BIG DATA: CHALLENGES AND PROSPECTS

Sarika Choudhary[1], Ritika Saroha[2], Yatan Dahiya[3]

[1,2] M.tech (Network Security), School of Engineering & Sciences,

BPS Mahila Vishwavidyalaya, Sonepat, Haryana, (India)

[3]M.Tech (CSE), Baba Mastnath College of Engg., MD University, Rohtak (India)

ABSTRACT

The problems start during data acquisition, when the bulk data requires us to make decisions, currently in an ad hoc manner, about what data to keep and what to discard, and how to store what we keep reliably with the right metadata. Many data today is not natively in structured format, for e.g.: blogs and tweets are weakly structured pieces of text, while images and video are structured for storage and display, but not for semantic content and search, so transforming such content into a structured format for later study is a major test. The objective of this paper is to discuss the characteristics of big data as well as the challenges and opportunities for big data analytics – the process of extracting knowledge from sets of big data.

However, it is hard, requiring us to rethink data analysis systems in fundamental ways. A major speculation in Big Data, properly directed, can result not only in major scientific advances, but also place the foundation for the next generation of advances in science, medicine, and business.

Keywords: Data Acquisition, Big Data Analysis, Heterogeneity, Privacy, Query Processing.

I INTRODUCTION

In a broad range of application areas, data is being collected at extraordinary scale. Decisions that previously were based on guesswork, or on painstakingly constructed models of reality, can now be made based on the data itself. Such Big Data analysis now drives nearly every aspect of our modern society, including mobile services, manufacturing, financial services and life sciences etc.

The field of Astronomy is being changed from one where taking pictures of the sky was a large part of an astronomer's job to one where the pictures are all in a database already and the astronomer's task is to find interesting objects and observable fact in the database.

In the biological sciences, there is now a well-established tradition of depositing technical data into a public repository, and also of creating public databases for use by other scientists. In fact, there is a whole discipline of bioinformatics i.e. largely devoted to the duration and analysis of such data. As technology advances, particularly with the initiation of Next Generation Sequencing, the size and number of experimental data sets available is increasing exponentially.

Imagine a world in which we have access to a huge database where we gather every detailed calculate of every student's academic performance. This data could be used to plan the most helpful approaches to education, starting from reading, writing, and math, to advanced, college-level, courses. We are far from having access to such data. In particular, there is a strong trend for massive Web exploitation of educational activities, and this will produce a gradually larger amount of detailed data about students' performance.

The sheer size of the data, of course, is a major challenge, and is the one that is most easily recognized. However, there are others. Industry analysis companies like to point out that there are challenges not just in Volume, but also in Variety and Velocity. By Variety, they usually mean heterogeneity of data types, representation, and semantic interpretation. By Velocity, they mean both the rate at which data arrive and the time in which it must be acted upon. While these three are important, this short list fails to include additional important requirements such as privacy and usability.

The analysis of Big Data involves various distinct phases as shown in the figure below, each of which introduces challenges. Many people unfortunately focus just on the examination/modeling phase: while that phase is critical, it is of little use without the other phases of the data analysis pipeline. Even in the analysis phase, which has received much attention, there are poorly understood complexities in the context of multi-tenanted clusters where several users' programs run concurrently. Many significant challenges extend beyond the analysis phase, for e.g. Big Data has to be managed in context, which may be noisy, heterogeneous. Doing so raises the need to track provenance and to handle uncertainty and error: topics that are crucial to success, and yet rarely mentioned in the same breath as Big Data.

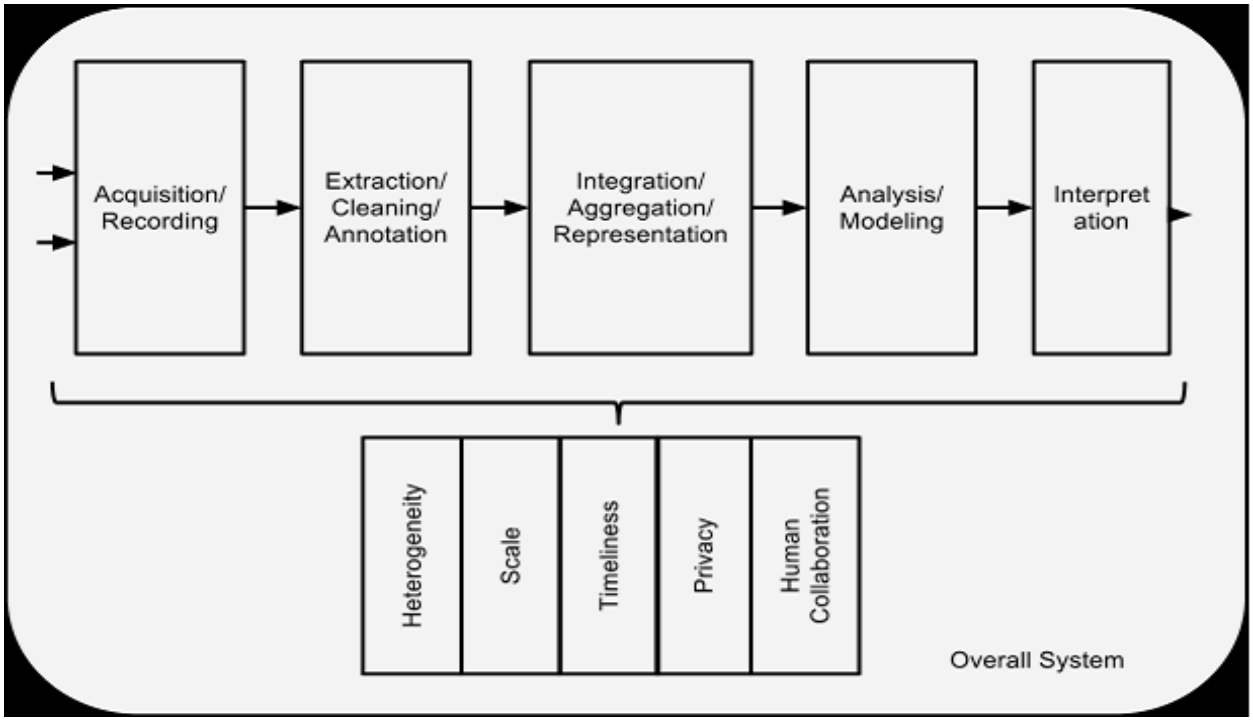


Fig: The BDA pipeline. Major steps in analysis of big data are shown in the flow at top. Below it are big data needs that make these tasks challenging.

Fortunately, existing computational techniques can be applied, either as is or with some extensions, to at least some aspects of the Big Data problem. For example, relational databases rely on the notion of logical data independence: users can think about what they want to compute, while the system (with skilled engineers designing those systems) determines how to compute it efficiently. Similarly, the SQL standard and the relational data model provide a uniform, powerful language to express many query needs and, in principle, allows customers to choose between vendors, increasing competition. The challenge ahead of us is to combine these healthy features of prior systems as we devise novel solutions to the many new challenges of Big Data. In this paper, we consider each of the boxes in the figure above, and discuss both what has already been done and what challenges remain as we seek to exploit Big Data. We begin by considering the five stages in the pipeline, then move on to the five cross-cutting challenges, and end with a discussion of the architecture of the overall system that combines all these functions.

II PHASES IN THE PROCESSING PIPELINE

2.1 Data Acquisition and Recording

Big Data does not arise out of a vacuum: it is recorded from some data generating source. For example, consider our ability to sense and observe the world around us, from the heart rate of an elderly citizen, and presence of toxins in the air we breathe, to the planned square kilometer array telescope, which will produce up to 1 million terabytes of raw data per day. Much of this data is of no interest, and it can be filtered and compressed by orders of magnitude. One challenge is to define these filters in such a way that they do not discard useful information. The second big challenge is to automatically generate the right metadata to describe what data is recorded and how it is recorded and measured. For example, in scientific experiments, considerable detail regarding specific experimental conditions and procedures may be required to be able to interpret the results correctly, and it is important that such metadata be recorded with observational data. Metadata acquisition systems can minimize the human burden in recording metadata. Another important issue here is data provenance.

2.2 Information Extraction and Cleaning

The information collected will not be in a format ready for analysis. For example, consider the collection of electronic health records in a hospital, comprising transcribed dictations from several physicians, structured data from sensors and measurements, and image data such as x-rays. We cannot leave the data in this form and still effectively analyze it. Rather we require an information extraction process that pulls out the required information from the underlying sources and expresses it in a structured form suitable for analysis.

2.3 Data Integration, Aggregation, and Representation

Data analysis is considerably more challenging than simply locating, identifying, understanding, and citing data. For effective large-scale analysis all of this has to happen in a completely automated manner. This requires differences in data structure and semantics to be expressed in forms that are computer understandable, and then

"robotically" resolvable. There is a strong body of work in data integration that can provide some of the answers. However, considerable additional work is required to achieve automated error-free difference resolution.

We must enable other professionals, such as domain scientists, to create effective database designs, either through devising tools to assist them in the design process or through forgoing the design process completely and developing techniques so that databases can be used effectively in the absence of intelligent database design.

2.4 Query Processing, Data Modeling, and Analysis

Methods for querying and mining Big Data are fundamentally different from traditional statistical analysis on small samples. Big Data is often noisy, dynamic, heterogeneous, inter-related and untrustworthy. Nevertheless, even noisy Big Data could be more valuable than tiny samples because general statistics obtained from frequent patterns and correlation analysis usually overpower individual fluctuations and often disclose more reliable hidden patterns and knowledge. Further, interconnected Big Data forms large heterogeneous information networks, with which information redundancy can be explored to compensate for missing data, to crosscheck conflicting cases, to validate trustworthy relationships, to disclose inherent clusters, and to uncover hidden relationships and models. A knowledge-base constructed from related data can use associated symptoms or medications to determine which of two the physician meant.

Big Data is also enabling the next generation of interactive data analysis with real-time answers. In the future, queries towards Big Data will be automatically generated for content creation on websites, to populate hot-lists or recommendations, and to provide an ad hoc analysis of the value of a data set to decide whether to store or to discard it. Scaling complex query processing techniques to terabytes while enabling interactive response times is a major open research problem today. A problem with current Big Data analysis is the lack of coordination between database systems, which host the data and provide SQL querying, with analytics packages that perform various forms of non-SQL processing, such as data mining and statistical analyses.

2.5 Interpretation

A decision-maker, provided with the result of analysis, has to interpret the results. This interpretation cannot happen in a vacuum. Usually, it involves examining all the assumptions made and retracing the analysis. Furthermore, as we saw above, there are many possible sources of error: computer systems can have bugs, models almost always have assumptions, and results can be based on erroneous data. For all of these reasons, no responsible user will cede authority to the computer system. Rather she will try to understand, and verify, the results produced by the computer. This is particularly a challenge with Big Data due to its complexity. There are often crucial assumptions behind the data recorded. Analytical pipelines can often involve multiple steps, again with assumptions built in. In short, it is rarely enough to provide just the results. Rather, one must provide supplementary information that explains how each result was derived, and based upon precisely what inputs. Such supplementary information is called the provenance of the (result) data.

III CHALLENGES IN BIG DATA ANALYSIS

Having described the multiple phases in the Big Data analysis pipeline, we now turn to some common challenges that underlie many, and sometimes all, of these phases.

3.1 Heterogeneity and Incompleteness

When humans consume information, a great deal of heterogeneity is comfortably tolerated. However, machine analysis algorithms expect homogeneous data, and cannot understand gradation. In consequence, data must be carefully structured as a first step in data analysis. The three design choices listed have successively less structure and, conversely, successively greater variety. Greater structure is likely to be required by many data analysis systems. However, the less structured design is likely to be more effective for many. However, computer systems work most efficiently if they can store multiple items that are all identical in size and structure.

Even after data cleaning and error correction, some incompleteness and some errors in data are likely to remain. This incompleteness and these errors must be managed during data analysis. Doing this correctly is a challenge. Recent work on managing probabilistic data suggests one way to make progress.

3.2 Scale

The first thing anyone thinks of with Big Data is its size. After all, the word “big” is there in the very name. Managing large and rapidly increasing volumes of data has been a challenging issue for many decades. In the past, this challenge was mitigated by processors getting faster, following Moore’s law, to provide us with the resources needed to cope with increasing volumes of data. But, there is a fundamental shift underway now: data volume is scaling faster than compute resources, and CPU speeds are static.

First, over the last five years the processor technology has made a dramatic shift - rather than processors doubling their clock cycle frequency every 18-24 months, now, due to power constraints, clock speeds have largely stalled and processors are being built with increasing numbers of cores.

The second dramatic shift that is underway is the move towards cloud computing, which now aggregates multiple disparate workloads with varying performance goals (e.g. interactive services demand that the data processing engine return back an answer within a fixed response time cap) into very large clusters. This level of sharing of resources on expensive and large clusters requires new ways of determining how to run and execute data processing jobs so that we can meet the goals of each workload cost-effectively, and to deal with system failures, which occur more frequently as we operate on larger and larger clusters.

A third dramatic shift that is underway is the transformative change of the traditional I/O subsystem. For many decades, hard disk drives (HDDs) were used to store persistent data. HDDs had far slower random IO performance than sequential IO performance, and data processing engines formatted their data and designed their query processing methods to “work around” this limitation.

3.3 Timeliness

The flip side of size is speed. The larger the data set to be processed, the longer it will take to analyze. The design of a system that effectively deals with size is likely also to result in a system that can process a given size of data set faster. However, it is not just this speed that is usually meant when one speaks of Velocity in the context of Big Data. There are many situations in which the result of the analysis is required immediately. Given a large data set, it is often necessary to find elements in it that meet a specified criterion. In the course of data analysis, this sort of search is likely to occur repeatedly. Scanning the entire data set to find suitable elements is obviously impractical. Rather, index structures are created in advance to permit finding qualifying elements quickly.

3.4 Privacy

The privacy of data is another huge concern, and one that increases in the context of Big Data. For electronic health records, there are strict laws governing what can and cannot be done. Managing privacy is effectively both a technical and a sociological problem, which must be addressed jointly from both perspectives to realize the promise of big data.

Consider, for example, data gleaned from location-based services. These new architectures require a user to share his/her location with the service provider, resulting in obvious privacy concerns. Note that hiding the user's identity alone without hiding her location would not properly address these privacy concerns. An attacker or a (potentially malicious) location-based server can infer the identity of the query source from its (subsequent) location information. This is because with location-based services, the location of the user is needed for a successful data access or data collection, while the identity of the user is not necessary.

3.5 Human Collaboration

In spite of the tremendous advances made in computational analysis, there remain many patterns that humans can easily detect but computer algorithms have a hard time finding. Indeed, CAPTCHAs exploit precisely this fact to tell human web users apart from computer programs.

In today's complex world, it often takes multiple experts from different domains to really understand what is going on. A Big Data analysis system must support input from multiple human experts, and shared exploration of results. These multiple experts may be separated in space and time when it is too expensive to assemble an entire team together in one room. The data system has to accept this distributed expert input, and support their collaboration.

IV CONCLUSION

We have entered an era of Big Data. Through better analysis of the large volumes of data that are becoming available. However, many technical challenges described in this paper must be addressed before this potential can be realized fully. The challenges include not just the obvious issues of scale, but also heterogeneity, lack of structure, error-handling, privacy, timeliness, provenance, and visualization, at all stages of the analysis pipeline from data acquisition to result interpretation. These technical challenges are common across a large variety of application domains, and therefore not cost-effective to address in the context of one domain alone.

Furthermore, these challenges will require transformative solutions, and will not be addressed naturally by the next generation of industrial products.

In databases, there is considerable work on optimizing individual operations, such as joins. It is well-known that there can be multiple orders of magnitude difference in the cost of two different ways to execute the same query. Fortunately, the user does not have to make this choice – the database system makes it for her. In the case of Big Data, these optimizations may be more complex because not all operations will be I/O intensive as in databases. So standard database optimization techniques cannot directly be used. However, it should be possible to develop new techniques for Big Data operations inspired by database techniques.

The very fact that Big Data analysis typically involves multiple phases highlights a challenge that arises routinely in practice: production systems must run complex analytic pipelines, or workflows, at routine intervals, e.g., hourly or daily. New data must be incrementally accounted for, taking into account the results of prior analysis and pre-existing data. And of course, provenance must be preserved, and must include the phases in the analytic pipeline. Current systems offer little to no support for such Big Data pipelines, and this is in itself a challenging objective.

REFERENCES

[1] The Age of Big Data. Steve Lohr. *New York Times*, Feb 11, 2012. http://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html

[2] Kuo, M-H., Sahama, T., Kushniruk, A.W., Borycki, E.M. and Grunwell, D.K. (2014) 'Health big data analytics: current perspectives, challenges and potential solutions', *Int. J. Big Data Intelligence*, Vol. 1, Nos. 1/2, pp.114–126.

[3] *Nature* (2012) 'Seven days – the news in brief', Vol. 484, pp.10–11.

[4] Agency for Healthcare Research and Quality, *What Is Comparative Effectiveness Research* [online] http://effectivehealthcare.ahrq.gov/index.cfm/what-iscomparative-effectiveness-research1/ (accessed 2 November 2013).

[5] Aggarwal, C. and Wang, H. (2010) 'Managing and mining graph data', *Series: Advances in Database Systems*, Vol. 40, Springer, ISBN 978-1-4419-6045-0.

[6] Aggarwal, C.C. and Yu, P.S. (2008) *Privacy-Preserving Data Mining- Models and Algorithms*, Springer, ISBN 978-0-387-70991-8.

[7] Agrawal, D. et al. (2012) *Challenges and Opportunities with Big Data*, Big Data White Paper- Computing Research Association [online] http://cra.org/ccc/docs/init/bigdatawhitepaper.pdf (accessed 5 November 2013).

[8] http://www.cra.org/ccc/files/docs/init/bigdatawhitepaper.pdf

[9] http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2819144/

EFFECT OF PRESSURE ANGLE OF SPUR GEARS ON BENDING AND CONTACT STRESSES: A COMPARATIVE STUDY USING FINITE ELEMENT SOFTWARE

Krishanu Gupta[1], Sushovan Chatterjee[2]

[1]*M.Tech. Scholar, Department of Mechanical Engineering, NIT Silchar (India)*
[2]*Assistant Professor, Department of Mechanical Engineering, NIT Silchar (India)*

ABSTRACT

The principle objective of this paper is the comparison study of the static stresses for spur gear with different pressure angles. The analyzed results of a symmetric type involute profiled spur gear pair at different pressure angles are compared. Gears are one of the most important and crucial component in a mechanical power transmission unit and also in most of the industrial rotating machineries. Generally, a spur gear pair in action undergoes two types of stresses: the bending stress and the contact stress. In this paper, both these stresses on the gear tooth pair are analyzed using the finite element analysis and are compared. The stresses on the gear tooth are first analyzed using a finite element software and then those results are validated using the conventional formulae for finding stresses in gear tooth.

Keywords*: *Bending Stress, Contact Stress, Finite Element Analysis, Involute Profiled Spur Gear, Pressure Angle.

1. INTRODUCTION

Gears are important mechanical components that are used in the power transmission unit of different mechanical and automobile systems. Therefore, it becomes a necessary and an important area of research in order to improve the efficiency of different mechanical power transmission systems by improving the workability of gear systems. The finite element static analyses of the involute profiled spur gears are carried out in order to obtain different static stresses in gears for the performance of gears. The static stresses are found out within the elastic limit of the gear, i.e., the linear static analysis of involute profiled spur gear pair. In [1] the analysis was carried out by charging the structure with a normal concentration of force along the side of the tooth. The outcomes of [1] was, the areas that undergo highest stress are those closest to the tooth root fillet. Symmetric spur gears are those whose pressure angle at both coast and drive sides are the same, i.e., the commercially used involute teeth profiled spur gears. The stress

analysis, determination of the dynamics loads, the transmission errors, gear noise, and the optimal design for gear pairs are still a major concern in gear design and analysis.

In this paper, both the bending stresses and the contact stresses are analyzed. Firstly, in the bending stress analysis, the stresses that are induced at the gear tooth fillet are obtained by the finite element analysis. This bending stress that is obtained, if more than that of the allowable stress of the gear material, the gear is prone to bending tooth breakage, one of the tooth failure. Secondly, in the contact stress analysis, the stresses that are induced at the induced at the gear tooth face are obtained by the finite element method.

In this paper, to validate the obtained bending and the contact stress results by the finite element method, two theoretical formulae have been used, namely, the LEWIS BENDING stress equation for the static bending analysis, and AGMA CONTACT Stress Equation.

The 3D modeling of the gear pairs with different pressure angles are done using one of the solid modeling software. The solid model of the gear pairs with different pressure angles are converted from the basic solid model format to IGES or PARASOLID format and then import to the finite element software and then analyzed to get the different stress results.

II EQUATIONS AND CALCULATIONS

This chapter includes the discussion about the three dimensional model of the gear and pinion in mesh and also the finite element method that has been used to analyse the static conditions and calculate analytically the maximum and minimum stresses and strains when the spur gear are in mesh, for the spur gear pairs with different pressure angles (14.5°, 20°, 25° and 30°).

The 3D models of the pinion and the gear are created in a CAD software.

2.1. Gear Calculation formulae used in this paper:

1. Circular pitch, $p = \pi \cdot d'/N_P$
2. Diametral pitch, $P = N_P / d'$
3. Module, $m = 1.26 \times \sqrt[3]{\frac{T}{y[\sigma b] \psi m N_P}}$
4. Tip circle diameter, $d_a = d' + 2 \cdot m$
5. Root circle diameter, $d_t = d' - (2 \times 1.25 \cdot m)$
6. Base circle diameter, $d_b = d' \times \cos \phi$
7. Addendum, $h_a = m$
8. Dedendum, $h_f = 1.157 \cdot m$
9. Clearance, $c = 0.157 \cdot m$
10. Fillet radius, $r = 0.4 \times m$
11. Face width, $B = 9.5 \times m$
12. Working depth, $h_k = 2 \cdot m$

13. Whole depth, h_t =2.157·m
14. Tooth thickness on pitch circle, s = (π× m)/2
15. Addendum circle radius, r_A=Pitch circle radius× Addendum
16. Angular velocity of pinion, $\mathbf{w}_1$= (2 π n_p)/60
17. Pitch line velocity, v = $\mathbf{w}_1$× Pitch circle radius

From the Appendix of the Handbook of Gear Design [5], the standard dimensions for the symmetric spur gears are taken, as follows:

For Pinion, shaft diameter = 10mm.

For Gear/Wheel, shaft diameter = 10mm

2.2 Material Selection for the gear and the pinion

The materials for the pinion and the gear are chosen as ASTM Class 35 Cast Iron and ASTM 1045 or well known as C45 steel respectively. The reason behind choosing of these materials are, firstly, that these two are standard materials used for the gear pair and secondly, their availability. Also, the machining easiness of these materials lead to choosing of the materials. The mechanical properties of these materials are listed.

2.2.1. ASTM Class 35 Cast Iron

1. Young's Modulus=1.14×10^5MPa
2. Density= 7150 kg/m^3
3. UTS= 252 MPa
4. Poisson's ratio= 0.29
5. Yield Strength= 165 MPa
6. HB= 200 to 260

2.2.2. ASTM 1045 or C45 steel

1. Young's Modulus=2×10^5MPa
2. Density= 7870kg/m^3
3. UTS= 565 MPa
4. Poisson's ratio= 0.29
5. Yield Strength= 310 MPa
6. HB= 175-215

2.3 The calculations for the other gear pairs are the same except the base circle diameters.

Table 2.1. Calculated base circle diameters for 20°, 25°, and 30° involute profile gear pair

Profile		20°	25°	30°
Base Circle Diameters	Pinion	52.63 mm	50.75 mm	48.49 mm
	Gear	63.89 mm	61.63 mm	58.89 m

2.4 Meshing of Gears

Meshing is a very important criteria in solving Finite Element Analysis (FEA) problems. The basic theme of Finite Element Method is to make calculations at only finite number of points and interpolating the results of entire surface or volume of a body or an object.

The gear pairs are meshed with hexa-hedron meshing, which is commonly known as Hex-Dominant mesh type or Brick type meshing in FEA. This type of meshing has the advantage that they can be highly controlled and also can be generated automatically for optimal solution efficiency and accuracy [4].

2.5 Contact criteria for the contact stress in gears

For finding the contact stress in gears, Multi-point constraints (MPC) linear contact formulation is being used. Bonded (pure penalty) contact is a linear form of contact based connection. This contact connection between two bodies or surfaces must have contact elements on one body and target elements on other.

III REULTS AND DISCUSSIONS

The 3D models of different symmetric spur gear assemblies were modeled in CAD software with the dimensions mentioned in the precious chapter.

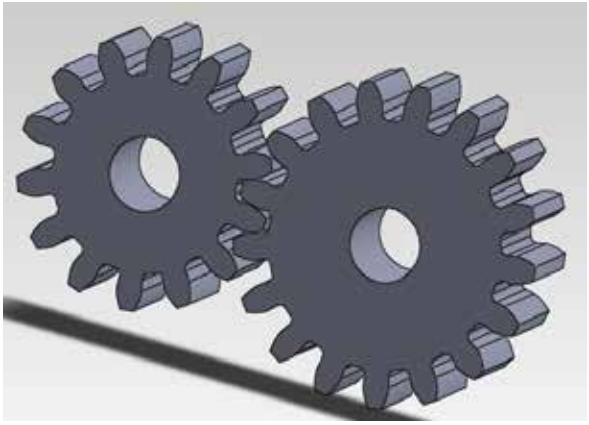


Fig.1. 14.5° Involute Teeth Profile

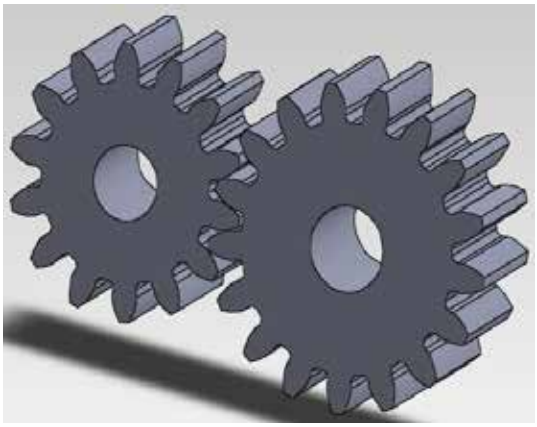


Fig.2. 20° Involute Teeth Profile

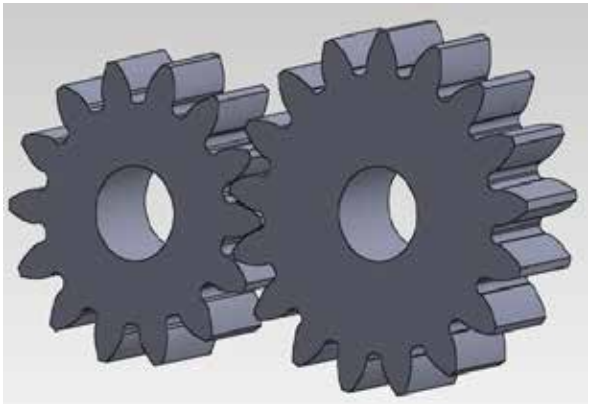


Fig. 3. 25° Involute Teeth Profile

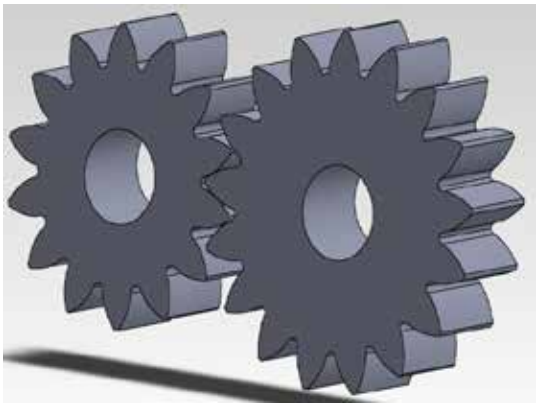


Fig.4. 30° Involute Teeth Profile

The four types of the spur gear assembly with different pressure angles (14.5°, 20°, 25° and 30°) were then analyzed using the finite element method based finite element software, in order to get the bending stress on the pinion tooth fillet and contact stress on the area where the two teeth of the gear pair are in contact with eachother.

3.1 Bending Stress analyses

The bending stress and maximum deformation of 14.5° involute profiled spur gear is shown.

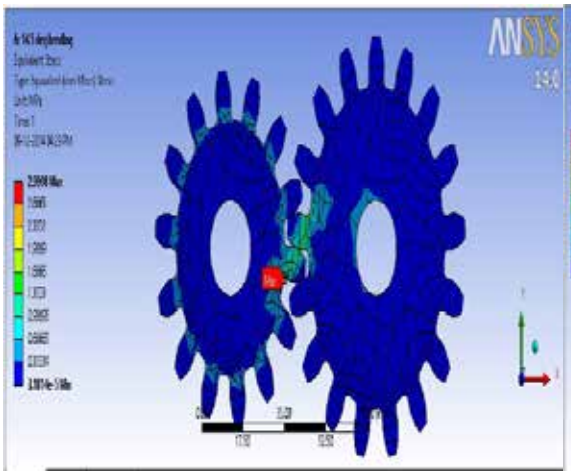


Fig. 5. Maximum Bending stress

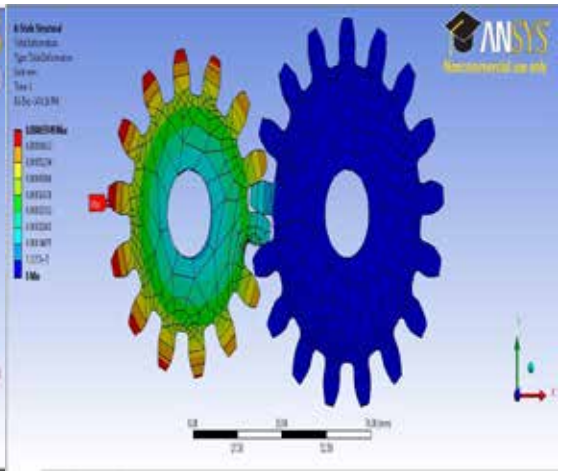


Fig. 6. Maximum Deformation

The bending stress and maximum deformation of 20° involute profiled spur gear is shown

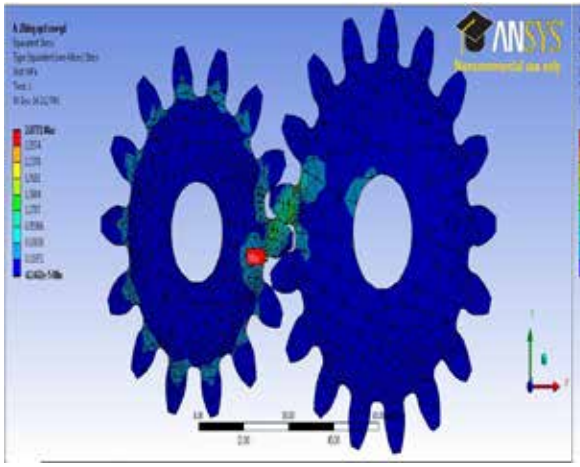


Fig. 7. Maximum Bending stress

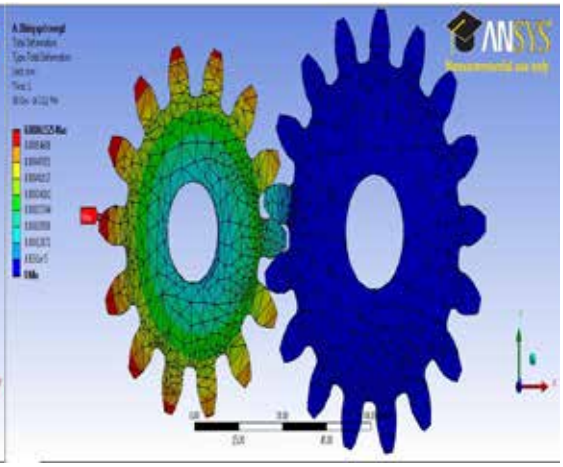


Fig. 8. Maximum Deformation

The bending stress and maximum deformation of 25° involute profiled spur gear is shown

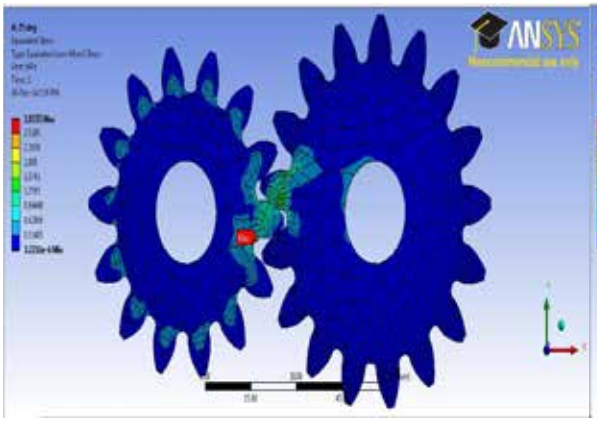


Fig. 9. Maximum Bending stress

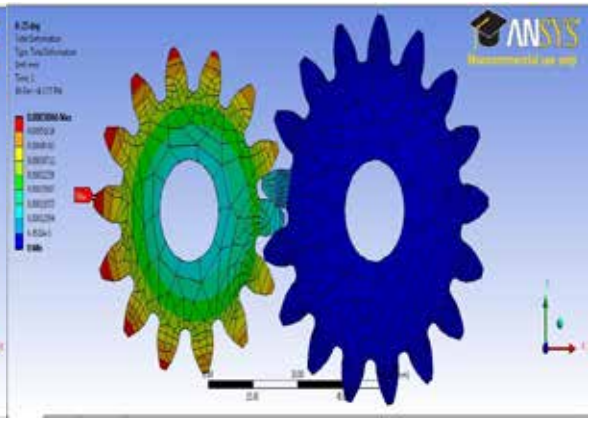


Fig. 10. Maximum Deformation

The bending stress and maximum deformation of 30° involute profiled spur gear is shown

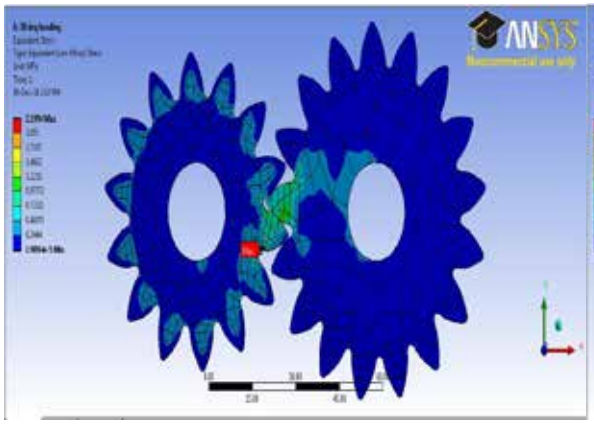


Fig. 11. Maximum Bending stress

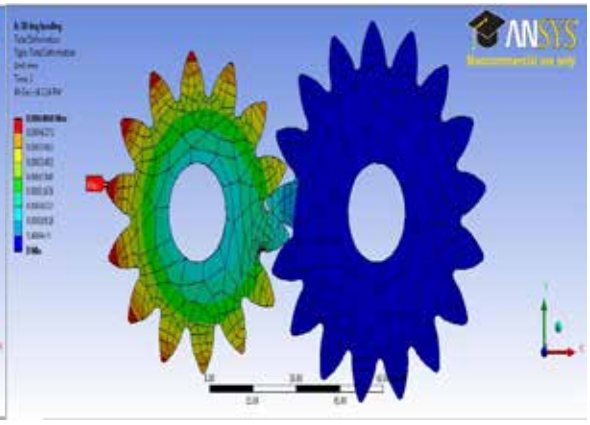


Fig. 12. Maximum Deformation

3.2 Contact Stress analyses

The Contact Stresses on the mating tooth surface of pinion and gear for the different pressure angle values of symmetric gear pair arrangement.

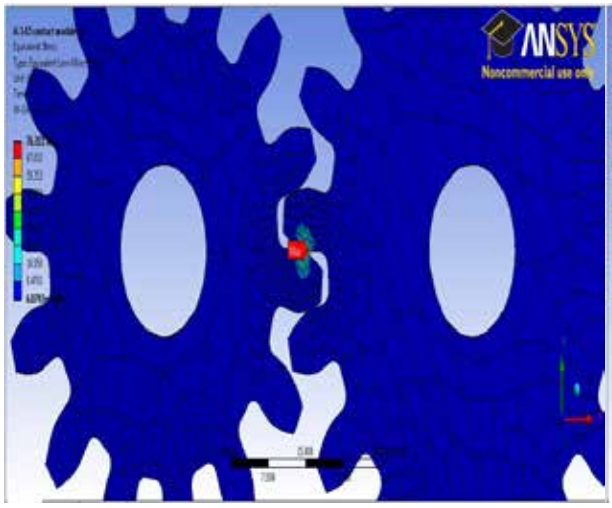


Fig. 13. Contact stress (14.5° gear assembly)

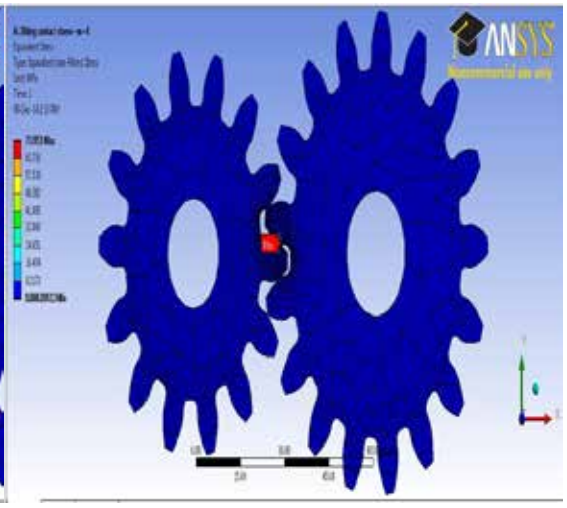


Fig. 14. Contact stress (20° gear assembly)

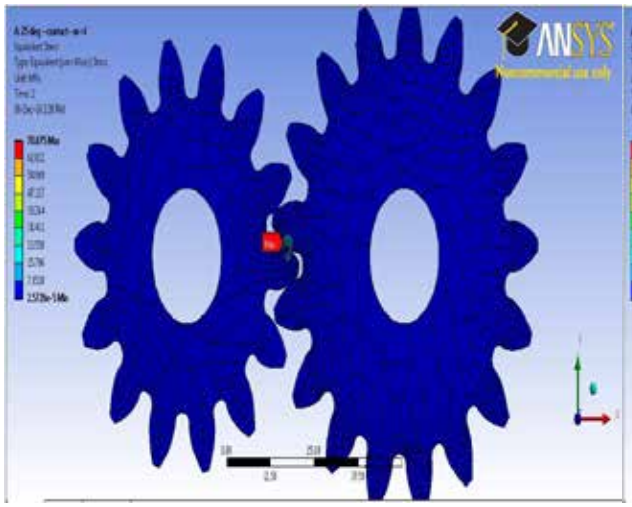


Fig. 15. Contact stress (25° gear assembly)

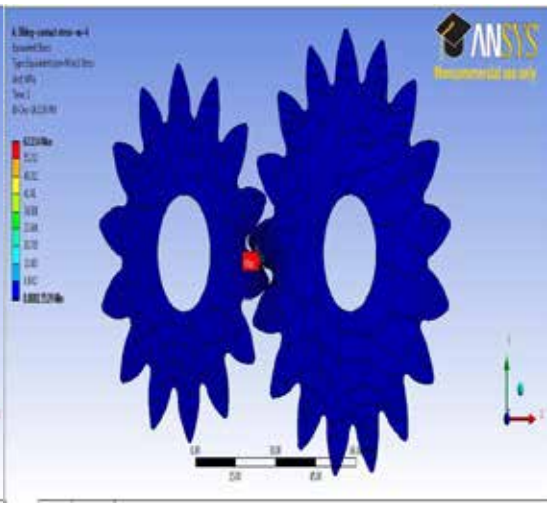


Fig. 16. Contact stress (30° gear assembly)

Table 3.1.Comparison of stresses on pressure angles

Pressure angles (in degrees)	Bending Stress (in MPa)	Contact Stress (in MPa)
14.5	2.9998	76.311
20	2.8771	73.953
25	2.8335	70.675

30	2.1994	62.114

3.3 Theoretical formulae for the stresses

1. LEWI'S BENDING STRESS EQUATION:

$$\sigma_t = \frac{F_t \times P_d}{B \times y}$$

where,

σ_t– Max. Bending stress

F_t- Tangential load on gear tooth

P_d- Diametral pitch

B- Face width

y- Lewis form factor

Using the equations, **σ_t= 2.7224 N/mm^2**

2. AGMA CONTACT STRESS EQUATION:

$$\sigma_H = C_p \sqrt{\frac{F_t}{B \times d_1 \times I} k_v . k_o . k_m}$$

where,

σ_H – Contact stress

C_p– Elastic coefficient = $0.564 \times \sqrt{\frac{1}{\frac{1-v_1^2}{E_1} \times \frac{1-v_2^2}{E_2}}}$

I – Geometry factor = $\frac{\sin\phi \cos\phi}{2} \times \frac{i}{i+1}$

k_v, k_o, k_m – Velocity factor, Overload factor,

and Load distribution factor respectively

$d_1 = \frac{d1_v}{\sin\phi}$;

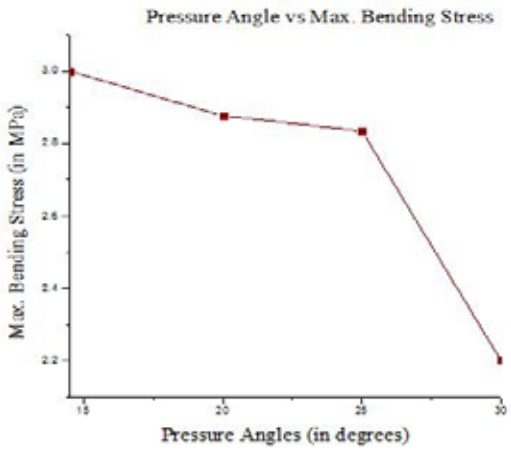
k_v=1,

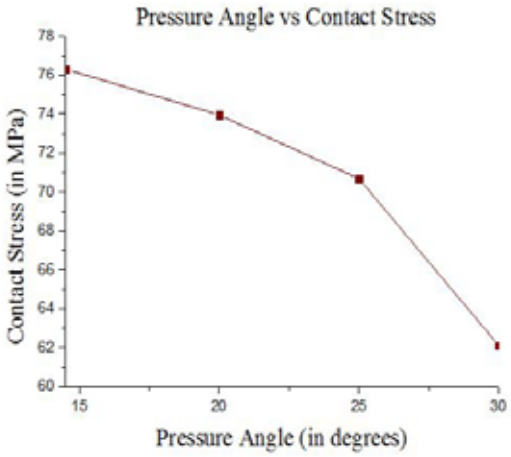
k_o=1(for uniform load),

k_m= 1.3

Using the equations, **σ_H= 76.11 N/mm^2**

3.4 Graphs plotter between the bending stress and pressure angle and also between contact stress and pressure angle.





Both the graphs above shows that, with the increase in the pressure angles, making the profile different, decreases or reduces the bending stress and also the contact stress.

IV CONCLUSION

In this paper, the equivalent stresses and strains of the symmetric involute spur gears were studied through finite element meshing simulation for finding out the gear pair with least stress when the pressure angles are increased from 14.5° to 30°.This paper finds a comprehensive study on the variation of static stresses with four different pressure angles that might be developed in spur gear teeth (while they are in contact) using a commonly used finite element based software package. As a case study, four different pressure angles of 14.5°, 20°, 25° and 30° were considered. Available fundamental equations along with classical standard (AGMA) were also consulted while carrying out this preliminary analysis.

GEAR NOMENCLATURE

N_P and N_G	Number of teeth on Pinion and Gear
m	Module
p	Circular pitch
P	Diametral pitch
d′	Pitch circle diameter
d_a	Tip circle diameter
d_b	Base circle diameter
d_t	Root circle diameter

ϕ	Pressure Angle
h_a	Addendum
h_f	Dedendum
c	Clearance
h_t	Whole depth
h_k	Working depth
s	Tooth thickness on pitch circle
r_A	Addendum circle radius
w_1	Angular velocity of pinion
v	Pitch line velocity
α	Half angle of tooth
σ	Bending Stress on tooth fillet
T	Torque transmitted
B	Face width
y	Lewis form factor

REFERENCES

[1] S.P. Shinde, A.A. Nikam, T.S. Mulla, *Static Analysis of Spur Gear using Finite Element Analysis; IOSR Journal of Mechanical and Civil Engineering (IOSR-JMCE),ISSN: 2278-1684, 26-31*.

[2] Y. Pandya, A. Parey; *Crack behavior in a high contact ratio spur gear tooth and its effect on mesh stiffness; Engineering Failure Analysis 34 (2013) 69–78.*

[3] G. M Maitra (*Handbook of Gear Design*, Second Edition; Tata McGraw-Hill Publishing Company Limited).

[4] N. S Gokhale, S. S. Deshpande, S. V Bedekar, A. N Thite, *Practical Finite Element Analysis* (Finite To Infinite, 2008).

[5] *Design Data book of Engineers complied by PSG College of Technology*, 2010,8.1-8.22.; KalaikathirAchchagam, Coimbatore, Tamilnadu, India.

[6] J.E. Shigley (*Mechanical Engineering Design*, First Metric Edition; McGraw-Hill Book Company,1986).

COMPARISON OF OWNCLOUD AND AMAZON CLOUD PERFORMANCE

Maha A. Sayal[1], Dr. Ayad A. Abdulsalam[2], Dr.AsmaaQ.Shareef[3]

[1]*Computer Science Department-College of Science – Baghdad University*

[2]*Computer Science Department-College of Education for women – Baghdad University*

[3]*Computer Science Department-College of Science – Baghdad University*

ABSTRACT

Owncloud is a software system for what is commonly termed file hosting. Its open source files sync and share software from individuals operation with free and open-source, to allow installing and operating it without any charge on a private server. Amazon cloud, on the other side, is the provisioning of services to allow the scaling up and down of resources from Amazon Company to customers or organization. In this paper, an exploiting to the features of owncloud and Amazon cloud, this is done by comparing their performance in order to prevent the confusing when selection of the proper cloud to be used is occurred.

Keywords: Owncloud , Private server, Amazon cloud

INTRODUCTION

Owncloud was started and is still maintained by Frank Karlitschek, the German open source software developer. He presented at Camp KDE in 2010 [1]. Owncloud provides safe, secure and compliant file sync and share solution on servers to be controlled. It was described in detail in [2]

Amazon cloud has a long history of using a decentralized Information Technology (IT) infrastructure. This arrangement enabled development teams to access, compute and store resources on demand, and it has increased overall productivity and agility. By 2005, Amazon built and managed the large-scale, reliable, and efficient IT infrastructure that powered one of the world's largest online retail platforms. Figure1 illustrates the Amazon web Services [3].

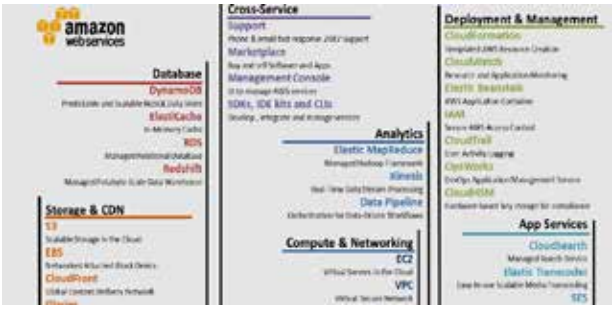


Figure 1- Services According to the Requirements

Requisition compute power, storage, and other services in minutes with flexible chose to the development platform or programming model, which makes the most sense for the problems tried to be solved by using Amazon Web Services (AWS), the payment only for what is used, with no up-front expenses or long-term commitments, making AWS a cost-effective way to deliver applications [3].

II. RELATED WORKS

[2] demonstrated the way of creating, and configuring Owncloud on own computer using Ubuntu12.04 and LAMP stack, and developed it to store and share documents, calendars and contacts in a secure way. [4] demonstrated how to host WordPress on own computer using Ubuntu and Apache web server to overcome some difficulties occur in the server such as server failure or slow loading happened at opening the blogger, this solved by proposing WordPress blog toll, this features exploited by installing, configuring and hosting on any other server. [5] presented performance measurement study of network I/O applications in virtualized cloud. The focus of measurement based analysis on performance impact of co-locating applications in a virtualized cloud in terms of throughput and resource sharing effectiveness, including the impact of idle instances on applications that are running concurrently on the same physical host. [6] designed a flexible framework to test hypothesis, which is called FlexPRICE as a user presented a job to the cloud. The cloud found different schedules to execute the job and presented a set of quotes to the user in terms of price and duration for the execution. The user then chose a particular quote and the cloud is obliged to execute the job according to the chosen quote. [7] described cloud computing, a computing platform for the next generation of the Internet, and defined clouds, types of cloud Provides, Comparison of Cloud Computing with Grid Computing, applications and concerns of Cloud Computing , Concept of Virtualization in Cloud Computing. [8] presented the possibility of making backup copies of data in the cloud, and mainly focused on performance and economic issues of making backups in the cloud in comparison to traditional backups.

III. METHODOLOGY

Both the Owncloud and Amazon clouds have been used to compare their features, this is done by hosting site on Owncloud in order to test the performance, which includes using CPU, Memory, Swap, consuming time, received data, sent data, transfer rate of receiving and sending data. And also hosting the same site on Amazon cloud to test the performance. After that an analysing to the results and comparing between their performance took please. The test is achieved by using system monitor program. Two methods have been applied and tested:

3.1 Hosting Web Application on Owncloud

Before hosting web application on Owncloud, it should be created and configured, also MySQL should be configured to reach final configuration of the system. Owncloud is opened, and then files from the Application list are selected. By using icon named (New), text file or folder can be saved. The selection of save site from link is done by using the URL. Now the web application is saved in the selected place, that mean it is hosting on Owncloud thus could be downloaded and opened from Owncloud. This is illustrated in figure 2 [2].

Figure 2- Hosting Web Application on the Owncloud

3.2 Hosting Web Application on Amazon Cloud

An account must be created before uploading web application, the creation is instance , then LAMP stack must be installed, which is an acronym for an archetypal model of web service solution stacks, originally consisting of largely interchangeable components: Linux, the Apache HTTP Server, the MySQL relational database management system, and the PHP programming language [4]. Services can be chosen according to the user requirements, there is a need to host web application and speed up transfer rate, therefore; EC2 service is chosen, EC2 gives the virtual server. Amazon gives free service for one year to new customers; Steps to Host Web Application on Amazon Cloud then user should pay for the used services. Figure 3 illustrates the steps of a generating phase, and the following instructions are used for uploading user web application:

First, type “Ls” to see the empty home directory that is connected as a root user with “Sudo su “ and “cd” to the directory , /var/www/html/.Ls Sudosu – cd /var/www/html

Using “wget” to download the file containing our web site, if the file is zip then unzip the file in the same folder by typing wget http://univ2maha.blogspot.com/ Unzip univ2maha.blogspot.com.zip suing “ls” to see the name of web application. To make the web application visible, move it from that sub directory to the main one, the “index.html“ file should be available. mv univ2maha.blogspot.com.zip/*.

Now, this is the checking phase in the AWS, the public IP of EC2 instance will be copied to the new browser window. Figure 4 illustrates the running up of the resultant web application.

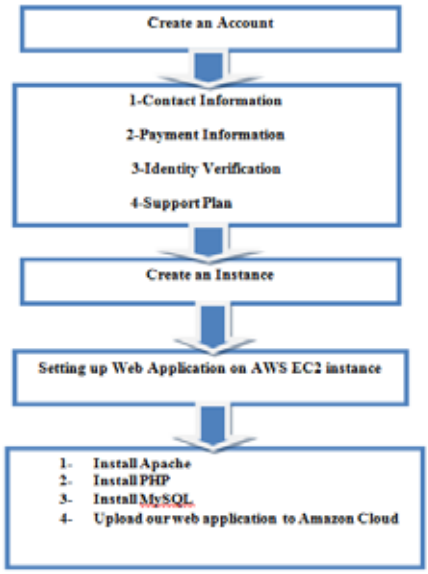


Figure 3- Steps to Host Web Application on Amazon Cloud

Figure 4- Web Application Host in Cloud

IV. THE SIMULATED RESULTS

System monitor program, which is supported by Linux operating system, has been used to test web applications, figure 5 and figure 6 are the resultant. Table 1 contains the results of the compared clouds' performance.

Figure 5- Test of Web Application Hosting on Hosting Owncloud

Figure 6- Test of Web Application on Amazon Cloud

Table 1- Test results of Owncloud Vs. Amazon Aloud

Type of Test	Ratio of receiving data	Ratio of sending data	Total received data	Total sent data	Ratio of CPU utilization	Using of Memory	using of swap	Consuming time to see video is 3.19s
Owncloud	13.5 KBPS	3.8 KBPS	115.0 MB	22.2 MB	58.2%	562.6MB (56.2%) of 1001.2 MB	27.9 MB (2.7%) of 1022.0MB	3.20 s
Amazon cloud	36.5 KBPS	1.3 KBPS	126.5 MB	22.8 MB	49.0%	581.0MB (58.1%) of 1001.2	33.8 MB (3.3%	3.20

						MB	) of 1022. 0MB	

V. CONCLUSION

From the tests that are made by using system monitor program on web applications to compare the performance of Owncloud Vs. and Amazon cloud, the following could be concluded:

1- Ratio of receiving data in Amazon Cloud is higher than ratio of receiving data in Owncloud, that's due to that Amazon cloud server has Default 8 G storage verses Default 5 G storage in Owncloud server .

2- Ratio of sending data and Ratio of CPU utilization in Owncloud are higher than that in Amazon cloud, because the setting in Owncloud is on private computer, while the setting in Amazon cloud is on Amazon computers that just have hosted on it.

3- Concede that the Owncloud is more secure than Amazon cloud because it is a private cloud, in opposite to the Amazon cloud, which is owned by Amazon company, i.e. to be installed and configured by the Amazon developers.

4- All other tests are almost same.

The selection of the suitable cloud is related to the requirements of the application, briefly, Amazon cloud provides speed, while Owncloud provides security.

REFERENCES

1- Rachell Joy ,2012. *OwnCloud_Configuration_and_Usage_Guide*, Tech Desk a division of media and academic computing , http:// techdesk.ysu.edu

2- Asmaa Qasim Shareef, Ayad A. Abdulsalam, Maha Abd ULatif Sayal,2014. Private Cloud Development to Improve Reliability and Security. *International Journal of Computer Science and Mobile Computing*, Vol.3 Issue.12, pg. 160-165

3- Tavis & Fitzsimons, 2012. *Web Application Hosting in the AWS Cloud*, Amazon Web Services. Web Application Hosting in the AWS Cloud: Best Practices, pg. 1-14

4- Ayad A. Abdulsalam, Asmaa Q. Shareef, Maha A. Sayal, 2014. Bloggers Performance Improving by Exploiting (WordPress) Tools with Ubuntu 12.04 and Apache HTTP Server, *International Journal of Advanced Research in Computer Science and Technology (IJARCST) for publication*, Vol. 2 Issue 4, *Pg.24-27*

5- Yiduo Mei, Ling Liu, Xing Pu, Sankaran Sivathanu, 2010. Performance Measurements and Analysis ofNetwork I/O Applications in Virtualized Cloud, IEEE Computer Society, 3rd International Conference on Cloud Computing, Pg.59-66

6- Thomas A. Henzinger Anmol V. Singh Vasu Singh Thomas Wies Damien Zufferey, 2010. FlexPRIC: Flexible Provisioning of Resources in a Cloud Environment, IEEE Computer Society, 3rd International Conference on Cloud Computing, Pg.83-90

7- Pankaj Sareen, 2013. Cloud Computing: Types, Architecture, Applications, Concerns, Virtualization and Role of IT Governance in Cloud, *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol.3 Issue.3, pg. 533-538

8- Aljaz Zrnec, Dejan Lavbic, 2011. Comparison of Cloud vs. Tape Backup Performance and Costs with Oracle Database, *The Journal of Indian Orthodontic Society (JIOS)*, VOL. 35, NO. 1, PP. 135-142

OPTIMIZATION OF ORGANIC RANKINE CYCLE USING WASTE HEAT BY GENETIC ALGORITHM

Asad Parvez[1], Feroz Ahmad[2], Shravan Thakur[3], Tabish Zareef[4]

[1,2,3,4] *Department of Mechanical Engineering, Jamia Millia Islamia, New Delhi, (India)*

ABSTRACT

An organic Rankine cycle (ORC) is similar to a conventional steam cycle energy conversion system, but uses an organic fluid such as refrigerants and hydrocarbons instead of water. Available heat resources are: solar energy, geothermal energy, biomass products, surface seawater, and waste heat from various thermal processes. This report presents existing applications and analyzes their maturity. Binary geothermal and binary biomass CHP are already mature. Provided the interest to recover waste heat rejected by thermal devices and industrial processes continue to grow, and favorable legislative conditions are adopted, waste heat recovery organic Rankine cycle systems in the near future will experience a rapid growth. OTEC power plant operating mainly on offshore installations at very low temperature has been advertised as total resource systems and interest on this technology is growing in large isolated islands. Potential source of waste heat are textile, steel, oil refinery, paper, etc which generally have temperature below 300^{o}C. There are no means by which this energy can be technically and economically utilized. Organic Rankine cycle is one of the way in which this energy can be utilized. To find the different parameters for the optimization of this energy is aim of our project.

Keywords: Organic Rankine Cycle, Optimization, Waste Heat.

I. INTRODUCTION

Organic Rankine cycle is not much different from traditional Rankine cycle but it uses heat source which is at low temperature generally below 300^{o}C. Utilizing this energy to run rankine cycle is definitely a way to extract energy from sources which is generally discarded. It is technically sound and economically feasible. It will not only reduce demand of electricity but also helps in reducing thermal pollution. What's more important is that unlike process heating or cogeneration it directly gives us the electricity which is most convenient form of energy. In our project we have selected the organic fluid on different parameters, obtain various correlation and to select the organic fluid which gives the maximum power output. As the critical component in an ORC system, an expander determines whether the whole system is relatively efficient and cost effective. Expanders, can be categorized into many types, such as axial turbine rotary expanders, scroll expanders and reciprocal piston expanders. The dynamic modeling and control are also very significant for ORC systems. The design methods are the guarantees of the efficient and cost effective ORC systems.

A working fluid in organic Rankine cycle machine plays a key role. It determines the performance and the economics of the plant. This justifies the abundant literature dedicated to fluids selection for very different heat recovery applications from which characteristics of good fluids can be extracted

• Vapor saturation curve with zero or positive slope (ds/dT)

• High latent heat of vaporization

• High density (liquid/vapor phase)
• High specific heat
• Moderate critical parameters (temperature, pressure)
• Acceptable condensing and evaporating pressures (>1 bar and <25 bar resp.)
• Good heat transfer properties (low viscosity, high thermal conductivity)
• Good thermal and chemical stability (stable at high temperature)
• Good compatibility with materials (noncorrosive)
• High thermodynamic performance (high energetic/exergetic efficiency)
• Good safety characteristics (nontoxic and nonflammable)
• Low environmental impacts (low ODP, low GWP)
• Low cost and good availability

II. DETAIL STUDY OF ORGANIC RANKIE CYCLE

For each process in a power cycle, it is possible to assume a hypothetical cycle or ideal process which represents the basic intended operation and involves no external effects. For the steam boiler, this would be a reversible constant pressure heating process of organic fluid, for turbine the ideal process would be a reversible adiabatic expansion of vapour, for the condenser it would be a reversible constant pressure heat rejection and for the pump it would be reversible adiabatic compression of the fluid ending at the initial pressure. When all these four processes are ideal, the cycle is the ideal cycle, called a RANKINE CYCLE. For the purpose of analysis the Rankine cycle is assumed to be carried out in a steady flow operation

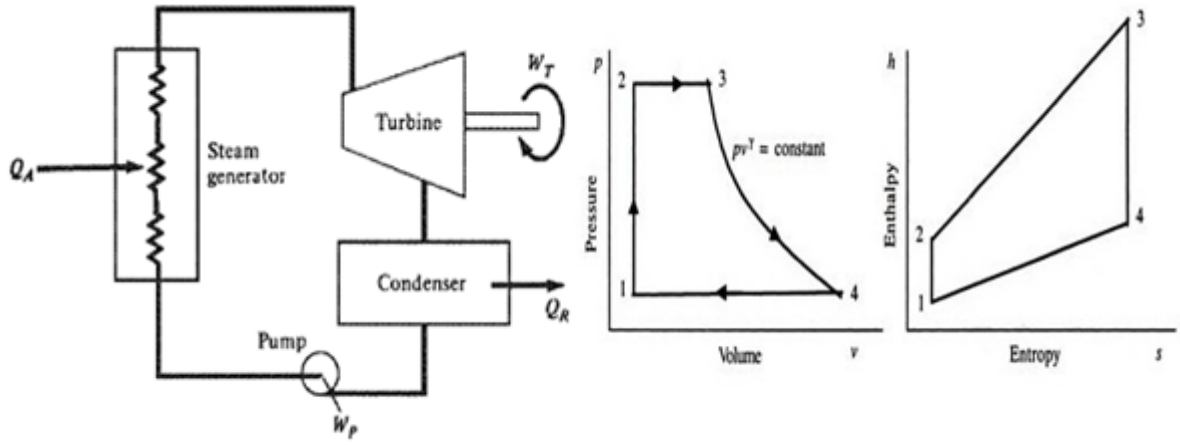


Fig.1. Rankine CycleFig.2.p-V and T-s diagram for Rankine Cycle

Process1-2: It is a reversible adiabatic or isentropic compression which is carried out by pump. Here change in volume of fluid is to be negligible so that we assume constant volume process.

For reversible adiabatic compressionby use of general property relation

Tds=dh-vdp

ds=0 (for isentropic process)

dh=vdp.

$h_2 - h_1 = v_1 (p_2 - p_1)$ …(1)

Process2-3: This process is carried out by boiler in which fluid convert from liquid to vapour at constant pressure.

For boiler heat addition, $Q_1 = h_3 - h_2$ …(2)

Process3-4: This process is carried out by turbine which is to be ideal to obtain maximum work output. For ideal process we assume that there is no irreversibility such as friction and hence there will be no entropy generation within the turbine. Also we assume turbine is insulated from its surrounding so that there will be no heat energy transfer from the turbine to its surrounding and hence no entropy change will take place due to heat transfer within the turbine.

For the turbine work output can be given by

$W_T=h_3-h_4$... (3)

Process4-1: This process is carried out by condenser where 1vapour condense into liquid at constant pressure.

Heat rejection from condenser can be written as,$Q_2=h_4-h_1$...(4)

Cycle Efficiency=Net work output/Heat addition

$= ((h_3-h_4)-(h_2-h_1))/(h_3-h_2)$… (5)

Neglecting pump work in comparison to turbine output

$= (h_3-h_4)/ (h_3-h_2)$...(6)

III. THERMODYNAMIC ANALYSIS OF THE ORC

We have a power plant that have a rated capacity of 120 KW and a turbine having efficiency of 90%. Heat is entered at different temperature ranging from 90°C to 180°C which is characteristic of typical waste heat that is rejected from different waste heat source such as steel industry, iron ore industry, mills, power plants etc. If heat enters at a temperature in the range of 120°C to 130°C than mean temperature of heat addition will be 125°C. When it gives heat to the working fluid than assume some loss in the heat exchanger than temperature of working fluid will be 123°C. At this temp fluid is assumed to be saturated and enthalpy corresponding to this temperature is taken from Refprop. Ambient temperature is assumed to be 32°C. At the exit quality of fluid is assumed to be 90%. So enthalpy of fluid at exit is again calculated from Refprop. Now we have enthalpy of fluid at inlet and outlet and power output. So from here we have calculated mass flow rate for various refrigerant at various temperature. Result is tabulated below.

3.1. Analysis of R11

This Tabular data shows the variation of mass flow rate of R11, Enthalpy at turbine inlet and corresponding Efficiency variation.

Table 1

Temprature Range	Avg. Temp of waste heat	Avg. Temp of refrigerant	Enthalpy at turbine inlet(KJ/Kg)	Enthalpy at turbine outlet(KJ/Kg)	Mass Flow rate (kg/s)	Efficiency
170-160	165	163	457.32	388.403	1.934694391	0.13563
160-150	155	153	455.86	388.403	1.976567789	0.13318
150-140	145	143	453.61	388.403	2.044770245	0.12938
140-130	135	133	450.77	388.403	2.137882748	0.12452
130-120	125	123	447.47	388.403	2.257323604	0.1188
120-110	115	113	443.8	388.403	2.406869205	0.11234
110-100	105	103	439.02	388.403	2.634161118	0.10377
100-90	95	93	435.58	388.403	2.826235948	0.09748

3.1.1. Graphs of Refrigerant R11

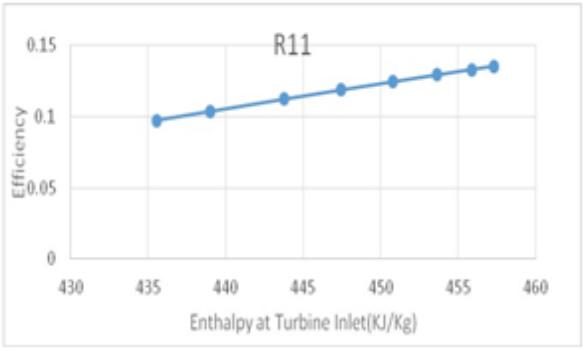


Fig. 3.Variation of efficiency and Entalpy at Turbineinlet

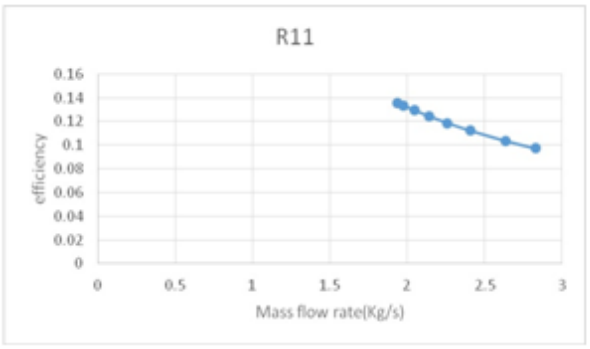


Fig.4. Variation of efficiency and mass flow rate

3.2. Analysis of R245fa

This Tabular data shows the variation of mass flow rate of R245fa, Enthalpy atturbine inlet and corresponding efficiency variation.

Table 2.

Temprature Range	Avg. Temp of waste heat	Avg. Temp of refrigerant	Enthalpy at turbine inlet(KJ/Kg)	Enthalpy at turbine outlet(KJ/Kg)	Mass Flow rate (kg/s)	Efficiency
150-140	145	143	492.2	410	1.622060016	0.1503
140-130	135	133	491.94	410	1.627206899	0.14991
130-120	125	123	488.76	410	1.692906721	0.14503
120-110	115	113	484.12	410	1.798884691	0.13779
110-100	105	103	478.56	410	1.944768573	0.12894
100-90	95	93	472.41	410	2.136409763	0.1189

3.2.1. Graphs of Refrigerant R245fa

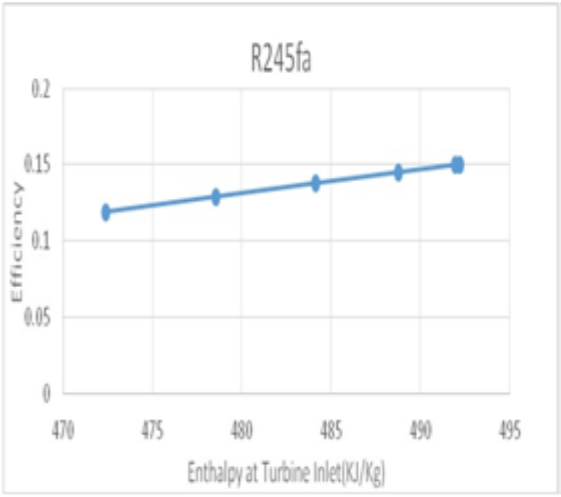


Fig. 5.Variation of efficiency and Entalpy at turbine inlet.

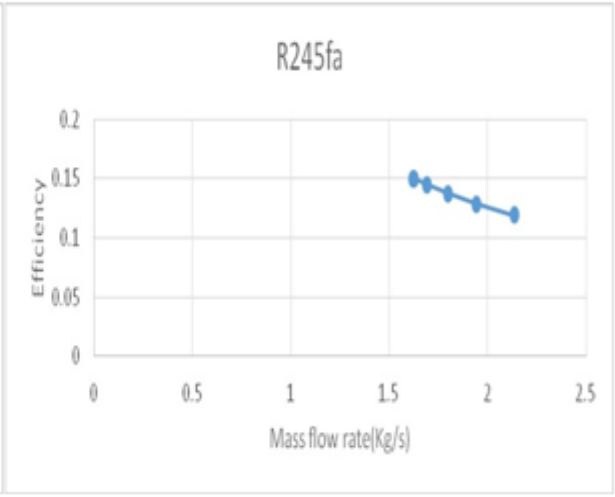


Fig. 6. Variation of efficiency and mass flow Rate.

3.3. Analysis of R141b

This Tabular data shows the variation of mass flow rate of R245fa, Enthalpy at turbine inlet and corresponding efficiency variation.

Table 3.

Temprature Range	Avg. Temp of waste heat	Avg. Temp of refrigerant	Enthalpy at turbine inlet(KJ/Kg)	Enthalpy at turbine outlet(KJ/Kg)	Mass Flow rate (kg/s)	Efficiency
160-150	155	153	536.38	435.257	1.318526283	0.16968
150-140	145	143	529.59	435.257	1.413432556	0.16031
140-130	135	133	524.3	435.257	1.497403876	0.15285
130-120	125	123	518.62	435.257	1.599430603	0.14467
120-110	115	113	512.64	435.257	1.723031329	0.13585
110-100	105	103	506.43	435.257	1.873369583	0.12648
100-90	95	93	500.03	435.257	2.058470865	0.11658

3.3.1. Graphs of Refrigerant R141b

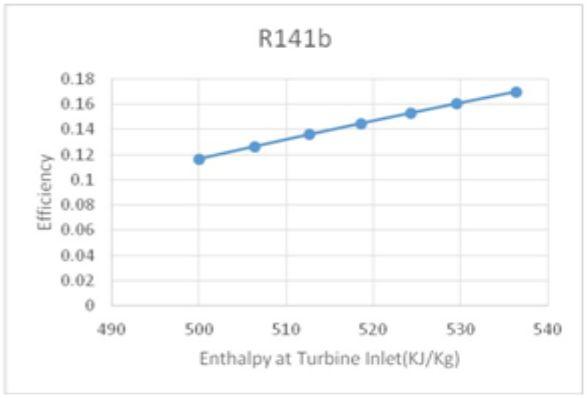


Fig. 7. Variation of efficiency and Entalpy at turbine inlet

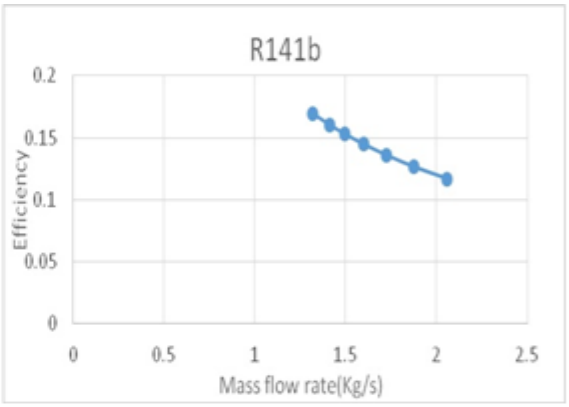


Fig. 8. Variation of efficiency and mass flow rate.

V. RESULT

Efficiency of rankine cycle decreases with increase inambient temperature, it have detrimental effect onamount of work extracted from turbine. Further withincrease in mass flow rate power output increases. Forsame power output mass flow rate is minimum for R141b.Also due to absence of chlorine it is environment friendly sothis fluid is selected. For large cycle power output efficiencyfurther increases though still it is quite low as compared totraditional rankine cycle which have efficiency in the rangeof 40%. For our cycle efficiencyis around 13%.

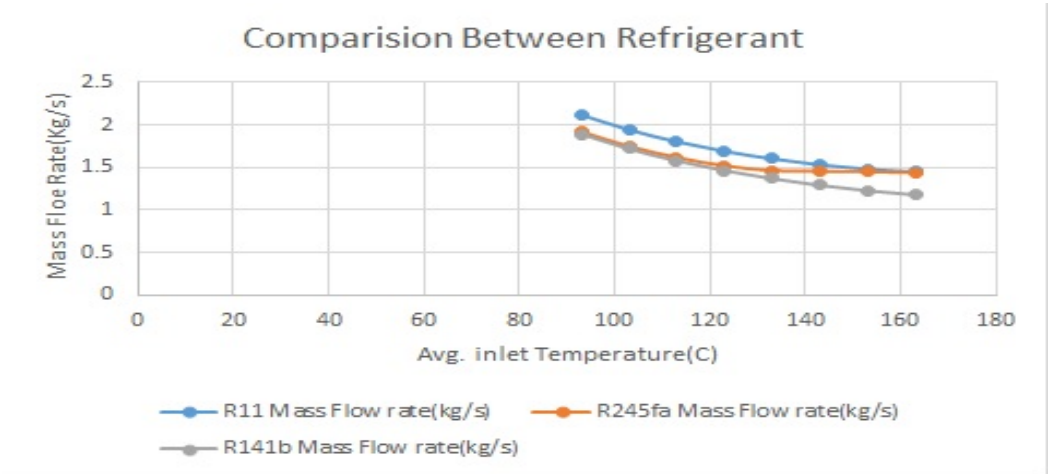


Fig. 9.Comparison between Different Refrigerant on the Basis of Mass Flow Rate

VI. CONCLUSION

Organic rankine cycle is a sure way of utilizing waste heat and convert it into work i.e. electricity. By using different optimized value we can increase the performance. There are various sources which have large amount of waste heat which is discarded. We try to find alternatives of different sources of electricity, orc is a way in which there is no extra fluid is burnt. It takes heat from already existing resources and also technically viable and economically feasible. Therefore we must have to go for ORC in today's scenario countries like India which in spite of 5th in electricity generation still a deficit of 4.7%. Therefore we must have to look all other alternative source but first of all we have to look possibilities where we just discard energy.

NOMENCLATURE

Q_A Heat given to steam Generator (KJ/s)

Q_R Heat rejected by condenser (KJ/s)

W_T Turbine Work (KW)

W_P Pump work (KW)

REFERENCES

[1] Ali Alajmiet. al.[2014]"Selecting the most efficient genetic algorithm sets in solving unconstrained buldin[g" "International Journal of sustainable built environment"69,169-173.

[2] AnttiUsitaloet. al.,[2014]"Thermo dynamic analysis of waste heat recovery" "Applied Thermal Engineering"70,33-41.

[3] Ben-Ran Fu et.al.,[2014]" Effect of off-design heat source temperature on heat transfer characteristics and system performance of a 250-kW organic Rankine cycle system" "applied thermal engineering" vol 70 page 7-12.

[4] Dexin Wang et. al.,[2012]"Caol Power Plant Flue Waste Heat and water Recover" "Applied Energy"91,341-348.

[5] GequnShu, GuopengYu,et.al.,[2014]" A Multi-Approach Evaluation System (MA-ES) of Organic Rankine Cycles(ORC) used in waste heat utilization" "applied energy"vol 132 page no 325-338

[6] Hamid Taghavifaret. al.[2014]"energy loss optimsation using genetic algorithm" "Information processing in agriculture"16,66-68.

[7] ImenElksbiet. al.[2014]"Development and optimization of a non conventional extraction process of narural dye from olive solid waste" "Food Chemistry"161,345-352.

[8] Jhonatan da Roza et.al.[2013]"Coevolution of AI using genetic algorithm" "Procedia Computer science"18,692-701.

[9] Jianhuanzhanget. al. ,[2013]"Generalised predictive control applied in waste heat recovery power plant" "Applied Energy"102,320-326.

[10] Li Zhao , JunjiangBao,[2014]" Thermodynamic analysis of organic Rankine cycle using zeotropic Mixtures" "applied energy" vol 130,page no 748-756.

[11] MA Guang-yu et.al.,[2012]"Analytical Research on waste Heat Recovery in Iron and Steel Industry" "Energy Procedia" 14,1022-1028.

[12] Michaël Marion et.al.," Wind effect on the performance of a solar organic Rankine cycle" "renewable energy" vol 68 page no 651-661

[13] Michele De Monte et.al.[2003],"Waste Heat recovery in a Plant" "Applied Thermal Engineering"23,1033-1044.

[14] Organic Rankine Cycle system for binary-cycle geothermal power plants" "applied thermal engineering" vol 71 page no 175-183

[15] PavelRaskaet. al.[2014]"Testing optimization methods on discrete events simulation models and testing functions" "Procedia Engineering"69,768-777.

[16] RazvanCazacu et.al.[2014]"steel truss optimization using genetic algorithm" "Procedia Technology"12,339-346.

[17] Umut Tosun [2014]"new recombination operator for the genetic algorithm" "Procedia Computer science"32,29-36.

[18] Xiafoei He et. al.[2014]"Performance optimization of HVAC system" "Energy and Buildings"81,371-380.

[19] Xin She Yang et. al.[2014]"Computational optimization, modelling and simulation ppf" "Procedia Computer science" 29,754-758.

[20] Yuanyuan Zhou et. al.[2014]"Optimization of plate fin heat exchanger" "International Journal of heat and mass transfer"78,942-946.

FAULT DIAGNOSIS OF VSI FED INDUCTION MOTOR DRIVE USING FUZZY LOGIC APPROACH

Naveena G J[1], Basawaraj Hebbale[2], Surya N S[3]

[1, 2, 3] *PG Scholar, Dept. of studies in EEE, UBDT College of Engineering, Davangere (India)*

ABSTRACT

Condition monitoring of induction motors is becoming increasingly important mainly in industries. There are many condition monitoring methods, including vibration monitoring, thermal monitoring, chemical monitoring, acoustic emission monitoring but all these monitoring methods requires expensive sensors or specialized tools whereas current monitoring out of all does not require additional sensors. This is because the basic electrical quantities associated with electromechanical plants such as current and voltage are readily measured by tapping into the existing voltage and current transformers that are always installed as part of the protection system. As a result current monitoring is non-intrusive and may even be implemented in the motor control center remotely from the motors being monitored. The present work intends the current monitoring techniques applied to detect the various types of induction motor faults such as electrically related faults.

Knowledge based fuzzy logic approach helps in diagnosing the induction motor faults. In fact, fuzzy logic is reminiscent of human thinking processes and natural language enabling decisions to be made based on vague information. Therefore, current work applies fuzzy logic to induction motor fault detection and diagnosis. The motor condition is described by using linguistic variables. Fault condition is diagnosed based on the current amplitude in addition to the knowledge expressed in rules and membership function. The model is implemented in MATLAB/SIMULINK with the data obtained under both healthy and different faulty conditions.

Keywords: Diagnosis, Fuzzy Logic, Fuzzy Inference, Knowledge Base and Stator Current Amplitude.

I. INTRODUCTION

Three phase induction motors are work horses in many of the industrial applications because of its simple structure and reliability. In an industrial application these motors are utilized in between 40% to 50% in wide range applications. However, these machines owe due to the thermal, electrical and mechanical stresses which are unavoidable. Early detection of these abnormal disturbances helps in avoiding the severe failures in the system. This helps the electrical drive system to reduce maintenance cost and unscheduled downtimes which impact more on the production and financial income loss. Modern industry has widely used the fast acting and high reliable techniques for the maintenance and diagnosing the faults in the system, such that the techniques can reduce the unexpected failures and down time. It's essential that the operation of the machine in unsafe condition must be avoided. Nevertheless failures are unavoidable, and statistics of failures [8] in the induction motor components are mentioned as follows. A statistical study by the Electric Power Research Institute (EPRI) provides that bearing faults of 41%, stator faults of 37%, rotor faults of 10% and other faults of 12% [8]. It's important to spot the stator winding related faults as they are making up to 38% of all the faults, else they can lead to the total destruction of motor.

Therefore, reliable system with continuous monitoring is essential for the detection or diagnosing of such type of faults at early stage. The present work is devoted to fault diagnosis of induction motor drive using fuzzy logic approach. In this approach, the fault is diagnosed based on the knowledge from the rules which are generated in rule base. This method has been chosen because fuzzy logic has proved that it has ability in resembling the human decisions, and different faults can be easily monitored by using this technique. In this paper, the fuzzy logic controller will diagnose different faults such as different electrical faults such as single line to ground fault, line to line Fault, double line to ground fault, three phase to ground fault, open circuit, overload fault of an induction motor over a period of duration. Circuit Model is simulated using MATLAB® SIMULINK and simulation results are presented.

1.1 Different Faults in IM Drive

Induction motor owe due to the thermal, electrical and mechanical stresses which are unavoidable. These stresses lead to severe faults. Short turn winding faults, rotor faults, bearing faults, gear fault and misalignment are common internal faults of induction motor. The common internal faults can be mainly categorized into 2 groups:

- Electrical faults
- Mechanical faults

Electrical faults include faults caused by winding insulation problems, and some of the rotor faults. Mechanical faults include bearing faults, air gap eccentricity, load faults and misalignment of shaft.

In general, motor current signature analysis is used for the diagnosing these faults, whereas in this current paper different faults are created and diagnosed by using fuzzy logic in the system based on the stator current amplitude monitoring.

Under healthy condition, there is a balanced three phase currents in all the three phases. During the period of fault, these balanced three phase currents become unbalanced three phase currents, and this results in open circuit or leads to another severe phase faults.

II. METHODOLOGY OF THE SYSTEM

The system developed is devoted to fault diagnosis of induction motor drive using fuzzy logic approach. The block diagram explaining the methodology of the project is as shown in Fig. 1. In the system shown voltage source inverter converts fixed DC supply to variable frequency variable voltage AC. Voltage source inverter (VSI) is fed from an ideal voltage source V_{dc} which gives a constant DC voltage. VSI converts this constant DC voltage to variable frequency three phase AC voltage using IGBT as a switching device. The three phase AC output voltage of VSI is fed to Induction motor. VSI along with induction motor constitutes an Induction motor drive. One of the steps for fault diagnosis is to develop an analysis technique that can be used to diagnose the observed current signal to get information. Here the signal processing technique used is Fast Fourier Transform (FFT). The continuous stator currents are selected out of the available motor output characteristics and are converted to corresponding discrete values using FFT technique.

In induction motor fault diagnosis, it is required to interpret data that are frequently inconclusive. Hence fuzzy logic approach is used. The output signal from FFT block is given to fuzzy logic controller which diagnoses the fault using knowledge from the rules which are generated in rule base. Fuzzy rules and membership functions

are constructed by observing the data set. The Motor condition is displayed as crisp value. The entire motor model is implemented in Simulink.

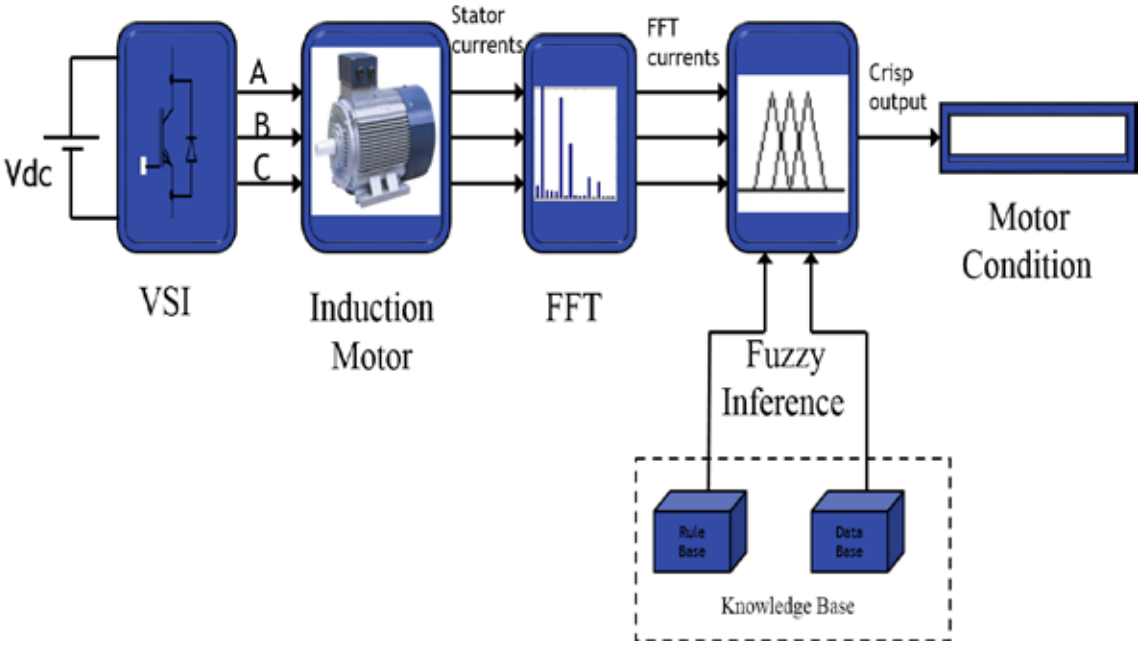


Fig. 1 Block diagram of the system

III. FUZZY SYSTEM IMPLEMENTATION

Fuzzy detection system essentially consists of data processing where the stator current values are used as inputs to the fuzzy system, and based on the knowledge acquisition and rule base, inference system finally decides the status of stator condition i.e., which type of fault occurred on the stator side can be diagnosed using this system. The main reason for choosing a fuzzy approach is the very nature of the changes in the attributes. It is nonlinear, and in addition, it would be unreasonable to expect that each time the same level of a particular fault arises; the attributes would measure exactly the same values. The diagnosis procedure is based on the analytical and heuristic knowledge symptoms of the VSI fed motor behavior. Heuristic knowledge in the form of qualitative process models can be expressed as if-then rules. The task is achieved by a fault decision process which specifies the type of the fault.

3.1 Fuzzy System Input & Output Variables

The induction motor condition can be deduced by observing the stator current amplitudes. Interpretation of results is difficult as relationships between the motor condition and the current amplitudes are vague. Therefore, using fuzzy logic, numerical data are represented as linguistic information. Fuzzy input and output variables are:

· **Input - Stator currents:** The stator current of an induction motor is readily measured by tapping into the existing voltage and current transformers that are always installed as part of the protection system. Thus, most suitable measurements for diagnosing the faults under consideration, in term of easy accessibility, reliability and sensitivity are the stator current amplitudes I_{sa}, I_{sb} and I_{sc}. These amplitudes are monitored by the system and fed as input to the fuzzy controller. The input variables I_{sa}, I_{sb}, and I_{sc} are interpreted as linguistic variables, with T (Q) = {s, m, l, vl} where, Q = I_{sa}, I_{sb}, I_{sc} respectively.

· **Output - Motor Condition:** The motor condition is chosen as the output variable in fuzzy logic approach for fault diagnosis. The term set T (MC), interpreting motor condition, MC, as a linguistic variable, could be:

T (MC) = {Healthy, LG_A, LG_B, LLG_B, LLLG ….}

where, each term in T (MC) is characterized by a fuzzy subset, in a universe of discourse MC. Healthy might be interpreted as a motor with no faults, LG_A as line to ground fault in phase A, similarly LG_B in phase B, LLG_B as double line to ground fault in phase B, LLLG as three phase fault.

3.2 Membership Functions

Based on the stator current data obtained under different fault conditions, the membership functions and corresponding limits are assigned for both input linguistic variables and the output linguistic variables. It was found that the combination of trapezoidal and triangular membership function is most suitable for the fault diagnosis of induction motors. Fuzzy membership functions for the both input linguistic variables and output linguistic variables are shown below. Input membership functions are membership functions will be generated for small(s), medium(m), large(l) and very large(vl) as shown in fig. 2. Output variables are described by membership functions viz., Healthy – H, Single line to ground faults - LG_A, LG_B, LG_C, line to line faults- LL_AB, LL_BC, LL_CA, double line to ground fault - LLG_AB, LLG_BC, LLG_CA, LLLG, over voltage - OV, under voltage - UV, overload – OL as shown in fig 3.

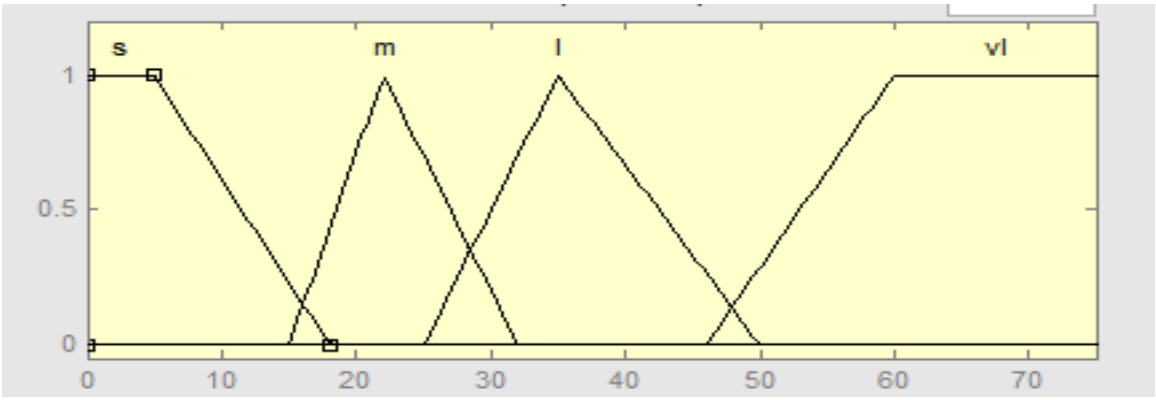


Fig. 2 Input Membership Functions

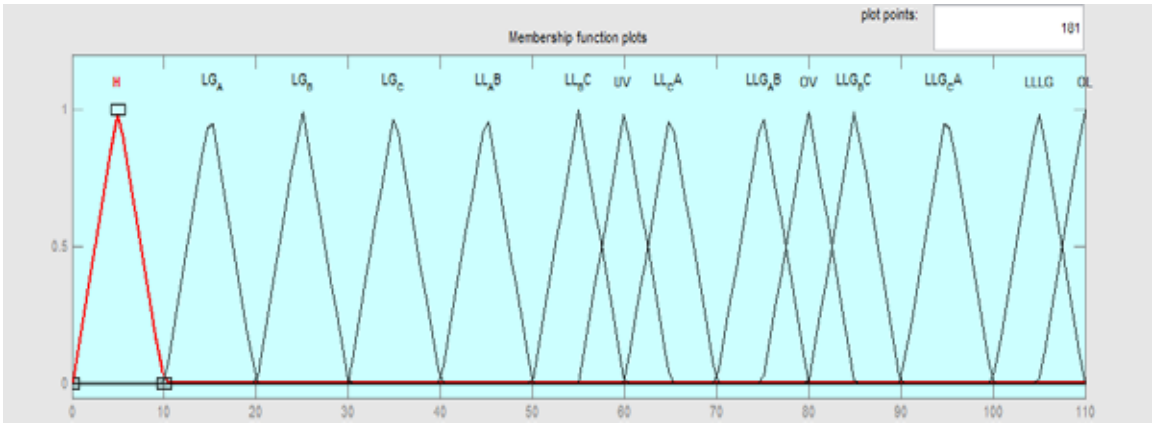


Fig 3 Output Membership Functions

3.3 Fuzzy Inference System

In this case rules are framed based on the knowledge obtained from the system simulated. Fuzzy inference system essentially consists of getting knowledge and the formation of rules. The inference method, due to

Mamdani and Assilian, is the most common in practice and hence it is used in this work. Mamdani method is widely accepted for capturing expert knowledge. It allows us to describe the expertise in more intuitive, more human-like manner. Based on all possible combinations with three currents and four linguistic variables a total of 24 rules are framed. This set of rules contains knowledge and gives the machine condition. The list of rules is:

1. If (isa is s) and (isb is s) and (isc is s) then (MC is H)
2. If (isa is l) and (isb is s) and (isc is l) then (MC is LG_A)
3. If (isa is vl) and (isb is s) and (isc is l) then (MC is LG_A)
4. If (isa is l) and (isbis l) and (isc is s) then (MC is LG_B)
5. If (isa is l) and (isb is vl) and (isc is s) then (MC is LG_B)
6. If (isa is s) and (isb is l) and (isc is l) then (MC is LG_C)
7. If (isa is s) and (isb is l) and (isc is vl) then (MC is LG_C)
8. If (isa is m) and (isb is l) and (isc is l) then (MC is LL_AB)
9. If (isa is m) and (isb is m) and (isc is l) then (MC is LL_AB)
10. If (isa is l) and (isb is m) and (isc is m) then (MC is LL_BC)
11. If (isa is l) and (isb is m) and (isc is l) then (MC is LL_BC)
12. If (isa is m) and (isb is l) and (isc is m) then (MC is LL_CA)
13. If (isa is l) and (isb is l) and (isc is m) then (MC is LL_CA)
14. If (isa is m) and (isb is l) and (isc is vl) then (MC is LLG_AB)
15. If (isa is l) and (isb is l) and (isc is vl) then (MC is LLG_AB)
16. If (isa is vl) and (isb is m) and (isc is l) then (MC is LLG_BC)
17. If (isa is vl) and (isbis l) and (isc is l) then (MC is LLG_BC)
18. If (isa is l) and (isb is vl) and (isc is m) then (MC is LLG_CA)
19. If (isa is l) and (isb is vl) and (isc is l) then (MC is LLG_CA)
20. If (isa is s) and (isb is m) and (isc is s) then (MC is LLLG)
21. If (isa is s) and (isb is l) and (isc is s) then (MC is LLLG)
22. If (isa is vl) and (isb is vl) and (isc is vl) then (MC is OL)
23. If (isa is m) and (isb is m) and (isc is m) then (MC is OV)
24. If (isa is vl) and (isb is vl) and (isc is vl) then (MC is UV)

Fuzzy rule table is shown below in Table 1.

In the final stage, the fuzzy values are converted into crisp ones using centroid method. In this method, affected membership is cut at a level of previous max rule, and then center of gravity of possible distribution is computed and becomes the numerical output value [7].The algebraic expression for centroid method is given below:

$$z^* = \frac{\int \mu_{MC}(z) \cdot z dz}{\int \mu_{MC}(z) dz} \qquad (1)$$

where, z^* is defuzzified value,

$\mu_{MC}(z)$ is output membership function and $\int$ denotes algebraic integration.

Isb Isc / Isa	SS	SM	SL	SVL	MS	MM	ML	MVL	LS	LM	LL	LVL	VLS	VLM	VLL	VLVL
S	H				LLLG				LLLG		LG_C	LG_C				
M						OV	LL_AB			LL_CA	LL_AB	LLLG_AB				
L			LG_A			LL_BC	LL_BC		LG_B	LL_CA	UV	LLG_AB	LG_B	LLG_CA	LLG_CA	
VL			LG_A				LLG_BC			LLG_BC						OL

Table 1 Fuzzy rule table

IV. SIMULATION CIRCUITS AND RESULTS

Fig. 4 shows the simulink circuit of a three phase voltage source inverter (VSI) fed induction motor drive under healthy condition with fuzzy system.

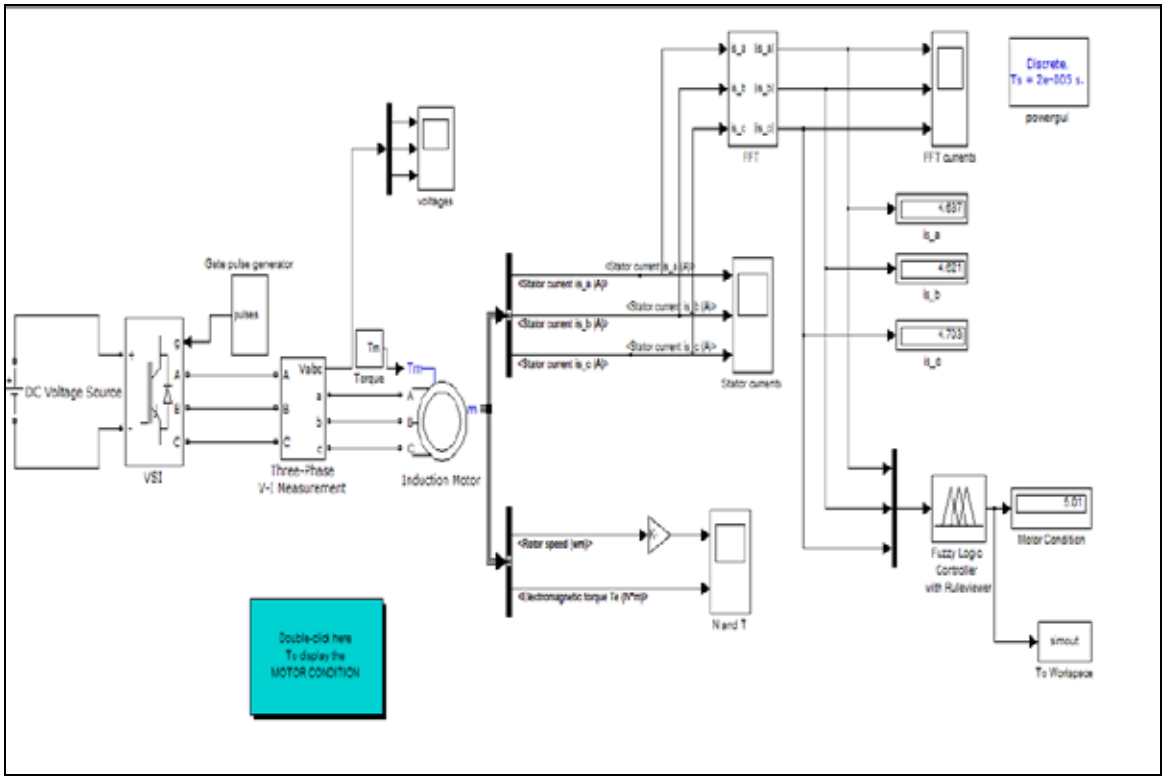


Fig. 4 Healthy motor simulation circuit with fuzzy logic controller

A fault is any abnormal electric current flowing in the system. The simulation is carried out for the following types of motor faults:

· Earth faults -

§ Single line to ground faults (LG) – LG_A, LG_B, LG_C

§ Line to line fault (LL) – LL_A, LL_B, LL_C

§ Double line to ground fault (LLG) – LLG_AB, LLG_BC, LLG_CA

§ Three phase fault (LLLG)

· Other electrically related faults -

§ Over voltage

§ Under voltage

§ Overload

§ Unbalance

§ Open circuit

4.1 Single Line to Ground Fault (LG)

Single line to ground fault involves any one phase and ground. In this fault, charges from faulty phase flow into the earth. The SIMULINK model under LG fault in phase B is as shown in Fig. 5. The LG fault is created by connecting an ideal switch between phase B and ground.

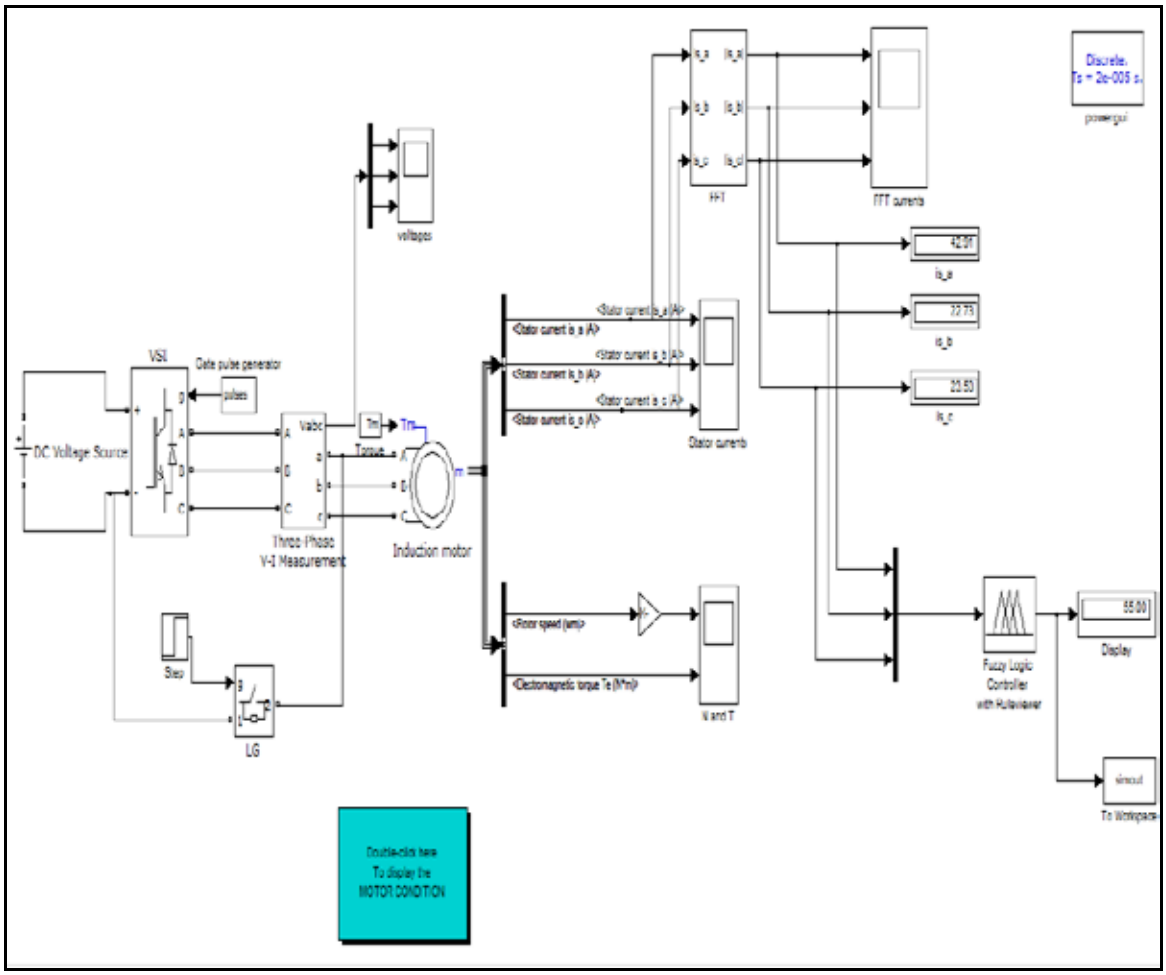


Fig. 5 Simulation circuit under LG on phase B

V. RESULTS AND DISCUSSION

The simulation results obtained from SIMULINK models under healthy and different faulty condition are discussed in the following sections. Fig. 6 shows the speed and torque variation of IM. The balanced stator currents under healthy condition and the discrete values of Fourier transform stator currents which is fed to fuzzy controller are shown in Fig. 7 and 8 respectively. The stator current variation from interval 0 to 0.5 is due to the transient operation. It is understood from these figures that the currents of phase A, B and C are in equal value for the healthy state of the drive. Fig. 9 shows the result of fuzzy detection circuit under healthy condition with an output value of 5 based on the input stator currents. This output is displayed as HEALTHY in command window using interfacing block.

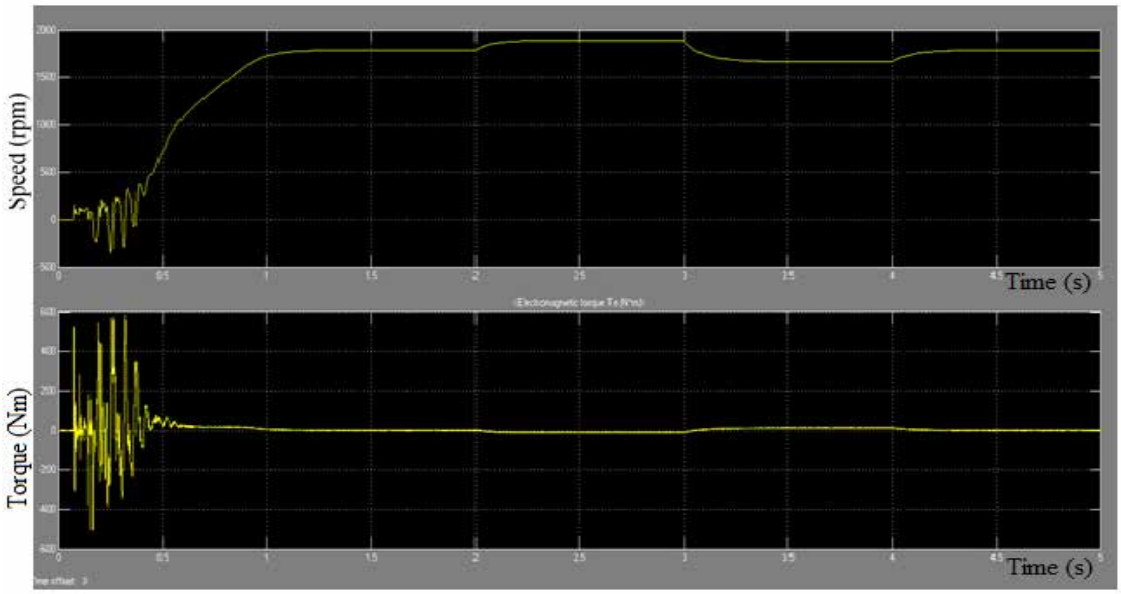


Fig. 6 Speed and torque variation of IM under healthy condition

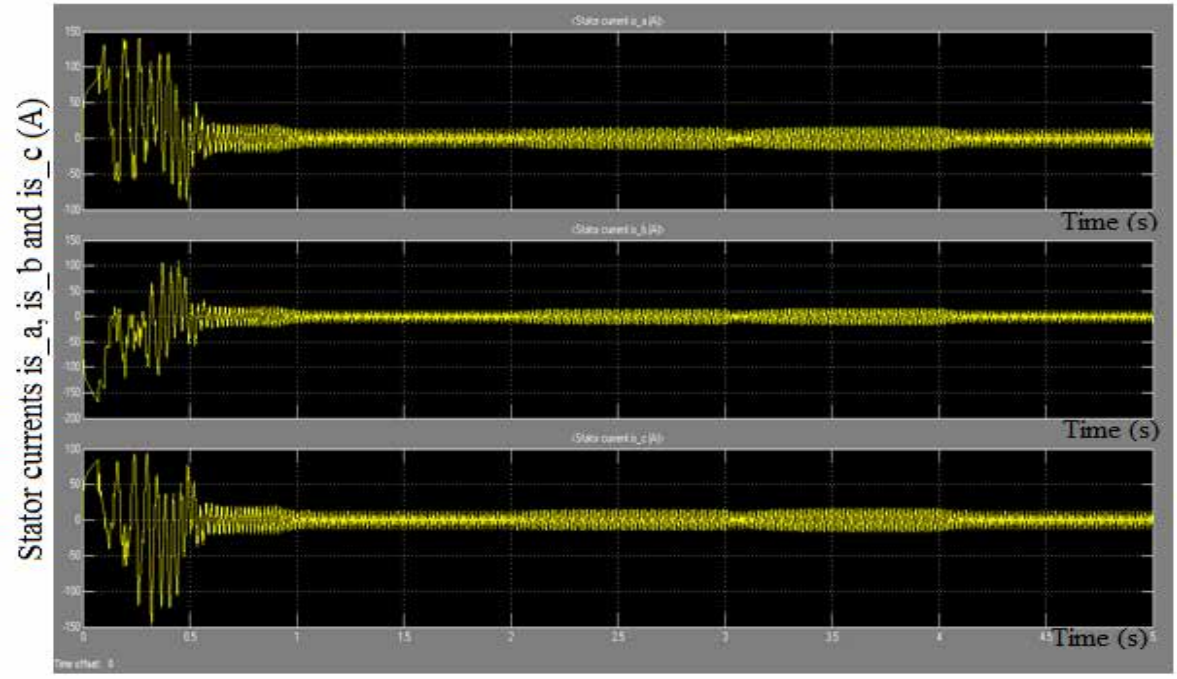


Fig. 7 Stator currents of IM under healthy condition

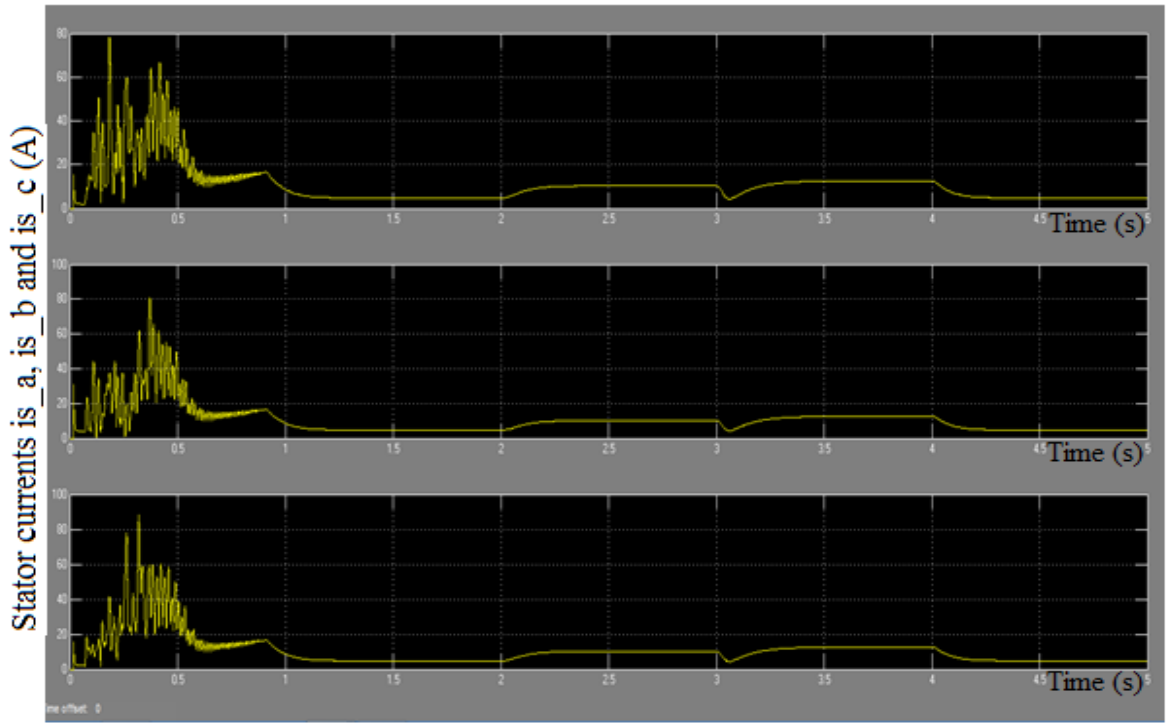


Fig. 8 Fourier Transform of stator currents under healthy condition

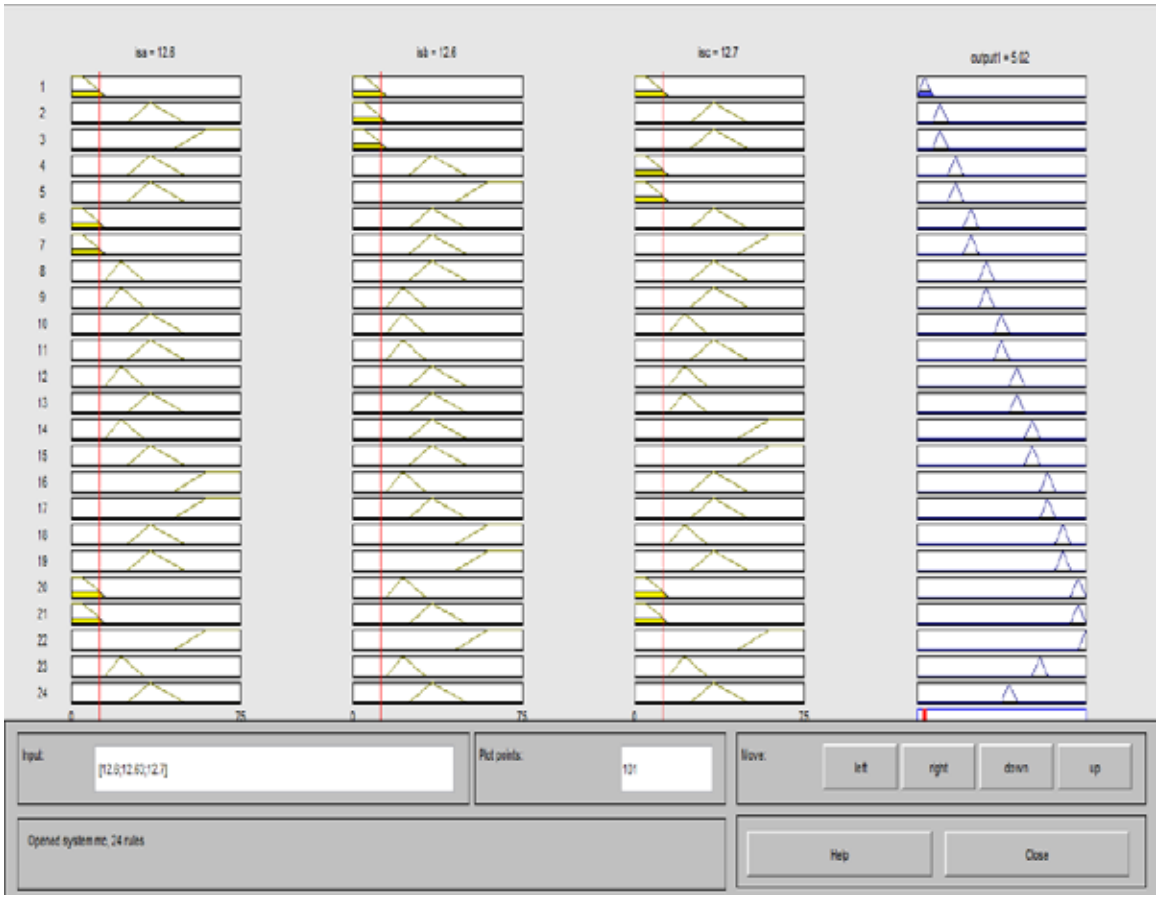


Fig. 9 Fuzzy inference diagram under healthy condition Single line to ground fault (LG)

Fig. 5.5 shows simulated stator currents of induction motor drive for the single line to ground fault in phase A. Fig 5.6 shows Fourier transform stator currents under LG fault. The magnitude of phase A, B and C currents differ each other with the magnitude of phase B being less due to LG fault in phase A. In this type of fault all the sequence impedances are present and are connected in series. Among the entire earth faults LG fault is least severe. The fuzzy output is obtained as 15 which is displayed as **LG fault in phase A** in command window.

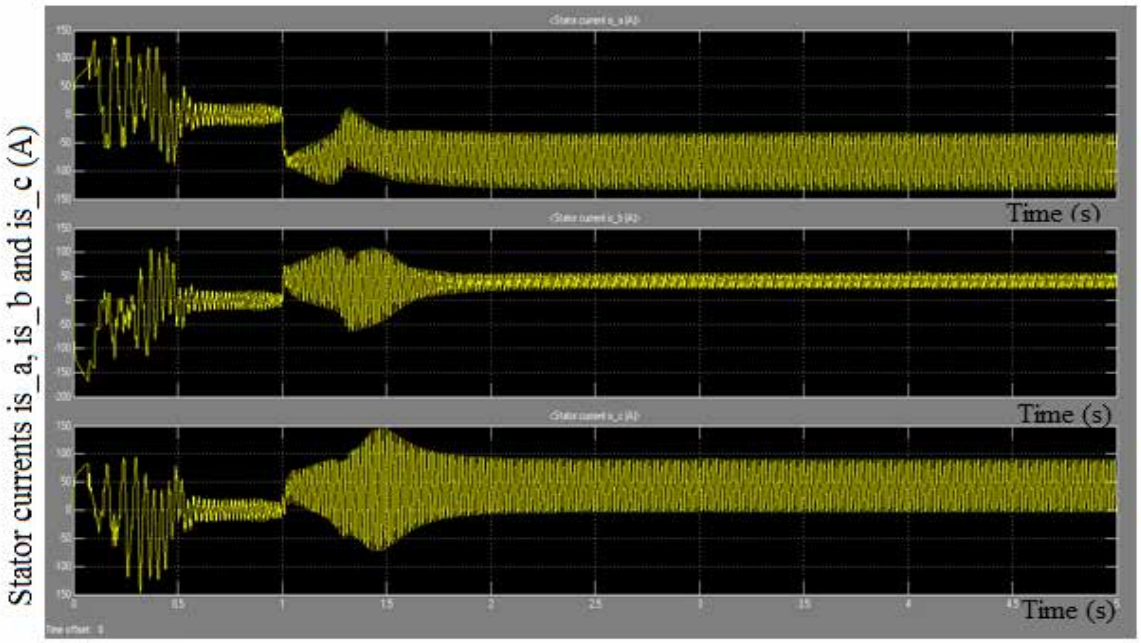


Fig. 10 Stator currents of IM under LG fault in phase A

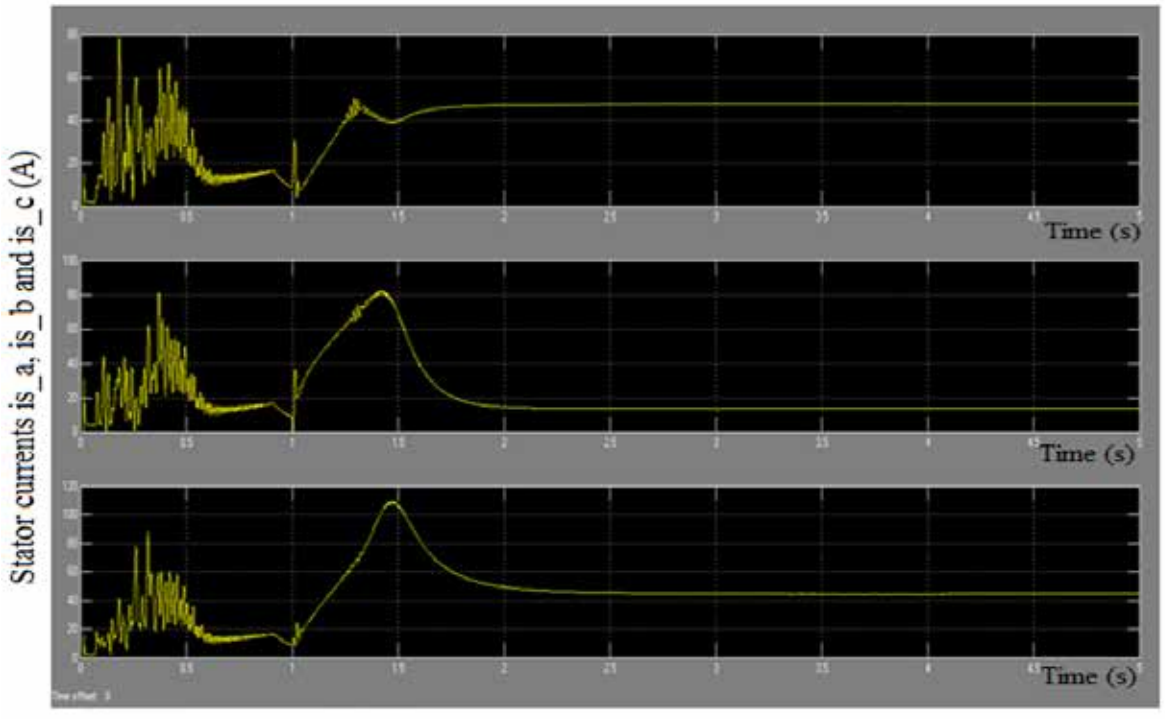


Fig. 11 Fourier Transform of stator currents under LG fault in phase A

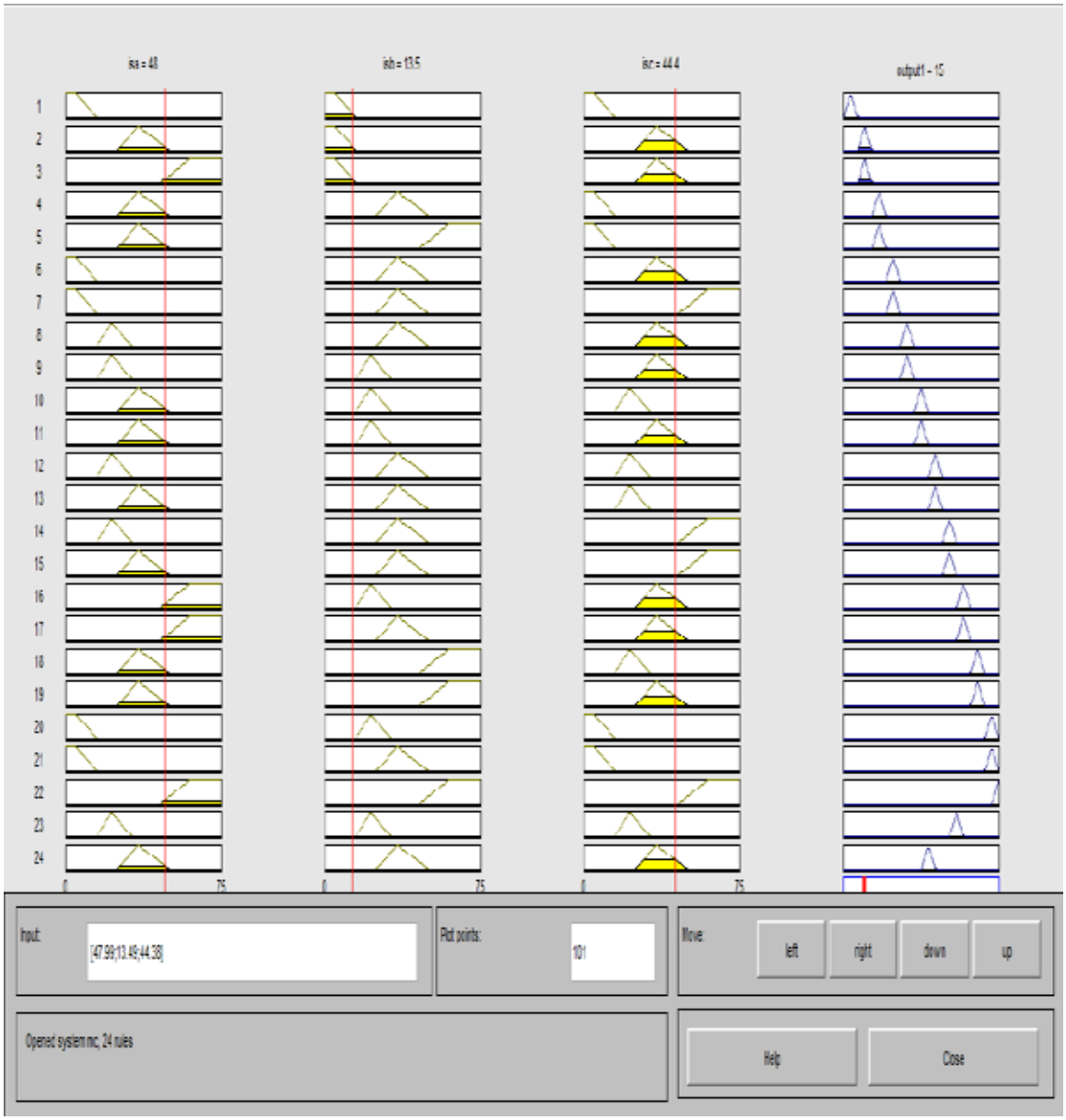


Fig. 12 Fuzzy inference diagram under LG fault in phase A

VI. CONCLUSION

In the present work effective detection of faults at early stages is possible. Fuzzy logic has the ability in resembling the human decisions. Fault is diagnosed based on the knowledge from the rules which are generated in rule base. Different faults can be easily monitored using fuzzy logic approach. The Fourier currents are applied to the fuzzy logic controller and the corresponding fuzzy logic rules are used to detect the faults occurring under different motor conditions. By processing the stator current signals and inputting them to a fuzzy decision system high diagnosis accuracy can be achieved. The motor condition is decided according to the output values of the fuzzy inference and it varies according to different fault conditions. This is a highly versatile technology for fault analysis of induction motors. The boundaries between two levels of a certain fault or between two faults are not sharply defined, and therefore the use of a fuzzy logic based diagnosis approach is highly justified.

REFERENCES

[1] K. Mohanraj, Sridhar Makkapati and S. Paramasivam, "Unbalanced and Double Line to Ground Fault Detection of Three Phase VSI Fed Induction Motor Drive using Fuzzy Logic Approach", *International Journal of Computer Applications*, vol. 47, no. 15, June 2012.

[2] P. C. Sen, "Principles of Electric Machines and Power Electronics" *John Wiley and sons.*

[3] Gopal K. Dubey, "Fundamentals of Electrical Drives" *Narosa publishing house*.

[4] M. Sudha and P. Anbalagan, "A Protection Scheme for Three-Phase Induction Motor from Incipient Faults Using Embedded Controller" *Asian Journal of Scientific Research*, 20-50, 2009.

[5] Ramazan Bayindir, Ibrahim Sefa "Novel approach based on microcontroller to online protection of induction motors"*Transaction on Energy Conversion and Management*, 48 (2007) 850–856.

[6] Mohamed El Hachemi Benbouzid, "A review of induction motors signature analysis as a medium for fault diagnosis" *IEEE Trans. Industrial Electronics*, vol. 47, no. 5, pp.984 – 993, Oct. 2000.

[7] William T. Thomson and Mark Fenger, "Current signature analysis to detect induction motor faults" *IEEE Industry Applications Magazine* July/August 2001.

[8] Dr. J. S. Chitode, "Power Electronics" *Technical publications*.

[9] Timothy J. Ross, "Fuzzy logic with engineering applications" *John Wiley and sons, third edition.*

[10] "SIMULINK Dynamic System Simulation for MATLAB", *The Mathworksinc.*

POWER AND AREA OPTIMIZED DESIGN OF 8-BIT ADDER ON 40NM FPGA USING BRAM

Shaina Verma[1], Bishwajeet Pandey[2]

[1]*Department of ECE, Chandigarh University, (India)*

[2]*Chitkara University Research and Innovation Network, Chitkara University,(India)*

ABSTRACT

This work deals with power and area optimized design 8-bit adder on FPGA. It is designed using 40nm FPGA. This design is implemented on Virtex-6 and device xc6vlx75t-3ff484. In this experiment, Xilinx 14.6 is used as simulator, Verilog is used as verification language and XPower is the power consumption estimator. Frequency scaling technique is used for the circuit design. LVCMOS IO standard is used for designing this circuit. In the circuit design without BRAM, there is a reduction of 99.9%, 100%, 100%, 99.92%, 7.51%, and 77.59% in clock, logic, signal, IO, leakage and total power respectively when the frequency is scaled down from 100GHz to 0.1GHz. In case of the circuit with BRAM, the reduction in clock, signal, IO, leakage and total power is 99.90%, 100%, 99.89%, 15.32% and 87.53% respectively on account of frequency scaling from 100GHz to 0.1GHz.

Keywords - 8-bit Adder, BRAM, Energy Efficient Design, Frequency Scaling, Power optimization

I. INTRODUCTION

The BRAM is a block of random access memory. BRAM consists of a memory cell array and control logic which can be configured to select one of the write modes to access the memory cell array. The control logic selects the write mode on the basis of configuration bits stored in the corresponding configuration memory cells of the programmable logic device(PLD) [1]. LVCMOS is Low Voltage Complementary Metal Oxide Semiconductor IO standard. It is a widely used switching standard implemented in CMOS transistors. There are various LVCMOS standards supported in Virtex-6 FPGAs which are as follows: LVCMOS12, LVCMOS15, LVCMOS18, and LVCMOS25 [2].

The Clock power represents the power consumed by different clock networks. A clock network includes the driver and any buffer or routing resource up to each load's clock input port. The Logic power is the power consumed by all the CLBs (Configurable Logic Blocks) used in the design. This includes look-up tables (LUTs), carry chain elements, and flip-flops. The Signal power represents the power consumed by all routing structures in the device that connect logic elements, I/Os and dedicated blocks. The IOs power represents the associated power required on each voltage supply and termination rail for all I/Os in the design. The leakage power represents the power consumed by the device when it is powered up without programming the user logic. The main contributor to this power is the junction temperature. Any change affecting the device operating environment will affect this power. The total power is the maximum power that the device will consume. The figure 1 shows the top level schematic of 8-bit adder.

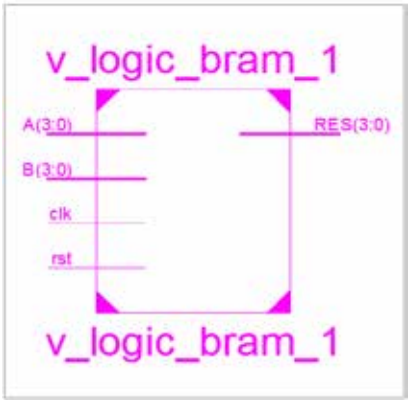


Figure 1: Top Level schematic of 8-bit Adder

There are a number of terms used in the design summary of 8-bit adder design with and without BRAM. IOs represent all the inputs and outputs. BELs are the basic element of logic that includes LUT (Look-up tables), GND, and VCC etc. FDC represents D Flip-Flop with asynchronous clear. BUFGP specifies the number of primary global buffers for a target device. IBUF and OBUF are the input/output buffers.

There is IO power reduction of 4.59%, 9.38%, 13.97% and 18.76% when capacitance is scaled down from 5pF to 4pF, 3pF, 2pF and 1pF respectively for the device operating on 40nm technology and 10 GHz operating frequency [3]. There is a reduction of 65.95%, 90.90%, 86.90% and 86.11% in clock power, BRAM power, leakage power and total power respectively for the circuit design with BRAM, when voltage is scaled down from 1.5V to 0.5V. There is a reduction of 66.66%, 86.95% and 84.49% in clock power, leakage power and total power respectively for the circuit design without BRAM when voltage is scaled down from 1.5V to 0.5V [4]. There is a dynamic power reduction of 67.04% with LVCMOS12 IO standard when migrated from 90-nm Spartan-3 FPGA to 40-nm Virtex-6 FPGA [5]. In [6], the power requirement of asynchronous and synchronous VLSI circuits was analyzed. It achieves an overall power reduction of 70.42% when asynchronous arithmetic circuit is used in place of synchronous circuits. The figure 2 and 3 shows the RTL schematic of 8-bit Adder with and without BRAM respectively.

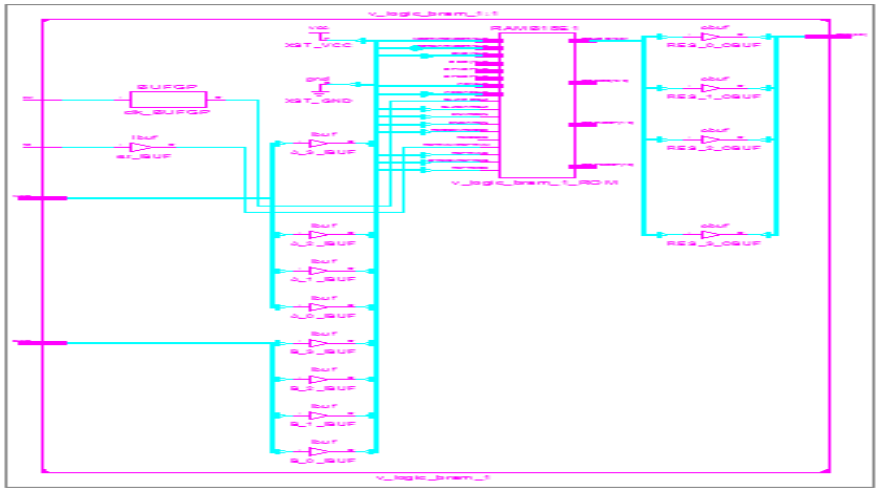


Figure2:RTL schematic of 8-bit Adder with BRAM

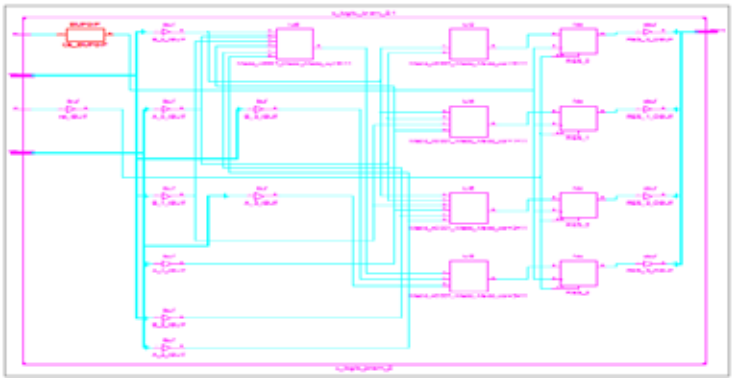


Figure3:RTL schematic of 8-bit Adder without BRAM

II. RESULTS

2.1 Power Dissipation for 8-bit Adder without BRAM

Table 1: Power Dissipation for 8-bit Adder without BRAM

Freq.→ Power ↓	0.1GHz	1GHz	10GHz	100GHz
Clocks	0.003	0.031	0.306	3.064
Logic	0.000	0.000	0.001	0.003
Signals	0.000	0.001	0.011	0.102
IOs	0.001	0.010	0.122	1.219
Leakage	1.293	1.294	1.303	1.398
Total	1.297	1.336	1.743	5.787

According to the above table, for the design of 8-bit adder without BRAM, there is a reduction of 99.9%, 98.98% and 90.01% in clock power as we scale down the frequency from 100GHz to 0.1GHz, 1GHz and 10GHz respectively. The logic power reduction is 100%, 100% and 66.66% on scaling down the frequency from 100GHz to 0.1GHz, 1GHz and 10GHz respectively. The signal power reduction is 100%, 99.02% and 89.22% as we scale down the frequency from 100GHz to 0.1GHz, 1GHz and 10GHz respectively.

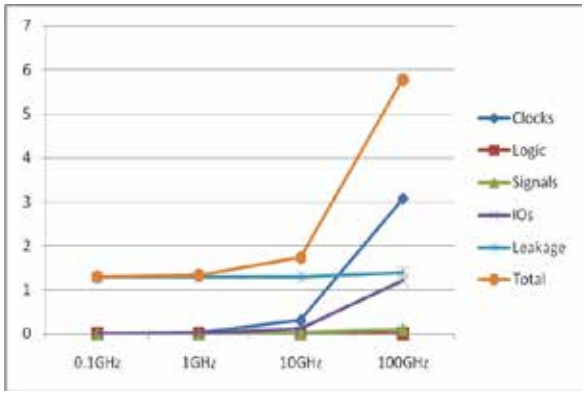


Figure 4: Power Dissipation for 8-bit Adder without BRAM

There is a reduction of 99.92%, 99.12% and 89.99% in IO power on scaling down the frequency from 100GHz to 0.1GHz, 1GHz and 10GHz respectively. There is a reduction of 7.51%, 7.44% and 6.79% in leakage power on scaling down the frequency from 100GHz to 0.1GHz, 1GHz and 10GHz respectively. The total power reduction is 77.59%, 76.91% and 69.88% as we scale down the frequency from 100GHz to 0.1GHz, 1GHz and 10GHz respectively.

2.2 Power Dissipation for 8-bit Adder with BRAM

Table 2: Power Dissipation for 8-bit Adder without BRAM

Freq.→ Power ↓	0.1GHz	1GHz	10GHz	100GHz
Clocks	0.003	0.031	0.313	3.130
Logic	0.000	0.000	0.000	0.000
Signals	0.000	0.001	0.012	0.123
BRAM	0.001	0.010	0.096	0.960
IOs	0.005	0.047	0.470	4.703
Leakage	1.293	1.295	1.313	1.527
Total	1.302	1.384	2.204	10.443

As per the table above, in case of 8-bit Adder with BRAM, there is a reduction of 99.90%, 99.01% and 90% in clock power as we scale down the frequency from 100GHz to 0.1GHz, 1GHz and 10GHz respectively. There is no reduction in logic power as we scale down the frequency. The signal power reduction is 100%, 99.19% and 90.24% as the frequency is scaled down from 100GHz to 0.1GHz, 1GHz and 10GHz respectively.

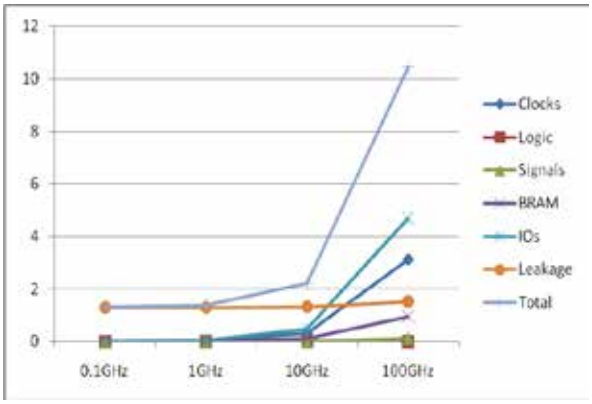


Figure 5: Power Dissipation for 8-bit Adder with BRAM

There is a reduction of 99.89%, 98.96% and 90% in BRAM power as we scale down the frequency from 100GHz to 0.1GHz, 1GHz and 10Ghz respectively. The IO power reduction is 99.89%, 99% and 90% on scaling down the frequency from 100GHz to 0.1GHz, 1GHZ and 10GHz respectively. There is 15.32%, 15.19% and 14.01% reduction in leakage power on scaling down the frequency from 100GHz to 0.1GHz, 1GHz and 10GHz respectively. There is a total power reduction of 87.53%, 86.75% and 78.89% as we scale down the frequency from 100GHz to 0.1GHz, 1GHz and 10GHz respectively.

2.3 Design Summary for 8-bit Adder without BRAM

Table 3: Design Summary for 8-bit Adder without BRAM

Device	Number
IOs	14
BELS	5
· LUT2	1
· LUT3	1
· LUT4	1
· LUT6	2
Flip-Flops/Latches	4
· FDC	4
Clock Buffers	1
· BUFGP	1
IO Buffers	13
· IBUF	9
· OBUF	4

The above table shows the design summary of 8-bit Adder without BRAM. There are 14 IOs, 5 BELs, 4 Flip-Flops, 1 Clock Buffers and 13 IO Buffers.

2.4 Design Summary for 8-bit Adder without BRAM

Table 4: Design Summary for 8-bit Adder with BRAM

Device	Number
IOs	14
BELS	2
· GND	1
· VCC	1
RAMS	1
· RAMB18E 1	1
Clock Buffers	1
· BUFGP	1
IO Buffers	13
· IBUF	9
· OBUF	4

The above table shows the design summary of 8-bit Adder with BRAM. There are 14 IOs, 2 BELS, 1 BRAM, 1 Clock Buffer and 13 IO Buffers.

III. POWER ANALYSIS

3.1 Clock Power Dissipation for 8-bit Adder

Table 5: Clock Power Dissipation for 8-bit Adder

Frequency →	0.1GHz	1GHz	10GHz	100GHz
Without BRAM	0.003	0.031	0.306	3.064
With BRAM	0.003	0.031	0.313	3.10

According to the above table, for the design of 8-bit adder without BRAM, there is a reduction of 99.9%, 98.98% and 90.01% in clock power as we scale down the frequency from 100GHz to 0.1GHz, 1GHz and 10GHz respectively.

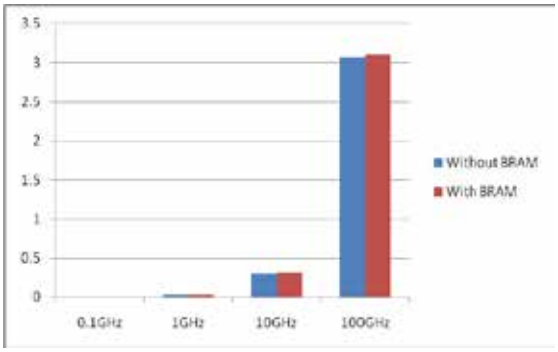


Figure 6: Clock Power Dissipation for 8-bit Adder

On the other hand, in case of 8-bit Adder with BRAM, there is a reduction of 99.90%, 99.01% and 90% in clock power as we scale down the frequency from 100GHz to 0.1GHz, 1GHz and 10GHz respectively.

3.2 Logic Power Dissipation for 8-bit Adder

Table 6: Logic Power Dissipation for 8-bit Adder

Frequency →	0.1GHz	1GHz	10GHz	100GHz
Without BRAM	0.000	0.000	0.001	0.003
With BRAM	0.000	0.000	0.000	0.000

In accordance to the above table, for the design of 8-bit adder without BRAM, the logic power reduction is 100%, 100% and 66.66% on scaling down the frequency from 100GHz to 0.1GHz, 1GHz and 10GHz respectively.

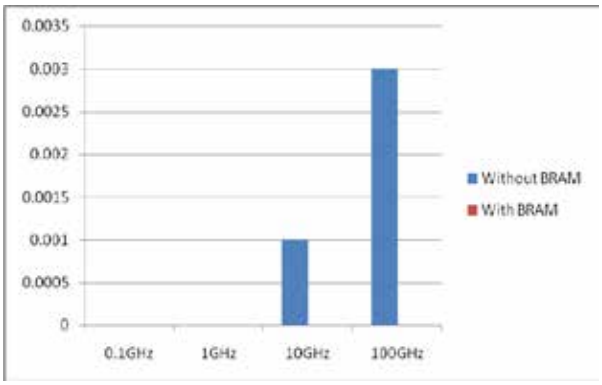


Figure 7: Logic Power Dissipation for 8-bit Adder

In the circuit design with BRAM, there is no change in leakage power for 8-bit Adder.

3.3 Signal Power Dissipation for 8-bit Adder

Table 7: Signal Power Dissipation for 8-bit Adder

Frequency →	**0.1GHz**	**1GHz**	**10GHz**	**100GHz**
Without BRAM	0.000	0.001	0.011	0.102
With BRAM	0.000	0.001	0.012	0.123

As per the above table, the signal power reduction is 100%, 99.02% and 89.22% as we scale down the frequency from 100GHz to 0.1GHz, 1GHz and 10GHz respectively in case of circuit design without BRAM.

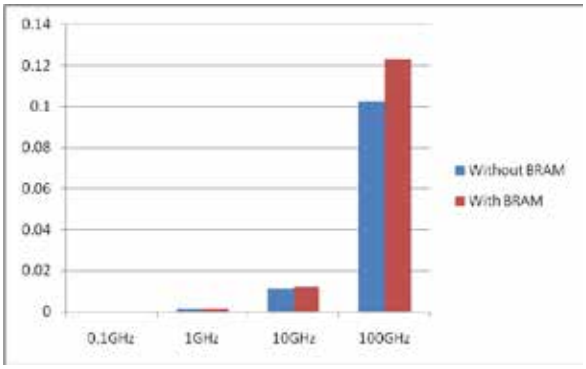


Figure 8: Signal Power Dissipation for 8-bit Adder

For the circuit design of 8-bit Adder with BRAM, the signal power reduction is 100%, 99.19% and 90.24% as the frequency is scaled down from 100GHz to 0.1GHz, 1GHz and 10GHz respectively.

3.4 IO Power Dissipation for 8-bit Adder

Table 8: IO Power Dissipation for 8-bit Adder

Frequency →	**0.1GHz**	**1GHz**	**10GHz**	**100GHz**
Without BRAM	0.001	0.010	0.122	1.219
With BRAM	0.005	0.047	0.470	4.703

According to the above table, for the circuit design of 8-bit Adder without BRAM, there is a reduction of 99.92%, 99.12% and 89.99% in IO power on scaling down the frequency from 100GHz to 0.1GHz, 1GHz and 10GHz respectively.

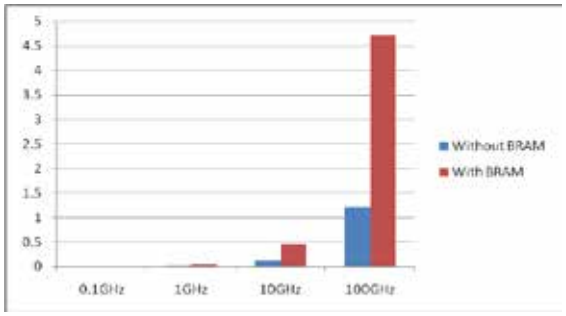


Figure 9: IO Power Dissipation for 8-bit Adder

The IO power reduction in case of circuit designed with BRAM is 99.89%, 99% and 90% as we scale down the frequency from 100GHz to 0.1GHz, 1GHZ and 10GHz respectively.

3.5 Leakage Power Dissipation for 8-bit Adder

Table 9: Leakage Power Dissipation for 8-bit Adder

Frequency →	0.1GHz	1GHz	10GHz	100GHz
Without BRAM	1.293	1.294	1.303	1.398
With BRAM	1.293	1.295	1.313	1.527

In accordance to the above table, for the design of 8-bit adder without BRAM, there is a reduction of 7.51%, 7.44% and 6.79% in leakage power on scaling down the frequency from 100GHz to 0.1GHz, 1GHz and 10GHz respectively.

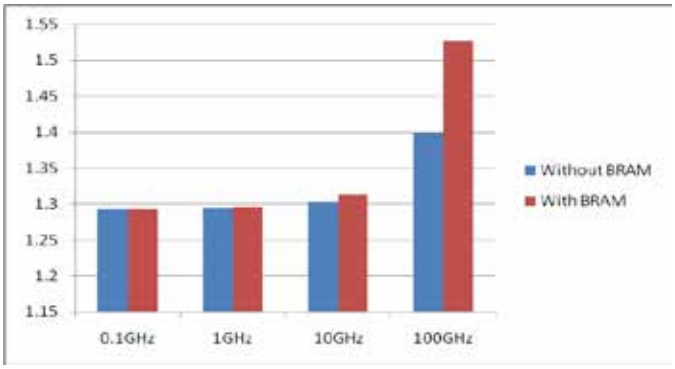


Figure 10: Leakage Power Dissipation for 8-bit Adder

In case of circuit design with BRAM, there is 15.32%, 15.19% and 14.01% reduction in leakage power on scaling down the frequency from 100GHz to 0.1GHz, 1GHz and 10GHz respectively.

3.6 Total Power Dissipation for 8-bit Adder

Table 10: Total Power Dissipation for 8-bit Adder

Frequency →	0.1GHz	1GHz	10GHz	100GHz
Without BRAM	1.297	1.336	1.743	5.787
With BRAM	1.302	1.384	2.204	10.443

In accordance to the above table, for the design of 8-bit Adder without BRAM, the total power reduction is 77.59%, 76.91% and 69.88% as we scale down the frequency from 100GHz to 0.1GHz, 1GHz and 10GHz respectively.

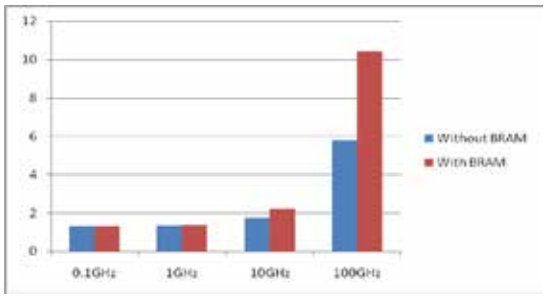


Figure 11: Total Power Dissipation for 8-bit Adder

In case of circuit design with BRAM, there is a total power reduction of 87.53%, 86.75% and 78.89% as we scale down the frequnecy from 100GHz to 0.1GHz, 1GHz and 10GHz respectively.

IV. CONCLUSION

There is a reduction of 99.9%, 100%, 100%, 99.92%, 7.51%, and 77.59% in clock, logic, signal, IO, leakage and total power respectively when the frequency is scaled down from 100GHz to 0.1GHz in the circuit design without BRAM, In case of the circuit with BRAM, the reduction in clock, signal, IO, leakage and total power is 99.90%, 100%, 99.89%, 15.32% and 87.53% respectively on account of frequency scaling from 100GHz to 0.1GHz. It can be clearly seen that the total power reduction is maximum in the circuit designed with BRAM. Hence power optimization has been achieved.

REFERENCES

Patents:

[1] C. Raymond, et al. "Block RAM having multiple configurable write modes for use in a field programmable gate array"(US patent 6346825 B1, 12 Feb 2002)

Website link:

[2] http://www.xilinx.com/support/documentation/user_guides/ug190.pdf

Journal Papers:

[3] B. Pandey, et al. "Capacitance Based Low Power ALU Design and Implementation on 28nm FPGA", *International Journal of Scientific Engineering and Technology* , Volume No.2, Issue No.6, pp : 465-468.(June 2013)

[4] S. Verma, et al. "BRAM and LUTs Based Area and Energy Efficient Signed Up Counter Design on FPGA", *Bilingual International Conference on Information Technology: Yesterday, Today, and Tomorrow, DESIDOC 2015*, pp. 108-113.(February 2015)

Proceedings Papers:

[5] J. Yadav, et al. "Energy Efficient Design and Implementation of ALU on 40-nm FPGA", *IEEE International Conference on Energy Efficient Technologies for Sustainability-(ICEETs),* pp.45-50.(April 2013)

[6] B. Pandey, et al. "Energy Efficency of Asynchronous and Synchronous VLSI Circuit on 40nm and 90nm FPGA", *IEEE International Conference on Energy Efficient Technologies for Sustainability (ICEETS), 2013 International Conference*, pp. 57-60.(April 2013)

SIMULATION OF GRANULE SIZE IN UPFLOW ANAEROBIC SLUDGE BLANKET REACTOR USING DIMENSIONLESS APPROACH

Vidya Singh

Research Scholar, Department of Chemistry,

Motilal Nehru National Institude of Technology, Allahabad, U.P, (India)

ABSTRACT

A dimensionless approach was used to simulate the granule size variation in upflow anaerobic sludge blanket (UASB) reactor under different operating condition like organic loading rate (O), polymer loading (P_L), upflow velocity (V_{up}), operation time (t_0), density of water (r_g) and density of granule (r_g). The experimental results of different investigators on polymer loading, OLR, upflow velocity, operation time and granule density were collected and developed a mathematical model to the enhancement of granule size in UASB reactor. Using MATLAB software indices of power multiplier function obtained can be used to predict the granule size (D_g) variations in UASB reactor.

Keywords*: *Dimensionless Approach, Granule Size, Non Linear Regression, Organic Loading Rate, UASB

I. INTRODUCTION

As compared to other anaerobic treatment technologies, such as anaerobic filter, anaerobic sequencing batch reactor, anaerobic expanded bed and fluidized bed reactors, the UASB system performance is highly dependent on granulation and the type of organic wastewaters treated. Anaerobic granular sludge is the core component of a UASB process. Microbial granulation is a complex process, involving different trophic bacterial groups and their physico-chemical and microbiological interactions. Granulation initiated by bacterial adsorption and adhesion to inert matters or inorganic participates provides a better settling characteristics and granule stability [1, 2].

UASB process performance can be judged by evaluating its performance within as well as beyond the granulation period and or start-up phase, as the system behaviour is under highly transient conditions within the granulation period [2-5].

Successful performance of UASB reactor can be achieved within a short period, if granules are developed quickly within the sludge bed under the proper environmental and operating conditions within the reactor [6]. Granulation process is affected by various factors like organic loading rate, upflow velocity, settling velocity, sludge volume index (SVI), gas production rate, liquid flow rate, polymer loading, Percent COD removal and effluent COD concentration. Granulation is also affected by several other factors such as pH and alkalinity, temperature, microbial ecology, production of exo-cellular polymeric substances by anaerobic bacteria, nutrients and trace metals, heavy metals etc.

Granules may range from 0.1 to 5 mm in size or even higher than 5 mm and are differentiated from flocculated sludge by their high shear strength [3, 7]. Approximately 2-3 % of the granules in the reactors were reported in the size range of 0.5-4.5 mm by [8]. [9] have documented that about 14 % granules were observed larger than 4.0 mm in size in UASB reactor. After increment in the organic loading rate, the granule sizes were reduced due to shearing of granules caused by high flow velocity and possible washout of lighter microorganisms [2, 3, 10]. An empirical model for gas production rate, effluent substrate concentration was developed for performance evaluation of UASB reactors treating poultry manure wastewater under different operational conditions [11].

In the present work, the independent variables like polymer loading, organic loading rate, upflow velocity, operation time and granule density influencing the granule size in UASB reactor have been collected from the literatures. Further a mathematical model was developed by non linear regression using MATLAB2010a software for prediction of granule size in UASB reactor. Various statistical measures such as standard deviation (S.D), root mean square error (R.M.S.E), R^2, sum of residuals of errors (SR), average residuals of errors (AR), residuals sum of squares (RSS) and standard error of estimate (SEE) were done between predicted output and experimental data of granule size to check the accuracy of developed model. It is believed that the developed model and tested in the present study may prove useful in assessing the granule size in UASB reactor.

II. DATA COLLECTION AND METHODOLOGY

In the analysis of granule size development in UASB reactor, the experimental results of [4, 6] have been used. These experimental data were read either from the figures or taken directly from the tables provided in [4, 6]. In [4] influent substrate concentration (S_0) was maintained at 4 g COD/L in all the four reactors R1 to R4 and OLR was varied in the range of 730-16030 g COD/m^3.d. Reactor R4 provided the shortest period of granulation compared to other reactors. In [6], influent substrate concentration was varied in range of 0.55 g/L to 0.65 g/L throughout the study in all four reactors R1 to R4. Organic loading rate was varied in the range of 1400-5700 g COD/m^3.d. Reactor R2 provided the shortest granulation period and large size of granule compared to other reactors. Subsequent granules characterization indicated that the granule developed in R4 reactors in [4] and R2 reactor in [6] exhibited the best settleability, short start-up period and good methanogenic activity at all COD loading rates, so analysis of these reactors considered in this study .

The organic loading rate (O) in the reactor can be varied either by varying influent COD concentration or by varying in flow rate. Using the experimental results of [4, 6] the variation of granule size as a function of organic loading rate is shown in figure 1. From fig. 1, it is evident that as organic loading rate increases, size of granules also increases.

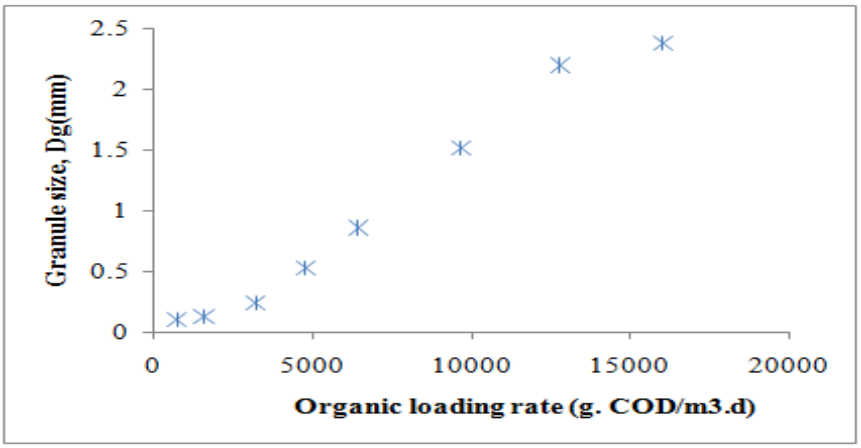


Fig.1. Variation of Granule Size with Organic Loading Rate

Granule formation and characteristics are strongly influenced by the liquid upflow velocity and at high upflow velocities (>1m/h), the granules may disintegrate due to shearing and resulting fragments may wash out of the reactor. Vigorous gas evolution at high organic loading and upflow velocity may result in vigorous shearing of bacterial cells from granule surface leading to granule erosion. The variation of granule size as a function of upflow velocity is shown in figure 2. From this figure, it is evident that granule size increases with increase in upflow velocity.

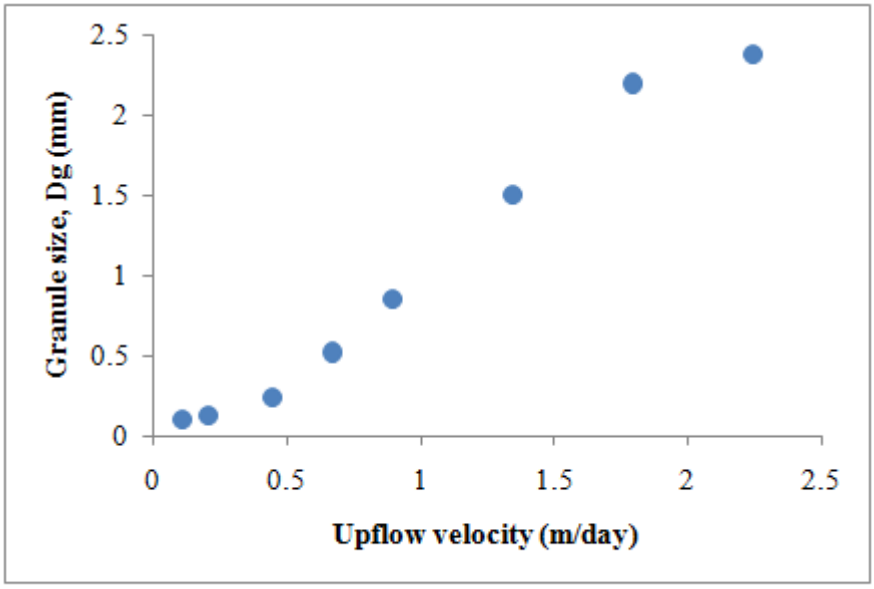


Fig.2. Variation of granule size with up flow velocity

III. RESULTS AND DISCUSSION

3.1 Dimensionless Approach

In the present work, a dimensionless approach using Buckingham π - theorem has been applied to developed model for granule size (D_g) in UASB reactor. As evident from the literature, granulation process is dependent on several factors enumerated in the proceeding section and hence the granule size is considered to be dependent on several independent variables such as operation time (t_o), COD loading rate (O), upflow velocity (V_{up}), polymer loading (P_L), acceleration (g), specific density of granule (ρ_g) and specific density of water (ρ_w). Therefore, it can be written as:

$$D_g = f\,(t_o, O, V_{up}, P_L, \rho_g, \rho_w, g) \quad (1)$$

By using Buckingham π - method, found some relationship between dependent and independent variables, then make 4 dimensionless groups which are given below in equation (2). Dimensionless groups are:

$$\left[\frac{D_g}{t_o.V_{up}}\right]\left[\frac{P_L}{O.t_o^3.V_{up}^3}\right]\left[\frac{t_o.g}{V_{up}}\right]\left[\frac{\rho_g}{\rho_w}\right] \quad (2)$$

Therefore, ($D_g/t_o.V_{up}$) can be written as:

$$\left[\frac{D_g}{t_o.V_{up}}\right] = f\left[\frac{P_L}{O.t_o^3.V_{up}^3}\right]\left[\frac{t_o.g}{V_{up}}\right]\left[\frac{\rho_g}{\rho_w}\right] \quad (3)$$

Equation (3) can be written as-

$$D_g = \left(t_o.V_{up}\right)\left[\frac{P_L}{O.t_o^3.V_{up}^3}\right]\left[\frac{t_o.g}{V_{up}}\right]\left[\frac{r_g}{r_w}\right] \quad (4)$$

Another attempt was made to develop a power multiplier function for prediction of granule size by raising the powers of each dimensionless groups of Eq. (4) and is expressed as:

$$\left[\frac{D_g}{t_o.V_{up}}\right] = \left[\frac{P_L}{O.t_o^3.V_{up}^3}\right]^a \left[\frac{t_o.g}{V_{up}}\right]^b \left[\frac{r_g}{r_w}\right]^c \quad (5)$$

Simplifying the equation (5) and can be written as:

$$D_g = \left(t_o.V_{up}\right)\left[\frac{P_L}{O.t_o^3.V_{up}^3}\right]^a \left[\frac{t_o.g}{V_{up}}\right]^b \left[\frac{r_g}{r_w}\right]^c \quad (6)$$

Where, D_g is a function containing each dimensionless term as power function used, and a, b and c are indices raised to the dimensionless groups formed in Eq. (6) used for prediction of granule size.

3.2 Prediction of granule size (D_g)

In this modelling work; the indices a, b and c were determined by non-linear regression analysis by fitting the Eq. (6) using NLINFIT tool in MATLAB 2010a. Equation (6) has been tested on experimental data of [4] and also validated by the data of [6] results are discussed in the succeeding sections.

a multiplier power function (D_g) containing powers of each dimensionless terms of Eq. (6) is developed by simulating the granule size term (R.H.S term of Eq. (6)) with the experimental results of [4] using NLINFIT tool of MATLAB 2010a and the resulting non-linear best fit equations for R4 reactors are given below as equation (7) .

$$D_g = \left(t_o.V_{up}\right)\left[\frac{P_L}{O.t_o^3.V_{up}^3}\right]^{0.073}\left[\frac{t_o.g}{V_{up}}\right]^{-0.292}\left[\frac{r_g}{r_w}\right]^{0.110} \quad (7)$$

From equation (7) predicted data of granule sizes are observed, compare these output predicted values of granule size with experimental data of granule sizes and obtained percentage error are 15 %. Fig. 3 illustrates the agreement between the proposed non linear regression model outputs and the experimental data.

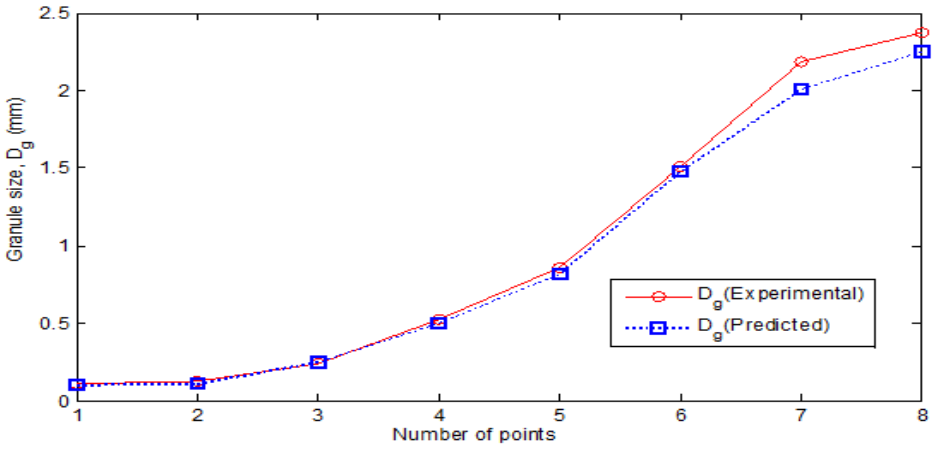


Fig.3. Agreement between the proposed model outputs and experimental data in testing

From Fig.3. It can be seen that predicted output data of granule sizes were very close to experimental data of granule size, means a better fitting was predicted between observed output data and experimental values of granule sizes. Proposed model gives better results for prediction of granule sizes in UASB reactor.

3.3 Validation of the proposed model

Multiplier power function (D_g) obtained in equation (7) are validated by experimental data of [6] for reactor R2 and compared these output predicted values of granule size with experimental data of granule sizes and obtained percentage error are 10 %. Fig. 4 illustrates the agreement between the proposed non linear regression model outputs and the experimental data.

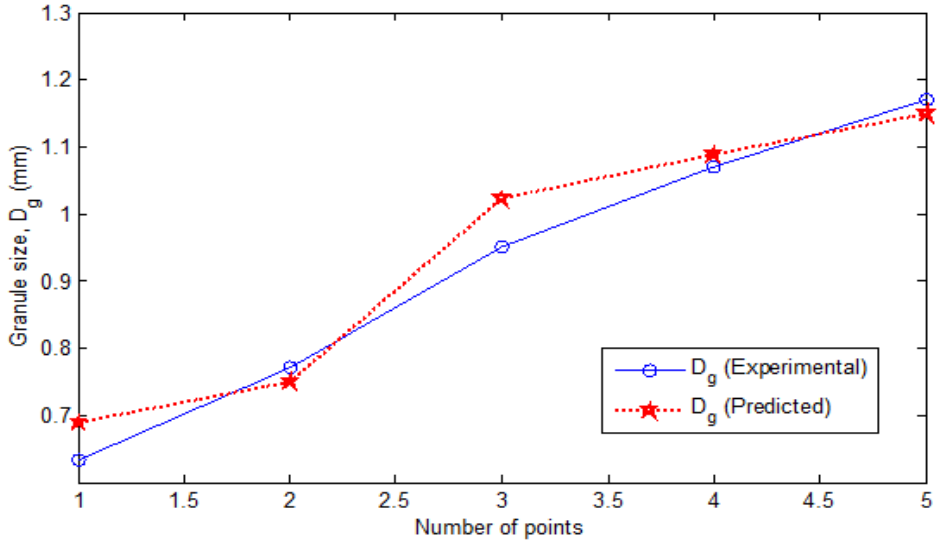


Fig.4. Agreement between the proposed model outputs and experimental data for validation

Statistical error estimates are determined to evaluate the goodness of fit using sum of residuals (SR), average residual errors (AR), Residuals sum of squares (RSS), standard errors of estimate (SEE), standard deviation (S.D) and root mean square error (RMSE). These statistical error estimates in experimental and predicted (D_g) values for all the six reactors are presented below in Table 1. SR measures the variance between experimental and predicted data. Small values of SR indicate a tight fitting of experimental and predicted values. RSS measures the amount of error between the regression function and the experimental data set. SEE measures the discrepancy between experimental data and model estimates. Similar to SR, the small SEE value indicates a tight fitting of data set. Standard deviation (S.D) measures the amount of variation or dispersion from the average. A low S.D values indicates that the data points tend to vary close to the mean values and a high S.D value indicates that the data points are spread out over a large range of values. RMSE is a measure of the difference between predicted values and observed experimental values.

Table1. Descriptive statistics of the residuals errors in prediction of D_g values

Residual statistics Calculation	Calculation	Regression results	
		In Testing	In Validation
The sum of residuals of the errors	$SR = \sum_{i=1}^{n} (D_e - D_p)$	3.18E-04	1.34E-04
The average residuals of the errors	$AR = \frac{1}{n} \sum_{i=1}^{n} (D_e - D_p)$	3.97E-05	2.68E-05
The residuals sum of squares	$RSS = \sum_{i=1}^{n} (D_e - D_p)^2$	1.43E-07	6.63E-09

The standard error of estimate	$SEE = \sqrt{\frac{\sum_{i=1}^{n} (D_e - D_p)^2}{n - p}}$	**3.78E-04**	**7.59E-05**
Correlation coefficient	$R^2 = \frac{\sum_{i=1}^{n} (D_p - D_m)^2}{\sum_{i=1}^{n} (D_e - D_m)^2}$	**0.976**	**0.961**
Root mean square error	$RMSE = \sqrt{\frac{1}{n - 2} \sum_{i=1}^{n} (D_e - D_p)^2}$	**1.47E-04**	**2.14E-05**
Standard deviation		**9.56E-04**	**2.54E-04**

D_e, experimental granule size; D_p, predicted granule size; D_m, mean granule size, n, no. of experimental data point.

From Table 1 all statistical error estimates are low for both analysis testing as well as validation, means observed predicted outputs are very close to experimental values. Predicted output granule sizes shows better fitting with experimental data of granule sizes, means proposed model for power multiplier function (D_g) gives better results for prediction of granules sizes in UASB reactor.

V. CONCLUSION

In dimensionless approach six independent variables operation time, organic loading rate, polymer loading, up flow velocity, specific density of granule and specific density of water are considered, which dependent on granule size in UASB reactor. From these dependent and independent variables make four dimensionless groups by using dimensionless approach Buckingham π - theorem. Indices of power multiplier function obtained by using NLINFIT tool of MATLAB2010a and simulate the granule size which are close to the experimental data of granule size. % error between experimental data and predicted output of granule size is approximately 15% in analysis of testing and 10% found in analysis of validation, means less % error shows closeness between predicted output and experimental data of granule size. Low values of statistical error and higher correlation coefficient R^2 (equal to 0.976 in testing and 0.961 in validations) indicates accuracy in predicted output of granule size in UASB reactor. From nonlinear regression obtained power multiplier function of D_g is used for the prediction of granule size in UASB reactor.

VI. ACKNOWLEDGMENTS

Authors are grateful to MHRD, New Delhi MNNIT, Allahabad for their help in compiling and preparing this manuscript.

REFERENCES

[1] Y. Liu, HL. Xu, KY. Show, JH Tay, Anaerobic granulation technology for wastewater treatment, World Journal of Microbiology and Biotechnology, 18(2), 2002, 99-113.

[2] Y .Kalogo, Se´ka AM 'Bassiguie, W. Verstraete, Enhancing the start-up of a UASB reactor treating domestic wastewater by adding a water extract of Moringa oleifera seeds, Applied Microbiology and Biotechnology, 55 (5), 2001, 644-651.

[3] KY. Show, Y. Wang, S.F. Foong, JH. Tay. Accelerated start-up and enhanced granulation in upflow anaerobic sludge blanket reactors. Water Research, 38 (9), 2004, 2293-2304.

[4] Y.Wang, KY. Show, JH. Tay, KH. Sim, Effects of cationic polymer on start-up and granulation in upflow anaerobic sludge blanket reactors, Journal of Chemical Technology & Biotechnology,79 (3), 2004, 219-228.

[5] S. Chong, KS. Tushar, A. Kayaalp, HM. Ang, The performance enhencements of upflow anaerobic sludge blanket(UASB) reactors for domestic sludge treatment-A State- of-the-art review water research, 46, 2012, 3434-3470.

[6] JS. Wang, YY. Hu, CD. Wu, Comparing the effect of bioflocculant with synthetic polymers on enhancing granulation in uasb reactors for low-strength wastewater treatment Water SA, 31(2), 2005, 177-182.

[7] J.E. Schmidt, B.K. Ahring, Granular sludge formation in upflow anaerobic sludge blanket (UASB) reactors, Biotechnology and Bioengineering, 49 (3), 1996, 229-246.

[8] M. Tiwari, S. Guha, C. Harendranath, S. Tripathi, Enhanced granulation by natural ionic polymer additives in UASB reactor treating low-strength wastewater, Water Research, 39 (16), 2005, 3801-3810.

[9] Q. Yu, HHP. Fang, JH. Tay, Effects of Fe^{2+} on sludge granulation in upflow anaerobic sludge blanket reactors, Water Science and Technology, 41 (12), 2000, 199-205.

[10] P. Bhunia, M.M. Ghangrekar, Effects of cationic polymer on performance of UASB reactors treating low strength wastewater, Bioresource Technology, 99 (2), 2008, 350-358.

[11] K.Yetilmezsoy, S. Sakar, Development of empirical models for performance evaluation of UASB reactors treating poultry manure wastewater under different operational conditions, J Hazard Mater, 153, 2008, 532–543.

STEADY STATE SOLUTION OF ONE DIMENSIONAL HEAT EQUATION USING MARKOV CHAINS

A Bernick Raj[1], K Vasudevan[2]

[1] *Department of Mathematics, B S Abdur Rahman University, Chennai (India)*

[2] *Department of Mathematics, Presidency College, Chennai (India)*

ABSTRACT

Although the pedagogical value of introducing numerical methods such as the finite element methods, finite difference methods, moment methods, and Markov Chain methods in potential problems. In this paper, we make use of Markov chain method to find the steady state solution of one dimensional heat equation in the rod at equal distance nodes in elementary matrix operations.

Keywords: Markov Chain, One Dimensional Steady State Equation.

I. INTRODUCTION

There are different methods to solve Steady State Solution of One Dimensional Heat Equation like the finite element methods, finite difference methods, moment method and Markov chains method [3]. We have attempted to make use of a simple technique modifying the Markov Chains method to find the Steady State solution of one dimensional heat equation. The technique basically calculates the transition probabilities using Markov chains.

II. MARKOV CHAINS

Consider a sequence of random variables $X_0, X_1, ...$, and suppose that the set of possible values of these random variables is $\{0,1,...,M\}$. It will be helpful to interpret X_n as being the state of some system at time n, and, in accordance with this interpretation, we say that the system is in state i at time n if $X_n = i$. The sequence of random variables is said to form a Markov Chain if each time the system is in state i there is some fixed probability – call it p_{ij} – it will next be in state j. That is, for all $i_0, ..., i_{n-1}, i, j$.

$$p_{ij} = P(x_{n+1} = j / x_n = i, x_{n-1} = i_{n-1}, ..., x_1 = i_1, x_0 = i_0)$$

$$= P(x_{n+1} = j / x_n = i), j \in X, n = 0,1,2,...$$

The Markov chain is characterized by its transition probability matrix P, defined by:

$$P = \begin{pmatrix} p_{00} & p_{01} & \cdots \\ p_{21} & p_{22} & \cdots \\ \cdots & \cdots & \cdots \end{pmatrix}$$

P is a stochastic matrix, meaning that the sum of the elements in each row is unity, i.e. $\sum_{j \in X} p_{ij} = 1, i \in X$

A Markov process is a type of random process that is characterized by the memory less property [6-9]. It is a process evolving in time that remembers only the most recent past and whose conditional probability distributions are time invariant. Markov Chains are mathematical models of this kind of process. The Markov Chain is the random walk and the states are the grid nodes. The transition probability p_{ij} is the probability that a random-walking particle at node i moves to node j.

Suppose that this method is to be applied in Steady State One dimensional heat Equation:

$$\frac{d^2U}{dx^2} = 0 \text{ in the real line X.} \qquad (1)$$

Subject to dirichlet boundary conditions:

$$U = U_P \text{ on boundary B} \quad (2)$$

The real line X is divided into n nodes. If we assume that there are f free nodes (non-absorbing) and p fixed (absorbing) nodes, the size of the transition matrix p is n. Where $n = f + p$. (3)

If the absorbing nodes are numbered first and the non-absorbing states are numbered last, the $n \times n$ transition matrix becomes:

$$P = \begin{pmatrix} I & 0 \\ R & Q \end{pmatrix} \qquad (4)$$

Where the $f \times p$ matrix R represents the probabilities of moving from non-absorbing nodes to absorbing ones; the $f \times f$ matrix Q represents the probabilities of moving from one non-absorbing node to another; I is the $p \times p$ identity matrix representing transitions between the absorbing nodes ($p_{ii} = 1 \& p_{ij} = 0$); and 0 is the null matrix showing that there are no transitions from absorbing to non-absorbing nodes. For the solution of equation in (1), we obtain the elements of Q from (4) as:

$$Q = \begin{cases} \frac{1}{2}, if \quad i \quad is\, directly \quad connected \quad to \quad j \\ 0, if \quad i = j\, or \quad i \quad is\, not \quad directly \quad connected\, to \quad j \end{cases} \qquad (5)$$

The same applies to R_{ij} except that j is an absorbing node.

The probability matrix B is: $B = [R \quad Q]$ (6)

Where R_{ij} is the probability that a random-walking particle originating from a non-absorbing node i will end up at the absorbing node j. B is a $f \times n$ matrix and is stochastic like the transition probability matrix, i.e.

$$\sum_{j=1}^{n_p} B_{ij} = 1, i = 1, 2, ..., f. \qquad (7)$$

If U_f and U_n contain potentials at the free and fixed nodes respectively, then

$$U_f = BU_P \qquad (8)$$

The equation (8) will give the f number of equations where f is the number of free nodes. Solving these equations we get the solution of free nodes U_f.

III. ILLUSTRATIVE EXAMPLES

Two simple examples will corroborate the claims above. Neither requires any computer programming.

Example 1: Consider an infinitely long homogeneous rod with surface are insulated of sides A and B with $0^0 C$ and $100^0 C$ respectively. We wish to determine the heat potential at the centre. Mathematically, the problem is posed as: $\frac{d^2U}{dx^2} = 0$ Subject to U (0) = 0, U(x) = 100

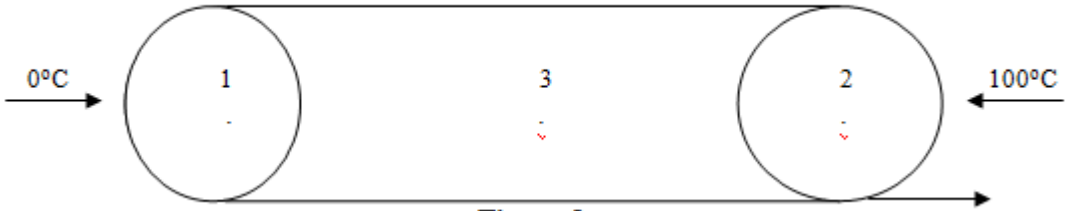


Figure 1

To apply Markov Chain Technique, we number the nodes in equal distance as in fig. 1, node 3 is the only free node so that $n_f = 1, n_p = 2$. The transition probability matrix is given by:

$$P = \begin{array}{c} \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & 0 \end{bmatrix} \end{array}$$

It is evident that:

$$Q = 0 \text{ and } R = \begin{bmatrix} 1 & \frac{1}{2} \end{bmatrix}$$

Thus: $$B = [R \quad Q] = \begin{bmatrix} 1 & \frac{1}{2} & 0 \end{bmatrix}$$

And $$U_f = BU_n = \begin{bmatrix} 1 & \frac{1}{2} & 0 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix}$$

$$u_3 = \begin{bmatrix} 1 & \frac{1}{2} & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 100 \\ u_3 \end{bmatrix}$$

$$u_3 = \frac{1}{2} \times 0 + \frac{1}{2} \times 100$$

$$u_3 = 50$$

This gives the centre node temperature which is equal to actual method value of the centre node.

Example 2: This is the same problem as in example 1 except that we are now to calculate the heat potential equal distance three points as shown in fig.2.

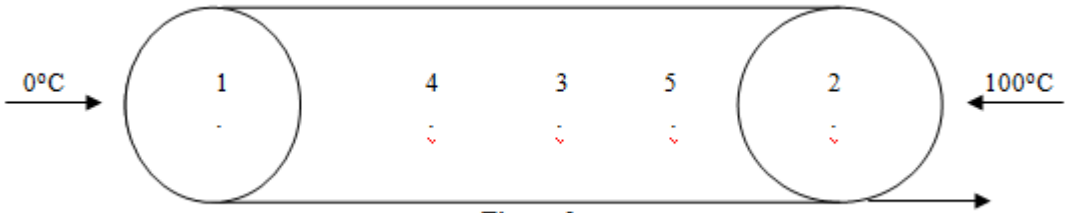


Figure 2

The transition probability matrix is obtained by inspection as:

$$P = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 & 0 \end{pmatrix} \end{array}$$

From P, we obtain:

$$R = \begin{array}{c} \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{cc} 1 & 2 \end{array} \\ \begin{pmatrix} 0 & 0 \\ \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \end{array} \quad \text{And} \quad Q = \begin{array}{c} \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccc} 3 & 4 & 5 \end{array} \\ \begin{pmatrix} 0 & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 0 & 0 \\ \frac{1}{2} & 0 & 0 \end{pmatrix} \end{array}$$

$$B = [R \quad Q] = \begin{pmatrix} 0 & 0 & 0 & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 & 0 \end{pmatrix}$$

Now $U_f = BU_p$

$$\begin{pmatrix} u_3 \\ u_4 \\ u_5 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 & 0 \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_5 \end{pmatrix}$$

$$\begin{pmatrix} u_3 \\ u_4 \\ u_5 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 100 \\ u_3 \\ u_4 \\ u_5 \end{pmatrix}$$

Hence, we have $2u_3 - u_4 - u_5 = 0$

$2u_4 - u_3 = 0$

$2u_5 - u_3 = 100$

Solving the above equation by iterative method we get $u_3 = 50, u_4 = 25 \& u_5 = 75$

Table 1

Node	Markov Chain Solution	Exact Solution
3	50	50
4	25	25
5	75	75

From Table 1 it is evident that Markov Chain Solution gives the exact solution.

IV. CONCLUSION

This paper has presented a means for using Markov Chain Method to solve steady state solution of one dimensional heat equation in the rod at equal nodes. The approach uses Markov Chains to calculate the transition probabilities. This approach is not subject to randomness because a random-number generator is not required. Without knowing the length of the rod the temperature in equal distance can be found out using this method.

REFERENCES

Journal Papers

[1] M. N. O. Sadiku, *Elements of Electromagnetics*, New York: Oxford Univ. Press, 2nd ed., 1994, pp. 237-2.545.

[2] M. N. O. Sadiku and R. C. Garcia, *Whole field computation using Monte Carlo method*, Inter. J. Numer. Model., 10, 1997, pp. 303-2.512.

[3] Clarence N Obiozor, Keming Gu and M. N. O. Sadiku, *Regional Monte Carlo Potential Calculation using Markov Chains*, Int. J. Engng Ed. Vol.18, No.6, pp.745-752, 2002

[4] A Bernick Raj, K Vasudevan, *Solution of Laplace Equation Using Markov Chains*, Int. J. Contemp. Math. Sciences, Vol. 7, 2012, no. 30, 1487 - 1493

Books

[5] Fusco, V. F. and Linden, P. A., *A Markov chain approach for static field analysis*, Microwave and Optical Technology Letters, 1, 6, Aug. 1988, pp. 216-2.520.

[6] M. E. Woodward, *Communication and Computer Networks*, Los Alamitos, CA: IEEE Computer Society Press, 1994, pp. 53-57.

[7] J. G. Kemeny and J. L. Snell, *Finite Markov Chains*, New York: Spring-Verlag, 1976, pp. 43-68.

[8] M. Iosifescu, *Finite Markov Processes and their Applications*, New York: John Wiley & Sons, 1980, pp. 45, 99-106.

[9] G. J. Anders, *Probability Concepts in Electric Power Systems*. New York: John Wiley & Sons, 1990, pp. 160-170.

AN INTEGRATED EVADER DEFENDANT SCHEME FOR CLIENT CERTIFICATION PROCESS

S.Karthika[1], Dr.P.Devaki[2]

[1] Student, [2] Assistant Professor

Computer Science and Engineering, Kumaraguru College of Technology, Coimbatore, (India)

ABSTRACT

Graphical passwords are knowledge-based authentication mechanisms where users enter a shared secret as evidence of their identity. Graphical passwords are composed with images and sketches with human memory for visual information. Improved password memorability and strength against guessing attacks are the key benefits of graphical password schemes. Captcha as graphical passwords (CaRP) is a graphical password scheme used for user authentication. CaRP is click-based graphical password where a sequence of clicks on an image is used to derive a password. Dynamic captcha challenge image is used for each login attempt in CaRP. Text Captcha and image-recognition Captcha are used in CaRP scheme. CaRP schemes can be classified into two categories as recognition based CaRP and recognition-recall based CaRP. Recognition-based CaRP seems to have access to an infinite number of different visual objects. Recognition-recall based CaRP requires recognizing an image and using the recognized objects as cues to enter a password. Recognition-recall combines the tasks of both recognition and cued-recall. Password information is transferred and verified using hash codes. Secure channels between clients and the authentication server through is Transport Layer Security (TLS). The CaRP scheme is enhanced with strength analysis and security features.

Keywords: Captcha, Cortcha, Graphical Password, IRC, TLS

I. INTRODUCTION

Security methods are required to handle unauthorized user access attempts. Security practitioners and researchers have made strides in protecting systems and, correspondingly, individual users' digital assets. The problem arises that, until recently, security was treated wholly as a technical problem – the system user was not factored into the equation. Users interact with security technologies either passively or actively [1]. For passive use understandability may be sufficient for users. For active use people need much more from their security solutions: ease of use, memorability, efficiency, effectiveness and satisfaction. Today there is an increasing recognition that security issues are also fundamentally human-computer interaction issues. Authentication is the process of determining whether a user should be allowed access to a particular system or resource. It is a critical area of security research and practice. Alphanumeric passwords are used widely for authentication, but other methods are also available today, including biometrics and smart cards. There are problems of these alternative technologies. Biometrics raise privacy concerns and smart cards usually need a PIN because cards can be lost. As a result, passwords are still dominant and are expected to continue to remain so for some time. Yet traditional alphanumeric passwords have drawbacks from a usability standpoint and these usability problems tend to translate directly into security problems. That is, users who fail to choose and handle passwords securely

open holes that attackers can exploit. The "password problem," as formulated by Birget, arises because passwords are expected to comply with two conflicting requirements, namely:

1. Passwords should be easy to remember and the user authentication protocol should be executable quickly and easily by humans.
2. Meeting these conflicting requirements is almost impossible for humans, with the result that users compensate by creating weak passwords and handling them in an insecure way.

Many problems that users have with alphanumeric passwords are related to memorability of secure passwords. In an attempt to create more memorable passwords, graphical password systems have been devised. In these systems authentication is based on clicking on images rather than typing alphanumeric strings. Several kinds of graphical passwords have been invented. In this paper a new kind of graphical password system, called PassPoints and have done studies of its human factors characteristics compared to alphanumeric password. This paper also report on further research on usability and memorability of our system under different conditions. In specific this paper investigate the effect of the tolerance, or the margin of error, allowed when entering one's password points and the effect of the choice of images used in the password system.

Various graphical password schemes have been proposed as alternatives to text-based passwords. Research and experience have shown that text-based passwords are fraught with both usability and security problems that make them less than desirable solutions [2]. Psychology studies have revealed that the human brain is better at recognizing and recalling images than text; graphical passwords are intended to capitalize on this human characteristic in hopes that by reducing the memory burden on users, coupled with a larger full password space offered by images, more secure passwords can be produced and users will not resort to unsafe practices in order to cope.

II. BACKGROUND AND RELATED WORK

Most current graphical password schemes, require users to enter the password directly, typically by clicking or drawing. Hence, passwords are easily exposed to a third party who has the opportunity to record a successful authentication session. There have been a few graphical password schemes devoted to secure passwords against spyware attacks. In the following, several representatives will be described. Man, et al proposed that users remember a number of text strings as well as several images as pass-objects. To pass the authentication, users should enter the unique codes corresponding to the displayed pass-object variants and a code indicating the relative location of the pass-objects in reference to a pair of eyes. It is relatively hard to crack this kind of password, but the complex memory requirement is an obstacle to its popularity.

In [6], users need to recognize pass-objects and click inside the convex hull formed by all of the pass-objects. If properly designed, this method can provide good security. From time to time the convex hull is either too small to click or too large, creating a guessing problem. Moreover, to provide a large password space may result in a crowed screen and indistinguishable objects. The method to resist shoulder-surfing is a trivial trick, where a user must click a group composed of both the pass-object and decoy-object rather than click the pass-objects directly. The prototype presented does not provide sufficient security, having only two objects in each group.

In 2006, Weinshall proposed another challenge-response protocol that relied on a shared secret set of pictures [8]. To reduce the amount of information given out with each authentication session, the image set memberships are used to select a certain path on an image mosaic, with the user providing only a code that depends on the path's endpoint. This scheme was claimed to be so strong that an observer who fully records any feasible series

of successful interactions could not compute the user's password. It was demonstrated by Golle and Wagner [9] that the attacker can learn a user's secret key with a SAT solver after observing as few as six successful user logins. In essence, the above methods adopt a challenge-response protocol to confuse the spyware. They can prevent the passwords being cracked by the spyware and falling into the hand of an adversary, along with resisting replay attacks. Taking the previous mechanisms for reference, our scheme also uses a challenge-response protocol to enhance security. But, unlike these methods, our scheme innovatively applies CAPTCHA to graphical passwords to create a highly secure authentication method.

III. EXISTING WORK

3.1 Captcha as Graphical Passwords (CaRP)

In CaRP, a new image is generated for every login attempt, even for the same user. CaRP uses an alphabet of visual objects to generate a CaRP image, which is also a Captcha challenge. A major difference between CaRP images and Captcha images is that all the visual objects in the alphabet should appear in a CaRP image to allow a user to input any password but not necessarily in a Captcha image. CaRP schemes are clicked-based graphical passwords. According to the memory tasks in memorizing and entering a password, CaRP schemes can be classified into two categories: recognition and a new category, recognition-recall, which requires recognizing an image and using the recognized objects as cues to enter a password [7]. Recognition-recall combines the tasks of both recognition and cued-recall and retains both the recognition-based advantage of being easy for human memory and the cued-recall advantage of a large password space. Exemplary CaRP schemes of each type will be presented later.

In principle, any visual Captcha scheme relying on recognizing two or more predefined types of objects can be converted to a CaRP. All text Captcha schemes and most IRCs meet this requirement [3]. Those IRCs that rely on recognizing a single predefined type of objects can also be converted to CaRPs in general by adding more types of objects. In practice, conversion of a specific Captcha scheme to a CaRP scheme typically requires a case by case study, in order to ensure both security and usability. We will present several CaRPs built on top of text and image-recognition Captcha schemes. Some IRCs rely on identifying objects whose types are not predefined. A typical example is Cortcha which relies on context-based object recognition wherein the object to be recognized can be of any type. These IRCs cannot be converted into CaRP since a set of pre-defined object types is essential for constructing a password.

Like other graphical passwords, we assume that CaRP schemes are used with additional protection such as secure channels between clients and the authentication server through Transport Layer Security (TLS). A typical way to apply CaRP schemes in user authentication is as follows [10]. The authentication server AS stores a salt s and a hash value $H(\rho, s)$ for each user ID, where ρ is the password of the account and not stored. A CaRP password is a sequence of visual object IDs or clickable-points of visual objects that the user selects. Upon receiving a login request, AS generates a CaRP image, records the locations of the objects in the image, and sends the image to the user to click her password. The coordinates of the clicked points are recorded and sent to the user ID. AS maps the received coordinates onto the CaRP image, and recovers a sequence of visual object IDs or clickable points of visual objects, ρ, that the user clicked on the image. Then AS retrieves salt s of the account, calculates the hash value of ρ' with the salt, and compares the result with the hash value stored for the account. Authentication succeeds only if the two hash values match. This process is called the basic CaRP authentication.

Advanced authentication with CaRP challenge-response will be presented. We assume in the following that CaRP is used with the basic CaRP authentication unless explicitly stated otherwise. To recover a password successfully, each user-clicked point must belong to a single object or a clickable-point of an object. Objects in a CaRP image may overlap slightly with neighboring objects to resist segmentation. Users should not click inside an overlapping region to avoid ambiguity in identifying the clicked object. This is not a usability concern in practice since overlapping areas generally take a tiny portion of an object.

IV. PROPOSED WORK

The CaRP scheme is enhanced with strength analysis and security features. Pattern based attacks are handled with Color and Spatial patterns. Pixel colors in click points are considered in the color pattern analysis model. Pixel location patterns are considered in the spatial pattern analysis model. Dictionary attacks and transmission attacks handling process is also improved with high security. Password security level assessment mechanism is used in the graphical password construction process. Cryptography (RSA) and data integrity (SHA) schemes are also integrated with the system to improve the security level in online applications. CAPTCHA and graphical password schemes are used for the user authentication process. Pixel physical and spatial properties are used in the strength analysis process. Transmission security is improved with integrity verification mechanisms.

The system is divided into six major modules. They are CaRP with Text CAPTCHA, authentication server, CaRP with image Recognition CAPTCHA, pattern analysis, attack handler and enhanced CaRP scheme. Character sequence selection is used in CaRP with Text CAPTCHA scheme. The authentication server is designed to manage and verify the user accounts. CaRP with Image Recognition CAPTCHA scheme uses the recognition and recall mechanism with image objects. The color and spatial patterns are analyzed under the pattern analysis module. The directory and shoulder surfing attacks are handled under attack handler module. Enhanced CaRP Scheme integrates the security and attack control mechanism for user authentication process.

4.1 Working

4.1.1 CaRP with Text Captcha

Textual characters based CAPTCHA is used in Text CaRP scheme. Password is constructed by selecting character sequences in the text CAPTCHA collection. The textual CAPCHA characters are dynamically rearranged at the time of recognition process. Password details are converted into hash codes and applied in verification process.

4.1.2 Authentication Server

The authentication server application is used to authenticate the users. User registration and password management operations are carried out under the server. Password verification is carried out under the server. Key and signature values are maintained under the server.

4.1.3 CaRP with Image Recognition Captcha

Image objects are used in recognition-recall based CaRP Recognition CAPTCHA. Object recognition and click cue identification mechanism are used in the system. Rectangular regions are used in the cued recall process. CAPTCHA-Zoo image object collection is used for the password construction process.

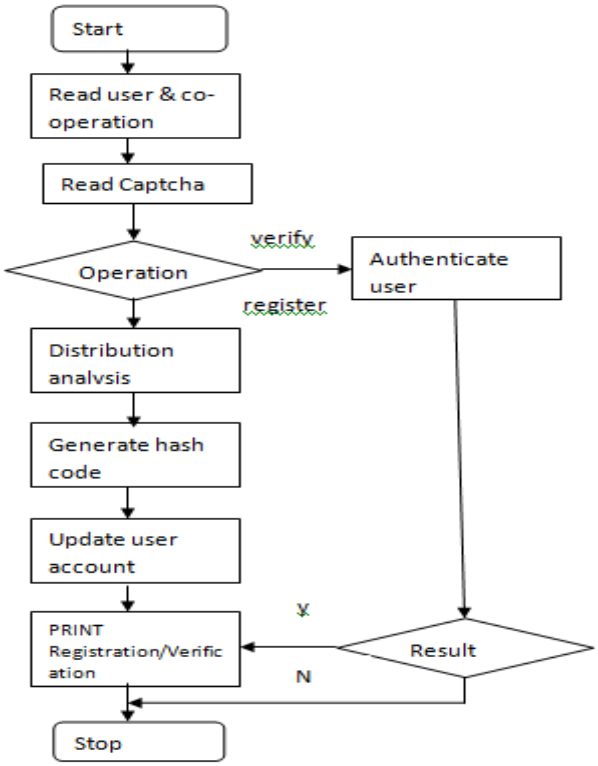


Fig. No: 1.1 Integrated Evader Defendant Scheme for Client Certification

4.1.4 Pattern Analysis

Color and spatial patterns are analyzed in the system. Pixel color for click points are used in the color pattern analysis. Spatial patterns are extracted from location information. Password complexity is assessed with pattern information.

4.1.5 Attack Handler

Directory and shoulder surfing attacks are managed by the system. RSA algorithm is used to perform password encryption/decryption tasks. Image dimming mechanism is used to control shoulder surfing attacks. Mouse cursor size and location are automatically adjusted for attack handling process.

4.1.6 Enhanced CaRP Scheme

CaRP scheme and attack handling mechanism are integrated in the Enhanced CaRP scheme. Distribution, strength and pattern analysis schemes are integrated with CaRP scheme. The Secure hashing algorithm (SHA) is used to generate password signatures. Reusability level is analyzed.

V. CONCLUSION

The graphical passwords are used to ensure the high level security for the remote logins. CAPTCHA techniques are used to verify the source type of request. Captcha as Graphical Passwords scheme integrates the text and image captchas to construct graphical password scheme. CaRP scheme is enhanced with strength based password construction and attack resistant user authentication model. Password complexity prediction system is integrated to improve password construction process. The system increases the success and recall rates. User interface is upgraded to avoid capture attacks in password recall process. Efficient shoulder surfing attack controlling models are used to protect the system from attackers.

REFERENCES

[1] S. Wiedenbeck and Memon, "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice," Proc. First Symp. Usable Privacy and Security, July 2005.

[2] S. Chiasson, P. van Oorschot and R. Biddle, "Graphical Password Authentication Using Cued Click Points," Proc. European Symp. Research in Computer Security, 2007.

[3] HP TippingPoint DVLabs, Vienna, Austria. Top Cyber Security Risks Report, SANS Institute and Qualys Research Labs [Online]. Available: http://dvlabs.tippingpoint.com/toprisks 2010.

[4] Mun-Kyu Lee, "Security Notions and Advanced Method for Human Shoulder-Surfing Resistant PIN-Entry", IEEE Transactions On Information Forensics And Security, April 2014

[5] N.Joshi.Koobface Worm Asks for CAPTCHA [Online]. Available:http://blogs.mcafee.com/mcafee-labs/koobface-worm-asksfor- CAPTCHA, 2009

[6] S. Wiedenbeck. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In Proceedings of the Working Conference on Advanced Visual Interface, New York, NY : ACM Press, 2006. pp. 177-184.

[7] Napa Sae-Bae and Kowsar Ahmed, "Multitouch Gesture-Based Authentication" IEEE Transactions On Information Forensics And Security, Vol. 9, No. 4, April 2014

[8] D. Weinshall. Cognitive Authentication Schemes Safe Against Spyware. In Symposium on Security and Privacy, 2006.

[9] P. Golle and D.Wagner. Cryptanalysis of a Cognitive Authentication Scheme. In Symposium on Security and Privacy, 2007.

[10] Sooyeon Shin and Sarang Na, "Covert Attentional Shoulder Surfing: Human Adversaries Are More Powerful Than Expected", IEEE Transactions On Systems, Man, And Cybernetics: Systems, June 2014.

[11] Bin B. Zhu, Jeff Yan, Maowei Yang and Ning Xu, "Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems" IEEE Transactions On Information Forensics And Security, Vol. 9, No. 6, June 2014.

[12] Xiaoyuan Suo ,Ying Zhu, G. Scott. Owen "Graphical Passwords: A Survey" in Computer world, May 10, 2006.

[13] Ved Prakash Singh, Preet Pal "Survey of Different Types of CAPTCHA" International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 2242-2245.

[14] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in *Proc. ACM CCS*, 2002, pp. 161–170.

[15] P. C. van Oorschot and S. Stubblebine, "On countering online dictionary attacks with login histories and humans-in-the-loop," *ACM Trans. Inf. Syst. Security*, vol. 9, no. 3, pp. 235–258, 2006.

PROTECTION OF SECURITY AND PRIVACY FOR MEDICAL DATA IN WIRELESS MEDICAL SENSOR NETWORKS

C.Gayathri[1], D.Sathya[2]

[1]*Department of Computer Science and Engineering, Kumaraguru College of Technology, Coimbatore, Tamil Nadu, (India)*

[2]*Assistant Professor, Department of Computer Science and Engineering, Kumaraguru College of Technology, Coimbatore, TamilNadu, (India)*

ABSTRACT

Wireless Sensor Networks (WSN) is an emerging technology that has the potential to transform the way of human life. Healthcare applications are considered promising fields for Wireless Medical Sensor Network, where patient's health can be monitored using Medical Sensors. Wireless Medical Sensor Networks (WMSNs) are the key enabling technology in healthcare applications that allows the data of a patient's vital body parameters to be collected by wearable biosensors. Current WMSN healthcare research trends focus on patient reliable communication, patient mobility and energy-efficient routing. Security and Privacy protection of the collected data is a major unsolved issue. To overcome these issues, symmetric algorithms and attribute based encryptions techniques are adopted, which secures the data transmission and access control system for MSNs.

Keywords- Access Control, Data Transmission, Medical Sensor Networks, Privacy, Security.

I. INTRODUCTION

Wireless Sensor Network (WSN) is a self-configure network of small sensor nodes, where the sensor nodes can communicate among themselves using radio signals, and these sensor nodes can sense, monitor and understand the physical environment. It consists of spatially distributed sensors to monitor physical or environmental conditions and to pass the data through the network to a destination location. The bi-directional modern networks enable to control the activity of the sensors. The development of the wireless sensor networks was motivated by military applications such as battlefield surveillance and is also used in many industrial and consumer applications like industrial process monitoring and control, machine health monitoring, etc [3]. The WSN is built of "nodes", where one or more sensor is connected to each node. Each sensor node consist of several parts, like radio transceiver with an internal antenna to an external antenna, microcontroller, electronic circuit for interfacing with the sensors and an energy source like a battery.

II. WIRELESS MEDICAL SENSOR NETWORKS

WSNs deployed at a large scale in a distributed manner, and their data rates differs based on their applications, where the Wireless Medical Sensor Networks have direct human involvement are deployed on a small scale

must support mobility (a patient can carry the devices), and WMSNs requires high data rates with reliable communication. Physiological conditions of patients are closely monitored by deploying Wireless medical sensor motes.

These medical sensors are used to sense the patient's vital body parameters and transmit the sensed data in a timely fashion to some remote location without human involvement. Using these medical sensor readings the doctor can get the details of a patient's health status. The patient's vital body parameters include heart beats, body temperature, blood pressure, sugar level, pulse rate [3].

WMSNs carry the quality of care across wide variety of healthcare applications. In addition, other applications that also benefit from WMSNs include sports-person health status monitoring and patients self-care. Several research groups and projects have started to develop health monitoring using wireless sensor networks.

Wireless Medical healthcare application offers a number of challenges, like, reliable transmission of data, secured data transmission, nodes mobility, detection of event delivery of data in time, power management, etc. Deploying new technologies in healthcare applications without considering security often makes patient privacy vulnerable. For instance, the patient's physiological vital signals are very sensitive so the leakage of the patient's diseased data could makes the patient embarrassed. Sometimes revealing disease information can make it impossible for them to obtain insurance protection and also result in a person losing their job [6].

Further, wireless medical sensor networks cover a broad range of healthcare applications, such as physiological data monitoring, activity monitoring in health-clubs, location tracking for athlete are the broad range of healthcare applications. WMSNs share individual data with physicians and insurance companies. Thus unauthorized collection and use of patient data by adversaries can cause life-threatening risks to the patient and make the patient's private matters publically available. For example, In[16] a simple scenario, a patient's body sensors transmit the body data to a nurse, the patient's privacy is breached when some attacker is eaves dropping. Later that attacker can post the patient data on social site and pose risks to the patient's privacy.

Indeed wireless healthcare can offer many advantages to patient monitoring, but the medical health data of an individual are highly vulnerable to various threats, so security and privacy become some of the big concerns for healthcare applications, when it comes to adopting wireless technology. A healthcare provider is subjected to strict civil and criminal penalties if Health Insurance Portability and Accountability Act (HIPAA) rules are not followed properly [4]. Thus the security and privacy of the sensed data is the major concern in healthcare applications**.**

III. LITERATURE SURVEY

Cryptographic algorithms are either symmetric algorithms which uses symmetric keys (secret keys), or asymmetric algorithms which uses asymmetric keys (public and private keys). In [12], both the algorithms have the following advantages and disadvantages.

3.1 Symmetric Algorithm

ADVANTAGE

- More secured
- Requires less space
- Same key for both encryption and decryption

DISADVANTAGE

· Key distribution problem

3.2 Asymmetric Algorithm

ADVANTAGE

· Solves key distribution problem

· Securely exchange message

DISADVANTAGE

· High computation time is required

· Requires more space

In [2], a lightweight and secure system for MSNs is proposed to provide a safe transmission of sensed data, the system employs hash-chain based mechanism and proxy-protected signature technique to achieve secure transmission of the sensed data and access control. The basic idea is as follows, the user registers to the network server, and the registered user is allowed to issue commands to access the collected PHI or control the biosensors according to their access privilege. To achieve this proxy-protected signature by warrant (PSW) is introduced into the system. An original signer and proxy signer are the two important participants. The original signer gives the proxy signer a warrant, and the proxy signer generates a proxy signature using the proxy key given by the original signer. The verifier validate proxy signatures with the public key of the original signer and also verifies the proxy key of the original signer. This prevents the unauthorized access and limits power consumption of sensor nodes.

In [1], in order to evaluate the behaviour of each node a secured multicast strategy is proposed; in this only trustworthy nodes are allowed to participate in communications so that the misbehaviour of malicious nodes is prevented. Trust is defined as “during the interaction with other node, how a node is trustworthy, secure, or reliable”. The criterion for choosing nodes for multicast technique is based on the trust value. By evaluating the node’s trust enables the trust system to track the behaviour of all the nodes, security evaluations feedback of other nodes are recorded, and corresponding reactions are made to the tracked behaviour. By this correct nodes can be chosen to participate in the communication and malicious nodes can be avoided.

In [9], the focus is on three secure sharing use cases; proof of ownership, where the data owner must prove the ownership of the data tracking, where the data owner must trace unauthorized sharing of the bio signal data and content authentication, and the data owner must prove whether the bio-signal data has been maliciously altered. To address these use cases, a robust watermarking technique is developed to embed security information into bio-signal data in order to protect the semantic fidelity of the data, the bio-signal waveforms are imperceptibly altered, and the watermark is not easily recovered, corrupted or spoofed by malicious attackers. Thus the integrity of the bio-signal is preserved by Water Marking and the data owners can easily track the usage of their data.

In [6], a secure and privacy-preserving opportunistic computing framework, called SPOC, is proposed for medical Healthcare emergency. Using SPOC smart phone resources including computing power and energy can be opportunistically gathered to process the computing-intensive personal health information (PHI) during m-Healthcare emergency with minimal privacy disclosure. To leverage the PHI privacy disclosure and the high reliability of PHI process and transmission in m-Healthcare emergency, an efficient user-centric privacy access

control in SPOC, which is based on an attribute-based access control and privacy-preserving scalar product computation (PPSPC) technique, allows a medical user to decide who can participate in the opportunistic computing to assist in processing his overwhelming PHI data.

In [10], a novel key agreement scheme that allows neighbouring nodes in BANs to share a common key generated by electrocardiogram (ECG) signals. The improved Jules Sudan (IJS) algorithm is proposed to set up the key agreement for the message authentication. The ECG-IJS key agreement secures data communications over BANs without any key distribution overheads. In this the simulation and experimental results are presented, which demonstrate that the ECG-IJS scheme can achieve better security performance in terms of performance metrics such as false acceptance rate (FAR) and false rejection rate (FRR) than other existing approaches. Based on the IJS algorithm described earlier, propose an ECG-IJS key agreement to secure data communication in BANs. Thus privacy and authentication are preserved in energy efficient way.

In [4], stochastic data traffic models for medical wireless sensor networks (WSN's) are presented that represent the traffic generated by a single WSN node monitoring body temperature and electrocardiogram (ECG) data. The models are based on public domain medical signal databases. For energy conservation, it is likely that some medical WSN nodes will employ source coding to reduce the amount of data that must be transmitted. The first scenario to consider is the straightforward case where the node simply transmits the raw 11 bit ECG data at the 360 Hz sampling rate. The second scenario is the more complex case where the node employs source coding. The work considers lossy compression due to the very high compression ratios possible with lossy techniques.

IV. EXISTING SYSTEM

A lightweight and secure system, for MSNs employs hash-chain based key updating mechanism and proxy-protected signature technique to achieve efficient secure transmission and access control. The basic idea of the existing system is given as follows. After a user registers to the network server, the user is allowed to issue commands to access the collected PHI or control the biosensors according to their privilege. To achieve this proxy-protected signature by warrant (PSW) is introduced into the system.

There are two kinds of participants, i.e., an original signer and proxy signers. The proxy signer registers in the network server, which is the original signer generates the proxy keys before the proxy server enters the MSN. Now after obtaining the keys the proxy user becomes the authorized user and can generate commands using those keys to get access to the data [2]. The validity of the key is verified by the network server so that it can prevent unauthorized users.

The system involves four phases. The system initialization phase is performed by the network server to set up an MSN. User joining phase is involved before a user can issue commands to the MSN. During the regular use phase, the data from each biosensor node are securely transmitted to the network server via the controller.

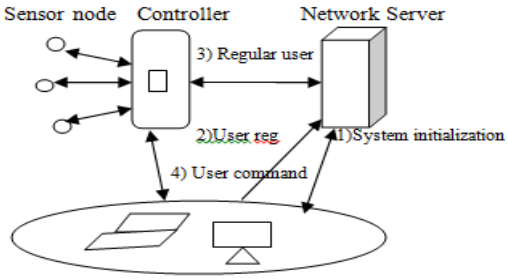


Figure 4.1 Flow of Security Information

In the user command phase, if a network user has a new command, he/she will need to construct the command and the proxy signature and then send them to the network server (or the controller of a target PAN). If the command verification passes, the network server (or the controller of a target PAN) responds to the user's command. The controller and node side programs are executed on the resource limited sensor nodes, and the network server programs are executed on the PC. Here AES encryption algorithm is used to encrypt the sensed data before transmission. Usually data block of 128 bits is encrypted using three different keys such as 128-bits, 192-bits and 256-bits of key length. MD5 is a one way hash function, where the hash value should match the received data correctly and is used to compress the data size in order to minimize the energy consumption.

V. PROPOSED SYSTEM

Even though AES is used for encrypting the data is less secured and requires more computation time.
In [2], the sensed data is transmitted individually and it requires more energy and data fusion is not done.
The enhancement of security and privacy of the sensed data can be achieved in the proposed system by implementing various symmetric encryption algorithms which are very efficient at processing large amounts of information and computationally less intensive than asymmetric encryption algorithms.
In Fig. 5.1, consist of various symmetric key algorithms such as mentioned in the below.

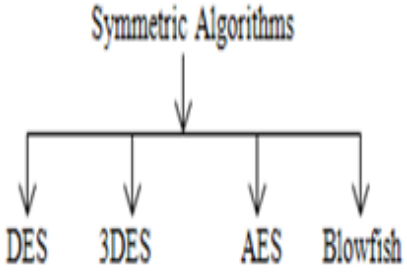


Fig 5.1:Symmetric Key Encryption

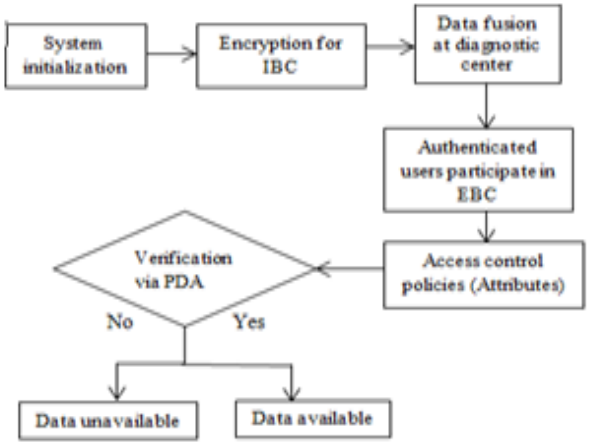


Fig 5.2: Architecture of Proposed System Algorithm

Symmetric algorithms like DES, 3DES, AES, Blowfish can be implemented to compare the different computation time take by various algorithms.

The above Figure 5.2 is the architecture of the proposed system. Since medical data is of a great privacy concern proper security mechanisms should be adopted while transmitting the data.

In the proposed work, the system is initialized by deploying the bio-sensors, and these sensors collect the vital body parameters like heartbeat, sugar level, blood pressure, etc. Various algorithms like DES, 3DES and Blowfish can be implemented and the best is chosen based upon their computation time. The collected data is encrypted using the best symmetric key encryption algorithm, In [11] blowfish algorithm which uses variable number of bits ranging from 32 to 448 bits encrypts the data 16 times than the other encryption algorithms and is said to be the fastest encryption algorithm, and is transmitted to the diagnostic center through controller via internet. Table a, provides the comparative study of different symmetric algorithms used for encryption.

Table a: Comparison of Symmetric Key Algorithms

Algorithms	Key length	Block size	Round	Attack
DES	128,192 256 bits	128,192, 256	9,11, 13	Side channel attack
3DES	168 bits	64	48	Theoretically possible
AES	56 bits	64	16	Brute force
BLOWFISH	32-448 bits	64	16	Not yet

The comparitive study shows that blowfish is the best among the implemeted algorithms as it is not exposed to any attack.

The type of communication between the sensor node and the controller is called as Intra Body Communication (IBC). Then data fusion will be done in the diagnostic center where several data is fused into one single packet in order to reduce the network traffic and transmission time. Omnibus data fusion model can be adopted where the sensed data is fused using either soft or hard data fusion and the sensor manager is used to manage the fusion. The fused data sent from controller to the diagnostic center and access control policies are adopted with the use of Attribute-based Encryption Signature. The Attribute-based Encryption algorithm consist of four steps:

1. Setup (λ, U) $\rightarrow$ (PK, MK)

The setup algorithm takes as input a security parameter λ and a universe description U. PK which is the public parameters and the master secret key MK is the output.

2. Encrypt (PK, M, S) $\rightarrow$ CT

The public parameters PK is given as input to the encryption algorithm, a message M and a set of attributes S and outputs a ciphertext CT associated with the attribute set.

3. KeyGen (MK, A) $\rightarrow$ SK

The key generation algorithm takes as input the master secret key MK and an access structure A and outputs a private key SK associated with the attributes.

4. Decrypt (SK, CT) $\rightarrow$ M

A private key SK associated with access structure A is given as input to the decryption algorithm and a cipher text CT associated with attribute set S and outputs a message M.

The communication between the controller and diagnostic center is called Extra Body Communication (EBC). The authenticated users can participate in EBC. The authentication is achieved through the email id, which is the Secret Key(SK) generated by the key generation algorithm. Strict access control policies can be adopted at the diagnostic center based on the user's attributes, i.e. doctors can gain access to the entire medical data, the technicians can access only few data of the patients, and the patients have very limited access to others data. The verification can be done via PDA at the center and the data is available only to the authorized user and unauthorized users cannot access the data.

VI. CONCLUSION

Healthcare applications are considered promising fields for WMSNs, where patients can be monitored. Transmission in wireless environment needs safety and privacy of medical data. The disadvantage of public-key algorithm is that they are more computationally intensive than symmetric algorithms, this is not significant for a short text message , hence Symmetric cryptographic algorithms can be used to provide security while transmitting the sensed data and access control policies are adopted by attribute based signature technique. Hence the privacy and integrity of data can be perceived during the transmission in wireless environment.

REFERENCES

[1] AzzedineBoukerche, and YonglinRen," A Secure Mobile Healthcare System using Trust-Based Multicast Scheme",IEEE Journal On Selected Areas In Communications, Vol. 27, No. 4, May 2009,316-325.

[2] Daojing He, Sammy Chan, Member, IEEE, and Shaohua Tang, Member, IEEE," A Novel and Lightweight System to Secure Wireless Medical Sensor Networks", IEEE Journal Of Biomedical And Health Informatics, Vol. 18, No. 1, January 2014,23-32.

[3] Denis Trcek And Andrej Brodnik, University Of Ljubljana," Hard And Soft Security Provisioning for Computationally Weak Pervasive Computing Systems In E-Health", IEEE Wireless Communications August 2013,45-53.

[4] Geoffrey G. Messier and Ivars G. Finvers," Traffic Models for Medical Wireless Sensor Networks", IEEE Communications Letters, Vol. 11, No. 1, January 2007,21-30.

[5] Oscar Garcia-Morchon, Thomas Falck, Tobias Heer, Klaus Wehrle,"Security for Pervasive Medical Sensor Networks", Vol.12, No.2, June 5th 2009,126-134.

[6] Rongxing Lu, Member, IEEE, Xiaodong Lin, Member, IEEE, and Xuemin (Sherman) Shen, Fellow, IEEE," SPOC: A Secure and Privacy-preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency", IEEE Transactions On Parallel And Distributed Systems, Vol. 12, No. 2, May 2012,452-461.

[7] Shu-Di Bao, Student Member, IEEE, Carmen C. Y. Poon, Student Member, IEEE, Yuan-Ting Zhang, Fellow, IEEE, and Lian-FengShen," Using the Timing Information of Heartbeats as an Entity Identifier to Secure Body Sensor Network", IEEE Transactions On Information Technology In Biomedicine, Vol. 12, No. 6, November 2008,155-162.

[8] S. Moller, T. Newea, S. Lochmannb," Prototype of a secure wireless patient monitoring system for the medical Community", 2011 Elsevier B.V. All rights reserved.

[9] VishwaGoudar and MiodragPotkonjak," A Robust Watermarking Technique for Secure Sharing of BASN Generated Medical Data", 2014 IEEE International Conference on Distributed Computing in Sensor Systems.

[10] Zhaoyang Zhang, Honggang Wang, Athanasios V. Vasilakos, and Hua Fang," ECG- Cryptography and Authentication in Body Area Networks", IEEE Transactions On Information Technology In Biomedicine, Vol. 16, No. 6, November 2012,321-332.

[11] E.surya,C.Divya, " A Survey on Symmetri Key Encryption Algorithms", International Journal of Computer Science & Communication Networks,Vol 2(4), 475-477.

[12] Tingyuan Nie, and Teng Zhang ,"A Study of DES and Blowfish Encryption Algorithm", IEEE, 2009.

[13] Singh, S preet, and Maini, Raman "Comparison of Data Encryption Algorithms", International Journal of Computer science and Communication,vol.2,No.1,January-June 2011,pp.125-127.A.

14] Behrouz A.Forouzan", Cryptography and Network Security", 2nd Ed, Tata Mcgraw hill.

[15] Himani Agrawal and Monisha Sharma,"Implementation and analysis of various Symmetric Cryptosystems", Indian Journal of science and Technology vol.3,No.12,December 2012.

[16] Pardeep Kumar and Hoon-Jae Lee," Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey", Published: 22 December 2011, Sensors 2012, 12, 55-91.