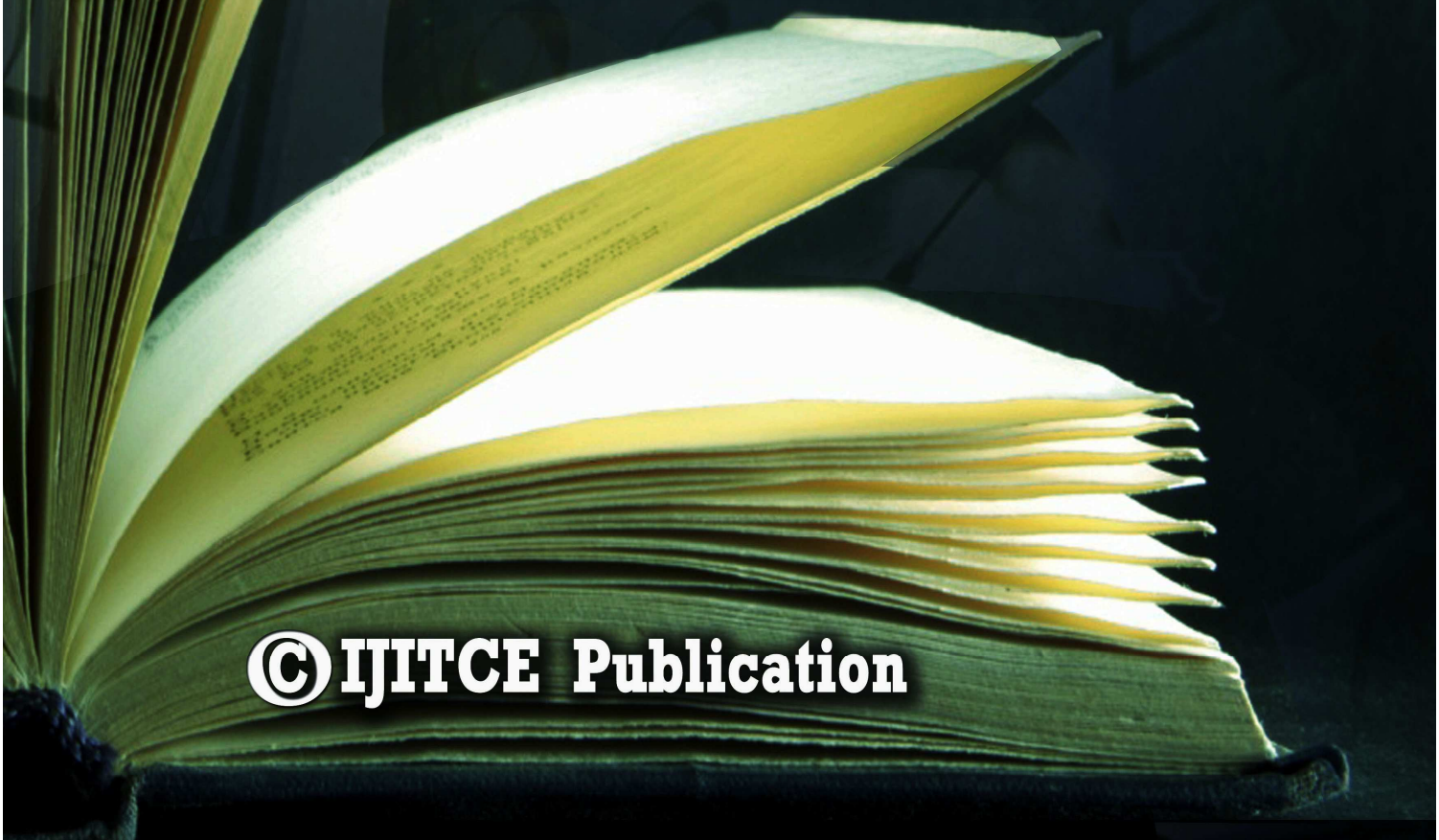
ISSN(online):2045-8711
ISSN(print):2045-869x

International Journal Of Innovative Technology & Creative Engineering

FEBRUARY 2012

vol-2 No-2



UK: Managing Editor
International Journal of Innovative Technology and Creative Engineering
1a park lane,
Cranford
London
TW59WA
UK
E-Mail: editor@ijitce.co.uk
Phone: +44-773-043-0249

USA: Editor
International Journal of Innovative Technology and Creative Engineering
Dr. Arumugam
Department of Chemistry
University of Georgia
GA-30602, USA.
Phone: 001-706-206-0812
Fax:001-706-542-2626

India: Editor
International Journal of Innovative Technology & Creative Engineering
Dr. Arthanariee. A. M
Finance Tracking Center India
17/14 Ganapathy Nagar
2nd Street
Ekkattuthangal
Chennai -600032
Mobile: 91-7598208700

IJITCE PUBLICATION

INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY & CREATIVE ENGINEERING

Vol.2 No.2

February 2012

www.ijitce.co.uk

From Editor's Desk

Dear Researcher,

Greetings!

Research articles in this issue discusses about angles of repose of digested palm fruit mash, analyzing the distribution system under uncertain variations in the loads, Semantic rich web search engine, analysis of the attacks on public key RSA cryptosystem.

Let us review research around the world this month; USB stick can sequence DNA in seconds. It looks like an ordinary USB memory stick, but a little gadget that can sequence DNA while plugged into your laptop could have far-reaching effects on medicine and genetic research. The UK company Oxford Nanopore Technologies built the device, called MinION, and claims it can sequence simple genomes - such as those of some viruses and bacteria - in a matter of seconds.

Single atom transistor gets precise position on chip. The basic unit of matter could become the basic unit of computing. A lone atom of phosphorus embedded in a sheet of silicon has been made to act as a transistor. It is not the first single-atom transistor, but it can be much more precisely positioned than its predecessors, potentially making it a lot more useful. To dictate the exact position of their single atom, Michelle Simmons at the University of New South Wales, Australia, and colleagues started by covering a silicon sheet with a layer of hydrogen. Then they used the tip of a scanning tunnelling microscope to remove hydrogen atoms according to a precise pattern. They exposed two perpendicular pairs of exposed silicon strips plus a tiny rectangle made of just six silicon atoms that sat at the junction between these strips.

Japan's third-largest mobile carrier launched a new high-speed service with a portable Wi-Fi router that will support download speeds of up to 76Mbps.Softbank said its 4G wireless network, first announced last year, will eventually support devices with speeds of up to 110Mbps, faster than many wired connections provide.

It has been an absolute pleasure to present you articles that you wish to read. We look forward to many more new technology-related research articles from you and your friends. We are anxiously awaiting the rich and thorough research papers that have been prepared by our authors for the next issue.

Thanks,
Editorial Team
IJITCE

Editorial Members

Review Board Members

Dr.A.Kathirvell, B.E, M.E, Ph.D,MISTE, MIACSIT, MENGG
Professor - Department of Computer Science and Engineering,Tagore Engineering College, Chennai

Dr. H. S. Fadewar B.sc,M.sc,M.Phil.,ph.d,PGDBM,B.Ed.
Associate Professor - Sinhgad Institute of Management & Computer Application, Mumbai-Banglore Westernly Express Way Narhe, Pune - 41

Dr. David Batten
Leader, Algal Pre-Feasibility Study,Transport Technologies and Sustainable Fuels,CSIRO Energy Transformed Flagship Private Bag 1,Aspendale, Vic. 3195,AUSTRALIA

Dr R C Panda
(MTech & PhD(IITM);Ex-Faculty (Curtin Univ Tech, Perth, Australia))Scientist CLRI (CSIR), Adyar, Chennai - 600 020,India

Miss Jing He
PH.D. Candidate of Georgia State University,1450 Willow Lake Dr. NE,Atlanta, GA, 30329

Jeremiah Neubert
Assistant Professor,Mechanical Engineering,University of North Dakota

Hui Shen
Mechanical Engineering Dept,Ohio Northern Univ.

Dr. Xiangfa Wu, Ph.D.
Assistant Professor / Mechanical Engineering,NORTH DAKOTA STATE UNIVERSITY

Seraphin Chally Abou
Professor,Mechanical & Industrial Engineering Depart,MEHS Program, 235 Voss-Kovach Hall,1305 Ordean Court,Duluth, Minnesota 55812-3042

Dr. Qiang Cheng, Ph.D.
Assistant Professor,Computer Science Department Southern Illinois University CarbondaleFaner Hall, Room 2140-Mail Code 45111000 Faner Drive, Carbondale, IL 62901

Dr. Carlos Barrios, PhD
Assistant Professor of Architecture,School of Architecture and Planning,The Catholic University of America

Y. Benal Yurtlu
Assist. Prof. Ondokuz Mayis University

Dr. Lucy M. Brown, Ph.D.
Texas State University,601 University Drive,School of Journalism and Mass Communication,OM330B,San Marcos, TX 78666

Dr. Paul Koltun
Senior Research ScientistLCA and Industrial Ecology Group,Metallic & Ceramic Materials CSIRO Process Science & Engineering

Dr.Sumeer Gul
Assistant Professor,Department of Library and Information Science,University of Kashmir,India

Dr. Chutima Boonthum-Denecke, Ph.D
Department of Computer Science,Science & Technology Bldg., Rm 120,Hampton University,Hampton, VA 23688

Dr. Renato J. Orsato
Professor at FGV-EAESP,Getulio Vargas Foundation,São Paulo Business School,Rua Itapeva, 474 (8° andar) 01332-000, São Paulo (SP), Brazil

Dr. Wael M. G. Ibrahim
Department Head-Electronics Engineering Technology Dept.School of Engineering Technology ECPI College of Technology 5501 Greenwich Road - Suite 100,Virginia Beach, VA 23462

Dr. Messaoud Jake Bahoura
Associate Professor-Engineering Department and Center for Materials Research Norfolk State University,700 Park avenue,Norfolk, VA 23504

Dr. V. P. Eswaramurthy M.C.A., M.Phil., Ph.D.,
Assistant Professor of Computer Science, Government Arts College(Autonomous), Salem-636 007, India.

Contents

INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY & CREATIVE ENGINEERING (ISSN:2045-8711)
VOL.2 NO.2 FEB 2012

DEVELOPING SEMANTIC RICH WEB SEARCH ENGINE

Mr. Suneet Joshi , Mr. Ashish Jain , Dr Binod Kumar
suneetjoshi_2000@yahoo.com
Assistant Professor in Medicaps Inst. of Science & Tech, Indore
Associate Professor IET DAVV , Indore
Assoc. Professor in Computer Sc. Dept. at Medi-Caps Institute of Science & Tech. , Indore

Abstract-The amount and variety of information on the World Wide Web (Web) is increasing in an unstructured way. This makes navigation and retrieval of information a difficult and sometimes frustrating process. For instance, Web search engines are becoming less effective as the documents available on the Web proliferate and users' queries return hundreds of links. Users may become lost or frustrated because navigation is unintuitive and semantic meanings are not used to evaluate the relevance of the links, most of which may be unrelated to what the user wants. Gathering useful and interesting information from the Web or discovering knowledge from hypertext data is a problem that may be solved by implementing measures to make Web information understandable by a Web search engine or other types of software [8]. This project discusses about to classify web search data according to the need of web search engine user. Classification leads' the sorting, indexing, combining different results, categorized the output data. More over it provide a help to write query for the search engine.

Keyword: www, web search engine, sorting, indexing, query.

I. INTRODUCTION

A web search engine is designed to search for information on the World Wide Web and FTP servers [1]. The search results are generally presented in a list of results and are often called hits. The information may consist of web pages, images, information and other types of files. Some search engines also mine data available in databases or open directories. Unlike web directories [2], which are maintained by human editors, search engines operate algorithmically or are a mixture of algorithmic and human input.

II. PROBLEM DEFINITION AND PROPOSED SOLUTION

The task is to apply semantic search which seeks to improve search accuracy by understanding searcher intent and the contextual meaning of terms as they appear in the searchable data space, to generate more relevant results.

- Our objective is to increase relevancy in existing web search by gathering useful information from the Web based on user's interest.
- To classify web search data according to the interest and need of web search engine user.
- The aim of introducing semantics and structures to the Web is to enhance the precision of search engines and to enable the use of logical reasoning in Web documents to answer users' queries.

A. Disambiguation

- By giving the query "Jaguar" user may mean either Jaguar car or Jaguar animal.
- By giving the query "Apple" user may mean either Apple company or Apple as a fruit.

B. Proposed Solution

We will develop a search engine which improves search accuracy by taking input from the user about what actually he/she wants to search (ex. "Apple" is either a fruit or a Company). Then our system will filter the contents of web pages, reject irrelevant web pages and displays the web pages which are most relevant and close to query condition to the top of the list.

III. SCOPE

We will develop web search engine that will do filtering and sorting of web pages [3]. We will develop a web search engine that becomes capable of analyzing all the data on the Web – the content, links, and transactions between people and computers.

IV. OBJECTIVE OF PROJECT

- Our objective is to improve retrieval effectiveness in web search by gathering useful information based on user's interest. That is, to identify that portion of the web that is truly relevant to one user's interests.
- To classify web search data according to the interest and need of web search engine user.
- The aim of introducing semantics and structures to the Web is to enhance the precision of search engines.
- The goal is to deliver the precise information queried by a user rather than have a user sort through a list of loosely related keyword results.

V. MY WORK

- I have made enhancement in search engine, in which I have captured search results of Yahoo!, Google and MSN and then filter and refine and then display those search results according to user's interests and inputs.
- A user profile is made and software gives accurate feedback to the information queried by user according to user logged in (web search personalization).

VI. TECHNIQUE USED- RELEVANCE FEEDBACK

- Relevance feedback is one of the techniques for improving retrieval effectiveness [5].
- Steps:

(1) The user first identifies some relevant and some irrelevant documents in the initial list of retrieved documents
(2) The system expands the query q by extracting some additional terms from the sample relevant and irrelevant documents to produce new query q'.
(3) Perform a second round of retrieval.

An enormous improvement can be seen after a single iteration of this technique.

I have used Google's Web search API and Yahoo! BOSS API to display and use search results for my project. It gives the ability to take the search results and re-use them in anyway we want.

VII. SYSTEM ARCHITECTURE

- To implement our system we divide our complete system into two parts; these two different parts work together to form a complete system:

(i) In the first phase we design search engine, knowledge base, and knowledge retrieval and adaptation system.
(ii) In the next phase we work on the results of the system. For this purpose we take input from the user and perform filtering and sorting on the search results [3]

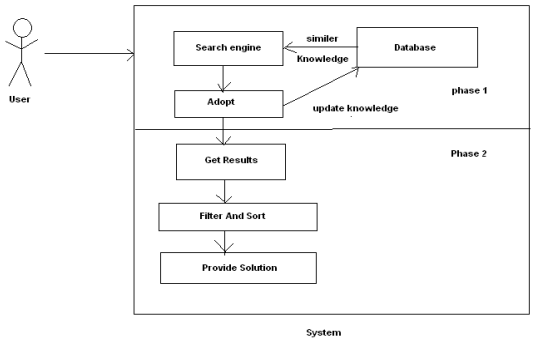


Fig 1 :System Architecture

A. *Subsystem Architecture*

Above given system is the combination of two phases to achieve the desired goal. These phases are created by the small and complete subsystems. In this section we discuss each of them.

Phase 1: This phase involve making a better search by writing the effective query using semantic knowledge.

a. Search engine: it is an existing web search engine to make a search for the user. User directly interacts with this.
b. Database: it is a knowledge base designed by us to store the user query and its use. This is for knowledge storage and retrieval for the system.
c. Adopt: it is an algorithm to fetch the similar knowledge from the database and provide help to the user to write a effective query for it. It is also used for make changes over the knowledge to design the representation of search results [6, 7].

Phase 2: in this phase we are concentrating on the result produced by the search engine and make it easy to use for the user.

d. Get results: we are collecting all output results on the temporary table to make effective and fast searchable results.
e. Filter and sort: in this step we get input a table that holds results temporarily and categorized and sort according to user need [4].
f. Provide solution: this is final step of our application system in this step we are map our results on the user screen.

B. *Algorithm Used*

1. Add Knowledge to database

(i.) Get a phrase by user (User Query).
(ii.) Add to different search engine
(iii.) Check the phrase in knowledge base
Check page hits on phrase
Else
Add to knowledge base and page hits.

2. pseudocode

(i.) Get inputphrase(User Query)
(ii.) Parse into words
(iii.) Apply on existing search engine

```
if (WordFound)
        {
          if (PageFound)
           {
             ListAllPages.Rankwise ();
           }
          else
           {
             add PageToKnowledgeBase();
           }
                                                    update PageRanks ();
                                                  }
                                                else
                                                  {
                                                    add new word to KnowledgeBase ();
                                                    update pages to KnowledgeBase ();
                                                  }
```

(v.) List predictive results as well as existing search results.

C. Implementation Steps

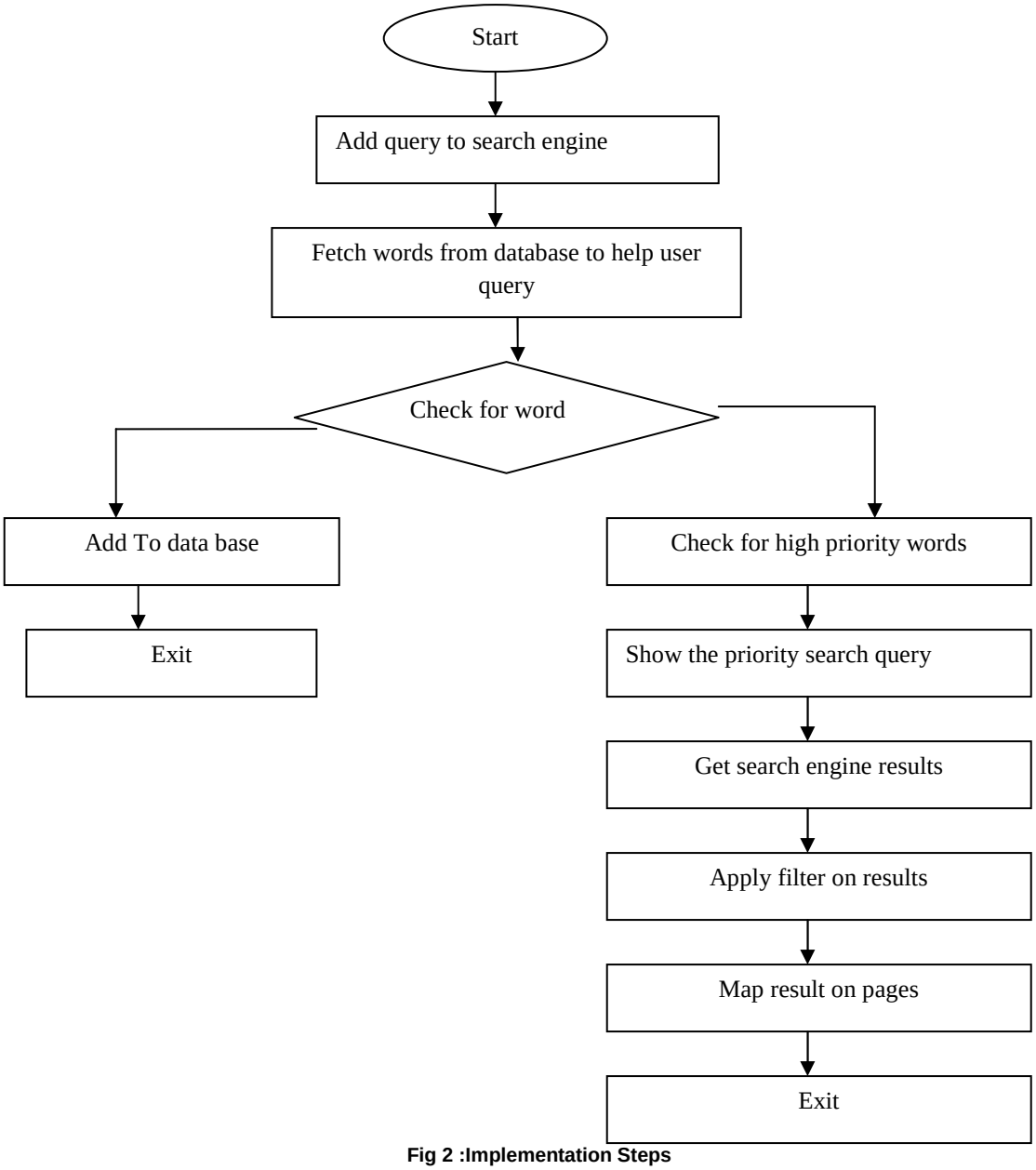
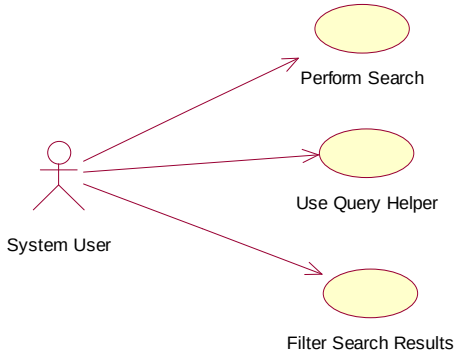


Fig 2 :Implementation Steps

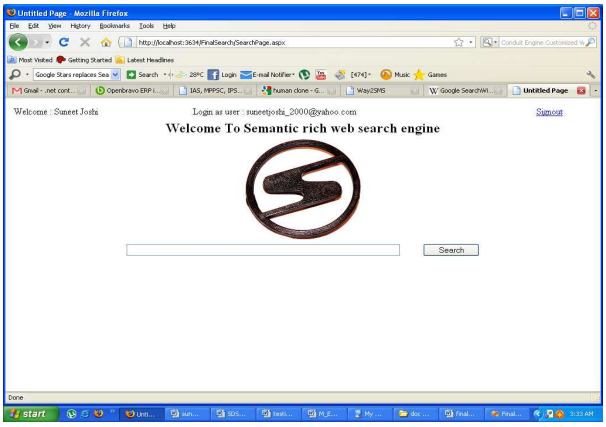
In above diagram we describe the basic steps to implement our application. When user want to make query to the search engine then according to the user query we will show the most common searches related to these word. These words are stored in database and using the probability function we get the direction of search. If word related to the user defined query is not found in database we add it to the database for future use. After that search engine return a result from web we store it to the temporarily and sort and categorized according to the user's last query.

VIII. USE CASE DIAGRAM

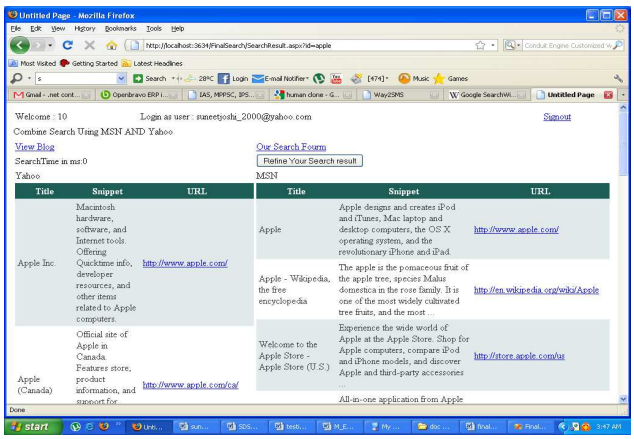


IX. SCREEN AND REPORT FORMATS

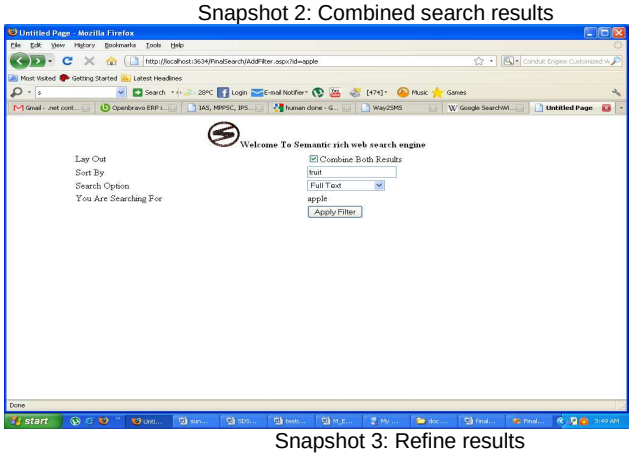
1. Home Page: there is an option for user to choose any search engine from yahoo, google, MSN and/or or optimize search engine.



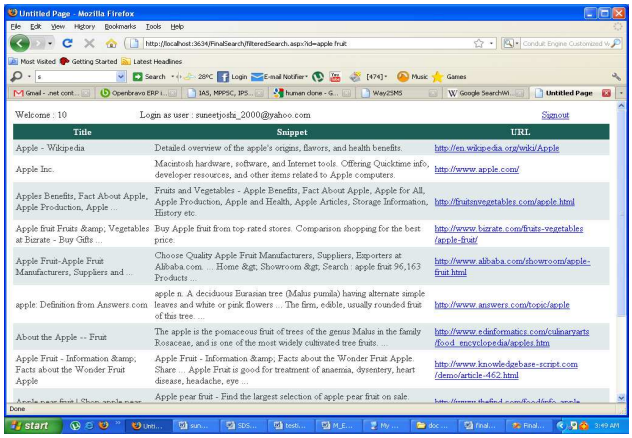
Snapshot 1: our optimized search engine



Snapshot 2: Combined search results



Snapshot 3: Refine results



Snapshot 4: Final Result

X. CODING FOR FINAL SEARCH (FILTER SEARCH RESULTS):

```
Imports net.bing.api
Imports System.Data
Partial Class filteredSearch
   Inherits System.Web.UI.Page
   Const AppId As String =
"A68DE51D46856A4F8B0E4AE5C6708E2DAFF68810"
   Public m_Resuls1 As New DataTable("MSN")
   Public dt As New DataTable("a")
   Public dtI As New DataTable("b")
   Public dtN As New DataTable("c")
   Protected Sub Page_Load(ByVal sender As Object, ByVal e
As System.EventArgs) Handles Me.Load
      Try
         If Session("User") = Nothing Then
            Response.Redirect("Login.aspx")
         End If
         Dim str As String
         str = Request.QueryString("id")
         Dim str1 As String
         str1 = Request.QueryString("type")
         Label1.Text = Session("User").ToString
         Label2.Text = Session("UName").ToString
         Using service As BingService = New BingService
            Try
               If str1 = "Relavent Search" Then
                  Dim request As SearchRequest =
BuildRequest(str, str1)
                  m_Resuls1.Columns.Add("title")
                  m_Resuls1.Columns.Add("snippet")
                  m_Resuls1.Columns.Add("url")
                  Dim response As SearchResponse =
service.Search(request)
                  Dim builder As New System.Text.StringBuilder
                  Dim result As WebResult
                  For Each result In response.Web.Results
                     Dim row As Data.DataRow
                     row = m_Resuls1.NewRow
                     row("title") = result.Title
                     row("snippet") = result.Description
                     row("url") = result.Url
                     m_Resuls1.Rows.Add(row)

                  Next
                  GridView1.DataSource = m_Resuls1
                  GridView1.DataBind()


   End Sub
```

XI. CONCLUSION

Search results of Google, Yahoo! And MSN search engines are filtered and refined. The precision of search engine is enhanced. The information queried by the user is precisely and unambiguously delivered. We are making enhancement according to user interest. Adding feed back to the system. Using intelligent data base refine search according to user data.

XII. FUTURE ENHANCEMENT

We can develop an improved rank algorithm for search engines based on domain ontology and categorization technology in order to make the algorithm simulate the actual user behaviors in browsing web pages more accurate. More iteration can be provided in order to improve search results (tree form) [until user satisfaction].

REFERENCES

[1] *Rakesh Agrawal, Thomas Imielinski, and Arun Swami. Mining associations between sets of items in massive databases. In Proc. of the ACM SIGMOD Int'l Conference on Management of Data, 1993.*

[2] *Sergey Brin and L. Page. The anatomy of large-scale hypertextual web search engine. In Proceedings of the Seventh International World Wide Web Conference, 1998.*

[3] *Robert Cooley, Pang-Ning Tan, and Jaideep Srivastava. Websift: The web site information filter system. In Proceedings of the Web Usage Analysis and User Profiling Workshop, 1999.*

[4] *J Dean and M. R. Henzinger. Finding related pages in world wide web. In Proceedings of the Eighth International World Wide Conference, 1999.*

[5] *Ronny Kohavi and Carla Brodley. Knowledge discovery and data mining cup part of SIGKDD 2000*

[6] *V.N. Padmanabham and J.C. Mogul. Using predictive prefetching to improve world wide web latency. Computer Communication Review, 1996..*

[7] *M. Deshpande and G. Karypis. Selective markov models for predicting web page accesses. Transactions on Internet Technology, 4(2):163–184, 2004.*

[8] *N. R. Mabroukeh and C. I. Ezeife. Using domain ontology for semantic web usage mining and next page prediction. In Proceedings of the 18th ACM Conference on Information and Knowledge Management (CIKM 2009), November, 2-6 2009.*

A Comparative analysis of the attacks on public key RSA cryptosystem

Varun Shukla

Research Scholar,RKDF-IST, RGPV,BHOPAL,Varun.shuklaa@gmail.com

Abhishek Choubey

Head of Department of Electronics and Communication,RKDF-IST,RGPV, BHOPAL
abhishekchoubey84@gmail.com

***Abstract*— The RSA is widely used public-key cryptosystem. RSA is intensively used for encryption methods and digital signature. It is purposely used in securing e-commerce and e-mail, providing authenticity of e- documents. It can be said that Internet security depends prominently on the security of the RSA cryptosystem. Since its discovery, the RSA cryptosystem has been extensively analysed for vulnerabilities. Years of cryptanalysis of RSA have given us a broad insight into its properties and provided valuable guidelines to us for proper use and implementation in different aspects. In this paper we propose an analysis of the main methods used in attacks on the RSA cryptosystem together with the new possible attack. Our focus is based on the underlying mathematical function.**

Keywords: Plaintext, RSA, Secure Sockets Layer (SSL), Chinese remainder theorem (CRT), Elliptic Curve

I THE RSA CRYPTOSYSTEM:

The RSA cryptosystem was discovered in 1977 [1] and named after its inventors. Ronald Rivest, Adi Shamir and Leonard Adleman. It is widely used to secure communication in the Internet, ensure confidentiality and authenticity of e-mail, and it has become fundamental to e-commerce. RSA is deployed in the most popular security protocols, including SET, SSH, S/MIME, PGP, DNSSEC, and SSL (Secure Sockets Layer) and TLS. It is implemented in most Web servers and browsers, and present in most commercially available security products. In fact, the implementation of RSA has placed it at the heart of modern information security. Many standards cover the use of RSA for encryption, digital signatures and key establishment. In fact, RSA is usually present wherever security of digital data does matters.

The mathematical structure of the RSA function is relatively easy and this might be paramount reason for its popularity; people do feel more familiar on working with an algorithm one can understand. It is based on basic algebraic operations on large integers.

II ATTACKS ON THE RSA FUNCTION:

(1) Trial Division:

Trial method is an attempt to divide n by all successive primes until one divisor is found. Since a composite number n must have a prime divisor $\leq n^{1/2}$ one has only to check for all primes up to the square root of n. It then follows from the Prime number theorem that the number of attempts is bounded by $(2\, n^{1/2})/(\log(n))$. Although this method is very effective when trying to factor a randomly selected composite integer or relatively small numbers [2] but it is useless against the kind of numbers currently used with RSA

(2) Low Private Exponent Attack:

The RSA decryption and signing are very calculation-intensive operations, which takes time linear to the length of the private exponent d. Thus some low-power devices may want to use a small d instead of a random one, in order to improve performance. However an attack due to small d can lead to a total break of the system. More accurately, if n is the modulus and d is the private exponent,

with $d < 1/3(n^{1/4})$, then given the public key (e, n), an attacker can efficiently recover d.

Actually, this means that for a typical 1024-bit RSA modulus, the private exponent d should be at least 300 bits in length. If the public exponent e is chosen to be 65,537 (the most commonly used value), and we calculate d as $de \equiv 1 \bmod (n)$, then we are guaranteed to have d nearly as long as n, and this attack should not pose a danger.

(3) Partial Key Exposure Attack:

A well-known principle in cryptography says that the security of any cryptographic system should rely mainly on the security of the private key. An attack on the RSA cryptosystem due to Boneh, Durfee and Frankel shows the importance of protection of the entire private exponent d [3].

They have shown that, if the modulus n is k bits long, given the $(k/4)$ least significant bits of d, an attacker can rebuilt all of d in time linear to $(e \log(e))$, where e is the public exponent. This means that if e is small, the exposure of a quarter of bits of d can lead to the recovery of the whole private key d.

The agenda of safeguarding of RSA private keys is a crucial one, but it is a concern that is often overlooked. In Secure socket layer (SSL)-enabled servers for example, it is not unusual to have the private key stored in the computer's hard disk, in plaintext form so that the server can be re-started without human interference because an encrypted file would require the encryption key in order to start the server[3],[4].

when e is small the RSA system always leaks half the most significant bits of d, plus a intelligent technique in which one searches for randomness in order to locate private keys in large volumes of data, such as the hard disk filing system (or memory), it should be clear how important the safe storage of the RSA private key is. The best solution is the use of tamper-resistant hardware modules or tokens, in which the private key is securely stored and the private operation is performed.

(4) Broadcast and Related Message Attacks:

If someone broadcasts the encryption of the same message M to a sufficient large number of recipients (which have different public keys (ei, ni)), Hastad has described an attack in which a malicious eavesdropper can efficiently recover M if all the public exponents are small. This attack can be extended to the case in which instead of sending $(M)^{ei} \bmod ni$ to each recipient, someone sends $(fi(M))^{ei} \bmod ni$, where fi are known polynomials (for example, some kind of known padding).This is done by solving a system of univariate equations modulo relatively prime composites, which can be efficiently done if sufficiently many equations are given. There is also an attack when one sends to other related encrypted messages using the same modulus. If $M1$ and $M2$ are 2 messages such that $M1 = f(M2)$, where f is again a known polynomial function, and one sends $C1 \equiv (M1)^e \bmod n$ and $C2 \equiv (M2)^e \bmod n$, then a malicious eavesdropper can again efficiently recover both messages if e is small. An example of such scenario is one where one sends the first encrypted message to another, which is intercepts by somebody else.

Both of these attacks are more effective if the public exponent e is 3, although they can be prevented if we remove the relation between the messages, usually by adding some kind of random padding.

(5) Short Pad Attack:

Related to the attacks above, Coppersmith has shown that an adversary can still be successful if the random padding Bob adds to the messages is not large enough. For example, if e is 3, the length of the random padding must be at least 1/9 of the message length. A variant of the attack is successful in decrypting a single ciphertext when a large fraction (2/3) of the message is known. For example, PKCS#1 standard recommends [5] the use of its simpler padding scheme (v1.5) only for encryption of relatively short messages which are typically a 128-bit symmetric key. If a long message is to be encrypted, or if part of a message is known, then the attack above may be a concern, in which case an alternative padding method should be used.

(6) Implementation Attacks:

All the attacks against the RSA as we have discussed so far, are applicable to the underlying cryptographic primitive and parameters. On the other hand, implementation attacks (side-channel attacks) always target specific implementation details.

In this case, an attacker typically uses some additional information leaked by the implementation of the RSA function or exploit faults in the implementation. The attacks are usually applied against smart cards and security tokens, and are more effective when the attacker is in possession of the cryptographic module.

Defense against side-channel attacks is hard; one usually tries to reduce the amount of information leaked or make it irrelevant to the adversary.

(7) Timing Attack:

Timing attacks [6] enjoy the advantage of the correlation between the private key and the runtime of the cryptographic operation. Recall that the RSA private operation consists of a modular exponentiation, using the private key d as exponent.

Modular exponentiations are usually implemented using an algorithm called repeated squaring algorithm. If the private key is k bits long, this consists of a loop running through the bits of d, with at most $2k$ modular multiplications. In each step the data is squared, with the execution of a modular multiplication if the current bit of the exponent is 1.

By calculating the runtime of the private operation on a large number of random messages, an attacker can recover bits of d one at a time, starting with the least significant bit (LSB). Note that in view of the partial key information attack described earlier, if a low public exponent is used, the attacker needs only to find the first $k/4$ bits using this method; the remaining bits can be found using the previous method.

To defend against timing attacks, one must understand the correlation between the runtime and the private exponent. One solution is to add a delay, so that every modular operation takes the same fixed time. This naturally affects the performance of the operation, which many times may not be a concern.

(8) Fault Analysis:

Fault Analysis attacks work by exploiting errors on key-dependent cryptographic operations. These errors can be random, latent (e.g. due to bugs in the implementation) or induced. There are a number of fault analysis attacks against public-key and symmetric-key cryptographic devices. In 1997 Boneh, DeMillo and Lipton [7] introduced an attack against RSA, which exploits possible errors on the RSA private operation in cryptographic devices.

As we have mentioned, the RSA private operation is a very calculation-intensive operation, consisting of a modular exponentiation using numbers typically in the range of 300 decimal digits. Many realizations of RSA decryption and signing use a technique known as the Chinese Remainder Theorem (CRT), which by working modulo p and q (instead of module $n = pq$), can give a four-fold enhancement in the performance. Boneh, DeMillo and Lipton explained a technique, which by exploiting an error occurring during the decryption or signing and analyzing the output, an adversary could factor the modulus n and therefore recover the device's private key. Both the output and the input of the operation are vital for the attack to succeed (making it more effective against signing devices). To perform this kind of attack, one needs only to induce an error into the device during the private operation (for example, by voltage or clock speed variation). We should also note that unlike many of the attacks described before, the difficulty of this one is independent of the key length.

This fault attack against RSA can be easily prevented by requiring the device to verify the operation with the public key before outputting the result. This should not particularly degrade the performance, as the RSA public operation is very fast. Also we note that the attacker needs to have full knowledge of the actual string being signed or decrypted; the addition of random padding that is unknown to the attacker by the device prior to the operation would also prevent this type of attack.

Nevertheless the existence of fault analysis attacks stresses the need for special care when implementing secure cryptographic applications.

(9) Key Size –RSA keys should be long enough so as to make attacks against the system infeasible. The selection should take into consideration a number of factors such as the value of data being protected, the expected lifetime of the data, the threat model, and the best possible attacks. Many of the current standards require a minimum length of 1024 bits for RSA keys. Since the solution of the RSA-155 challenge [10], there is a general consensus that 512-bit keys are too short and should not be used.

(10) Strong Primes - Apart from a minimal length, some cryptographic standards also need that the primes used for RSA have some special properties [6]. In particular, that p –1 needs to have a large prime factor. These so-called strong primes are required in order to prevent Pollard's $p - 1$ factorization method. In spite of that, Rivest and Silverman [8] find these requirements unnecessary. In view of the Elliptic Curve and Number Field Sieve methods (which have better runtime than Pollard's $p - 1$ method), they believe that strong primes offer a negligible increase in security when compared with random primes. The real security comes from actually choosing large enough primes p and q.

(11) Multi-prime RSA – To speed up the RSA private operation, there are proposals of using more than two primes to generate the modulus. Using CRT, the speedup of an RSA system using k primes over the standard RSA is of around $k^2/4$. For illustration, a system deployed with 1024-bit modulus n, which is the product of 4 distinct (256-bit) primes, would perform around 4 times faster than the standard two-prime system. While the Number Field Sieve method cannot take advantage of this special form of n, 256-bit primes are currently considered within the bounds of the Elliptic Curve method (which is quite effective in finding small primes). Therefore, it is not recommended that 1024-bit modulo use more than three factors.

(12) Public Exponent – Mostly in RSA implementations, the public exponent e is chosen to be either 3 or $2^{16}+1$ (= 65,537), with which the public operation takes 2 and 17 modular multiplications (instead of ~ 1000 multiplications expected for a randomly chosen e). Particularly, 65,537 is more secure and can be used.

(13) Private Exponent – Wiener's low private exponent attack is quite effective, and if successful, can result in total recovery of the private exponent d. For the typical 1024-bit key, the private exponent should be at least 300 bits long. One should also pay special concern to the safety of the private key. The knowledge of a fraction of the key might allow the recovery of the entire key. The hardware solution is the most secure and should be considered whenever possible.

III THE NEW PROPOSED ATTACK ALGORITHM:

Here we address the million dollar question: is there a possible attack on the RSA cryptosystem other than factoring n*?* The answer is yes [9], there are few methods that attack the RSA scheme that does not involve finding the factoring of the modulus n but most of them carrying some deficiencies [3].

We will now prove the very interesting result that, as long as the exponent key e is known, then n can be factored in polynomial time by means of a randomized algorithm. Therefore we can say that computing this method is no easier than factoring n*.* However, this does not rule out the possibility of breaking the RSA cryptosystem without involving e . Notice that this result is of much more than theoretical interest.

In this paper we proposed a method that breaking the RSA scheme based on the knowing public key (e, n) . This method will work efficiently if the exponent key e . It is possible to recover the entire private exponent *d* and therefore factor the modulus n .

Algorithm: The steps are in this manner

1. Find entity public key A (e,n)
2. Change the modules n into its binary equivalent
3. Number of bits in n is equal to b.
4. Calculate d=⌈ b/4⌉
5. Find ed1+k(n-s-1)mod 2^b

6. Repeat k from 1 to e until

$P^2 - s*p+n \equiv 0 \bmod 2^b$ is true

And calculate $ed \equiv 1+k(n-s+1) \bmod 2^d$

Also calculate $p^2 - s*p+n \equiv 0 \bmod 2^d$

7. Find $p_0 \equiv p \bmod 2^d$

8. Find $q_0 * p_0 \equiv n \bmod 2^d$

9. Find θ(n) by computing:

$n \equiv (2^d * x+p_0)*(2^d * y+q_0)$

$p=(2^d * x+p_0)$, $q=(2^d * x+q_0)$

So θ(n)= (p-1)(q-1)

10. Finally d=e*d-k* θ(n)=1

IV AN EXAMPLE TO ILLUSTRATE:

1. Suppose that the public key (e=23, n=1633)
2. Convert n into its binary equivalent i.e. $(11001100001)_2$
3. b=11
4. $d=\lceil 11/4 \rceil = 3$
5. (e= 23*d=d) $\equiv 1+k(n=1633-s+1) \bmod (2^b=8)$

   $69 \equiv 1+k(1634-s) \pmod 8$

   69 mod 8=5

   Now, $5 \equiv 1+k(1634-s) \pmod 8$

   $4 \equiv k(1634-s) \pmod 8$

6. For k=1 to 23 do
   (a) $4 \equiv 1(1634-s) \pmod 8$
   $s \equiv (1634-4) \pmod 8$

   s=1630 mod 8

   s=6

   (b) $p^2-(s=6)*p+(n=1633) \equiv 0 \bmod (2^d=8)$
   $p^2-6p+1633 \equiv 0 \bmod 8$

   $p^2-6p \equiv -1633 \bmod 8$

   $p^2-6p \equiv 7 \bmod 8$

   $7^2-6*7 \equiv 7 \bmod 8$

   $49-42 \equiv 7 \bmod 8$

   $7 \bmod 8 \equiv 7 \bmod 8$

   So p=7

   It means $p^2-(s=6)*p+(n=1633) \equiv (0 \bmod 2^b=8)$ holds true

   So as a result, loop must be stopped.

7. $p_0 \equiv (p=7) \pmod{2^d \equiv 8}$
   $p_0 \equiv 7$

8. $q_0 * (p0=7) \equiv (n=1633 \bmod 2^d=8)$

   $7q_0 \equiv 1633 \bmod 8$

   $7q_0 \equiv 1 \bmod 8$, inverse of 7 mod 8 is 7

   $q_0 \equiv 7 \bmod 8$

   So $q_0 \equiv 7$

9. Find θ(n)

   $n \equiv (2^d * x+p_0)*(2^d * y+q_0)$

   $1633 \equiv (8*x+7)(8y+7)$

   $1633 \equiv (8*2+7)(8*8+7)$

   $1633 \equiv (23)(71)$

1633□1633

S0 x=2 and y=8

That means p=23, q=71

θ(n)=(23-1) (71-1)

θ(n)=1540

10. (e=23*d-(k=1)*(θ(n)=1540) □ 1
23d□1541

d= 67 (By multiplicative inverse method)

V CONCLUSION:

Since RSA is applicable in e-commerce and digital signatures, its security is a million dollar question. There are so many attacks already defined on RSA based on factoring. Methods like trial division are time taking and low private attack contains a limitation that the private exponent d should be at least 300 bits in length. The new proposed method is essentially based on public key (e,n) and does not have all these limitations. So we can say that the new algorithm is suitable for implementation aspects.

References:

(*1) R. Rivest, A. Shamir and L. Adleman. A Method for Obtaining Digital*
Signatures and Public Key Cryptosystems. Communications of ACM 21
(1978) 120-125
(2) B. Canvel. Password Interception in a SSL/TLS Channel.
(3) D. Boneh. Twenty Years of Attacks on the RSA Cryptosystem.
Notices of the American Mathematical Society, 46(2):203--213, 1999.
(4) A.Shamir and N. van Someren. Playing hide and seek with stored keys.
Lectures in Computer Science, 1998
(5) RSA Laboratories. PKCS #1 v2.1 - RSA Encryption Standard. June 2002.
(6) B. Kaliski. Timing Attacks on Cryptosystems. RSA Laboratories' Bulletin
No. 2, January 1996
(7) B. Kaliski and M. Robshaw. Comments on Some New Attacks on
Cryptographic Devices. RSA Laboratories' Bulletin No. 5, July 1997.
(8) R. Rivest and R. Silverman. Are Strong Primes Needed for RSA?
RSA Laboratories Technical Notes and Reports
(9)C. KAUFMAN, R. PERLMAN, "Network Security −private communication in a public world", 2nd edition, Prince Hall PTR, 2002.
(10)RSA Laboratories. Factorization of RSA-155.

Angle of Repose of Digested Oil Palm Fruit Mash and Pulp on Steel

Nwankwojike, B. Nduka

Department of Mechanical Engineering, Michael Okpara University of Agriculture, Umudike, Nigeria.

jikeobodo@yahoo.com

Abstract

The angles of repose of digested palm fruit mash and pulp on mild and stainless steel were determined in this study because of it important in the design and fabrication of palm nut-pulp separating machine proposed for total elimination of nut breakage and its associated losses in all mechanized palm fruit processing. The experimental plan was based on completely randomized design (CRD) while the data obtained were tested and compared using Analysis of variance (ANOVA). Results showed that the angle of repose of digested palm fruit mash on both mild and stainless steel is same and equal to 46.01^0 while that of digested palm fruit pulp on these two structural materials is 47.91^0. ANOVA results revealed that there are no significant differences (at α = 0.05) in angles of repose of the test specimens obtained from the dura and tenera palm fruits and also that the values of this parameter obtained as per each test is independent of the weight of the specimen used.

Key Words: Angle of repose, mild and stainless steel, nut breakage, nut- pulp separating machine, pressing

I. INTRODUCTION

The oil palm *(Elaeis guineensis)* is one of the world's most important oil producing plants. Its fruits produce two types of oil; the palm oil which is extracted from the fruit pericarp (pulp) and palm kernel oil from its seeds (palm kernel), both of which are very important in the world trade due their wide industrial and domestic applications [1], [2] , [3], [4]. The three main varieties of the oil palm distinguished by their fruits characteristics are dura, pisifera and tenera, however, successful processing of the fruits into palm oil and kernel products is only possible with dura and tenera fruits due to shelless nature of pisifera [5]. Ref. [6] and [7], said that the extraction of palm oil and kernel from the fruits involves field and factory/house operations. The field processes include cutting ripe fruit bunches from the palm tree and transporting them to the factory/house while cooking and digestion of the fruits, squeezing of palm oil out of the digested fruit pulp and clarification/purification of the extracted palm oil constitutes the factory operations

The two variant methods of carrying out these factory operations are the traditional and mechanical methods [3]. The mechanized process with screw press as the means of palm oil extraction is the most commonly used in the modern palm fruit processing because it requires less power and capital cost for a given pressing capacity and also its palm oil extraction rate is independent of the efficiency of the sterilization and digestion processes unlike other presses/other palm oil extraction equipment [8]. However, the major problem of using screw press for palm oil extraction is nut breakage and previous efforts on total elimination of this problem caused excessive loss of palm oil to pressed fibre [4] [5]. According to [9], mechanically processed palm nuts usually contains 10 to 15% broken nuts when screw press is used for palm oil extraction at an optimal 9 to 10% palm oil loss to pressed fibre. Also, [8], indicated 9 to 22% nut breakage depending on the type of fruit being processed with 8% oil content in the pressed fibre while an average palm oil loss to fibre of 10.7% with a screw press was reported by [10]. Ref.[4] further showed that in a small scale process where the breakage was not checked to achieve 2-3% palm oil content of the pressed fibre, the bleachability and oxidation conservation of the palm oil extracted was adversely affected. Ref. [11], explained that the quality of palm oil extracted in this later process was negatively affected because some small nuts/kernels crushed during pressing released traces of palm kernel oil into the extracted palm oil and the two oils cannot be separated by simple methods.

Furthermore, absent of palm nut-pulp separation process in all the mechanized palm fruit processing method as contained the traditional technique was identified as the major cause of the nut breakage associated the use of pressing for palm oil extraction [11]. The traditional palm fruit processing separates

digested palm fruit mash into nut and pulp before hand squeezing of palm oil out of the digested fruit pulp while in the mechanized system, the digested mash is subjected to pressing without removing the nuts. Thus, nut breakage during palm oil extraction is not encountered in the traditional palm fruit processing. But [4], said that all mechanized palm fruits processing machinery/equipment were developed based on the observation of the traditional technique of West Africa. Also it is only the pulp part of the fruit that contains palm oil extracted at this stage [1], [3], [4]. It was based on these facts that [11], proposed a unit operation sequence modification in the mechanized palm fruit processing to include a palm nut-pulp separating machine between the digester and press as shown in Figure 1 for total elimination of nut breakage and its other associated losses in this sector.

In order to design and develop the proposed palm nut-pulp separating machine, some engineering properties of the digested palm fruit mash (the raw material input to the proposed machine) and those of the digested pericarp (pulp) and wet palm nuts (output materials from the machine) are required.

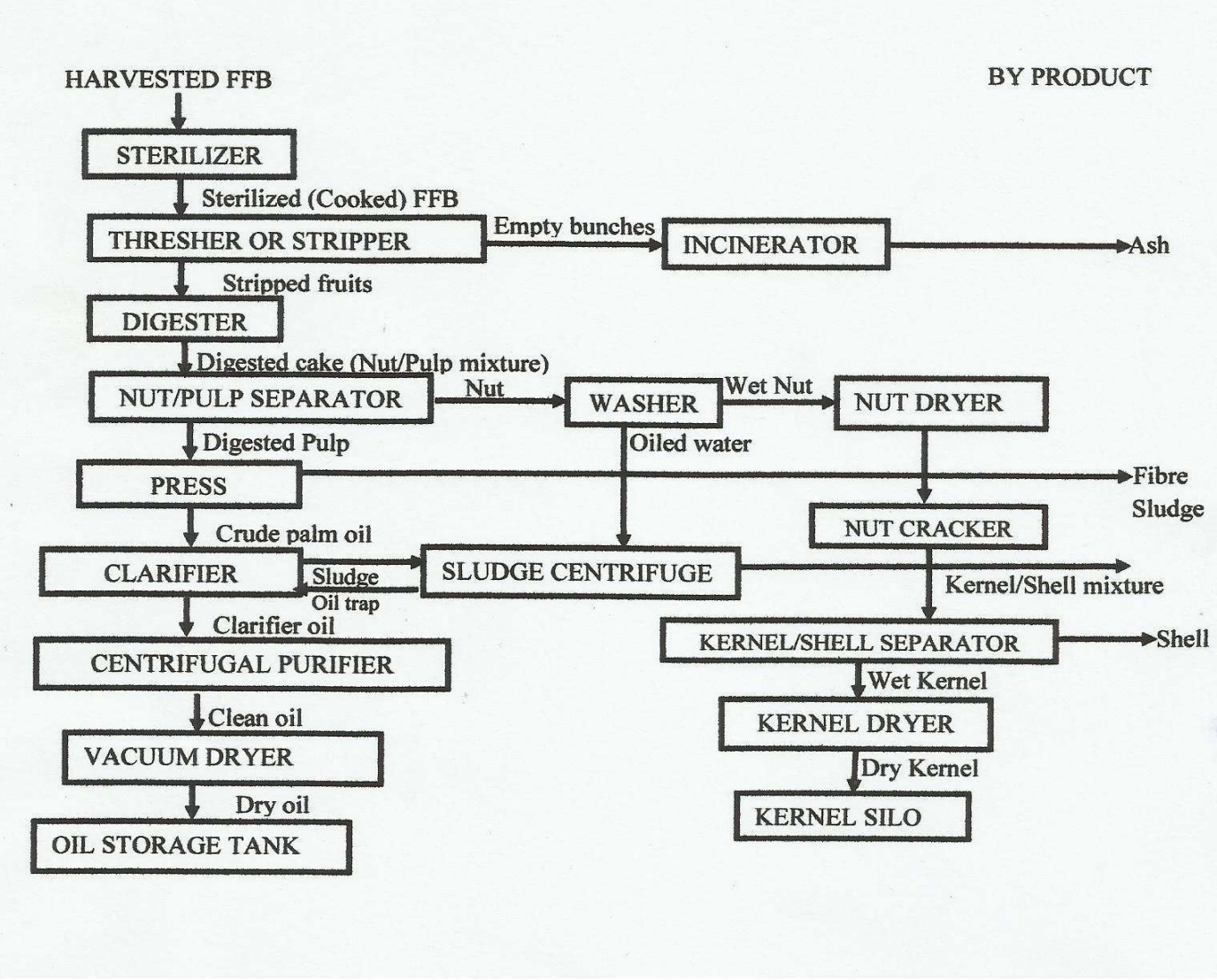


Figure 1: Flow diagram of palm oil and kernel extraction by mechanical methods with the proposed palm nut-pulp separation unit operation.

The engineering properties of these biomaterials required in the design of this machine include density, size and shape, hardness, compressive strength and angle of repose/coefficient of friction of the materials on mild and stainless steel. The values of these parameters are highly required in this proposal because engineering properties of biomaterials constitute essential data in design of machines, structures, processes and controls. Ref. [12] said that they are useful in the analysis and determination of the efficiency of machines, development of new products and equipment, and the final quality of products. According to [13], size and shape are very important in determining methods of separation and cleaning methods while density and specific gravity are used in calculating thermal diffusivity and volume/weight capacity of machine components. Mechanical properties such as hardness and compressive strength are used for predicting resistance of produce to cracking and energy required in size reduction respectively [13]. Compressive strength is also relevant in the choice of stack height to avoid damage of produce during storage. Angle of repose/coefficient of friction of materials on various structural surfaces is very important in predicting the movement of the materials in the processing equipment and pressure exerted on the walls of the equipment. A separation technique based on the coefficient of friction of a modified inclined plane is also in use for separating palm kernel and shell.

Some documented information on the measurement of some properties of digested palm fruit mash, digested pulp and palm nuts exist in some literatures. Ref. [8], reported the densities of the digested palm fruit mash, digested pulp, pressed fibre, un-pressed dura and tenera nuts from experimental measurement as 1060kg/m^3, 0.925 kg/dm^3, 1.04kg/dm^3, 781 g/dm^3 and 656 g/dm^3 respectively. Medium (average) size fibres are approximately 25mm long and 250 micron in diameter [8]. Although, engineering properties of biomaterial are dependent on factors such as species and climate of its environment, [8], further confirmed experimentally that despite the fact that the proportion of mesocarp to fruit varies widely according to fruit types, the composition of sterilized/digested mesocarp (digested pulp) is relatively constant comprising 54% palm oil, 28% water and 18% non-oil solids. In addition, [13], showed that the major, intermediate and minor diameters of dura nuts varies from 26.5 to 44mm, 21.5 to 34.5mm and 16.5 to 28mm respectively. Compression strength of dura nuts in terms of its fraction and cracking resistance has been determined as 0.2 to 3.7kN [14]. Also, other properties of the seed under compression have been investigated [12] [15] and [16]. However, despite an extensive literature search, there is no published information on the measurement of the angle of repose and coefficient of friction of digested palm fruit mash and pulp with respect to mild and stainless steel. Generally, coefficient of friction, μ of any structural surface with respect to another is related to its angle of repose, θ as follows:

$$\mu = \tan\theta \qquad (1)$$

Mild and stainless steel are among engineering materials commonly used for machine/equipment fabrication in most developing nations like Nigeria because the materials are non-toxic, easily to fabricate and machinable, not easily worn out and strong with high carrying capacity and also usually available locally at an affordable cost [17]. Thus, the cost of production and maintenance of the proposed palm nut-pulp separating machine will low if its design and fabrication is based on these steel materials. Since the angles of repose/coefficients of friction of digested palm fruit mash and pulp with respect to these two structural materials are vital parameters in the design and fabrication of the separating mechanism, feeding and discharging units of the proposed machine, it is therefore, the specific objective of this work to determine the angles of repose of digested oil palm fruit mash and digested pulp with respect to mild and stainless steels.

II. MATERIALS AND METHODS

The dura and tenera palm fruits used in this study were procured from Onyeije Oil Palm Plantation, Amawom and Abia State Small Holders Oil Palm Management Unit, Akoli-Imenyi respectively. The fruits were processed to digested fruit mash and pulp (test specimens) using small scale processing equipments at Okey Oil Mill factory, Ozuitem by Ahia Orie Ugba, Umuahia in Abia State of Nigeria. A completely randomized design (CRD) involving eight batches of fifteen experimental tests per batch was used for this investigation. The angles of repose of digested dura mash with respect to mild and stainless steels were determined in the first and second batch of the trails respectively. The third and fourth, fifth and sixth, and the seventh and eighth batches of the trials respectively explored the angles of repose of digested dura pulp with mild and stainless, tenera mash with mild and stainless, and tenera pulp with mild and stainless. In each test the emptying angle of repose between a weighed specimen (digested mash or pulp) and the structural materials (mild or stainless steel) was determined using the inclined plain procedure as

described by [18]. A four sided topless and bottomless plywood box with dimensions 150mm x100mm x 40mm were filled with a weighed specimen and placed on the surface of an adjustable tilting table. Two adjustable tilting tables with one having a new mild steel plate surface while the other with a new stainless steel plate surface were used. The box was raised 2mm to allow only the specimen to be in contact with the structural surface. The structural surface with the box on its top was gradually tilted until the box just starts to slide down. The vertical distance or height of the inclined plane as the specimen is about to slide was measured in each case and recorded. Thereafter, the angle of repose, θ was computed from the data obtained as per each experimental run using Equation (2).

$$\theta = \tan^{-1}\left(\frac{h}{l}\right) \qquad (2)$$

where h and l are the vertical (height) and fixed horizontal (280mm) distances of the inclined plane just before the specimen slides. The data obtained from this investigation were tested and compared using Analysis of Variance (ANOVA).

III. RESULTS AND DISCUSSION

The experimental results obtained with digested dura palm fruit mash and pulp samples are presented in Table 1 while those of the samples obtained from tenera fruits are shown in Table 2. These results (Tables 1 and 2) showed no difference between the mean values obtained for the angle of repose of digested palm fruit mash on the mild and stainless steel and also that of digested pulp on the mild and stainless steel. The analysis of variance results of the data presented in these tables showed no significant difference (at α = 0.05) in angles of repose obtained for digested palm fruit mash on the mild and stainless steel irrespective of the fruit specie from which the specimen was obtained and this is also observed in the values of this parameter for the digested pulp on both materials.

Table 1: Angle of Repose of Digested Dura fruit Mash and Pulp with respect to Mild and Stainless Steel

S/No.	Mass of Specimen (g)	Horizontal Distance (mm)	Digested Palm Fruit Mash				Digested Pulp			
			Mild Steel		Stainless Steel		Mild Steel		Stainless Steel	
			Vertical Distance (mm)	Angle of Repose (^{0})	Vertical Distance (mm)	Angle of Repose (^{0})	Vertical Distance (mm)	Angle of Repose (^{0})	Vertical Distance (mm)	Angle of Repose (^{0})
1	30.00	280.00	290.10	46.02	291.00	46.10	310.00	47.91	310.00	47.91
2	35.00	280.00	290.00	46.01	290.00	46.01	309.90	47.90	310.00	47.91
3	40.00	280.00	290.00	46.01	289.80	45.99	310.20	47.93	310.00	47.91
4	45.00	280.00	289.80	45.99	290.00	46.01	310.20	47.93	309.90	47.90
5	50.00	280.00	289.90	46.00	289.80	45.99	310.00	47.91	310.00	47.91
6	55.00	280.00	290.10	46.02	290.10	46.02	310.00	47.91	309.90	47.90
7	60.00	280.00	290.00	46.01	290.00	46.01	310.00	47.91	309.80	47.89
8	65.00	280.00	290.00	46.01	289.80	45.99	309.90	47.90	310.50	47.96
9	70.00	280.00	289.80	45.99	289.80	45.99	309.90	47.90	310.00	47.91
10	75.00	280.00	290.00	46.01	289.90	46.00	309.90	47.90	310.00	47.91
11	80.00	280.00	290.10	46.02	290.10	46.02	310.00	47.91	309.90	47.90
12	85.00	280.00	290.10	46.02	290.00	46.01	310.40	47.95	310.00	47.91
13	90.00	280.00	290.10	46.02	289.90	46.00	309.90	47.90	310.00	47.91
14	95.00	280.00	290.00	46.01	290.00	46.01	310.00	47.91	309.90	47.90
15	100.00	280.00	290.00	46.01	290.10	46.02	310.00	47.91	310.00	47.91
TOTAL				***690.15***		***690.17***		***718.68***		***718.64***
AVERAGE				**46.01**		**46.01**		**47.91**		**47.91**

Table 2: Angle of Repose of Digested Tenera fruit Mash and Pulp with respect to Mild and Stainless Steel

S/No.	Mass of Specimen (g)	Horizontal Distance (mm)	Digested Palm Fruit Mash				Digested Pulp			
			Mild Steel		Stainless Steel		Mild Steel		Stainless Steel	
			Vertical Distance (mm)	Angle of Repose (^{0})	Vertical Distance (mm)	Angle of Repose (^{0})	Vertical Distance (mm)	Angle of Repose (^{0})	Vertical Distance (mm)	Angle of Repose (^{0})
1	30.00	280.00	290.00	46.01	290.10	46.02	309.90	47.90	310.00	47.91
2	35.00	280.00	289.80	45.99	290.00	46.01	310.00	47.91	310.00	47.91
3	40.00	280.00	290.00	46.01	289.80	45.99	310.00	47.91	310.50	47.95
4	45.00	280.00	289.90	46.00	290.10	46.02	310.00	47.91	310.00	47.91
5	50.00	280.00	290.10	46.02	290.10	46.02	310.00	47.91	310.00	47.91
6	55.00	280.00	291.00	46.10	289.80	45.99	309.80	47.89	309.90	47.90
7	60.00	280.00	289.80	45.99	290.00	46.01	310.00	47.91	309.90	47.90
8	65.00	280.00	289.80	45.99	290.00	46.01	309.90	47.90	310.00	47.91
9	70.00	280.00	289.80	45.99	289.80	45.99	310.00	47.91	309.90	47.90
10	75.00	280.00	290.00	46.01	290.00	46.01	309.90	47.90	309.90	47.90
11	80.00	280.00	290.10	46.02	290.00	46.01	310.00	47.91	310.00	47.91
12	85.00	280.00	289.90	46.00	291.00	46.10	310.20	47.93	310.00	47.91
13	90.00	280.00	289.80	45.99	289.80	45.99	310.00	47.91	310.00	47.91
14	95.00	280.00	289.80	45.99	290.00	46.01	310.00	47.91	310.00	47.91
15	100.00	280.00	290.10	46.02	290.00	46.01	309.90	47.90	310.10	47.92
TOTAL				***690.13***		***690.19***		***718.61***		***718.66***
AVERAGE				**46.01**		**46.01**		**47.91**		**47.91**

Results also revealed that the values of this parameter obtained are independent of the weight of the specimen under investigation. These observations are in agreement with [8] which reported that the composition of both the digested palm fruit mash and pulp are relatively constant and independent of the fruit specie from which it was obtained. However, it is also obvious from these tables that the angle of repose of digested palm fruit mash ($\theta = 46.01^0$) on both structural materials investigated differs from that of digested pulp which is 47.91º.

IV. CONCLUSION

The angle of repose of digested palm fruit mash with respect to both mild and stainless steel is 46.01^0 while that of the digested pulp on these structural materials is 47.91^0. This study revealed that the value of this parameter is independent of the oil palm fruit specie (dura or tenera) from which the specimens were obtained but depends on the structural materials (mild and stainless steel) and the nature of the specimen (digested mash or pulp).

Acknowledgements

Financial support from Directorate of Research and Development of Michael Okpara University of Agriculture Umudike, through 2008/2009 research grant (EIT/08/02) is acknowledged with gratitude.

References

[1] C .W.S. Hartley. The Oil Palm. Longman Group Limited London. pp. 1-256, 282-767, 1988.

[2] M. A. Hussien. Palm oil use in North Africa and West Asia. Food and Nutrition Bulletin. Vol. 15. No. 2. 1994.

[3] RMRDC. Report on Survey of Selected Agricultural Raw Materials in Nigeria on Oil Palm. Raw Material Research and Development Council, Federal Ministry of Science and Technology, Abuja. pp. 41-89, 2004.

[4] FAO. Small-scale Palm Oil Processing in Africa Food and Agricultural Organization (FAO) Agricultural Series 148. pp. 1-55, 2005.
http://www.fao.org/document/Y4355E03.htm.

[5] NIFOR. Nigerian Institute for Oil Palm Research (NIFOR) Oil Mill Division Annual Production Report of the year 2000. NIFOR Press, Benin City.

[6] NIFOR, "A Manual on Oil Palm Production". Nigerian Institute for Oil Palm Research (NIFOR) 3rd Edition. pp: 39-41, 1975

[7] G. A.Badmus. Factors Affecting the Design of a Fruit Bunch Harvesting System of Tall Oil Palm Treesin Plantations. Nigeria Journal of Palms and Seeds11 pp. 102-1114, 1990.

[8] R. N. Muthurajah. Palm Oil Factory Hand Book, Palm Oil Res. Institute New Delhi. pp: 35-56, 2002.

[9] A.B.N. Norilia Report of Industrial Training at FePalm Industries Mempaga palm Oil Mill 28600Karak, PahangDarul Makmur, Malaysia. pp.18-19, 2008.

[10] K.A. Stephen and S. Emmanuel. Modification in the design of already existing Palm nut-Fibre Separator.

[11] B. N. Nwankwojike, A. O. Odukwe, and J. C. Agunwamba, Modification of Sequence of Unit Operations in Mechanized Palm Fruit Processing, Nigerian Journal of Technology,Vol. 30 No.3. pp. 41- 49, 2011.

[12] N. N. Mohsenin. Physical Properties of Plant and Animal Materials. 2nd Edition. Gordon and Breach Science Publisher, New York. 1986.

[13] Y. Mijinyawa, and S. Omoikhole. Determination of Some Physical Properties of Palm Kernel. Proceedings of Nigerian Institution of Agricultural Engineers held at Yenagoa. Vol. 27. pp. 157-160, 2005.

[14] S.I. Manuwa, Modeling Fracture and Cracking Resistance of Palm Nuts (Dura Variety), AU J.T. 10(3): 184-190, 2007.

[15] G.C. Zoerb and C.W. Hall, Some mechanical and rheological properties of grains. J. Agric. Eng. Res. 5: 83-8, 1960.

[16] W.K. Bilanski and R. Lal, Behaviour of threshed materials in vertical wind tunnel. Trans. ASAE 8: 411-6, 1965.

[17] E. H. Cornish. Materials and the Designer, Cambridge University Press, Cambridge, pp. 28-29.1991.

[18] O.I. Adejumo, A. A. Alfa,. and A. Mohammed. Physical Properties of Kano White Variety of Bambara Groundnut. Proceedings of Nigerian Institution of Agricultural Engineers held at Yenagoa. Vol. 27. pp. 203-210, 2005.

Linguistic Display of Status of System to Support Distribution Sub-Station Operator

M.S.Giridhar, Sreenivasa Institute of Technology and Management Studies, District Chittoor, A.P, INDIA
S.Sivanagaraju, Department of Electrical Engineering, J.N.T.U.College of Engineering, Kakinada,A.P,INDIA
(e-mail: munigoti7@yahoo.co.in).

***Abstract*-- This paper presents a new method of analyzing the distribution system under uncertain variations in the loads. The measured load variation data collected from a practical radial distribution system have been modeled as Type-2 Fuzzy Sets, which represents the uncertain variations in the load. The developed Type-2 membership function models have been validated using Mambdani-FIS by computing the centroid values of voltages at each bus (Consequent) for the centroid values of Type-2 fuzzy set modeled as load at each bus (Antecedent) and these values are compared with voltages obtained by normal power flow solution for the centroid values of the load. Further the authors proposes a new Linguistic Display Aiding Tool for the Substation Operator, by displaying the status of Voltage Drops, Line Flows in each branches of the Feeder and Laterals Linguistically where the substation operator gets the display of the status in his local language. For which the authors uses a similarity measuring method between the standard type-2 fuzzy sets labeled with linguistic words and the Type-2 fuzzy sets of voltages at each bus or the voltage drops in each branches of the laterals or the losses in each line. The measures of uncertainty such as centroid, cardinality, fuzziness, Skewness and Variance of the IT2 FS of loads and voltages are computed. These are useful to compute two types of uncertainties associated with a word: intra-personal uncertainty and inter-personal uncertainty.**

***Index Terms*—Transformer-load-model, Interval Type-2 Fuzzy set, uncertainty, load duration curve, fuzzy Inference System, Similarity measure of Uncertainty.**

I. INTRODUCTION

An integral part of distribution automation is the real-time monitoring and control of distribution circuits to facilitate feeder analysis functions such as volt/var control, feeder reconfiguration and restoration, and demand-side management. To accomplish this task of real-time monitoring and control requires a distribution circuit state estimator tool which can provide real-time estimates of circuit states, i.e. bus voltages and line flows. A requirement of any distribution circuit state estimator is a load modeling (estimation) procedure which can provide real-time estimates of customer load demands. This is needed due to the limited availability of real-time measurements on distribution circuits. Previous load modeling techniques have generally been used for a system peak-type power flow analysis [7, 8]. Thus, they have largely ignored the normal variations in load demands that occur throughout the day. Another drawback of traditional load modeling procedures is their inability to provide a measure of uncertainty regarding its estimates. Kuo and Hsu [7] do propose a time-of-day dependent load modeling technique which makes use of fuzzy logic and transformer kVA.

Probabilistic modeling of random uncertainty focuses to a large extent on methods that use at least the first two moments of a probability density function (pdf)—the mean and the variance. To just use the first order moments would not be very useful, because random uncertainty requires an understanding of dispersion about the mean and this information is provided by the variance. In fuzzy logic (FL), we may view computing the defuzzified output of a type-1 FLS as analogous to computing the mean of a pdf. Just as variance provides a measure of dispersion about the mean and is almost always used to capture more about probabilistic uncertainty in practical statistical-based designs, FLS's also need some measure of dispersion to capture more about rule uncertainties than just a single number. Type-2 FL provides this measure of dispersion and seems to be as fundamental to the design of systems that include linguistic and/or numerical uncertainties that translate into rule uncertainties as variance is to the mean [11]. Application of fuzzy set theory in distribution system analysis can sharpen professional judgment and past experiences in planning, design and operations of distribution system. In distribution system, uncertainty

in load can directly be taken into account with the help of the concepts from the fuzzy set theory. A special feature of this fuzzy set approach is that it enables us to deal with uncertain terms, such as load currents in a systematic manner. Furthermore, generally certain linguistic terms such as heavily loaded, lightly loaded, etc. are used to describe system loading conditions. Fuzzy set approach provides us not only with a meaningful and powerful representation of measurement uncertainties, but also with a meaningful representation of vague concepts expressed in natural language. The concept of type-2 FS was introduced by Zadeh [10] as an extension of the concept of an ordinary fuzzy set, i.e., a type-1 fuzzy set. Type-2 FS have grades of membership that are themselves fuzzy [7, 8]. A type-2 membership grade can be any subset in the primary membership; and, corresponding to each primary membership, there is a secondary membership (which can also be in) that defines the possibilities for the primary membership. A type-1 fuzzy set is a special case of a type-2 fuzzy set; its secondary membership function is a subset with only one element-unity.

In this paper modeling of the distribution transformer load variation for a day using the statistics and fuzzy sets is presented. A standard rural distribution transformer load variation that is uncertain which vary statistically over a period of 24-hour duration is modeled as fuzzy trapezoidal membership functions (Type-1). In a practical distribution system the upper and lower limits of membership function are uncertain. These membership functions are modeled as Type-2 fuzzy membership functions. Here a rural distribution feeder is considered as our test system, for which the current readings of the feeder are collected at the substation for a month. Total kVA load of the feeder for 31-days and 24-hrs is measured, from which the kVA loading at each node is obtained based on the kVA ratings of the respective transformers at that nodes. A trapezoidal membership function (Type-1) is modeled for each transformer rating for one-day; like that we get 31-trapezoidal membership functions (Type-1) for one-month. The trapezoidal membership functions (Type-1) for one-month together is represented as Interval Type-2 Trapezoidal membership function, so that the uncertainties in the load variations at the transformer is taken into consideration. We use type-2 fuzzy logic systems in which the antecedent or consequent membership functions are type-2 fuzzy sets. The knowledge used to construct rules in a fuzzy logic system (FLS) is uncertain. This uncertainty leads to rules having uncertain antecedents and/or consequents, which in turn translates into uncertain antecedent and/or consequent membership functions. The mappings between input and output data pairs are uncertain due to load dynamics and exact unknown line-length in distribution system [3, 5, and 11]. These linguistic and numerical data uncertainties lead type-1 fuzzy logic systems to perform poorly. However, type-2 fuzzy sets are able to handle these uncertainties.

I. Introduction to Type-2 Fuzzy sets

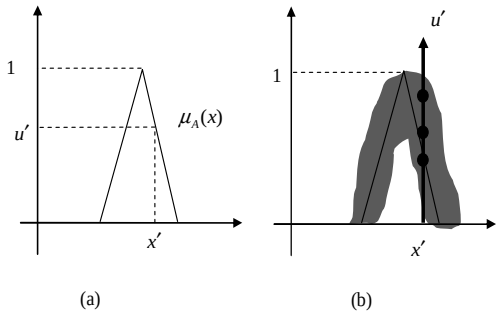


Figure 1-(a) An example of the general fuzzy set; (b) an example of the type-2 fuzzy set.

Figure 1 depicts the examples of the general fuzzy set and the type-2 fuzzy set. In Fig. 1-(a), at a specific value of x, say x', the membership function has a single value in the general fuzzy set. By contrast, the membership function takes on values wherever the vertical line intersects the blur in Fig. 1-(b). Those values need not all is weighted the same; hence, an amplitude distribution is assigned to all of those points. According to all $x \in X$, a three-dimensional membership function, a type-2 membership function is used to characterize a type-2 fuzzy set.

The definitions of type-2 fuzzy sets

According to [11], type-2 fuzzy sets are defined as follows. For the sake of simplicity, the universe of discourse is assumed as a finite set, although the definition can be applied for infinite sets.

A type-2 fuzzy set, $\tilde{A}$, is characterized by a type-2 membership function $\mu_{\tilde{A}}(x,u)$, where X is the universal set, $x \in X$ and $u \in J_x \subseteq [0,1]$; that is,

$$\tilde{A} = \{((x,u), \mu_{\tilde{A}}(x,u)) \mid \forall x \in X, \forall u \in J_x \subseteq [0,1]\}$$

,

where $0 \le \mu_{\tilde{A}}(x,u) \le 1$. $\tilde{A}$ can also be expressed as

$$\tilde{A} = \sum_{x \in X} \sum_{u \in J_x} \mu_{\tilde{A}}(x,u)/(x,u),\ J_x \subseteq [0,1],$$

where $\sum\sum$ indicates the union over all admissible *x* and *u*.

Accordingly, at each value of *x*, say $x = x'$,

$$\mu_{\tilde{A}}(x=x', u) \equiv \mu_{\tilde{A}}(x') = \sum_{u \in J_{x'}} f_{x'}(u)/u, \text{ for } u \in J_{x'} \subseteq [0,1] \text{ and } x' \in X$$

,

where $\mu_{\tilde{A}}(x)$ represents the secondary membership function.

Moreover, because the membership grades of type-2 fuzzy sets are the values of type-1 fuzzy sets, performing operations like union and intersection on type-2 fuzzy sets is like performing t-conorm and t-norm operations between type-1 fuzzy sets. Computations used with the Interval type-2 fuzzy sets [11, 14] are manageable. All of the results that are needed to implement an Interval type-2 fuzzy set (IT2 FS) can be obtained using Type-1 fuzzy sets (T1 FS) mathematics. An Interval type-2 fuzzy set is a set with all the secondary membership values equal to one.

The Jaccard similarity measure for IT2 FSs

Given a vocabulary consisting of N words with their associated IT2 FS $\tilde{\boldsymbol{B}}$, the goal is to find the $\tilde{\boldsymbol{B}}$ which closely resembles Ã, for which the similarity between two IT2 FS's is used. In the literature [9], Jaccard similarity measure is the most efficient method of measuring the similarity between the two IT2 FS's, so, the authors also adopt the same here.

Hence, consider two type-2 fuzzy sets $\tilde{A}$ and $\tilde{B}$, such that

$$\tilde{A} = \sum_{x \in X} \mu_{\tilde{A}}(x)/x = \sum_{x \in X} [\sum_{u \in J_x^u} f_x(u)/u]/x,\ J_x^u \subseteq [0,1]$$

,

and

$$\tilde{B} = \sum_{x \in X} \mu_{\tilde{B}}(x)/x = \sum_{x \in X} [\sum_{w \in J_x^w} g_x(w)/w]/x,\ J_x^w \subseteq [0,1]$$

.

S_j ($\tilde{\mathbf{A}}$, $\tilde{\boldsymbol{B}}$) =

(1)

(1)

$$\frac{\int_X \min\left(\bar{\mu}_{\tilde{A}}(x) + \bar{\mu}_{\tilde{B}}(x)\right) dx + \int_X \min\left(\bar{\mu}_{\tilde{A}}(x) + \bar{\mu}_{\tilde{B}}(x)\right) dx}{\int_X \max\left(\bar{\mu}_{\tilde{A}}(x) + \bar{\mu}_{\tilde{B}}(x)\right) dx + \int_X \max\left(\bar{\mu}_{\tilde{A}}(x) + \bar{\mu}_{\tilde{B}}(x)\right) dx} \quad (2)$$

Where $\bar{\mu}_{\tilde{A}}$ and $\bar{\mu}_{\tilde{B}}$ are the membership values of **Ã and $\tilde{\boldsymbol{B}}$** IT2FS's.

Transformer Load Modeling

(3)

In this section the load modeling of different rated transformers that are connected to the rural distribution feeder is considered [7, 8]. Here we use a technique to generally allocate telemeter substation power flows (or other metered flows) to various load points by using ratios obtained from connected transformer capacities.

$$P_i = P_m \left(\frac{TC_i}{\sum_{i=0}^{n} TC_i} \right)$$

(2)

For example, where P_i = real power demand at node I,

P_m = real power flow metered at node m,

TC_i = transformer capacity at node i, and 'n' represents the number of nodes served by power flowing through node *m.*

Fuzzy Load Model (Type-1)

If x_i where i=1,2,3…..n (n<30) be the empirical per unit load data for (a) Residential (b) Commertial and (c) Industrial then the Trapezoidal and Triangular fuzzy number [2] parameters are

$$l_1 = min(x_i)$$

$$p_1 = min(x_i) - \frac{E(x) - min(x_i)}{2}$$

$$p_2 = E(x) + \frac{\max(x_i) - E(x)}{2} \qquad (3)$$

$$r_2 = max(x_i)$$

Where, E(x) is the expected value of load from the load duration curve of one day.

Interval Type-2 Fuzzy membership function

If x_i where i=1,2,3…..n (n<30) be the empirical per unit uncertain load data for Rural distribution system, then the Triangular fuzzy number (Dotted) will have a triangular $\underline{FOU}$ (lower foot-print-of-uncertinity) and a trapezoidal $\overline{FOU}$ (upper foot-print-of-uncertinity) with the following membership functions. So, this type of load variation can be modeled using an Interval type-2 fuzzy membership function [3] as discussed in the previous section.

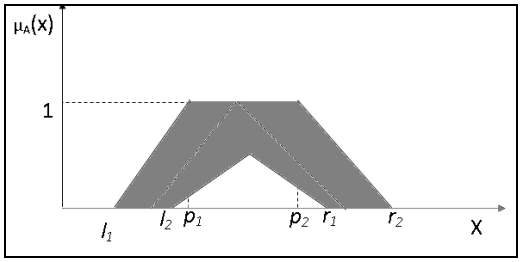


Fig-2: Type-2 fuzzy set trapezoidal upper membership function and lower triangular membership function

$$\underline{\mu(x)} = \underline{FOU(A)} = \begin{cases} 0 & x < l_2 \\ \frac{x - l_2}{p_2 - l_2} & x \geq \frac{r_1(p_2 - l_2) + l_2(r_1 - p_1)}{(p_2 - l_2) + (r_1 - p_1)} \\ \frac{r_2 - x}{r_2 - p_2} & x > \frac{r_1(p_2 - l_2) + l_2(r_1 - p_1)}{(p_2 - l_2) + (r_1 - p_1)} \\ 0 & x > r_2 \end{cases} \qquad (4)$$

$$\overline{\mu(x)} = \overline{FOU(A)} = \begin{cases} 0 & x < l_1 \\ \frac{x - l_1}{p_1 - l_1} & l_1 \leq x < p_1 \\ 1 & p_1 \leq x < p_2 \\ \frac{r_2 - x}{r_2 - p_2} & p_2 < x < r_2 \\ 0 & x > r_2 \end{cases} \qquad (5)$$

Where 'x' is the active and reactive power load, the corresponding membership function values μ(x) can be obtained for the lower and upper foot-print-of-uncertainties (FOU) as given by the above equations.

Representation of load variation by type-2 fuzzy sets

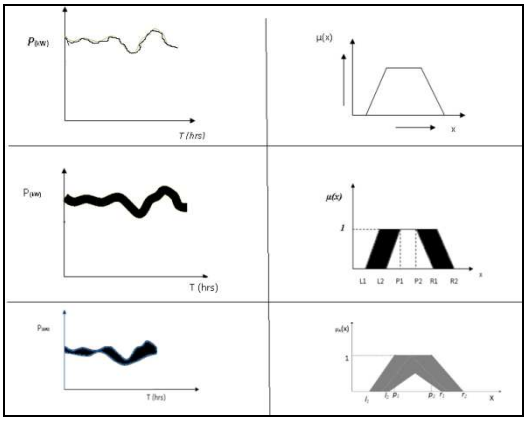


Fig-3: Represents load duration curves (left) replaced by a Type-2 fuzzy set with n-number of Type-1 fuzzy sets (row 2 and 3 in column 2).

II. INTERVAL TYPE-2 FUZZY INFERENCE SYSTEM

The membership functions are modeled by classifying the each load variation with linguistic variables Least, Very Very Small, Very Small, Small, High Medium, Medium, Low Medium, Large, Very Large, Very Very Large, Maximum, Extreme. The fuzzy rules permit expressing the available knowledge about the relationship between antecedent and consequents. To express this knowledge completely we normally have several rules, grouped to form what it is known a rule base, that is, a set of rules that express the known relationships between antecedent and consequents. For example the Rule: If Load is **Very large** then Voltage is **Very Small** this is for Single-Antecedent and Single-Consequent case. If Load is **large** and line-length is **small** then Voltage-drop is **Medium**. This is for Two-Antecedent and Single-Consequent case. Similarly other rules can be framed based on the distribution system considered. The developed type-2 FIS will have the sets of rules which can be framed based on the inputs (Load data) and the outputs (Voltage at each bus). The proposed algorithm is flexible for modification of inference rules. The program has been implemented in MATLAB R2007b.

A. Antecedent and Consequent membership functions [12,13]

Step-1: Initially the data (Active and Reactive power readings of the rural feeder for 48-samples per day, line data, load data and line lengths)is collected from the substation.

Step-2: Perform the power flow solution for the 31 days of a month with 48-samples of load data for each day, for all the 37-load points of the feeder.

Step-3: From the load data collected from step-1, using Eq.(4) and Eq.(5) the Interval Type-2 Fuzzy anticident membership function is determined.

Step-4: From the Computed feeder voltage-drops from step-2, using Eq.(4) and Eq.(5) the Interval Type-2 Fuzzy consiquient membership function is determined.

Step-6: Fuzzy inference rules are framed with two-inputs (Loads and Line-length) and one-output (Voltage drops) as shown in Table-1.

Step-7: A mamdani fuzzy inference system is used to relate the antesident and consiquent Interval Type-2 membership functions.

Step-8: Thus, an input-output relation Graph is obtained for the upper and lower Trapezoidal Interval Type-2 membership functions, Which can give information about the uncertain relationship that exists in practical distribution system between the loads, line-lengths and feeder voltage drops.

Implementation

$$\begin{bmatrix} B_1 \\ B_2 \\ B_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} I_2 \\ I_3 \\ I_4 \end{bmatrix}$$

$$\begin{bmatrix} B_1 \\ B_2 \\ B_3 \end{bmatrix} = I_2 \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + I_3 \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + I_4 \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

Where $I_2 = (P_2 - j*Q_2)/V_2^*$ Similarly I_3 and I_4.

$$\begin{bmatrix} V_2 \\ V_3 \\ V_4 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} - \begin{bmatrix} Z_1 \\ Z_1 \\ Z_1 \end{bmatrix} I_2 + \begin{bmatrix} Z_1 \\ Z_1 + Z_2 \\ Z_1 + Z_2 \end{bmatrix} I_3 + \begin{bmatrix} Z_1 \\ Z_1 + Z_2 \\ Z_1 + Z_2 + Z_3 \end{bmatrix} I_4$$

All the type-2 fuzzy load currents can be added using the above equation to calculate the type-2 bus voltages at bus-2,3and4 respectively. Z is a function of (R + j*X) Ohms/Km and length of the feeder in Kilometers. In the above equation if I_2, I_3, and I_4 are Type-2 Trapezoidal fuzzy membership functions, than the voltages obtained are also the Type-2 Trapezoidal fuzzy membership functions.

III. MEASURES OF UNCERTAINTY

The measures of uncertainties [16] of Type-2 Fuzzy numbers such as Fuzziness, Variance, Skewness, Cardinality and Centroid for the obtained outputs from the fuzzy inference system gives information in the uncertain voltage variations with the uncertain variation in the load. These uncertainty measures for IT2 FSs each are represented as interval, and the length of the interval is an indicator of uncertainty. The larger (smaller) the interval, the more (less) the uncertainty. The measures may also be used to measure the similarity between two IT2 FSs. Cardinality is the most representative uncertainty measure for an IT2 FS: its center is a representative intra-personal Uncertainty measure, and its length is a representative inter-personal uncertainty measure [12]. Centroid is a very important characteristic for IT2 FSs: its center can be used in ranking, and its length is a representative inter-personal uncertainty measure. Further the similarity measures of interval Type-2 fuzzy sets will help in identifying the **obtained output word** from the Type-2 FIS (Linguistic label), e.g., voltage in our case similar to the desired word (Linguistic label). The substation operator could take an appropriate decision with the obtained output results from Type-2 FIS. There are many similarity measures for Interval Type-2 Fuzzy Sets (IT2 FSs) in literature, Jaccard similarity measure is the most efficient method of measuring the similarity between the two IT2 FS's, so, and the authors also adopt the same here.

The developed Interval Type-2 Fuzzy Inference System (IT FIS) helps the system planner to get the overview of the state of the system for a longer duration (studied data for more than one-month), from the obtained IT2 FS's of voltages at each bus, line-voltage-drops, power flows and losses in each lines. Whereas at an instant of time of a day (snap-shot) for a particular loads at each of the bus, the developed IT2 FIS gives a point on the Trapezoidal IT2 FS (Example: Voltage), if the point falls numerically within the 12-test membership functions in Table- 1 the Jaccard similarity measure will produce a number

which is less than one, like this the similarity measure value is calculated by using eq.(1). Table-3 is produced with the standard membership functions along columns specified by 12-linguistic words, and the rows are the number of buses that are present in the considered distribution system. The highest value of number in the row of Table-3 which is given in the last column of Table-3, will display the status of the system with a linguistic word. This is depicted in Table-2 for a particular snap-shot of the day.

Table-1: Standard Linguistic Words which are modeled as IT2 FS.

Word Number	Linguistic Words
1	Alarm
2	Very Very Very Small
3	Small
4	High Medium
5	Medium
6	Low Medium
7	Large
8	Very Large
9	Very Very Large
10	Maximum
11	Good
12	

Table-2: Linguistic-word which indicates the status of the system by Jaccard similarity measure of the obtained IT2 FS from the FIS with standard Linguistic Words.

Bus Number	Linguistic Words	Word Number	Jaccard Similarity Number
1	Low Medium	7	0.2935
2	Large	8	0.4578
3	Good	12	0.4276
4	Low Medium	7	0.2798
5	Large	8	0.268
6	Maximum	11	0.37
7	Good	12	0.3075
8	Good	12	0.3415
9	Good	12	0.4188
10	Large	8	0.2603
11	Large	8	0.2816
12	Large	8	0.3607
13	Very Large	9	0.3472
14	Good	12	0.4447
15	Very Large	9	0.3284
16	Very Very Large	10	0.3386
17	Very Very Large	10	0.4219
18	Very Very Large	10	0.4837
19	Very Very Large	10	0.4152
20	Maximum	11	0.3282
21	Maximum	11	0.3661
22	Good	12	0.353
23	Good	12	0.3091
24	Good	12	0.4184
25	Large	8	0.3613
26	Large	8	0.3441
27	Very Large	9	0.3146
28	Good	12	0.4442
29	Very Very Large	10	0.3398
30	Very Very Large	10	0.4218
31	Very Very Large	10	0.484
32	Very Very Large	10	0.4113

33	Good	12	0.3119
34	Good	12	0.3974
35	Good	12	0.4186
36	Good	12	0.3092
37	Good	12	0.4188

Fig-4: Represents the uncertain interval relationship between one-input (load variations) and one-output (bus voltages) membership functions

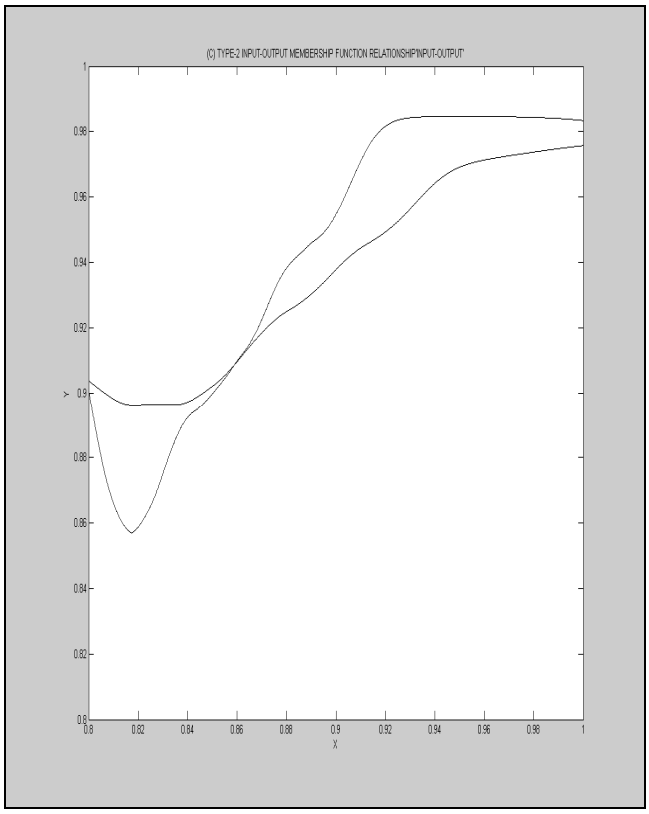
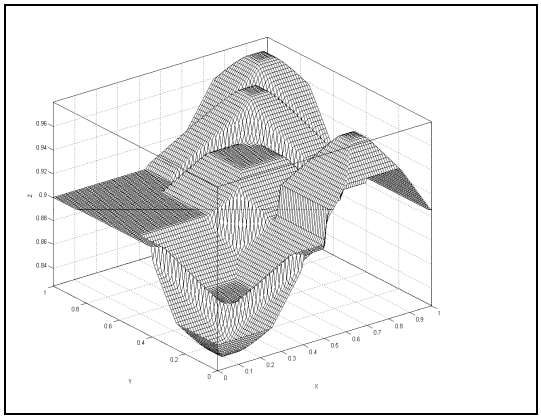


Fig-5: Represents the uncertain interval relationship between one-input (load variations), the second-input line-length uncertainty and output (bus voltages) membership functions



IV. RESULTS AND DISCUSSIONS

The uncertain input-output relationship revels the variation in the voltages with the variation in the load for an interval of values, these input-output relationship functions can be used to train the neural network learn the functions. The developed IT2 FIS can also be used for on-line studies, if the data from SCADA is synchronized with the developed program. Fig-5 represents the IT2 membership functions of losses in each branch, fig-6 represents the test membership function which are used for similarity measure with the voltage-drop and voltage membership functions, fig-7 and fig-8 represents the voltages and load s at each buses. The load at the substation is considered as zero, so the voltage at the substation is obtained as 1.0 p.u. so no membership functions are mentioned in the fig-7. Tables-3(Appendix) gives the Jaccard similarity measure values between the IT2FS of each branch voltage drop with the IT2FS of linguistic word. Also, the program is going to display, the branches where the voltage-drop is predominant and where there is less voltage-drop, so, at the substation the operator is able to view the status of each line with the linguistic label displays on the screen such as (small, considerable amount, high, medium,…..etc). By the above mentioned procedure it is also possible to find the status of bus-voltages Line-Currents and Power-Flows. The developed IT2 FIS has been validated by finding the centroid values of the output voltage membership functions with the resultant voltage obtained from the normal power-flow solution as mentioned by the procedure in section-III-B by taking the centroid values of the input load membership function.

APPENDIX

Word / Branch Number	Alarm	Very Very Small	Very Small	Small	High Medium	Medium	Low Medium	Large	Very Large	Very Very Large	Maximum	Good	Jaccard Similarity Number
1	0	0	0.0124	0.0007	0.0249	0.117	0.2158	0.2935	0.1317	0.0124	0	0	0.2935
2	0	0	0	0	0	0.0577	0.0837	0.4578	0.2149	0.098	0.0022	0	0.4578
3	0	0	0	0	0	0	0	0	0	0.0106	0.1144	0.4276	0.4276
4	0.0367	0.101	0.2798	0.2188	0.1358	0.13	0.0669	0.0802	0.0309	0.0023	0	0	0.2798
5	0	0.0183	0.2678	0.268	0.2527	0.2277	0.1078	0.1245	0.0528	0.0119	0	0	0.268
6	0	0	0	0	0	0.0241	0.0079	0.1225	0.1172	0.37	0.1729	0.0311	0.37
7	0	0	0	0	0	0.0082	0	0.0313	0.0336	0.3075	0.286	0.1038	0.3075
8	0	0	0	0	0	0	0	0	0	0	0.0506	0.3415	0.3415
9	0	0	0	0	0	0	0	0	0	0.0126	0.1229	0.4188	0.4188
10	0	0.0121	0.2368	0.258	0.2603	0.2484	0.1188	0.1297	0.0557	0.0144	0	0	0.2603
11	0	0.0048	0.1827	0.2306	0.254	0.2816	0.1399	0.1396	0.0596	0.0191	0	0	0.2816
12	0	0	0.0545	0.0651	0.1179	0.3607	0.2575	0.2011	0.0799	0.0431	0.0017	0	0.3607
13	0	0	0.0418	0.0422	0.0851	0.3472	0.284	0.2208	0.0884	0.0493	0.0029	0	0.3472
14	0	0	0	0	0	0	0	0	0	0	0.0687	0.4447	0.4447
15	0	0	0.0183	0.0067	0.0297	0.2416	0.3284	0.298	0.1262	0.0683	0.0095	0	0.3284
16	0	0	0.0116	0.0021	0.0191	0.2026	0.3055	0.3386	0.148	0.0766	0.0136	0	0.3386
17	0	0	0.0033	0	0.0056	0.1448	0.2136	0.4219	0.1998	0.0935	0.0237	0	0.4219
18	0	0	0	0	0	0.0989	0.1252	0.4837	0.278	0.1195	0.0376	0.0009	0.4837
19	0	0	0	0	0	0.067	0.0664	0.4152	0.3517	0.1647	0.0597	0.0036	0.4152
20	0	0	0	0	0	0.0463	0.0344	0.2711	0.3282	0.2463	0.0929	0.0099	0.3282
21	0	0	0	0	0	0.0267	0.0103	0.1389	0.1375	0.3661	0.159	0.0266	0.3661
22	0	0	0	0	0	0.01	0	0.0397	0.0399	0.353	0.2838	0.0886	0.353
23	0	0	0	0	0	0.003	0	0.0108	0.0131	0.1581	0.3091	0.1931	0.3091
24	0	0	0	0	0	0	0	0	0	0.0127	0.1233	0.4184	0.4184
25	0	0	0.0643	0.0814	0.1409	0.3613	0.2414	0.1908	0.0758	0.0396	0.0011	0	0.3613
26	0	0	0.041	0.0404	0.0828	0.3441	0.2837	0.2207	0.088	0.0483	0.0024	0	0.3441
27	0	0	0.0321	0.0236	0.0576	0.3146	0.3101	0.2454	0.0998	0.0562	0.0048	0	0.3146
28	0	0	0	0	0	0	0	0	0	0	0.0685	0.4442	0.4442
29	0	0	0.0114	0.002	0.0188	0.2013	0.3043	0.3398	0.1485	0.0768	0.0136	0	0.3398
30	0	0	0.0033	0	0.0056	0.1448	0.2137	0.4218	0.1998	0.0934	0.0237	0	0.4218
31	0	0	0	0	0	0.0983	0.1241	0.484	0.2791	0.1199	0.0377	0.0009	0.484
32	0	0	0	0	0	0.0664	0.0655	0.4113	0.3526	0.1658	0.0601	0.0037	0.4113
33	0	0	0	0	0	0.0026	0	0.0095	0.0116	0.1456	0.3119	0.2014	0.3119
34	0	0	0	0	0	0.0151	0.0013	0.0673	0.0593	0.3974	0.2449	0.0576	0.3974
35	0	0	0	0	0	0	0	0	0	0.0126	0.1231	0.4186	0.4186
36	0	0	0	0	0	0.003	0	0.0108	0.0131	0.1579	0.3092	0.1932	0.3092
37	0	0	0	0	0	0	0	0	0	0.0126	0.1229	0.4188	0.4188

Table-3: ***Voltage Drop*** in each branch is indicated by the JACCARD similarity MATRIX with the ***Rows as Branches*** and ***Columns as the Linguistic words*** along the Branches of the Practical Radial Distribution System

V. CONCLUSION

From the load data measured from the substation the Interval Type-2 Fuzzy Set (IT2 FS) of all the load buses are modeled. Consequent voltage IT2 FS is obtained by performing the power flow solution for 48 samples in a day and for 31-days of a month. Mamdani Interval Type-2 Fuzzy Inference System is developed, relationship between the load and voltage variations at each bus of the system can be used to find the voltage at each bus for a particular load at that bus. Once the consequent membership functions (IT2 FS's Voltages at each bus- **Ã**) are obtained for a particular IT2 FS's load, it is possible to map the IT2 FS **Ã** into a Word (Linguistic label). Given a standard vocabulary consisting of N words with their associated IT2 FS $\tilde{B}$, the goal is to find the Ã which closely resembles $\tilde{B}$, for which the similarity between two IT2 FS's is used. Jaccard similarity measure is the most efficient method of measuring the similarity between the two IT2 FS's, so, the authors also adopt the same here. The validity of the modeled IT2 FS of loads and the voltages have been verified by taking the centroid values of IT2 FS loads at each bus and performed the power-flow solution to find the centroid values of IT2 FS voltages at each bus. The measures of uncertainty of IT2FS have been computed. These uncertainty measures for IT2 FSs each are represented as interval, and the length of the interval is an indicator of uncertainty. The larger (smaller) the interval, the more (less) the uncertainty. The measures may also be used to measure the similarity between two IT2 FSs. The developed power-flow solution method can be used for Fault analysis, Contingency analysis, SMART GRID with bulk amount of uncertain data.

VI. References

[1] *P K Satpathy, D Das, P B Dutta Gupta, "Power Flow Analysis Using Fuzzy Set Approach", Journal of Inst. Of Engineers, Vol 85, June 2004, India.*

[2] *K. Kaulianiemi, "Fuzzy Models and Techniques for the Calculation of Radial Distribution Networks," IEEE Athens Power Tech Conference: Athens, Greece, Sept. 543, 1993.*

[3] *G.K. Viswanadha Raju P.R. Bijwe, "Reactive power/voltage control in distribution systems under uncertain environment", IET Gener. Transm. Distrib., 2008, Vol. 2, No. 5, pp. 752–763.*

[4] *Zorel Zisman, Gheorghe Cartina, "Estimation of Distribution Transformers Loading by Fuzzy Logic," 21st IEEE Convention of the Electrical and Electronic Engineers in Israel. Proceedings (Cat. No.00EX377) pp.303-307, 2000.*

[5] *Tsai-Hsiang Chen, Shyi-Wen Wang, "Simplified three-phase lateral and feeder models for fast distribution system calculations", Electric Power Systems Research 39 (1996) 47-53.*

[6] *G. Lambert Torres, D. Mukhedkar, "Distribution Feeder Load Modeling: An Approach Using FS," National Power System Conference-1985, India.*

[7] *Han-Ching Kou, Yuan-Yih Hsu, "Distribution System Load Estimation and Service Restoration Using a Fuzzy Set Approach", IEEE Transactions on Power Delivery, Vol. 8, No.4, pp. 1950-1957, October 1993.*

[8] *Atish K. Ghosh, David L. Lubkeman, Robert H. Jones, "Load Modeling For Distribution Circuit State Estimation," IEEE Transactions On Power Delivery, Vol. 12, No. 2, April 1997.*

[9] *P K Satpathy, D Das, P B Dutta, "Static Voltage Stability Analysis Using Fuzzy Set Approach Gupta", Journal of Inst. Of Engineers, Vol 85, June 2004, India.*

[10] *L.A. Zadeh, The concept of a linguistic variable and its application to approximate reasoning – I, Information Science, vol. 8 (1975) 199-249.*

[11] *Nilesh N. Karnik, Jerry M. Mendel, and Qilian Liang, "Type-2 Fuzzy Logic Systems", IEEE Transactions On Fuzzy Systems, Vol. 7, No. 6, December 1999.*

[12] *D. Wu, J.M. Mendel, Cardinality, fuzziness, variance and skewness of interval type-2 fuzzy sets, in: Proceedings of the First IEEE Symposium on Foundations of Computational Intelligence, Honolulu, HI, 2007, pp. 375–382.*

[13] *J.M. Mendel, Uncertain rule-based fuzzy logic systems: Introduction and new direction, Prentice Hall, NJ. (2001).*

[14] *Dongrui Wu, Jerry M. Mendel , "A comparative study of ranking methods, similarity measures and uncertainty measures for interval type-2 fuzzy sets", Information Sciences 179 (2009) 1169–1192.*

[15] *Kersting, W.H, Distribution System Modeling and Analysis, CRC press.*

[16] *ebsite: http://sipi.usc.edu./~mendel/report*


© IJITCE Publication