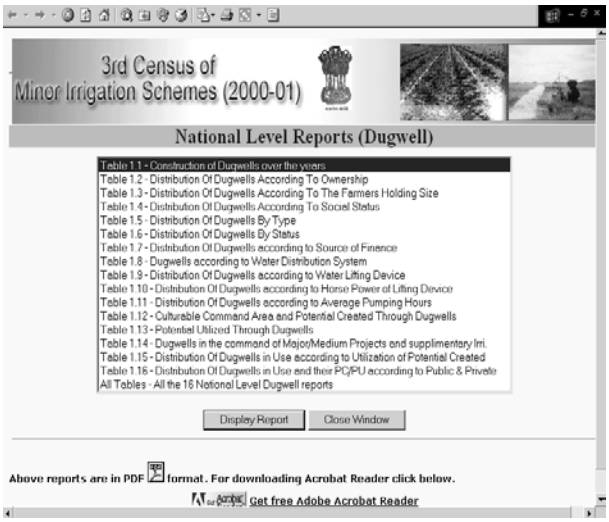


Figure 4

5.5 Screen Shots of Data entry software

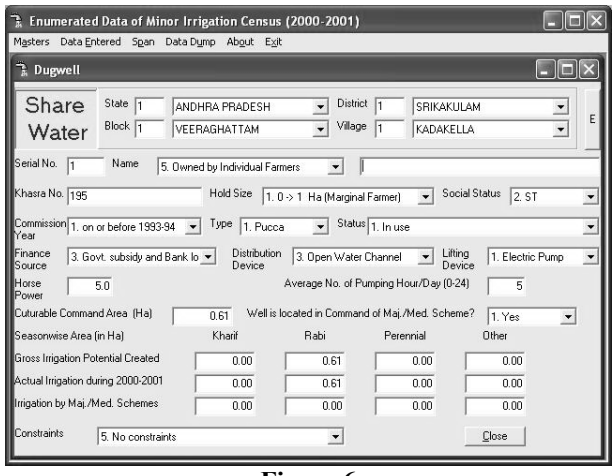


Figure 6

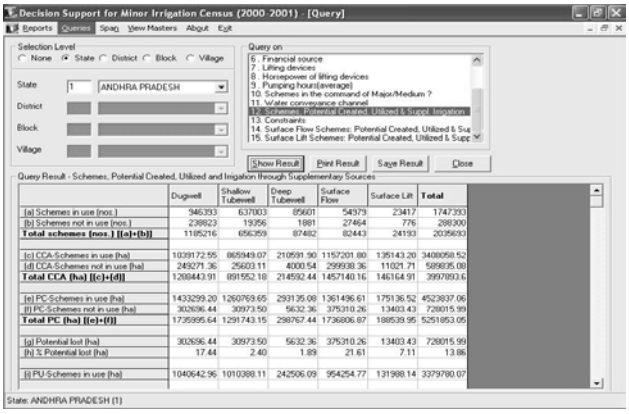


Figure 7

6. FUTURE SCOPE

The database will be of immense need for grassroots level development and planning for Water Resources Management. In addition to this, this database will also be useful to the other national level initiatives such as DISNIC-Plan: IT for Micro Level Planning, a Central Sector Schemes of NIC and recommended by Planning Commission (discnic.gov.in) and Agriculture Resources Information Systems (AgRIS), a Central Sector Scheme of the Department of Agriculture & Cooperation in Pilot Districts (agris.nic.in)

7. SOCIAL IMPACT

Minor Irrigation Schemes are environment friendly and provide gainful employment opportunities to the rural population, resulting in optimum utilization of resources. This also contributes to rural economic growth and plays an important role in increasing agricultural production to meet the needs of the growing population. In the States these schemes are being implemented by many departments / organisations like Agriculture, Rural Development, Irrigation, and Social Welfare. At the Central level also, a number of departments have been implementing programmes on minor irrigation. The government has been instrumental in providing credit to farmers for the development of minor irrigation through Commercial Banks, Regional Rural Banks, Co-operatives and National Bank for Agriculture & Rural Development (NABARD)

In order to develop and maintains firm database on minor irrigation, MI Census is conducted through the Minor Irrigation Division of the Ministry of Water Resources under the Centrally Sponsored Scheme "Rationalisation of Minor Irrigation Statistics (RMIS)". Minor Irrigation projects have smaller gestation period, require smaller investment and the benefit reach the farmers immediately. Ground water schemes provide irrigation through out the year and are more dependable which help in sustaining agricultural production over the years. Most of the Minor Irrigation projects are being executed and maintained by farmers.

8. CONCLUSION

The database thus created has been of immense use for all fields of people i.e. research scholars, students, planners, state governments etc.

Few facts of the data as MoWR have completed the analysis of data through the NIC tools :

1. Total nos. of schemes : 1,97,52,199
2. Ground Water Schemes : 18503268 (94 %)
3. Surface Water Schemes : 1248931 (6 %)
4. At all India level 97% MI Schemes are in Private Sector and 3% are in Public Sector
5. At all India level, MI Schemes owned by Small & Marginal Farmer is 63%
6. It is also found that nos. of schemes are under utilised because of various reasons out of which inadequate power supply contributes to 10 % of total schemes.
7. Potential created through MI is around 74.3 Mha
8. Potential utilized through MI is around 52.0 Mha .

REFERENCES

[1]. Guidelines for conducting the Minor Irrigation Census by Minor Irrigation Statistics Wing, Ministry of Water Resources (http://mowr.gov.in/micensus/mi3census/index.htm).

[2]. 3rd Minor Irrigation Census technical report (http://mowr.gov.in/micensus/mi3census/index.htm).

[3]. 2nd Minor Irrigation Census technical report (http://mowr.gov.in/micensus/mi2census/default.htm).

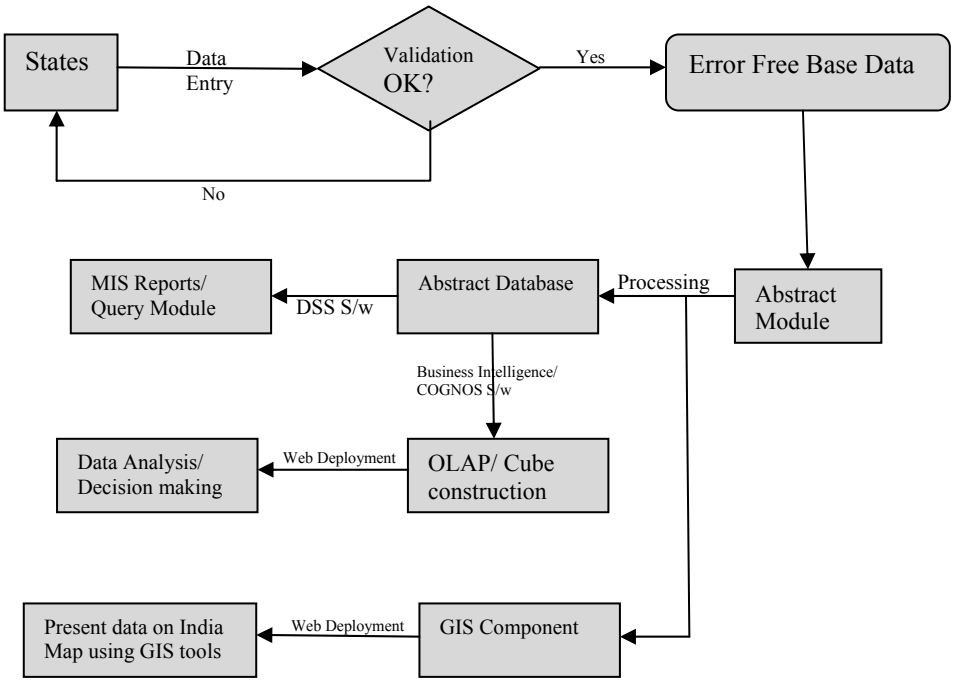

States
Data Entry
Validation OK?
Yes
Error Free Base Data
No
MIS Reports/ Query Module
DSS S/w
Abstract Database
Processing
Abstract Module
Business Intelligence/ COGNOS S/w
Data Analysis/ Decision making
Web Deployment
OLAP/ Cube construction
Present data on India Map using GIS tools
Web Deployment
GIS Component

Figure 2

Nonlinear Circuit Modeling Using Volterra Series

Akash Tayal[1], Harneet Kaur[2], Manika Babbar[3] and **Saumya Tyagi[4]**

Abstract - In this paper Volterra series has been used as a mathematical tool to look at the non linear behavior of various mechanical and electrical systems [4]. Volterra series has been introduced. Two methods for determination of volterra kernels are specified and harmonic input method is used for analysis. Simulations for different order harmonics are done which represent varying degrees of non linearity.

Index Terms - Volterra series, Non-linear systems

1. INTRODUCTION

Virtually all physical systems are non linear in nature. Sometimes it is possible to describe the operation of a physical system by a linear model, if the operation of the physical system does not deviate too much from the normal set of operating conditions. But in analyzing the behavior of any physical system, one often encounters situations where linear models are inadequate or inaccurate, that is the time when concepts like Volterra series prove useful. Volterra series takes into account the non linear behavior of a system.

2. REPRESENTATION

Any time-invariant, nonlinear system can be modeled as an infinite sum of multidimensional convolution integrals of increasing order. This is represented symbolically by the series of integrals called Volterra kernels. [2]

$$y(t)=\sum_{n=1}^{\infty}\left(\frac{1}{n!}\right)\int_{-\infty}^{\infty}(d\tau_1)\ldots\int_{-\infty}^{\infty}(d\tau_n)h(\tau_{1\ldots}\tau_n)\prod_{i=1}^{n}x(t-\tau_i) \qquad (2)$$

This series is known as the Volterra series. Here y(t) represents the system response. Each of the convolution integrals contains a kernel, either linear (h_1) or nonlinear (h_2,..,h_n), which represents the behavior of the system.

Volterra kernels, both linear and nonlinear, are input dependent. The first order kernel, h_1, represents the linear unit impulse response of the system. The second order kernel, h_2, is a two-dimensional function of time. It represents the response of the system to two separate unit impulses applied at two varying points in time. Similarly the other higher order kernels represent the response of the system to a combination of different signals at varying points of time.

3. IDENTIFICATION OF HARMONICS

Let the input to a system, with a first order kernel only, be $x(t)= e^{j\omega t}$

The output y(t) will be calculated as follows:

$$y(t)=\int_{-\infty}^{\infty}h_1(\tau)e^{j\varpi(t-\tau)}d\tau=e^{j\varpi t}\int_{-\infty}^{\infty}h_1(\tau)e^{-j\varpi\tau}d\tau$$

$$=H_{1\varpi}(j\varpi)e^{j\varpi t} \qquad (3)$$

where $H_{1\varpi}(j\varpi)=h_1(\tau)e^{-j\varpi\tau}d\tau$

The complex number $H_1\omega\ (j\omega)$ by which the output phasor is multiplied is called the transfer function or the first order harmonic. Similarly, higher order harmonics can be calculated.

4. DETERMINATION OF VOLTERRA KERNELS

When we have an equation relating the input x(t) to the output y(t) then we can obtain the volterra kernels by two methods [1]:

1. Harmonic input method: used for determination of kernels in frequency domain.
2. Direct expansion method: used for determination of kernels in time domain

4.1. Harmonic Input Method

[1]When the input is

$$x(t)=e^{j\varpi_1 t}+e^{j\varpi_2 t}+\ldots e^{j\varpi_n t} \qquad [1]\ (4.1)$$

where $\omega_i = 2\pi f_i$, i =1,2,…,n and the ω_i are incommensurable, then

$H_n\omega\ (j\omega_1,\ldots,\omega_n)$={coefficient of [$e^{j\varpi_1 t}+e^{j\varpi_2 t}+\ldots e^{j\varpi_n t}$]}

The complexity of this method increases rapidly with n. [2]

$H_n\omega\ (j\omega_1,\ldots,\omega_n)$ is the nth order harmonic.

4.2. Direct Expansion Method

In this method, the system equations are manipulated until they are brought into the form of a Volterra series, and the h_n are simply "read off" the representation. This method gives good results when the value of n is large [2].

5. SIMULATIONS

The steps followed in the simulation are:

1. The system is represented in the form of differential equations.
2. Its solution is expressed as a truncated Volterra series expansion as follows
   $y(t) = H_1[x(t)] + H_3[x(t)] + H_5[x(t)]$
3. Taking x(t) to be a sinusoidal input, we get

$y(t) = A*Re\{ H_1\omega\ (j\omega)\ e^{j\omega t}\}$
$+ 2(A/2)^3\ [Re\{ H_3\omega\ (j\omega, j\omega, j\omega)\ e^{j3\omega t}\}]$
$+ 2(A/2)^3\ [Re\{3\ H_3\omega\ (j\omega, j\omega, -j\omega)\ e^{j\omega t}]$
$+2(A/2)^5\ [Re\{ H_5\omega\ (j\omega, j\omega, j\omega, j\omega, j\omega)\ e^{j5\omega t}\}]$
$+2(A/2)^5\ [Re\{ 5H_5\omega\ (j\omega, j\omega, j\omega, j\omega, -j\omega)\ e^{j3\omega t}\}]$
$+2(A/2)^5[Re\{ 10H_5\omega\ (j\omega, j\omega, j\omega, -j\omega, -j\omega)\ e^{j\omega t}\}]$ (5)

where $H_1\omega$, $H_3\omega$ and $H_5\omega$ for different arguments can be found out by harmonic input method for determination of kernels.

[1, 2, 3, 4]Electronics and Communication Engineering Department, Indira Gandhi Institute of Technology, Guru Gobind Singh Indraprastha University (GGSIPU), Delhi
E-Mails: [1]akashtayal786@gmail.com, [2]harneet.monga@gmail.com, [3]babbar_manika@yahoo.co.in and [4]tyagi.saumya@gmail.com

4. The values of these kernels are then substituted in the system equation to determine the linear and the non-linear part.

5.1. Volterra Analysis Of A Non-Linear Spring

The equation of a nonlinear spring is given by

$y(t) = mx''(t) - b[x'(t)]^3 + kx(t)$ [1] (5.1)

Applying the harmonic input method and taking x(t) as $e^{j\omega t}$, we get

$H_1[x(t)] = A*Re((-m\omega^2+k)e^{j\omega t})$

$H_3[x(t)] = 2(A/2)^3*(Re((-2m\omega^2+2k)e^{3j\omega t}) + Re(3(-2m\omega^2+2k-12bj\omega^3)e^{j\omega t}))$

$H_3[x(t)] + H_5[x(t)] = 2(A/2)^3*(Re((-2m^2+2k)e^{3j\omega t}) + Re(3(-2m\omega^2+2k-12bj\omega^3)e^{j\omega t})) + 2(A/2)^5*(Re(5(64bj\omega^3)e^{3j\omega t}) + Re(10(-3m\omega^2+2k-54bj\omega^3)e^{j\omega t}))$

[1] Using the steps described in the section 4, this problem was simulated for A=2, b=2, m=0.001kg, k=3 and $\omega=\pi$ and graphs were obtained as shown in the figure:

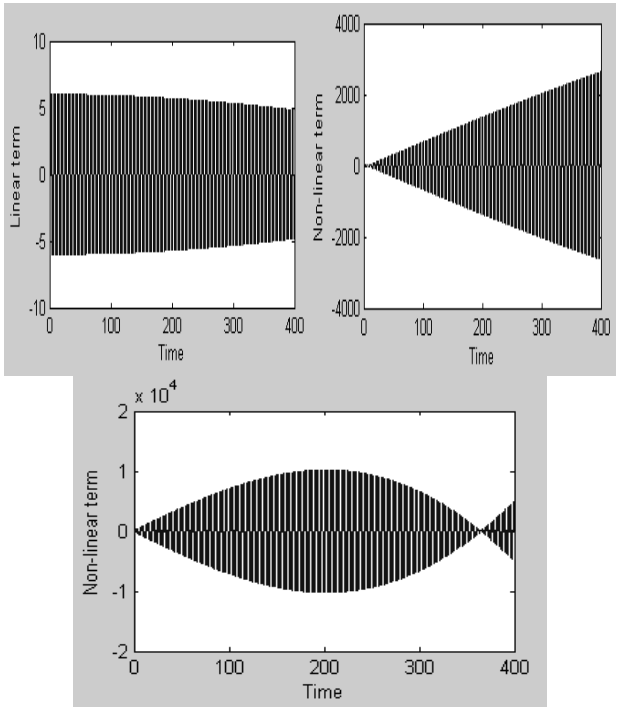


Figure 5.1: Simulation graphs for a Nonlinear Spring (Clockwise from top left) a) Linear part b) Third harmonic c) Third and fifth harmonic

5.2. Volterra Analysis of a Simple Pendulum

The equation of motion of a simple pendulum with linear damping is given by

$y(t) = x''(t) + ax'(t) + bsinx(t)$ [3] (5.2)

Normally for any non linear system we consider $sinx(t) \approx x(t)$ for small x(t). Here we consider Volterra systems to take into account the non-linearity caused by sine[1]

Using the steps described in the section 4, this problem was simulated for A=1, b=0.2, a=2, k=3, m=0.001 and $\omega=\pi/2$ and graphs were obtained as shown in the figure:

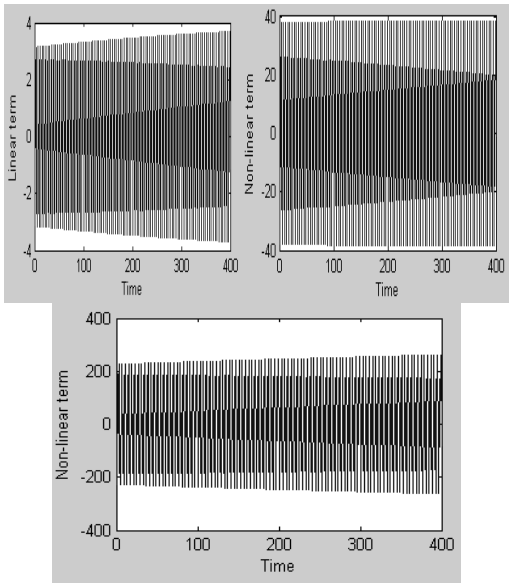


Figure 5.2: Simulation graphs for a simple pendulum (Clockwise from top left) a) Linear part b) Third harmonic c) Third and fifth harmonic

5.3. Volterra Analysis of a Lr Network

The differential equation for a LR network can be expressed as

$V(t) = Lq''(t) + Rq'(t)$ (5.3.1)

Where

V(t) is the voltage supplied

L is the inductor

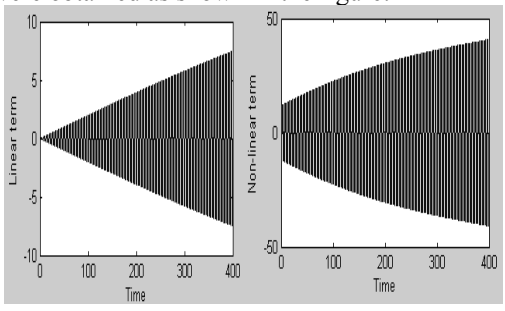
R is the resistor

q(t) is the charge

Using the force voltage analogy we get the following equation for a LR network

$y(t) = mx''(t) + b[x'(t)]^3$ (5.3.2)

Using the steps described in the section 4, this problem was simulated for A=2, b=2, m=0.001kg, k=3 and $\omega=\pi$ and graphs were obtained as shown in the figure:



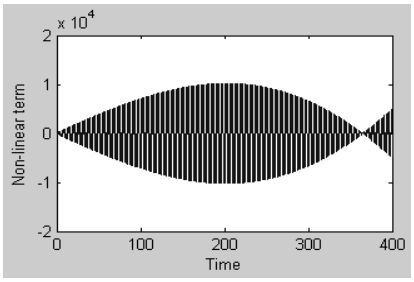


Figure 5.3: Simulation graphs for a LR network (Clockwise from top left) a) Linear part b) Third harmonic c) Third and fifth harmonic

5.4. Volterra Analysis of a Rc Network

The differential equation for a RC network can be expressed as

$$V(t) = Rq'(t) + q(t)/C \quad (5.4.1)$$

Using the force voltage analogy we get the following equation for a RC network

$$y(t) = cx'(t) + kx(t) - b[x'(t)]^3 \quad (5.4.2)$$

Using the steps described in section 4, this problem was simulated for A=2, b=2, k=3, $c=2*10^5$ and $\omega=\pi$ and graphs were obtained as shown in the figure:

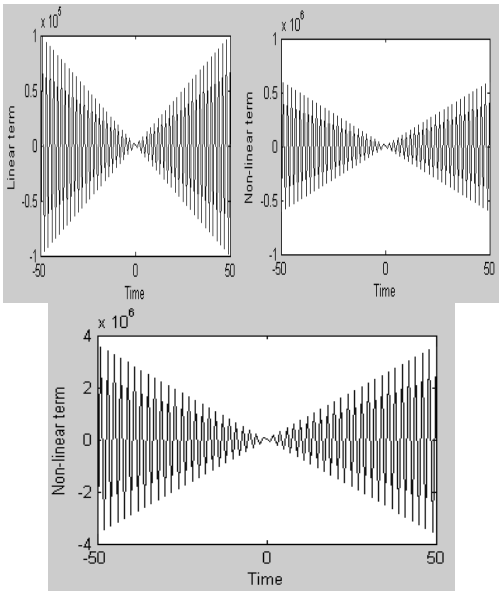


Figure 5.4: Simulation graphs for a RC network (Clockwise from top left) a) Linear part b) Third harmonic c) Third and fifth harmonic.

5.5. Volterra Analysis of A Rlc Network

The differential equation for a RLC network can be expressed as

$$V(t) = Lq''(t) + Rq'(t) + q(t)/C \quad (5.5.1)$$

RLC network can be realized by adding an external damper with the damping constant 'c' to the non linear spring system described above. This damper acts as the resistor.

The differential equation thus can be expressed as

$$y(t) = mx''(t) - b[x'(t)]^3 + c\,x'(t) + kx(t) \quad (5.5.2)$$

Applying the harmonic input method and taking x(t) as $e^{j\omega t}$, we get

$H_1[x(t)] = A*Re((cj\omega+k-m\omega^2)e^{3j\omega t})$

$H_3[x(t)] = 2(A/2)^3*(Re((27bj\omega^3)e^{3j\omega t}) + Re(3(2k-12bj\omega^3+2cj\omega)e^{j\omega t}))$

$H_3[x(t)] + H_5[x(t)] = 2(A/2)^3*(Re((27bj\omega^3)e^{3j\omega t}) + Re(3(2k-12bj\omega^3+2cj\omega)e^{j\omega t})) + 2(A/2)^5*(Re(5(64bj\omega^3)e^{3j\omega t}) + Re(10(-3m\omega^2+3k-54bj\omega^3+3cj\omega)e^{j\omega t}))$

Using the steps described in section 4, this problem was simulated for A=2, b=2, m=0.001kg, k=3, $\omega=\pi$ and $c=2*10^5$ and graphs were obtained as shown in the figure:

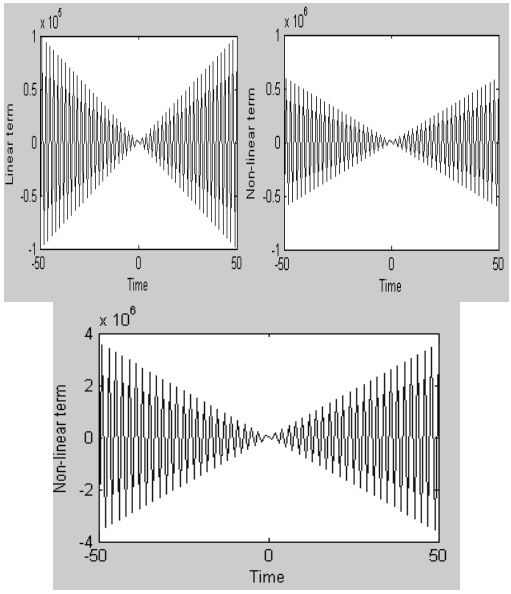


Figure 5.5: Simulation graphs for a RLC network (Clockwise from top left) a) Linear part b) Third harmonic c) Third and fifth harmonic.

6. APPLICATIONS OF VOLTERRA SERIES

The Volterra series finds application in a variety of fields ranging from medicine to system identification. It is widely used in biomedical engineering and neuroscience. It is used in electrical engineering to model intermodulation distortion in many devices including power amplifiers and frequency mixers. Its ability to provide closed form expressions for distortion components in terms of circuit parameters in analog circuits makes it an efficient method for analysis of distortion in such circuits [5].

General non-linear filters based on Volterra series are used for estimating signals corrupted by additive non Gaussian noise [6]. The series also finds use in nonparametric black-box modeling particularly for pharmacodynamics systems. These systems exploit the generality of higher order Volterra representations which can be used to describe and predict the response of an arbitrary pharmacokinetics or pharmacodynamics system without any prior knowledge on the structure of the system [7].

6. CONCLUSION

The paper discusses the application of Volterra series to non-linear mechanical as well as electrical circuits. The first, third and fifth harmonics of these non-linear systems have been simulated. The results of simulation of the differential equations of these systems show that the even order harmonics are zero while the odd order harmonics address the non linearity of the system. The results for higher order harmonics give a more accurate picture of the behavior of the system. These results show that incorporating the non-linearity of the system adds to the accuracy of system behavior representation.

FUTURE SCOPE

In an image-processing environment, it is known that linear filters are not able to remove the noise, in particular the impulsive one superimposed on a picture, without blurring the edges. Moreover, it is often necessary to take into account the intrinsic nonlinear behavior of the human visual system or of the optical imaging systems, resulting from the quadratic relation between the optical intensity and the optical field. For all these reasons, recently much attention has been drawn to the problem of nonlinear system modeling with a Volterra series expansion. Quadratic Volterra filters are used for such a purpose. Some other successful applications of volterra filters have been developed in system identification, signal processing, image processing, channel equalization, echo cancellation and telecommunication areas.

REFERENCES

[1]. Bharathy C., Sachdeva Pratima, Parthasarthy Harish, Tayal Akash, “An Introduction to Volterra Series and Its Application on Mechanical Systems”, Advanced Intelligent Computing Theories and Applications. With Aspects of Contemporary Intelligent Computing Techniques, Communications in Computer and Information Science, Volume 15. Springer-Verlag Berlin Heidelberg, 2008, p. 478.

[2]. James A Cherry, Distortion Analysis of Weakly Nonlinear Filters Using Volterra Series, Carleton University, Dept. Electronics, 1994.

[3]. Martin Schetzen, The Volterra and Wiener Theories of Nonlinear Systems, Krieger Publishing Co., Inc., Melbourne, FL, 2006.

[4]. Wilson J. Rugh, Nonlinear system theory: the Volterra-Wiener approach, Hopkins University press, London, 1981.

[5]. Euhan Chong, “The Volterra Series and the Direct Method of Distortion Analysis”, University of Toronto.

[6]. I.J. Morrison, P.J.W. Rayner, "The application of Volterra series to signal estimation," icassp, pp.1481-1484, Acoustics, Speech, and Signal Processing, 1991. ICASSP-91., 1991 International Conference on, 1991.

[7]. Verotta D ., “Volterra Series in Pharmacokinetics and Pharmacodynamics “Journal of Pharmacokinetics and Pharmacodynamics, Volume 30, Number 5, October 2003, pp. 337-362(26).

Energy Harvesting via Piezoelectricity

Tanvi Dikshit[1], Dhawal Shrivastava[2], Abhijeet Gorey[3], Ashish Gupta[4], Parag Parandkar[5] and Sumant Katiyal[6]

Abstract - In the present era, wireless data transmission techniques are commonly used in electronic devices. For powering them connection needs to be made to the power supply through wires else power may be supplied from batteries. Batteries require charging, replacement and other maintenance efforts. For example, in the applications such as villages, border areas, forests, hilly areas, where generally remote controlled devices are used, continuous charging of the microcells is not possible by conventional charging methods .So, some alternative methods needs to be developed to keep the batteries full time charged and to avoid the need of any consumable external energy source to charge the batteries.. To resolve such problems, Energy harvesting technique is proposed as the best alternative. There exists variety of energy harvesting techniques but mechanical energy harvesting happens to be the most prominent. This technique utilizes piezoelectric components where deformations produced by different means are directly converted to electrical charge via piezoelectric effect. Subsequently the electrical energy can be regulated or stored for further use. The proposed work in this research recommends Piezoelectricity as a alternate energy source. The motive is to obtain a pollution-free energy source and to utilize and optimize the energy being wasted. In this paper two important techniques are stressed upon to harness the energy viz Piezoelectric Windmill and Increased Bandwidth Piezoelectric Crystal. Current work also illustrates the working principle of piezoelectric crystal and various sources of vibration for the crystal.

Index Terms - Energy Harvesting, Piezoelectricity, Piezoelectric Windmill, Increased Bandwidth Piezoelectric Crystal

1. INTRODUCTION

Energy harvesting has been a topic of discussion and research since three decades. With the ever increasing and demanding energy needs, unearthing and exploiting more and more energy sources has become a need of the day. Energy harvesting is the process by which energy is derived from external sources and utilized to drive the machines directly, or the energy is captured and stored for future use. Some traditional energy harvesting schemes are solar farms, wind farms, tidal energy utilizing farms, geothermal energy farms and many more. With the advent of technology, utilization of these sources has increased by leaps and bounds [1]. When viewed on a large scale, energy harvesting schemes can be categorized as shown in Table I.

Type of Energy Harvesting	Energy Source	Solution	Ultimate Goal
Macro	Renewable sources like solar, wind, tidal etc.	Energy Management solutions	Reduce oil dependency
Micro	Small scale sources like vibration, motion, heat etc.	Ultra-low-power solutions	Driving low energy consuming devices

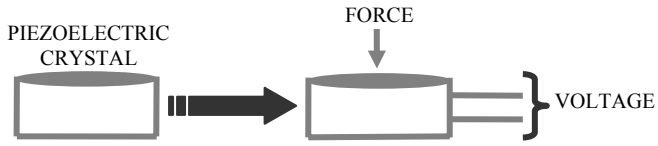
Table 1: Types of Energy Harvesting Schemes

Piezoelectric Energy Harvesting is a new and innovative step in the direction of energy harvesting. Not many researches have been carried out till now in this field, hence it is a challenging job to extract energy from piezoelectricity. Through this research paper, we will describe the basic working of a piezoelectric crystal. Then later in the paper, we have proposed the idea of combining energy from a number of piezoelectric crystals to obtain higher voltages. Certain ways of implanting the crystals at different places have also been sited in the paper. Piezoelectric crystals can be utilized to obtain voltages of very small values and hence can drive low voltage devices. Hence, Piezoelectric Energy Harvesting comes under the category of Micro scale energy harvesting scheme.

2. WORKING PRINCIPLE

The piezoelectric effect is a special material property that exists in many single crystalline materials. Examples of such crystalline structures are Quartz, Rochelle salt, Topaz, Tourmaline, Cane sugar, Berlinite ($AlPO_4$), Bone, Tendon, Silk, Enamel, Dentin, Barium Titanate ($BaTiO_3$), Lead Titanate ($PbTiO_3$), Potassium Niobate ($KNbO_3$), Lithium Niobate ($LiNbO_3$) etc.[2] There are two types of piezoelectric effect, direct piezoelectric effect and inverse piezoelectric effect. The direct piezoelectric effect is derived from materials generating electric potential when mechanical stress is applied and the inverse piezoelectric effect implies materials deformation when an electric field is applied. The energy harvesting via Piezoelectricity uses direct piezoelectric effect. The phenomenon will be clear from the diagram shown in Fig.1

[1,2,3,4,5] *Chameli Devi Institute of Technology and Management*
[6] *School of Electronics, DAV, Indore*
E-Mail: [1]tanvi.d27@gmail.com,
[2]shrivastava.dhawal@gmail.com,
[3]abhijeetgorey2006@gmail.com,
[4]ashishgupta72@rediffmail.com, [5]p_paragp@yahoo.com and
[6]sumant578@yahoo.com



Figurre1: Principle of direct piezoelectric effect

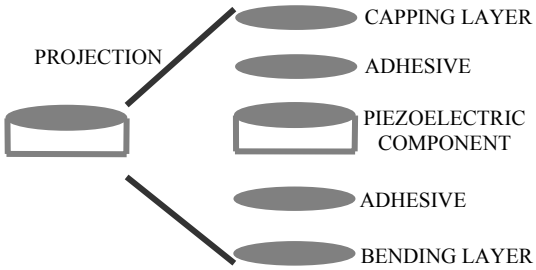


Figure 2: Structure of a piezoelectric component

Fig.2 shows the structure of a piezoelectric component being used for energy harvesting.

The output voltage obtained from a single piezoelectric crystal is in millivolts range, which is different for different crystals. And the wattage is in microwatt range. So in order to achieve higher voltages, the piezoelectric crystals can be arranged in cascading manner, that is, in series. The energy thus obtained is stored in lithium batteries or capacitors. This is the working principle behind piezoelectric energy harvesting system. Now the extreme engineering lies in optimization of piezoelectric energy, which is done in various ways. A lot of studies are being carried out in order to know which crystal will be the best to obtain maximum output voltage, what should be the structure of piezoelectric component, which type of circuit should be used at the output terminals of piezoelectric crystal in order to have maximum wattage. In the next section, we have mentioned a number of sources of vibration which are already being used for piezoelectric energy harvesting and a new idea in this direction has been proposed by us.

3. SOURCES OF VIBRATION FOR CRYSTAL PREVIOUS WORK

A. Power Generating Sidewalk

The piezoelectric crystal arrays are laid underneath pavements, side walks and other high traffic areas like highways, speed breakers for maximum voltage generation. The voltage thus generated from the array can be used to charge the chargeable Lithium batteries, capacitors etc. These batteries can be used as per the requirement [3].

B. Power Generating Boots Or Shoes

In United States Defense Advance Research Project Agency (DARPA) initiated a innovative project on Energy harvesting which attempts to power battlefield equipment by piezoelectric generators embedded in soldiers' boots [3]. However, these energy harvesting sources put an impact on the body. DARPA's effort to harness 1-2 watts from continuous shoe impact while walking were abandoned due to the discomfort from the additional energy expended by a person wearing the shoes.

C. Gyms and Workplaces

Researchers are also working on the idea of utilizing the vibrations caused from the machines in the gym. At workplaces, while sitting on the chair, energy can be stored in the batteries by laying piezoelectric crystals in the chair. Also, the studies are being carried out to utilize the vibrations in a vehicle, like at clutches, gears, seats, shock-ups, foot rests.

D. Mobile Keypad and Keyboards

The piezoelectric crystals can be laid down under the keys of a mobile unit and keyboards. With the press of every key, the vibrations created can be used for piezoelectric crystal and 1hence can be used for charging purpose [4].

E. Floor Mats, Tiles and Carpets

A series of crystals can be laid below the floor mats, tiles and carpets which are frequently used at public places.

F. People Powered Dance Clubs

In Europe, certain nightclubs have already begun to power their night clubs, strobes and stereos by use of piezoelectric crystals. The crystals are laid underneath the dance floor. When a bulk of people use this dance floor, enormous amount of voltage is generated which can be used to power the equipments of the night club [5].

4. PROPOSED WORK

A. Piezoelectric Wind Mill

In order to energize low power consuming devices, microcells are invariantly used. But these microcells need to be charged once they get discharged. Hence if the devices are placed at remote places like villages, border areas, forests, hilly areas, then continuous charging of the microcells is not possible by conventional charging methods. In such cases, alternative options like solar energy and wind energy can be utilized. But cloudy days and rains restrict the use of solar energy. So, wind energy comes out to be the best alternative [6]. The idea about a Piezoelectric Wind mill will be clear from Fig. 3.

The piezoelectric wind mill that we have proposed consists of a fan with three blades to effectively capture the wind flow. A lever arm is connected to the windmill fan rotor and a translator is connected with this lever arm to convert rotational motion into translatory motion. A disc is connected at the lower end of translator, such that whenever it moves upwards and downwards, it compresses the piezoelectric crystals. Hence for different speeds of wind also, that is for different frequencies, the Piezoelectric Wind mill may function. Hence, it has higher workable bandwidth. The constant compression of piezoelectric crystals causes a huge amount of energy to be generated, which can comfortably drive the remotely placed low power consuming devices [2]. Hence, the concept of

Piezoelectric Wind mill can be used to harness piezoelectric energy very efficiently and effectively.

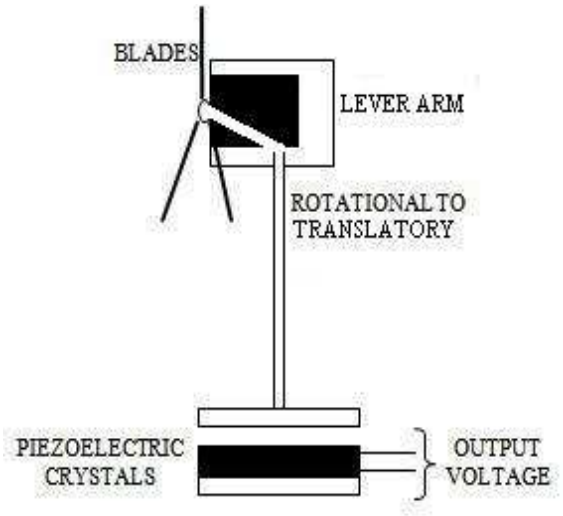


Figure 3: Piezoelectric Wind mill

B. Increased Bandwidth Piezoelectric Crystal

In order to increase the workable bandwidth, that is, in order to use piezoelectric crystals over a wide range of vibrations, we are proposing a new method. If in place of a single energy source, we make use of more than one, then the efficiency of harvesting system will definitely increase. Hence, we are making use of two energy converting techniques, one is the piezoelectric crystal and other is the electromagnetically induced voltage. Fig. 4 gives the structure of such type of system [7].

The system consists of a flexible strip, over which the piezoelectric crystals are mounted and at one end of the strip, a magnet is mounted. This magnet lies inside a stationary coil. At times, when intensity of vibration is high, voltage is obtained from piezoelectric crystals. Hence, at higher frequencies, piezoelectric crystals give the output. When intensity of vibration is less, the piezoelectric crystals do not give a considerable output. At lower frequencies, the magnet moves inside the stationary coil. This motion causes electromagnetic flux to be generated and hence an output voltage is obtained.

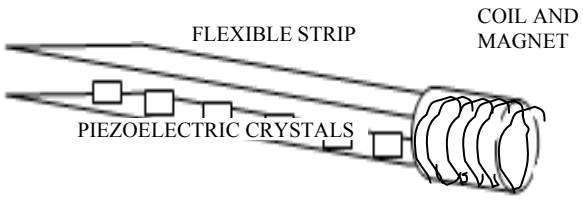


Figure 4: Piezoelectric crystals and electromagnetic energy

5. OUTPUT STAGE OF PIEZOELECTRIC ENERGY HARVESTING SYSTEM

The output of a piezoelectric crystal is alternating signal. In order to use this voltage for low power consuming electronic devices, it has to be first converted into digital signal [2]. This is done with the help of AC to DC converter as shown in Fig. 5. Fig.5 shows a simple diode rectifier to convert AC to DC. This is followed by a capacitor, which gets charged by the rectifier upto a pre-decided voltage, at which the switch closes and the capacitor discharges through the device. In this way, the energy can be stored in the capacitor, and can be discharged when required. But the energy harvesting capacity of this circuit is not appreciable. Hence, a DC to DC converter is used after bridge rectifier stage, which has been demonstrated in Fig. 6. The addition of DC-DC converter has shown an improvement in energy harvesting by a factor of 7.

A non-linear processing technique "Synchronized Switch Harvesting on Inductor" (SSHI) was also proposed in 2005 for harvesting energy [7]. It consists of a switching device in parallel with the piezoelectric element. The device is composed of a switch and an inductor connected in series. The switch is in open state except when the maximum displacement occurs in the transducer. At that instant, the switch is closed and the capacitance of the piezoelectric element and inductor together constitute an oscillator. The switch is kept closed until the voltage on the piezoelectric element has been reversed. This circuit arrangement of the output circuit is said to have a very high energy harvesting capacity. Fig. 7 shows the SSHI technique [6].

6. IMPLEMENTATION

Experimentation has been done on a Piezo-crystal and it is tested with a Light Emitting Diode (LED). The two terminals of the LED are connected with the two terminals of the crystal. Choice of Blue LED is being made for experimentation. Single stroke on the crystal blows blue LED with full intensity. Measured values of output voltage and current from the crystal come out to be 3.5 Volt and 100 milliamps. The only shortcoming of this using a single crystal and a LED was that both the voltage and current obtained exists instantaneously. To increase the range of voltage and current output, an assembly of 6 crystals in series and 6 such series has been put in parallel. When number of voltage sources are put in series, then the net voltage increases, while when a number of voltage sources are put in parallel, then the strength of signal, that is, current increases. This is the concept used behind the assembly. The output of parallel connection is fed to the current amplifier for signal strengthening and the output of series connection is fed to the amplifier for biasing purpose and also to the voltage amplifier. The assembly has been put under a doormat and the output obtained from amplifier has been very encouraging, which was around 6 V voltage and 1 ampere current. This magnitude of voltage and current can be certainly used to charge a battery. Fig. 8 shows the assembly used in our system.

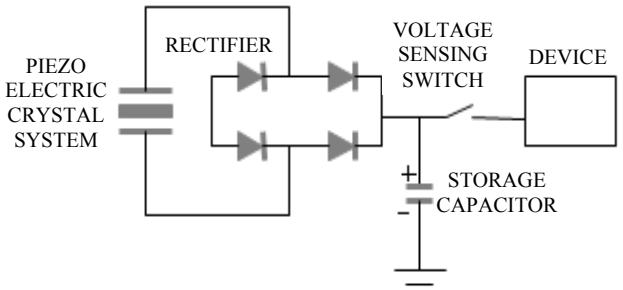


Figure 5: Bridge rectifier type AC to DC converter

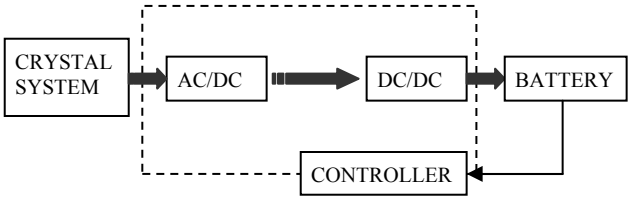


Figure 6: Energy Harvesting Circuit

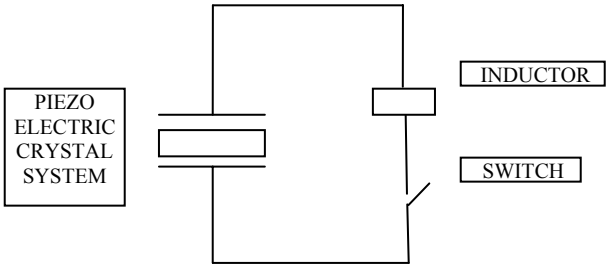


Figure 7: SSHI (Synchronized Switch Harvesting on Inductor) technique

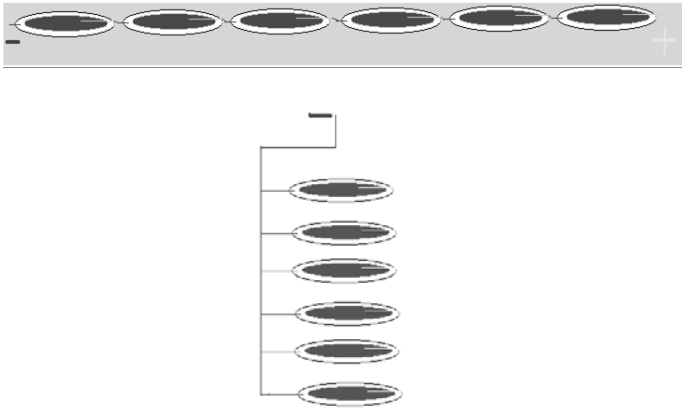


Figure 8: Series and parallel combination of crystals

6. COST EFFECTIVENESS

The assembly developed using series and parallel combination of piezo-crystals is very cost effective. A single crystal costs around 23 – 25 Rupees, and hence the cost of whole assembly is very less. It is very encouraging to get a good voltage and current at such a low cost at the same time utilizing the waste energy. So, the assembly improves on the concern of cost effectiveness to a great extent and we are working on it to further improve upon the results of the system.

7. FUTURE SCOPE

The proposed work portrays the concept of Piezoelectric Energy Harvesting and the results obtained after the implementation are very encouraging. Future work of the proposed idea encompasses further amplification of the crystal output to a greater extent. Future lies in the inclusion of advanced material used to design the piezoelectric crystal which further amplifies the crystal output in terms of voltage as well as current. A study could be carried out from the variety of piezoelectric crystals and after comparing the results, the choice of the optimum material for the best performing crystal could be devised.

8. CONCLUSION

The method used to perform power harvesting is to use PZT materials that can convert the ambient vibration energy surrounding them into electrical energy. This electrical energy can then be used to power other devices or stored for later use. This technology has gained an increasing attention due to the recent advances in wireless and MEMS technology, allowing sensors to be placed in remote locations and operate at very low power [7]. The need for power harvesting devices is caused by the use of batteries as power supplies for these wireless electronics. As the battery has a finite lifespan, recharging needs to be done once discharged. Charging of batteries in order to provide energy to the electronic devices in the applications such as borders or hilly regions is a tedious job to do. Through this paper, we have proposed two new ways of harnessing the piezoelectric energy. Implementation aspects focuses on the practical work carried out in this field of Piezoelectric Energy Harvesting. The idea of Piezoelectric Windmill will solve the problem of continuous microcell discharging in the devices being used at remote places or in rough terrains. The concept of combining two energy sources piezoelectric energy and electromagnetic energy has been proposed in the paper. So these two ideas can greatly help in harnessing the piezoelectric energy.

REFERENCES

[1]. U. K. Singh and R. H. Middleton, “Piezoelectric power scavenging of mechanical vibration energy” Australian Mining Technology Conference, 2-4 Oct. 2007, pp. 111-118.

[2]. Takeuchi M, Matsuzawa S, Tairaku K, Takatsu C. “Piezoelectric generator as power supply for RFID-tags and applications”, Proc. IEEE Ultrasonics Symposium, New York City, USA,28–31 Oct. 2007, pp. 2558–2561.

[3]. Ahola J, Särkimäki V, Ahonen T, Kosonen A, Tiainen R, Lindh T., “Design considerations of energy harvesting wireless sensors for condition monitoring of electronic motors, Proc. 5th Int. Conf. Condition Monitoring &

Machinery Failure Prevention Technologies 15–18 July 2008, Edinburgh, UK.

[4]. Roundy S., Wright P. K. and Rabaye J., "A. study of low level vibrations as a power source for wireless sensor nodes", Computer Communications 26 (2003) 1131–1144.

[5]. Steven R. Anton and Henry A. Sodano, A review of power harvesting using piezoelectric materials (2003-2006), Smart Materials and Structures 16 (2007).

[6]. Sujesha Sudevalayam, Purushottam Kulkarni, "Energy Harvesting Sensor Nodes: Survey and Implications", Dec. 19, 2008.

[7]. Y. C. Shu and I. C. Lien, "Analysis of power output for piezoelectric energy harvesting systems", Smart Materials and Structures 15 (2006), pp. 1499-1512.

Continued from page no. 254

Sr. No.	Shannon Characteristics of a Good Encryption System	Proposed Technique
3	The implementation of the process should be as simple as possible.	√
4	Errors in ciphering should not propagate and cause corruption of further information in the message.	√
5	The size of the enciphered text should be no larger than the text of the original message	√

7. LIMITATIONS

1. Every repeated word is converted by the technique to the same floating point number hence a cryptanalyst might be able to derive some information from it.
2. Any floating point no has some degree to which it can precisely store the information, the current system does not provide precision control to convert the entire string or file.

8. CONCLUSION

The proposed technique for the private key encryption system provides an excellent method of substitution of plaintext with floating point numbers that are calculated on the basis of 256 character key which user have supplied .It can be used to secure very sensitive data: - As the system provides you with two keys, in case of very high security requirements the resident key can also be altered frequently and can be used to encrypt a string or an entire file by a single floating point number thus providing a cryptanalysts almost no data to work with. As the technique compresses the original text hence can be developed as a compressing technique. It is faster, required memory space of less than 15kb and provides an efficient data security during communications.

REFERENCES

[1]. "Security in computing", Charles P.Pfleerer. W. Die, M.E. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory , 22, pp 644-654 , 1979.

[2]. Yehoshua Perl, Loizos Gabriel, Arithmetic Interpolation Search for Alphabet Tables, IEEE Transactions on Computers, v.41 n.4, p.493-499, April 1992.

[3]. Jeffrey Scott Vitter , P. Krishnan, Optimal prefetching via data compression, Journal of the ACM (JACM), v.43 n.5, p.771-793, Sept. 1996

[4]. www.apprendrenligne.net/crypto/bibliotheque/PDF/Kwang.pdf

[5]. Alistair Moffat, Radford M. Neal, Ian H. Witten, Arithmetic coding revisited, ACM Transactions on Information Systems (TOIS), v.16 n.3, p.256-294, July 1998.

[6]. X.Marsault, Compression et Cryptage des Données Multimédias, Hermes, 1997.

[7]. Eike Kiltz and John Malone-Lee. A General Construction of IND-CCA2 Secure Public Key Encryption. In: Cryptography and Coding, pages 152--166. Springer-Verlag, December 2003.

[8]. D.S Yadav "Foundations of Information Technology", 2nd Edition, New age Publishers, by, P71-79.2004.

[9]. James Keeler, Graphical implementation of Huffman and arithmetic coders, Journal of Computing Sciences in Colleges, v.19 n.5, p.289-290, May 2004.

[10]. Martijn Stam. A Key Encapsulation Mechanism for NTRU. In: Cryptography and Coding, pages 410--427. Springer-Verlag LNCS 3796, December 2005.

[11]. Bose, R. Pathak, S, A novel compression and encryption scheme using variable model arithmetic coding and coupled chaotic system ,IEEE Transactions on Circuits and Systems, Volume: 53 issue: 4 ,p. 848 - 857 ,ISSN: 1549-8328 ,April 2006.

BIJIT - BVICAM's International Journal of Information Technology

Paper Structure and Formatting Guidelines for Authors

BIJIT is a peer reviewed refereed bi-annual research journal having **ISSN 0973-5658**, being published since 2009, in both, Hard Copy as well as Soft copy. Two issues; **January – June** and **July – December**, are published every year. The journal intends to disseminate original scientific research and knowledge in the field of, primarily, Computer Science and Information Technology and, generally, all interdisciplinary streams of Engineering Sciences. **Original** and **unpublished** research papers, based on theoretical or experimental works, are published in BIJIT. We publish two types of issues; **Regular Issues** and **Theme Based Special Issues.** Announcement regarding special issues is made from time to time, and once an issue is announced to be a Theme Based Special Issue, Regular Issue for that period will not be published.

Papers for Regular Issues of BIJIT can be submitted, round the year. After the detailed review process, when a paper is finally accepted, the decision regarding the issue in which the paper will be published, will be taken by the Editorial Board; and the author will be intimated accordingly. However, for Theme Based Special Issues, **time bound Special Call for Papers** will be announced and the same will be applicable for that specific issue only.

Submission of a paper implies that the work described has not been published previously (except in the form of an abstract or academic thesis) and is not under consideration for publication elsewhere. The submission should be approved by all the authors of the paper. If a paper is finally accepted, the authorities, where the work had been carried out, shall be responsible for not publishing the work elsewhere in the same form. *Paper, once submitted for consideration in BIJIT, cannot be withdrawn unless the same is finally rejected*.

1. Paper Submission

Authors will be required to submit, MS-Word compatible (.doc, .docx), papers electronically *after logging in at our portal and accessing the submit paper link*, available at http://www.bvicam.ac.in/bijit/SubmitPaper.asp. Once the paper is uploaded successfully, our automated Paper Submission System assigns a Unique Paper ID, acknowledges it on the screen and also sends an acknowledgement email to the author at her / his registered email ID. Consequent upon this, the authors can check the status of their papers at the portal itself, in the Member Area, after login, and can also submit revised paper, based on the review remarks, from member area itself. The authors must quote / refer the paper ID in all future correspondences. Kindly note that we do not accept E-Mailic submission. To understand the detailed step by step procedure for submitting a paper, click at http://www.bvicam.ac.in/BIJIT/guidelines.asp.

2. Paper Structure and Format

While preparing and formatting papers, authors must confirm to the under-mentioned MS-Word (.doc, .docx) format:-

- The total length of the paper, including references and appendices, must not exceed **six (06) Letter Size pages**. It should be typed on one-side with double column, single-line spacing, 10 font size, Times New Roman, in MS Word.
- The Top Margin should be 1", Bottom 1", Left 0.6", and Right 0.6". Page layout should be portrait with 0.5 Header and Footer margins. Select the option for different Headers and Footers for Odd and Even pages and different for First page in Layout (under Page Setup menu option of MS Word). Authors are not supposed to write anything in the footer.
- The title should appear in single column on the first page in 14 Font size, below which the name of the author(s), in bold, should be provided centrally aligned in 12 font size. The affiliations of all the authors and their E-mail IDs should be provided in the footer section of the first column, as shown in the template.
- To avoid unnecessary errors, the authors are strongly advised to use the "spell-check" and "grammar-check" functions of the word processor.
- The complete template has been prepared, which can be used for paper structuring and formatting, and is available at http://www.bvicam.ac.in/BIJIT/Downloads/Template_For_Full_Paper_BIJIT.pdf.
- The structure of the paper should be based on the following details:-

Essential Title Page Information

- **Title:** Title should be Concise and informative. Avoid abbreviations and formulae to the extent possible.
- **Authors' Names** and **Affiliations:** Present the authors' affiliation addresses (where the actual work was done) in the footer section of the first column. Indicate all affiliations with a lower-case superscript letter immediately after the author's name

and in front of the appropriate address. Provide the full postal address of each affiliation, including the country name and e-mail address of each author.

- **Corresponding Author:** Clearly indicate who will handle correspondence at all stages of refereeing and publication. Ensure that phone numbers (with country and area code) are provided, in addition to the e-mail address and the complete postal address.

Abstract

A concise abstract not exceeding 200 words is required. The abstract should state briefly the purpose of the research, the principal results and major conclusions. References and non-standard or uncommon abbreviations should be avoided. As a last paragraph of the abstract, 05 to 10 Index Terms, in alphabetic order, under the heading Index Terms ***(Index Terms - …….)*** must be provided.

NOMENCLATURE

Define all the abbreviations that are used in the paper and present a list of abbreviations with their definition in Nomenclature section. Ensure consistency of abbreviations throughout the article. Do not use any abbreviation in the paper, which has not been defined and listed in Nomenclature section.

Subdivision - numbered sections

Divide paper into numbered Sections as 1, 2, 3, ….. and its heading should be written in CAPITAL LETTERS, bold faced. The subsections should be numbered as 1.1 (then 1.1.1, 1.1.2, ...), 1.2, etc. and its heading should be written in Title Case, bold faced and should appear in separate line. The Abstract, Nomenclature, Appendix, Acknowledgement and References will not be included in section numbering. In fact, section numbering will start from Introduction and will continue till Conclusion. All headings of sections and subsections should be left aligned.

INTRODUCTION

State the objectives of the work and provide an adequate background, with a detailed literature survey or a summary of the results.

Theory/Calculation

A Theory Section should extend, not repeat the information discussed in Introduction. In contrast, a Calculation Section represents a practical development from a theoretical basis.

RESULT

Results should be clear and concise.

DISCUSSION

This section should explore the importance of the results of the work, not repeat them. A combined Results and Discussion section is often appropriate.

CONCLUSION AND FUTURE SCOPE

The main conclusions of the study may be presented in a short Conclusion Section. In this section, the author(s) should also briefly discuss the limitations of the research and Future Scope for improvement.

APPENDIX

If there are multiple appendices, they should be identified as A, B, etc. Formulae and equations in appendices should be given separate numbering: Eq. (A.1), Eq. (A.2), etc.; in a subsequent appendix, Eq. (B.1) and so on. Similar nomenclature should be followed for tables and figures: Table A.1; Fig. A.1, etc.

ACKNOWLEDGEMENT

If desired, authors may provide acknowledgements at the end of the article, before the references. The organizations / individuals who provided help during the research (e.g. providing language help, writing assistance, proof reading the article, sponsoring the research, etc.) may be acknowledged here.

REFERENCES

Citation in text

Please ensure that every reference cited in the text is also present in the reference list (and vice versa). The references in the reference list should follow the standard IEEE reference style of the journal and citation of a reference.

Web references

As a minimum, the full URL should be given and the date when the reference was last accessed. Any further information, if known (DOI, author names, dates, reference to a source publication, etc.), should also be given. Web references can be listed separately (e.g., after the reference list) under a different heading if desired, or can be included in the reference list, as well.

Reference style

Text: Indicate references by number(s) in square brackets in line with the text. The actual authors can be referred to, but the reference number(s) must always be given. Example: '..... as demonstrated [3,6]. Barnaby and Jones [8] obtained a different result ....'

List: Number the references (numbers in square brackets) in the list, according to the order in which they appear in the text.

Two sample examples, for writing reference list, are given hereunder:-

Reference to a journal publication:

[1] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread-spectrum watermarking for multimedia", *IEEE Transactions on Image Processing*, Vol. 6, No. 12, pp. 64 – 69, December 1997.

Reference to a book:

[2] J. G. Proakis and D. G. Manolakis – Digital Signal Processing – Principles, Algorithms and Applications; Third Edition; Prentice Hall of India, 2003.

Mathematical Formulae

Present formulae using Equation editor in the line of normal text. Number consecutively any equations that have to be referred in the text

Captions and Numbering for Figure and Tables

Ensure that each figure / table has been numbered and captioned. Supply captions separately, *not attached to the figure*. A caption should comprise a brief title and a description of the illustration. Figures and tables should be numbered separately, but consecutively in accordance with their appearance in the text.

3. Style for Illustrations

All line drawings, images, photos, figures, etc. will be published in black and white, in Hard Copy of BIJIT. Authors will need to ensure that the letters, lines, etc. will remain legible, even after reducing the line drawings, images, photos, figures, etc. to a two-column width, as much as 4:1 from the original. However, in Soft Copy of the journal, line drawings, images, photos, figures, etc. may be published in colour, if requested. For this, authors will need to submit two types of Camera Ready Copy (CRC), after final acceptance of their paper, one for Hard Copy (compatible to black and white printing) and another for Soft Copy (compatible to colour printing).

4. **Referees**

Please submit, with the paper, the names, addresses, contact numbers and e-mail addresses of three potential referees. Note that the editor has sole right to decide whether or not the suggested reviewers are to be used.

5. Copy Right

Copyright of all accepted papers will belong to BIJIT and the author(s) must affirm that accepted Papers for publication in **BIJIT** must not be re-published elsewhere without the written consent of the editor. To comply with this policy, authors will be required to submit a signed copy of Copyright Transfer Form, available at http://bvicam.ac.in/bijit/Downloads/BIJIT-Copyright-Agreement.pdf, after acceptance of their paper, before the same is published.

6. Final Proof of the Paper

One set of page proofs (as PDF files) will be sent by e-mail to the corresponding author or a link will be provided in the e-mail so that the authors can download the files themselves. These PDF proofs can be annotated; for this you need to download Adobe Reader version 7 (or higher) available free from http://get.adobe.com/reader. If authors do not wish to use the PDF annotations function, they may list the corrections and return them to BIJIT in an e-mail. Please list corrections quoting line number. If, for any reason, this is not possible, then mark the corrections and any other comments on a printout of the proof and then scan the pages having corrections and e-mail them back, within 05 days. Please use this proof only for checking the typesetting, editing, completeness and correctness of the text, tables and figures. Significant changes to the paper that has been accepted for publication will not be considered at this stage without prior permission. It is important to ensure that all corrections are sent back to us in one communication: please check carefully before replying, as inclusion of any subsequent corrections cannot be guaranteed. Proofreading is solely authors' responsibility. Note that BIJIT will proceed with the publication of paper, if no response is received within 05 days.

BVICAM'S International Journal of Information Technology (BIJIT)

(A Biannual Publication; ISSN 0973 - 5658)

Subscription Rates

Category	I Year		3 Years	
	India	**Abroad**	**India**	**Abroad**
Companies	Rs. 400	US $ 45	Rs. 1000	US $ 120
Institution	Rs. 300	US $ 40	Rs. 750	US $ 100
Individuals	Rs. 250	US $ 30	Rs. 600	US $ 075
Students	Rs. 150	US $ 25	Rs. 375	US $ 050
Single Copy	Rs. 250	US $ 25	-	-

Subscription Order Form

Please find attached herewith Demand Draft No._____ dated _____

For Rs._____ drawn on _____Bank in favor of **Director, "Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi"** for a period of 01 Year / 03 Years

Subscription Details

Name and Designation _____

Organization _____

Mailing Address _____

_____ PIN/ZIP _____

Phone (with STD/ISD Code)_____FAX_____

E-Mail (in Capital Letters)_____

Date: **Signature**

Place: (with official seal)

Filled in Subscription Order Form along with the required Demand Draft should be sent to the following address:-

Prof. M. N. Hoda
Chief Editor – BIJIT,
Director, Bharati Vidyapeeth's
Institute of Computer Applications & Management
A-4, Paschim Vihar, Rohtak Road, New Delhi-110063 (INDIA).
Tel.: 91 – 11 – 25275055 Fax: 91 – 11 – 25255056 E-Mail: bijit@bvicam.ac.in
Visit us at: www.bvicam.ac.in

Announcement & Call for Papers

BHARATI VIDYAPEETH PUNE

Bharati Vidyapeeth's Institute of Computer Applications & Management

A-4, Paschim Vihar, Rohtak Road, New Delhi-63

Jointly with

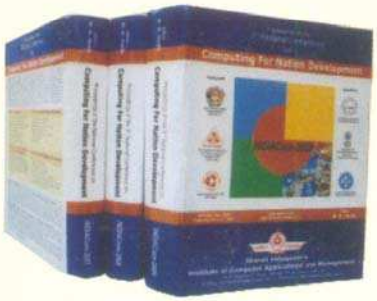
GURU GOBIND SINGH INDRAPRASTHA UNIVERSITY

IEEE COMPUTER SOCIETY Delhi Section

The Institution of Electronics and Telecommunication Engineers (IETE), Delhi Centre

ISTE, Delhi Section

BVP CSI Students' Branch, New Delhi



(Copies of the proceedings of past ***INDIACom***s)

Correspondence

All correspondences related to the conference may be sent to the address:

Prof. M. N. Hoda
Chief Convener, *INDIACom* - **2011**
Director, Bharati Vidyapeeth's
Institute of Computer Applications and Management
A-4, Paschim Vihar, Metro Station Paschim Vihar (E),
Rohtak Road, New Delhi-63
Tel.: 011-25275055, TeleFax: 011-25255056, 09212022066 (Mobile)
E-Mails: conference@bvicam.ac.in, indiacom2011@gmail.com
For further details, visit us at: http://www.bvicam.ac.in

INDIACom-2011

5th National Conference on

Computing For Nation Development

(10th-11th March, 2011)

Information and communication technologies play a dramatic impact on effectiveness, efficiency, growth and development in various areas such as education, health-care & modernization. Foreseeing the importance and impact of the above and encouraged by the resounding success met with the previous Four editions of the INDIACom(s); INDIACom-2010, INDIACom-2009, INDIACom–2008 and INDIACom– 2007; we hereby announce **INDIACom – 2011**, which aims to develop a strategic plan for balanced growth of our economy through IT in critical areas like E-Governance, E-Commerce, Disaster Management, GIS, Nano-Technology, Intellectual Property Rights, AI and Expert Systems, Networking, Software Engineering and other Emerging Technologies.

The **INDIACom - 2011** intends to bring eminent academicians, scientists, researchers, industrialists, technocrats, government representatives, social visionaries and experts from all strata of society, under one roof, to explore the new horizons of innovative technology to identify opportunities using IT and defining the path forward. This new path will envision to eliminate isolation, discourage redundant efforts and promote scientific progress aimed to accelerate India's overall growth to prominence on the International front. The INDIACom - 2011 will feature regular paper presentation sessions, invited talks, key note addresses, panel discussions and poster exhibitions. More than 700 papers have been received from over 950 authors from all over country. Eminent speakers from Academia, Industry and Government have already confirmed to participate in INDIACom -2011. Our previous editions of Pre-Conference Proceedings have widely been appreciated from all academic circles. As earlier, this year also, we will publish both soft and hard copies of the Pre-Conference Proceedings with ISSN and ISBN serials. Maximum benefits from this event can be derived by participating in huge number and together making it a grand success. Further details are available at our website **www.bvicam.ac.in/indiacom**.

Registration Fee :

	Early Bird on or before 18th December, 2010 (in Rs.)		After 18th December, 2010 (in Rs.)		Spot Registration (only in Cash)	
Category of Delegates/ Authors	***CSI/IETE IEEE/ISTE Members**	**General**	***CSI/IETE IEEE/ISTE Members**	**General**	***CSI/IETE IEEE/ISTE Members**	**General**
Students# (Delegates only)	600.00	800.00	800.00	1000.00	1000.00	1200.00
Teachers/Research Scholars	2200.00	2500.00	2700.00	3000.00	3000.00	3500.00
Industry	3000.00	3500.00	3500.00	4000.00	4000.00	4500.00

10% discount will be given on three or more registrations from one organization in General Category only.

* Members must mention their membership number of CSI / IETE /IEEE/ISTE.

#***Authors can not register under Students Category.*** Bonafide students as on 31st January, 2011, must submit the Bonafide certificate from their Institute / College /Department. Students will not be given the hard copy of the Conference Proceeding. Soft copy will only be given.

The registration fee includes tea, lunch, conference kit and the Soft and hard copies of Conference Proceedings along with other printed materials related to the conference. The payment can be made in Cash in the office of the Institute or by Demand Draft in favour of **Director, Bharati Vidyapeeth's Institute of Computer Applications and Management,** payable at **New Delhi.**

NSC-2011

4th National Students' Convention on

Computing For Nation Development

(12th March, 2011)

Bharati Vidyapeeth's CSI Students' Branch is also organizing 4th National Students' Convention (NSC-2011) on the same theme of **"Computing For Nation Development"** on 12th March, 2011. Further details are available in the attached brochure and also on the website **www.bvicam.ac.in/nsc**