Proceeding
Of
4th International Conference on Computer Science and Information Technology (ICCIT 2015)
&

4th International Conference on Progress in Production, Mechanical and Automobile Engineering (ICPMAE-2015)

Date: 8th March 2015
Gujarat

Editor-in-Chief

Dr. Priyanka Sharma
Professor (IT - M. Tech Cyber Security)
Raksha Shakti University
New Mental Corner, Meghaninagar,
Ahmedabad Gujarat INDIA.

Organized by:

TECHNICAL RESEARCH ORGANISATION INDIA
Website: www.troindia.in

ISBN: 978-93-85225-08-6

About Conference

Technical Research Organisation India (TROI) is pleased to organize the 4th International Conference on Computer Science and Information Technology (ICCIT 2015) & 4th International Conference on Progress in Production, Mechanical and Automobile Engineering (ICPMAE-2015)

ICCIT is a comprehensive conference covering the various topics of Engineering & Technology such as Computer Science and IT. The aim of the conference is to gather scholars from all over the world to present advances in the aforementioned fields and to foster an environment conducive to exchanging ideas and information. This conference will also provide a golden opportunity to develop new collaborations and meet experts on the fundamentals, applications, and products of Computer science and IT. We believe inclusive and wide-ranging conferences such as ICPMAE can have significant impacts by bringing together experts from the different and often separated fields of Production, Mechanical and Automobile Engineering. It creating unique opportunities for collaborations and shaping new ideas for experts and researchers. This conference provide an opportunity for delegates to exchange new ideas and application experiences, we also publish their research achievements. ICPMAE shall provide a plat form to present the strong methodological approach and application focus on Production, Mechanical and Automobile Engineering that will concentrate on various techniques and applications. The ICPMAE conference cover all new theoretical and experimental findings in the fields of Production, Mechanical and Automobile Engineering or any closely related fields.

Topics of interest for submission include, but are not limited to:
Computer Science Engineering
Information Technology
Production Engineering
Automobile Engineering
Mechanical Engineering
Nano-Technology
Network Engineering
Software Engineering

And many more....

Organizing Committee

Dr. Bhasker Gupta
Assistant Professor. Jaypee University of Information Technology, Himachal Pradesh

Dr. A. Lakshmi Devi,
Professor, department of electrical engineering,
SVU college of Engineering, Sri Venkateswara university, Tirupati

Prof. Shravani Badiganchala

Assistant professor, Shiridi sai institute of science and engineering

Prof. Surjan Balwinder Singh
Associate Professor in the Electrical Engineering Department,
PEC University of Technology, Chandigarh.

Prof (Dr) Punyaban patel.
Department of Computer science and engineering ,
Chhatrapati shivaji institute of technology, Durg

Dr. Shilpa Jindal ,
PEC University of Technology (Deemed University), Chandigarh
ji_shilpa@yahoo.co.in

Prof. S. V. Viraktamath
Dept. of E&CE S.D.M. College of Engg. & Technology Dhavalagiri, Dharwad

Subzar Ahmad Bhat
Assistant Professor, Gla University

Dr. G.Suresh Babu
Professor,Dept. of EEE,CBIT, Hyderabad

Prof .Ramesh
Associate Professor in Mechanical Engineering,
St.Joseph's Institute of Technology

Prof.Amit R. Wasnik
Sinhgad Institute of Technology, Pune, Maharashtra

IIT KHARAGPUR

Prof. Rajakumar R. V.

DEAN Acadedemic, rkumar @ ece.iitkgp.ernet.in

Prof. Datta D., ddatta @ ece.iitkgp.ernet.in

Prof. Pathak S S,r,ssp @ ece.iitkgp.ernet.in

Dr. Hansa Jeswani
Asso. Professor.,
Sardar Patel College of Engineering, Mumbai

TABLE OF CONTENTS

SL NO	TOPIC	PAGE NO

Editor-in-Chief

Dr. Priyanka Sharma

Editorial

The conference is designed to stimulate the young minds including Research Scholars, Academicians, and Practitioners to contribute their ideas, thoughts and nobility in these two integrated disciplines. Even a fraction of active participation deeply influences the magnanimity of this international event. I must acknowledge your response to this conference. I ought to convey that this conference is only a little step towards knowledge, network and relationship.

The conference is first of its kind and gets granted with lot of blessings. I wish all success to the paper presenters.

I congratulate the participants for getting selected at this conference. I extend heart full thanks to members of faculty from different institutions, research scholars, delegates, TROI Family members, members of the technical and organizing committee. Above all I note the salutation towards the almighty.

Editor-in-Chief:
Dr. Priyanka Sharma
Professor (IT - M. Tech Cyber Security)
Raksha Shakti University
New Mental Corner, Meghaninagar,
Ahmedabad Gujarat INDIA.

A SURVEY ON SECURE VIRTUAL PASSWORD AND PHISHING ATTACK

Ms. Himadri Tank[1], Mr. Vinay Harsora[2]

[1]M. Tech (CE), Second Year, RK University, Gujrat, India,
[2]Asst.Prof. RK University, Gujrat, India

Abstract: Nowadays, Most Commercial website offers on line services like net banking, on line payment, online shopping for people convenience. Online services require user ID and password for authentication. The peoples use mostly easy to remember password and these passwords are easily stolen by different attackers. There is a need to provide strong password scheme for password, but strong password are hard to remember. To conquer this problem virtual password scheme was introduced. This paper includes a detailed survey on different secure virtual password scheme, phishing attack concept and some techniques to defend against phishing attack through different virtual password scheme.

Index Term: Virtual Password, Secret little function, Phishing attack

I. INTRODUCTION

With the use of online transaction like online payment with credit cards, email conversation, net banking may invite some harmful task. Such online transactions require user identification and subsequent password. Generally, password schemes do not use random number because it is difficult to remember. Transport Layer Security and Secure Sockets Layer are basically cryptographic protocols designed to provide communication security over the internet [1], but it is based on plain text password and user ID. Again these authentication is easily stolen by some attacks including phishing, malicious Trojan horses, shoulder- surfing [13], malware (record the keystrokes) based attacks [15].

A one-time password avoids fixed password scheme since it generates a password which is valid for only one transaction [17]. A one-time password which is valid for only one transaction (OTP) provides security against replay attack because it is not fixed password. A time-synchronization method of OTP method requires the token and the computer system. Both are used to generate numeric version of current time which is then run it through algebraic process, but using OTP it is difficult for user with un-trusted machine [18].

Predefined encryption algorithm are based on conventional cipher and in modern ciphers keys are kept to secret. However, these authentication processes are at a standstill susceptible to known attacks like phishing attack, password stealing Trojan programs and shoulder surfing, key loggers, mobile malware attack.

Another online transaction on the internet referred as online banking is an electronic banking system allows user to access easily to their banking activities such as retrieving an account, history record of online transaction. To access online banking facility users have to register with their websites and need to set up password for user authentication. So, here user must keep their password as secret as being stolen by any adversary.

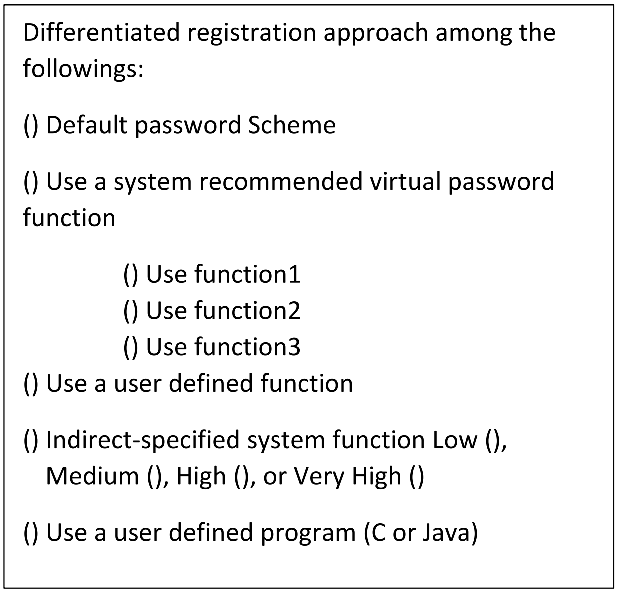
How to crack user password in online environment is not a new thing, but it has become an interesting research area. There are no of attacks like phishing attack which is continual threat, an example of phishing of cooperative commerce techniques used to mislead users, to crack the current web security technologies [3]. A famous method of thieving people password and personal information by capturing users shoulders using hidden camera [16]. A software application, Trojan Redirector [10] was designed to redirect end-users network traffic to a location to where it was not intended. This includes crime ware that changes hosts and other DNS specific information, crime ware browser-mobile objects that may install a network level driver or to redirect users to fraudulent locations [8].

Commercial websites require user ID for registering and password for user authentication. A system verifies a user using the user's unique ID and hidden password which is provided by the user. In this scheme user's ID and password are static, easily remembered, can be stolen by others and then used to crack the user's account. Furthermore, static password cannot take random number since it is difficult to remember. There is a need to change or add some complexity in static password system. There is no of applications to create strong dynamic password generator, virtual password generator, but all are based on conventional encryption algorithm.

A. Virtual Password Scheme:

To deal with above mentioned challenges, by [5] virtual password scheme can be used. A virtual password concept is based on arbitrary string, generated differently each time and further returned to the server for authentication.

A virtual password P is composed of two parts, a fixed alphanumeric X containing hidden parameters given by the user and a function F from S to S, where the S is the letter space which can be used for passwords. So, virtual password P is defined as (X,B) where hidden parameters X=x1,x2,x3,x4….xn ,xi£Z ,Z will be the all password characters and B (F,R) where R=r1,r2,r3,r4….rn. Some human computing is needed to generate virtual password based on after user registration system will pop up function that could use random salt and hidden parameters. In addition to this scheme, a secure method has been proposed with differentiated virtual password scheme [12] including secret security level from lower to higher provide by secret little functions with system recommended function, user specified approach and indirect approach.



Differentiated registration approach among the followings:

() Default password Scheme

() Use a system recommended virtual password function

() Use function1
() Use function2
() Use function3

() Use a user defined function

() Indirect-specified system function Low (), Medium (), High (), or Very High ()

() Use a user defined program (C or Java)

Fig 1. Differentiated Virtual Password Scheme Registration

Above figure shows a differentiated security mechanism for system registration in which the system allows users to choose a registration scheme ranging from the simplest one (default) to a relatively complex one, where a registration scheme includes a way to choose a virtual password function. For user authentication server needs to verify the user if F is a bijective functions. If F is not a bijective function, than the server has to find the user's record from the database on the user's ID, then it computes virtual password and compares it with the one provided by the user.

B. Phishing Attack:

Phishing is a frequent threat that keeps growing to this day. Phishing is the way of acquiring vulnerable information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication and Email spoofing and instant messages are web application in which phishing are typical carried out [3].

Various types of phishing attacks have now been identified like deceptive phishing, Malware – based phishing, Key loggers and Screen loggers, Session Hijacking. With phishing user cannot identify whether the website is fake or real.

Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password credit card, social security or bank account numbers. The website, however is bogus and set up only to steal the information which user enters on the page [21].

II. LITERATURE REVIEW

A lots of techniques have been discovered and defined to defend against phishing attack. The following section gives a brief review of various technique for the same and virtual password scheme.

Through phishing email users are directed to visit a bogus website where they are asked to update sensitive information such as a password, credit card or bank account numbers. Spam Assassin [9] is a computer program released under the Apache License 2.0 used for e-mail spam filtering based on content-matching rules, in which the program can be integrated with the mail server to automatically filter all for a site. It can also be run individual users on their own mailbox and integrates with several programs. These servers are not useful when an attacker hijacks virus-infected PC.

To deal with junk email M. Shahami [14] automated construction of filters to eliminate unwanted mail form the user mail stream using Bayesian classifier, a Bayesian network applied to classification task. They included approximately 20 non-phrasal, domain specific features into their junk e-mail filter.

An application, APS RBL is a real-time black hole list [21] with the use of DNS list to identify hosts which have been coupled with the sending of spam mail. Companies and ISPs can acquire from which IP addresses to obstruct traffic. Unwanted emails can be prevented using multiple black hole services. However blacklists of spamming/phishing mail servers are not useful when an attacker hijacks a PC and specified system require regular administrator.

By [6], a flexible sender validation small fry is a validation practice for sending some kind of fake email address. This system uses unneeded copies of IP data to permit both efficient use by very high-volume mail servers and simple implementation on low to moderate volume mail servers.

A re-encryption scheme [2] that recognize a stronger notion of security and proxy encryption as a method of adding access control to a secure file system.

Trust Bar [11] is a secure user interface add-on to browsers. It identifies the site and the certificate authority. To prevent unwanted pages Trust Bar displays highly visible warning. For defending against phishing websites, they developed some web browser toolbars to inform a user of the reputation and origin of the websites which they are currently visiting. Phishing filters and toolbars are designed to protect the web surfer from collectively engineered phishing scams which try to trick the intended victim into visiting a fraudulent website disguised to look like a valid e-Commerce or banking site.

The Net craft Anti-phishing [20] toolbar is a community-based reporting indicative which gives higher weight to report from expert or highly trusted users. This helps ensure rapid discovery and prevention of newly discovered phishing sites while lowering the potential for false positives.

In [4] a browser extension, password hashing technique that transparently produces a different password for each site, improving web password security and defending against password phishing and other attacks, the authors implemented password hashing. It is an extension of the web browser, a web proxy, or a stand-alone Java Applet.

Diffie-Hellman protocol [7] which is also known as exponential key exchange is one kind of digital encryption for establishing a shared secret over an unsecured communication channel and first published by Whitfield Diffie and martin Hellman in 1976.

One time password [17] is valid for one time login and it protects the password against replay attack. One password is based on approaches like time synchronization and depend on the challenge. The advantage is, it is a dynamic password [18].

In [5] a new way of protecting users from adversary, a virtual password scheme was introduced. This scheme include small amount of human computing for security purpose and can be used for authentication. They have adopted user determine randomized linear generation function. The user hidden parameters and system generated function are collectively formed into virtual password.

Defend against Phishing Attack using virtual password:

The virtual password scheme to protect user from password theft with randomized linear function for phisher where c, a, x1, x2, are unknown. They only know k1, k2, k3…... kn, y1, y2…yn. And this scheme can remove the possibility of multiple attack.

Among differentiated virtual password scheme [12] authors also purposed two other schemes codebook and reference switching. These schemes can defend phishing attack by secret little function. Since each time the system read only virtual password, the phishing attacker could get virtual password but it could not get hidden parameters.

III.CONCLUSION

The survey of this paper makes knowledge about the most aggressive password stealing attack and protection method available for the online network communication. The protection of the password is a critical thing in online system. Using different schemes for virtual password mechanism for online transactions people can prevent their password being stolen. In future we try to implement new mechanism from this survey that makes help to provide security against phishing attack.

IV. REFERENCE

[1] Allen, Dierks and C. " The TLS Protocol Version 1.0 ." *IETF RFC 2246* (Jan.1999).

[2]Ateniese, K. Fu, M. Green, and S. Hohenberger. "Improved proxy re-encryption schemes with applications to secure distributed storage, ." *Proc. 12th Annu. Netw. Distributed Syst. Security Symp.* (2005).

[3]Available http://en.wikiPedia.org/wiki/Phishing

[4] B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. Mitchell. "“Stronger password

authentication using browser extensions," ." *Proc. 14th USENIX Security Symp.* (n.d.).

[5] Chung- Chih Li, Ming Lei, and Susan V. Vrbsky. "Virtual Password Scheme to Protect Passwords Communications ." *ICC '08. IEEE International Conference* (May 2008).

[6] Damiani, S. D. C. di Vimercati, S. Paraboschi, P. Samarati, A. Tironi, and L. Zaniboni. "Spam attacks: P2P to the rescue." *Proc. 13th Int. World Wide Web Conf pp. 358359.* (2004).

[7] Diffie, W. and Hellman. ""New directions in cryptography"." *IEEE Transactions on Information Theory 22 (6): 644–654. doi:10.1109/TIT.1976.1055638.* (1976).

[8] "Government Minister avoids the train over visual data security fears"." (January 2013.).

[9] mason. "filtering with spamAssian." *Hetnet* (2002).

[10] C.Herlley and D. Florencio,"How to log in from internet café without worring about key loggers" in proc SOUPS, 2006

[11] Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler. "SPINS: Security protocols for sensor networks,." *Wirel. Netw. vol. 8, no. 5, pp. 521534* (2002).

[12] Yang Xiao, Senior Member, IEEE, Chung-Chih Li, Ming Lei, and Susan V. Vrbsky. "Differentiated Virtual Passwords, Secret Little Functions, and Codebooks for Protecting Users From Password Theft ." *IEEE SYSTEMS JOURNAL, VOL. 8, NO. 2* (JUNE 2014).

[13] "A PIN-entry method resilient against shoulder-sur_ng, ." *Proc. 11th ACM Conf. Comput. Commun. Security* (2004).

[14]Sahami, S. Dumais, D. Heckerman, and E. Horvitz,. " A Bayesian approach to flter junk e-mail learning for text categorization ." *Proc. Workshop* (May 1998.).

[15] Shimna M. S., Sangeeta P S. "Dynamic password schemes for protecting users from password theft ." *international journal of innovative technology and exploring engineering* (june 2013).

[16] "shoulder-surfing." *Proc. 11th ACM Conf. Comput. Commun. Security,pp. 236245. 22* (2004).

[17] Sivalingam, Lee and K. M. " An e_cient one-time password authentication scheme using a smart card, ." *J. Security Netw., vol. 4, no. 3, pp. 145152* (2009.).

[18] "An efficient one-time password authentication scheme using a smart card, Int. ." *J. Security Netw., vol. 4, no. 3, pp. 145152* (2009).

[19] Whateley, A. Meyer and B. "SpamBayes: Eective open-source, Bayesian based, e-mail classication system ." *Proc. CEAS* (2004).

[20] Antiphishing working group http://antiphishing.org

REVISITED PERFORMANCE ISSUES IN CONCURRENT TRANSACTION EXECUTION IN DISTRIBUTED DATABASE MANAGEMENT SYSTEM

[1]Mrs. Shefali Naik, [2]Dr. Samrat Khanna
[1]Assistant Professor, School of Computer Studies, Ahmedabad University
[2]Prof. & Head-MSc.(IT), Inst. Of Science & Technology for Advanced Studies & Research
Sardar Patel University
Email: [1]Shefali.naik@ahduni.edu.in, [2]sonukhanna@yahoo.com

Abstract – When the database is very large and accessed from remote machines, it is to be partitioned and stored on several machines or sites. For the faster data access, the partitions must be replicated and stored on local machines. It is a difficult task to update and synchronize data in all the replicas. There are various methods available for optimization. In the paper, the various issues related to performance issues of concurrent transaction execution in DDBMS are discussed.

Index Terms-Distributed Database, Partition, Performance issues, Replica, Concurrent transaction

I. INTRODUCTION

The database which is fragmented and stored on different machines is called Distributed Database. Different applications which are using this database access data stored in these fragments from different machines through transactions. Applications request data simultaneously which may result in conflict. Conflicting requirements are taken care by the Database Management System. The simultaneous execution of transaction is called concurrent execution. Without proper concurrency control and integration of data, concurrent execution may result into inconsistent data. Transactions in distributed database require distributed processing which is very difficult to manage. The data which are distributed across various machines are stored in different database management systems, it is called heterogeneous distributed database. In DDBMS, for faster data access, sometimes the fragments are replicated. Since database is distributed, there are some performance issues which need to be resolve for better execution of transactions. These issues are discussed in the paper.

II. PRINCIPLES OF DDBMS

Distributed database works on the following principles[1].

A. Partitioning[1] : Data is distributed through partitions across multiple computers. There are different types of partitioning techniques to divide data across the distributed system. The popular methods of partitioning are horizontal partitioning, vertical partitioning and hybrid partitioning. Partition is also called fragmentation.
B. Replication[1] : The partitioned data are replicated or duplicated and stored across multiple computers for fast access.

Synchronization is required in all the replicas.

C. Transparency at different levels[1] : When data is distributed, full transparent access should be provided at different levels. Full transparent access means that user can write and execute a query without paying any attention to distribution of data, location, partition or replication. Transparency should be provided in the form of Data independence, Network transparency, Replication transparency and Fragmentation transparency.

D. Distributed Query Processing[1] **:** Query processing deals with optimization. It involves designing of algorithms that analyze queries and convert them into a series of data manipulation operations.

E. Distributed Concurrency Control[1] : Concurrency control involves the synchronization of data accesses so that the integrity of the database is maintained.

F. Replication Protocols[1] : If the distributed database is replicated partially or fully, it is necessary to implement protocols that ensure the consistency of the replicas.

G. Heterogeneity[1] : Heterogeneity may occur in various forms in distributed systems such as hardware, network, DBMS, Data models, query languages, transaction management protocols, etc. Representing data with different modeling tools creates heterogeneity because of the inherent expressive powers and limitations of individual data models.

III. DISCUSSION OF DDBMS ISSUES

A. Replica Synchronization[1] : To provide faster data access, the database fragments are replicated on different machines. When data on any one replica is updated, the changes must also be reflected on other replica to provide up-to-date information. It is very difficult to synchronize the replicas.

B. ACID properties : Many of the present time applications are by nature distributed such Web-based applications, E-commerce applications, multimedia applications such as medical imaging, etc. The transaction in Relation Database Management System should satisfy the ACID(Atomicity, Consistency, Isolation, Durability) properties[2]. But in distributed database it is not possible to get all the four together. Eric Brewer [2010] has given the CAP theorem which states that it is impossible for a distributed database management system to provide Consistency, Availability and Partition tolerance simultaneously. i.e., a distributed database management system cannot satisfy all three of these guarantees at the same time. ACID properties also cannot be maintained across partitions; it is required to restore partitions to ensure it.

C. Data stream management[1] : When data comes in free form from the various machines from the internet, it is very difficult to manage through fixed schema. For these types of streamed data, better data stream management is required.

D. Query Optimization[3] : It is very difficult to optimize the join queries which are distributed in nature.

IV. RELATED WORK AND FUTURE SCOPE

M. Ozsu and P. Valduriez state that there are algorithms[1] given for partitioning or fragmentation. In internet-based applications data comes in the form of audio, video, documents and other formats which are called stream data. Real time data comes in the form of stream (unbounded sequence) from internet. These data are distributed across many machines, which are accessed by many users from their own machines.

D. Wang has proposed Cluster-and-Conquer algorithm[4] for optimizing distributed join over database federation with efficiently considering run-time conditions. Cluster-and-Conquer algorithm is motivated from real world observation in which author has proposed to view the whole database federation as clustered system, and provide each cluster of data sources with its cluster mediator. Finally author has implemented the prototype federation system with the proposed architecture and optimization algorithm. The experimental results showed the capabilities and efficiency of Cluster-and-Conquer algorithm and gave the target environment where the algorithm performs better than other related approaches. Currently the prototype system has two levels of mediators, but it is necessary to extend the system in order to support multi-level mediators whenever the environment demands. Another possible extension is to employ this algorithm to other distributed systems, such as distributed databases and grid computing systems. The philosophy of cluster-and-conquer is expected to be useful for large-scale distributed computing environments. So the algorithm can be extended for the processing of other types of operations, like aggregate (such as group-by, max and min), top-K, etc.

R. Taylor proposed a cost model[3] that allows inter-operator parallelism opportunities to be identified within query execution plans. This allows the **response time** of a query to be estimated more accurately. The author has merged two existing centralized optimization algorithms DPccp and IDP1 to create a practically more efficient algorithm IDP1ccp. He proposed the novel **Multilevel optimization algorithm** framework that **combines heuristics with existing centralized optimization algorithms.** The distributed multilevel optimization algorithm (DistML) proposed in this paper uses the idea of distributing the optimization phase across multiple optimization sites in order to fully utilize the available system resources. The future work on this cost model could be done to make it capable of handling pipelining between operators, which means that one operator feeds its output tuples directly into a parent operator when they become available without writing them to disk.

S. blanas has has evaluated the join methods on a 100-node system and shown the unique tradeoffs of these join algorithms[5] in the context of MapReduce. They have also explored how their join algorithms can benefit from certain types of practical preprocessing techniques. The valuable insights obtained from their study can help an optimizer select the appropriate algorithm
based on a few data and manageability characteristics.The proposed methods can be evaluated for multi-way joins, exploring indexing methods to speedup join queries, and designing an optimization module that can automatically select the appropriate join algorithms. Another important future direction is to design new programming models to extend the MapReduce
framework for more advanced analytic techniques.

For computations of cost from the optimization process, the optimizer must consult the data sources involved in an operation to find the cost of that operation. The mentioned analytical process in [6] indicate that, in many cases, especially when the physical database design is known to the optimizer, this query optimization algorithm works very well. But in absence of physical database design, more aggressive optimization techniques must be required.

In paper [7], through the research on query optimization technology, based on a number of optimization algorithms commonly used in distributed query, a new algorithm is designed, and experiments show that this algorithm can significantly reduce the amount of intermediate result data, effectively reduce the network communication cost, to improve the optimization efficiency. As a future work, the algorithm can be extended for distributed file system.

CONCLUSION AND RESEARCH DIRECTIONS

It is very difficult to find an ideal optimum solution for the distributed data. To obtain optimum solution, the cost of network, resources, response time, access time, memory usage, processing time, etc. should be minimized which could be done with the use of better algorithms for different principles of DDBMS, materialized views, on-the fly schema, caching of frequently used data, etc.

REFERENCES

1. M. T. Ozsu, and P. Valduriez, “Book : Principles of Distributed Database Systems, Third Edition, Springer
2. S. Naik, “Book-Concepts of Database Management System”, First Edition, Pearson
3. R. Taylor, “Thesis on Query Optimization for Distributed Database Systems”, University of Oxford, 2010
4. D. Wang, “Thesis on Efficient Query Optimization for Distributed Join in Database Federation”, Worcester Polytechnic Institute, March 2009
5. S. Blanas, J. M. Patel, V. Ercegovac, J. Rao, E. J. Shekita and Y. Tian, “A Comparison of Join Algorithms for Log Processing in MapReduce”, SIGMOD’10, June 6–11, 2010, Indianapolis, Indiana, USA.
6. D. Sukheja and U. Singh, “A Novel Approach of Query Optimization for Distributed Database Systems”, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July, 2011
7. F. Yuanyuan and M. Xifeng, “Distributed Database System Query Optimization Algorithm Research”, IEEE, 2010

A STUDY OF VARIOUS FILTERING TECHNIQUES FOR NOISE REDUCTION OF AN IMAGE

Meha Shah[1] Nidhi Barodawala[2] Heli Amin[3] Kruti Dangarwala[4]
Computer Science & Engineering Dept, SVMIT, Bharuch, India
Email:[1]s_meha_10@yahoo.com,[2]ni_dh_i9@yahoo.co.in,[3]helikamin@yahoo.com
[4]krutidangarwala@gmail.com

Abstract-For digital image processing, the input image is captured using devices such as digital cameras[17]. The captured image contains noise that degrades the quality of image[17]. So we have to remove that noise using appropriate image filtering algorithm. This main objective of this paper is to choose best filtering algorithm by analytically studying the methods and algorithms to reduce the noise from the image.

Keywords-Impulsive noise, Gaussian noise, Noise removal, Linear or nonlinear filter

I. INTRODUCTION:

Noises may be arisen in the capturing and transmission process of the image. The noise is usually divided into Gaussian noise, the balanced noise and the impulse noise. The arisen impulse noises display as light and dark noise pixels under random distribution on the image. This not only corrupts true information of the image, but also seriously affects the visual effects of the image. Therefore, the reduction of impulse noises has important significance to image processing and computer vision analysis[1].

For an image corrupted by noises, we can use linear or nonlinear filter methods to reduce noises. In the frequency domain, the details are high-frequency components of the image, which easily confused with high-frequency noises. Therefore, how to keep the image details and effectively filter random noises is the key to image filtering processing.

The median filter is a nonlinear filter and it has widely used in digital image processing because of its good edge keeping characteristics and reducing impulse noise ability. The median filter is a rankorder filter[1]. Its noise-reducing effects depend on the size and shape of the filtering mask; and its algorithm complexity mainly depends on how to get the median value.

For impulsive noise, the median filter is one of the best. But for Gaussian noise[2], it is less successful. Several researchers have attempted to generalize the standard median filter but such filters are seldom suitable for removing Gaussian noise.

In nonlinear diffusion equations called as an anisotropic diffusion algorithm have been proposed for Gaussian noise removal.

Need of Noise removal Process:

□ To remove dots/noise from an image.

□ Dots can be modeled as impulses (salt-andpepper) or continuously varying (Gaussian noise) can be removed by taking mean or median values of neighboring pixels.

□ Equivalent to low-pass filtering

II.TECHNIQUES:

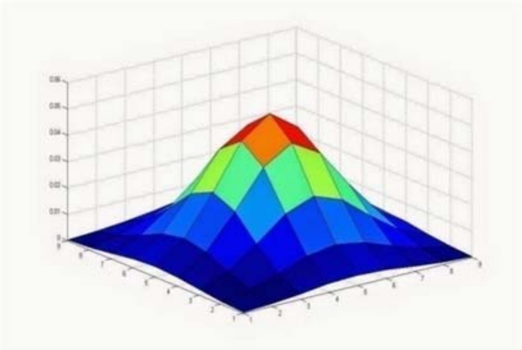
Following are some techniques for noise removing: Noise removal by Gaussian filter

- ➢ Noise removal by Salt and peeper
- ➢ Noise removal by Median filter

A. Gaussian Filter:

Gaussian noise is characterized by adding to each image pixel a value from a zero-mean Gaussian distribution[3]. Gaussian filter smooth noises effectively but blur edges.

The proposed algorithm removes Gaussian noise with edge preservation for low to high Gaussian noise corrupted images.
Gaussian Filter is used to blur the image. It is used to reduce the noise and the image details.



Gaussian Kernel 9x9 size with Standard Deviation
=1.76
Procedural steps for 2D Gaussian filtering:-[15]

1. Design the kernel

1.The formula to design 2D Gaussian Kernel

$$\frac{1}{2\pi\sigma^2}.e^{\frac{-(x^2+y^2)}{2\sigma^2}}$$

2. Let us consider the standard deviation , sigma=0.6 and kernel size=3x3

3.

$$\frac{1}{2\pi\sigma^2}=\frac{1}{2\times 3.14\times 0.6\times 0.6}=\frac{1}{2.2619}$$

4.The width of the kernel is x=3 and the height of the kernel is y=3

$$X=\begin{bmatrix}-1 & 0 & 1\\ -1 & 0 & 1\\ -1 & 0 & 1\end{bmatrix}\ and$$

$$Y=\begin{bmatrix}-1 & -1 & -1\\ 0 & 0 & 0\\ 1 & 1 & 1\end{bmatrix}$$

$$e^{\frac{-(x^2+y^2)}{2\sigma^2}}=\begin{bmatrix}-2.7778 & -1.3889 & -2.7778\\ -1.3889 & 0 & -1.3889\\ -2.7778 & -1.3889 & -2.7779\end{bmatrix}$$

The Gaussian kernel's center part (Here 0.4421) has the highest value and intensity of other pixel decrease as the distance from the center part increases.

Now the Gaussian Kernel =

$$\begin{bmatrix}0.0275 & 0.1102 & 0.0275\\ 0.1102 & 0.4421 & 0.1102\\ 0.0275 & 0.1102 & 0.0275\end{bmatrix}$$

2. Convolve the kernel and the local region in the image

Consider a local region from an Image:

$$\left[\begin{matrix}72 & 68 & 88 & 159\\ 69 & 66 & 87 & 162\\ 70 & 66 & 83 & 161\\ 70 & 66 & 78 & 154\end{matrix}\right]$$

Convolve the selected part and the kernel:

68 88 159 0.0275 0.1102 0.0275

[66 87 162] [0.1102 0.4421 0.1102
66 83 161 0.0275 0.1102 0.0275

1.8692 9.7009 4.3706
= [7.2757 38.4624 17.8585]
1.8142 9.1497 4.4256

Add up the values in the vector:
1.8692+9.7009+4.3706+7.2757+38.4624+17.8585+1.8142+9.1497+4.4256=94.9296

On convolution of the local region and the Gaussian kernel gives the highest intensity value to the center part of the local region(38.4624) and the remaining pixels have less intensity as the distance from the center increases. Sum up the result and store it in the current pixel location(Intensity = 94.9269) of the image.

$$\begin{bmatrix} \square & \square & \square & \square \\ \square & \square & \mathbf{94.9469} & \square \\ \square & \square & \square & \square \\ \square & \square & \square & \square \end{bmatrix}$$

Perform the above operation on all the parts of the region. The final result after Gaussian filter is:

$$\begin{bmatrix} 48.7478 & 59.2645 & 79.7865 & 100.2444 \\ 57.1176 & 69.7512 & 94.9296 & 121.1870 \\ 57.1740 & 68.9526 & 92.2220 & 119.6981 \\ 47.7534 & 59.9750 & 74.1254 & 96.7113 \end{bmatrix}$$

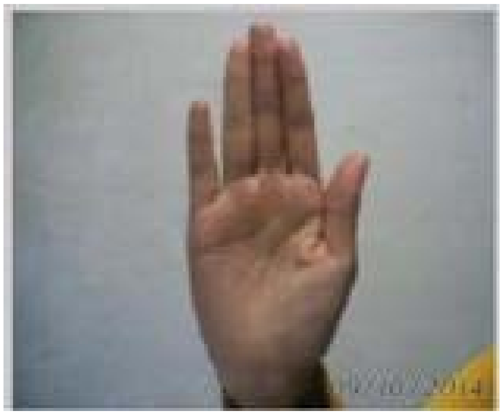


Fig.1 Original image

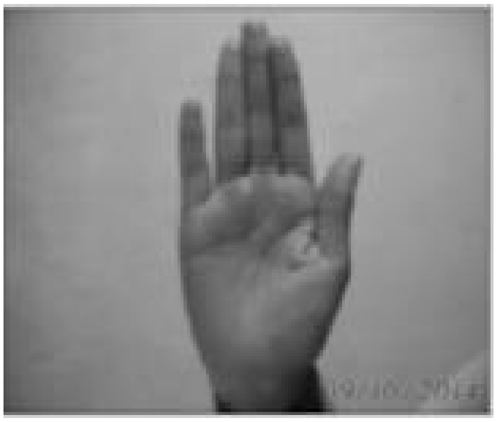


Fig. 2 Image after Gaussian filter

The main **drawback** is the image is blurred after applying.

B. Salt and Pepper Filter:

Many researches have been conducted and numerous algorithms were proposed to remove salt and pepper noise. Among these noise reduction techniques, majority splits the noise removal procedures into preliminarily detection of pixels corrupted by impulse noise followed by filtering[4].

Pixels detected by the noise detector will be considered as noise and shall further be processed in their respective noise reduction scheme[14].

The salt-and-pepper type noise (also Called impulse noise, shot noise or spike noise) is typically caused by Malfunctioning pixel elements in the Camera sensors, faulty memory locations, or timing errors in the digitization process.

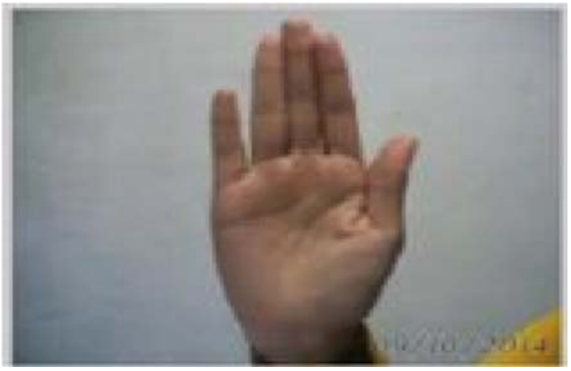


Fig.3 Original image

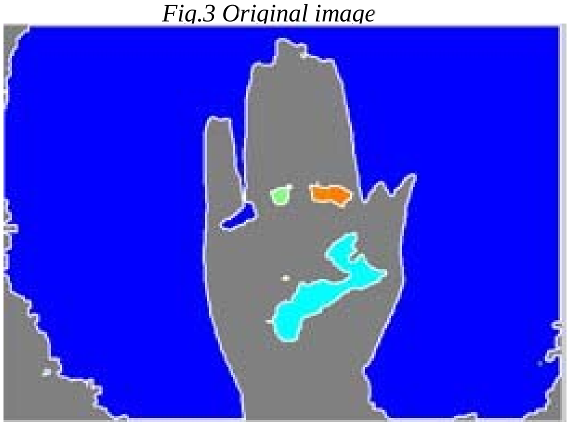


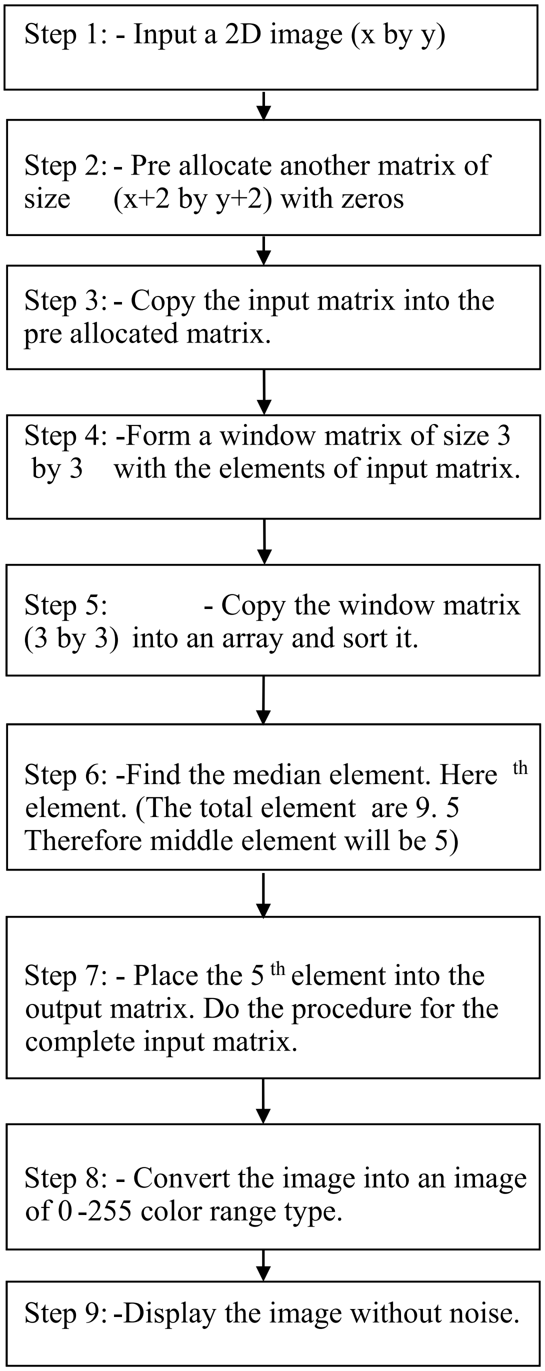
Fig.4 Image after salt & pepper

The **drawback** is that we can see in fig 4 that image is not detected clearly. The edge is detected but not clearly.

C. Median Filter:

The median filtering algorithm has good noisereducing effects, but its time complexity is not desirable. The complexity of the algorithm is decreased to O(N), and the performance of noise reduction has effectively improved[1].

Steps of the improved algorithm are shown as below.



Step 1: - Input a 2D image (x by y)

Step 2: - Pre allocate another matrix of size (x+2 by y+2) with zeros

Step 3: - Copy the input matrix into the pre allocated matrix.

Step 4: -Form a window matrix of size 3 by 3 with the elements of input matrix.

Step 5: - Copy the window matrix (3 by 3) into an array and sort it.

Step 6: -Find the median element. Here th element. (The total element are 9. 5 Therefore middle element will be 5)

Step 7: - Place the 5 th element into the output matrix. Do the procedure for the complete input matrix.

Step 8: - Convert the image into an image of 0 -255 color range type.

Step 9: -Display the image without noise.

The procedural steps for 2D median filtering[13]:

1. Consider the matrix

$$A=\begin{bmatrix}5 & 6 & 9\\ 2 & 5 & 3\\ 8 & 1 & 2\end{bmatrix}$$

2. Now pad the matrix with zeros on all sides

$$A=\begin{bmatrix}0 & 0 & 0 & 0 & 0\\ 0 & 5 & 6 & 9 & 0\\ 0 & 1 & 2 & 3 & 0\\ 0 & 8 & 1 & 2 & 0\\ 0 & 0 & 0 & 0 & 0\end{bmatrix}$$

3. Consider a window matrix of size 3 by 3. The window can be of any size. Starting from matrix A(1,1), place the window.

$$\text{Window}=\begin{bmatrix}0 & 0 & 0\\ 0 & 5 & 6\\ 0 & 5 & 2\end{bmatrix}$$

4. $\text{Window} = \begin{bmatrix}0 & 0 & 0\\ 0 & \enclose{circle}{5} & 6\\ 0 & 5 & 2\end{bmatrix}$

The value to be changed is the middle element[A(2,2)].

5. Sort the window matrix: $\begin{bmatrix}0 & 0 & 0\\ 0 & \enclose{circle}{0} & 2\\ 5 & 5 & 6\end{bmatrix}$

6. After the sorting, the output is placed with a value of 0 at (2,2) pixel position. The value of the output pixel is found using the median of the neighborhood pixels.

7. This procedure is repeated for all the values in the input matrix by sliding the window to next position i.e. A(1,2) and so on.

8. Output matrix is: $\begin{bmatrix}0 & 3 & 0\\ 2 & 5 & 2\\ 0 & 2 & 0\end{bmatrix}$

In this method there is no need of average value of pixels so it is better than other filters.

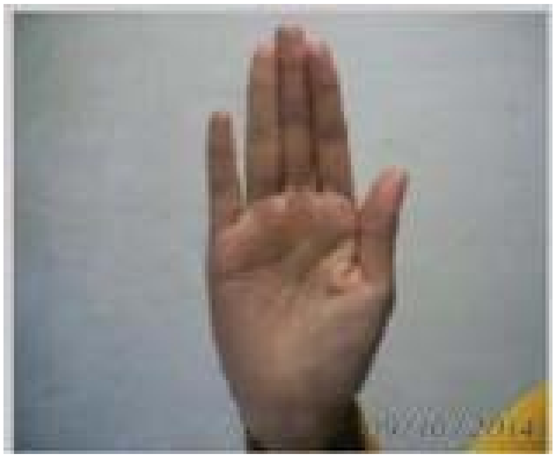


Fig.5 Original image

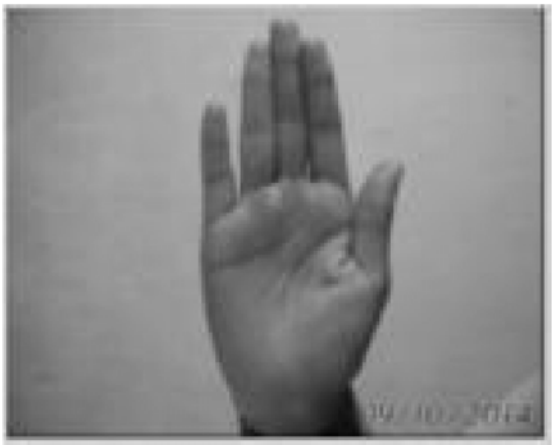


Fig.6 Image after median filter

As we can see that after applying median filter, image is better than above descripted filter.

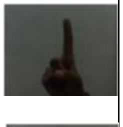
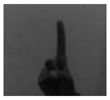
The main **advantage** of this filter is that it gives cleared, sharpened image and edge is detected, also it removes noise better than others.

The **drawback** of this method is it is slower so it is time consuming.

II. CONCLUSION:

As a conclusion, we conclude from above filters that median filter is the best one among all filters. It removes noise perfectly as we can see in resultant image (fig 6). It also detects edges clearly. It also takes median value instead of average values.

For above reasons, we proposed median filter for noise removal of an image.

No.	Methods	Input	Output
1	Gaussian Filtering	 	
2	Median Filtering	  	 
3	SaltPepper Filtering	 	

REFERENCES:

[1] Nayan Patel, Abhishek Shah ,Mayur Mistry, Kruti Dangarwala," A Study of Digital Image Filtering
Techniques in Spatial Image Processing " -(2014)

[2] Youlian Zhu, Cheng Huang ,"An Improved Median Filtering Algorithm for Image Noise Reduction" ,Physics Procedia 25(2012) 609 – 616
[3]V.R.Vijaykumar,P.T.Vanathi, P.Kanagasabapathy,"Fast and Efficient Algorithm to Remove Gaussian Noise in Digital Images"

[4] Roman Garnett, Timothy Huegerich, Charles Chui, "A Universal Noise Removal Algorithm With an Impulse Detector", *Fellow, IEEE*, and Wenjie He, *Member, IEEE*

[5] Tina Gebreyohannes and Dong-Yoon Kim,"Adaptive Noise Reduction Scheme For Salt and
Peeper "

[6] B.Smolkaa, K.N.Plataniotisb, A. Chydzinskia, M. Szczepanskia,A.N.Venetsanopoulosb,K Wojciechowskia,"Self-adaptive algorithm of impulsive noise reduction in color images"

[7] Lin Zhong, Sunghyun Cho, Dimitris Metaxas, Sylvain Paris, Jue Wang, "Handling Noise in Single Image Deblurring using Directional Filter",Rutgers University Adobe Research

[8] Aditi Kalsh and N.S. Garewal ,"Sign Language Recognition for Deaf & Dumb" (2013)

[9] P. V. V .Kishore and P. Rajesh Kumar,"A Model For Real Time Sign Language Recognition System"

[10] S. N. Omkar and M. Monisha, "Sign Language Recognition Using Thinning Algorithm"

[11] S. Nagarajan and T.S.Subashini,"Static Hand Gesture Recognition for Sign Language Alphabets using Edge Oriented Histogram and Multi Class SVM"

[12]"books?id=JeDGn6Wmf1kC&printsec=frontcover&dq=digital+image+processing+by+jayaraman&hl=en&sa=X&ei=HpbUVL2GCcSQuASA4AI&ved=0CB4Q6AEwAA#v=onepage&q=digital% 20 image%20processing%20by%20jayaraman&f=false "

STUDY OF SAND COMPOSITION ON MOULD PROPERTIES AND SELECTION OF TAGUCHI ORTHOGONAL ARRAY FOR DESIGN OF EXPERIMENTS

Dhruval Patel[1*], Prof. Vivek Deshpande[2], Prof. Ela Jha[3], Viral Patel[4]
Snikunj Desai[5], Jay Patel[6]

[1,4,5,6] B.E. 4th Year Students, Mechanical Engg., G H Patel College of Engineering & Technology, V. V. Nagar, Anand, Gujarat, India
[2,3] Asst. Prof. Mechanical Engg., G H Patel College of Engineering & Technology, V. V. Nagar, Anand, Gujarat, India
Email: drp9424@gmail.com[1], vivekdeshpande@gcet.ac.in[2], elajha@gcet.ac.in[3]
viral_patel3590@yahoo.com[4] snikunjdesai13@rediffmail.com[5], jay150,71992@gmail.com [6]

ABSTRACT

The quality of castings in green sand mould is influenced by its properties such as green compression strength, green shear strength, permeability etc. The relations of these properties with the input parameters like sand grains size, shape, binder, clay is complex in nature. Binders play a vital role on green sand mould to enhance specific mould properties. The mould properties such as compression strength, permeability, hardness & shear strength have been studied & comparison have made with different binders. As per the study, for steel casting, we require 3% to 5% moisture content and 7% to 9% clay content respectively. Cause and effect diagram has been used to identify the different caused for casting defects. For optimizing the mould properties, Taguchi parametric design is studied and L9 orthogonal array is selected to find out optimal solution.

Key words: Permeability, Green compression strength, Taguchi parametric design, Cause and effect diagram

1. INTRODUCTION

Casting is one of the important and versatile processes of manufacturing. Its prime purpose is to form solid or hollow objects, parts, etc. of desired shapes, sizes, etc. Incorrect sand condition result in the production of scrap. It is for this reason that majority of foundries today require costly laboratories for controlling existing foundry sands and for testing new sands to discover their foundry suitability. Foundry sand control can only by testing of all the raw materials; sands, binders, and additives prior to the preparation of the sand mix. Sands found in different locations can have wide variations in surface, physical, and chemical characteristics due to environmental, ecological, climatic and geological factors. Different sands have different foundry properties. One cannot therefore be sure of the suitability of a sand for casting a given metal until standard necessary laboratory tests are properly carried out on it.

Permeability is defined by the AFS as the physical property of molded sand, which allows the gases to pass through it. It is determined by measuring the rate of flow of air (2000 cm^3) through the metric standard rammed specimen (Ø50 mm×50 mm in height) under a standard pressure (10 g/cm^2). The amount of clay and moisture content has a significant role in improving the strength and permeability of green sand mould and it should be controlled to get defect free castings. For example, green sand properties for a mould prepared by using a jolt /squeeze machine are water (3-4%), live clay (5.5%) and permeability (80-110) while for the mould prepared by using a high pressure are water (2.5-3.2%), live clay (6-10%) and permeability (80-100) .

Clay (Bentonite) act as a binder, mixes with water to bind the sand particles and can be maintained in the range 5-7% to produce mould with better refractoriness and higher permeability If the clay content is higher in the sand mixture, the permeability is lowered due to fine clay particles occupied in the available spaces between the sand grains.

Water content in the mixture of 1.5% to 8%, activates the clay in the sand, causes the aggregate to develop plasticity and mold strength. Without water addition, no strength would be achieved, as the sand and clay would be just two different dry materials Too little water fails to develop adequate strength and plasticity where sands and clays grains are combined together apart thus the permeability is very poor. The clay adsorbs the water up to a limiting amount. Only the water rigidly held (adsorb) by the clay appears to be effective in developing strength and permeability. The development of bond strength between the grains depends upon on the hydration of clay. The green strength and permeability of a moulding mixture increases with water content up to an optimum value determined by the proportion of clay. Above this value, an additional % of water causes the permeability to diminish due to the increasing of the thickness of the water films. So, the clay becomes soft, lose its bonding power and less stiff and the sand grains are held further apart thus decrease the strength. Therefore, excess moisture must be avoided since it lowers the permeability and increases the chance of a blown casting. At the same time, plasticity and deformation of the mould will occur. Low permeability and green compression strength encourage the entrapment of gases and the washing away of sand by molten metal.

Figure 1 shows the effect of increasing the water content and the comparison between the sand mixtures bonded with 4% and 6% clay on the permeability of the moulding sand.

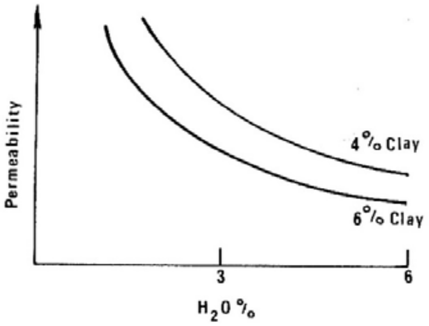


Figure 1: Effect of moisture content and clay on permeability

2. TAGUCHI METHODOLOGY

The Taguchi method involves reducing the variation in a process through robust design of experiments. The Taguchi method was developed by Dr. Genichi Taguchi of Japan who maintained that variation. The experimental design proposed by Taguchi involves using orthogonal arrays to organize the parameters affecting the process and the levels at which they should be varies. This allows for the collection of the necessary data to determine which factors most affect product quality with a minimum amount of experimentation, thus saving time and resources.

2.1 The Taguchi process

- Problem identification

- Brainstorming Session (identify: factors, factor settings, possible interactions, objectives)
- Experimental Design (Choose orthogonal arrays, design experiment)
- Run Experiment-Analyze Results
- Confirmation Runs

2.2 Parameters and level selection:

Cause and effect diagram is constructed as shown in Fig. 2 to identify the casting process parameters that may influence green sand casting defects. The process parameters can be listed in five categories as follows:

- Mould-machine related parameters
- Cast-metal related parameters
- Green-sand-related parameters
- Mould-related parameters
- Shake-out-related parameters

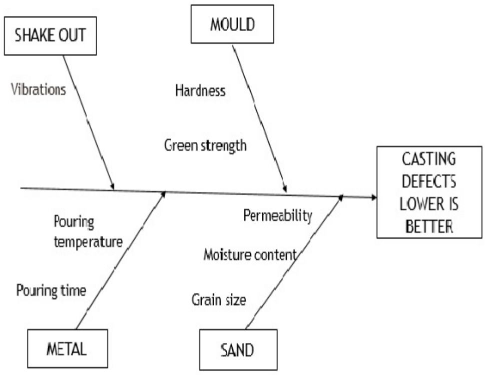


Figure 2: Cause and effect diagram for casting defect

From Fig. 2, we observe that sand related and mould related parameters are selected because, they have major impact on occurrence of selected casting defects. The selected casting process parameters, along with their ranges, are presented in Table 1.

Table 1: Parameters and their levels

Parameters	**Level 1**	**Level 2**	**Level 3**
Silica grains	Type 1	Type 2	Type 3
Clay %	7	8	9
Moisture %	3	4	5

Cause and effect diagram is a quality control tool that enables one to a systematic listing of causes (factors) that may lead to performance deviation or poor quality (effect). It is also called as fish bone diagram because of its appearance. This approach defines the problem clearly and lists all the possible factors contributing to the problem. It must be prepared after a brainstorming session and after gathering the opinion of as many people as possible in order to identify all the relevant factors (or causes). From Figure 2 it is clear that for this case the Signal to Noise ratio required is lower is better.

For lower-is-better characteristic, we use following equation:

$$\frac{S}{N} = -10log10\sum_i \frac{y_i^2}{n} \qquad (1)$$

2.3 Selection of orthogonal array

Once the problem is identified and the factors contributing to the problems are listed in the form of Cause and effect diagram, the next step is to identify the appropriate number of variables and the range (treatment levels) over which these variables would be tested. A design matrix is then constructed between the number of variables and the range over which they are tested. This type of specially designed matrix is called Orthogonal Array (OA).

Table 2: Rules for selecting orthogonal array

(When level and parameters are same)		(When level and parameters are not same)	
Number of Factors	**OA to be Used**	**Number of Factors**	**OA to be Used**
2-4	L_9	2-3	L_4
5-7	L_{27}	4-7	L_8
		8-11	L_{12}
		12-15	L_{16}

A Taguchi OA is denoted by $L_N (S^m)$, where ‘N’ is the number of experiments/test to be conducted, ‘S’ is the levels at which these experiments is to be conducted, ‘m’ is the number of variables/factors chosen in an N×m matrix, whose columns are mutually orthogonal. That is, for any pair of column, all possible combinations of factor levels appear equal number of times. For example, if a process is identified which consists of three variables and each variable has to be run at three different levels, then the actual number of experiments to be conducted will be 27 experiments have to be performed for optimizing a process. This design is called full factorial design. However, in many practical situations it is sufficient to run only a fraction of these full factorial experiments. This helps conserve both time and other valuable resources; therefore, for three factors running at three levels, one may obtain much information by conducting only 9 experiments using L9 (3^3) OA of 9×3 matrix (as given by Taguchi’s standard OA) rather than conducting 27 full factorial experiments as shown in Table 3. The various OAs can be obtained from Taguchi’s standard catalogue which is widely used.

Table 3: L_9 Orthogonal array

Experiment run	Level 1	Level 2	Level 3
1	1	1	3
2	1	2	2
3	1	3	1
4	2	1	2
5	2	2	1
6	2	3	3
7	3	1	1
8	3	2	3
9	3	3	2

CONCLUSION:

For improving the quality of casting we have to select the sand properties in appropriate range. For this we have to optimize the process parameters like silica grains, moisture and clay content. For this the knowledge of sand properties and effects should be known. The authors have investigated the desired ranges of process parameter for improving the quality by Taguchi. The L_9 orthogonal array was selected to carry out the further experimentation.

REFERENCES

[1] Bagchi Tapan P., (1993), Taguchi Methods Explained: Practical Steps to Robust Design, Prentice Hall of India Pvt. Ltd., New Delhi

[2] Beeley P.R, 2001, Foundry Technology, 2nd Edition, Elsevier Ltd.

[3] Brown J.R., Sand and Green Sand. Foseco Ferrous Foundryman’s Handbook, 11thEdition, Elsevier Ltd. (2000)

[4] Heine R.W., Loper C.R.Jr., and Rosenthal P.C., Molding Sands. Principles of Metal Casting. New York: McGraw-Hill Book Company (1967), pp. 86-89.

[5] Vivek Deshpande, “Effect of Machining parameters on Surface roughness in EDM process using Taguchi Technique”, Journal of Industrial Engineering, ISSN: 0970-2555, Vol. V & Issue No. 9, September 2012.

[6] Webster P.D., Refractories, Sands and Binders. Fundamentals of Foundry Technology, Surrey, Portcullis Press, Redhill. (1980)

MODELING AND STRESS ANALYSIS OF COMPOSITE MATERIAL FOR SPUR GEAR UNDER STATIC LOADING CONDITION

Utkarsh.M.Desai1[1], Prof.Dhaval.A.Patel[2]

P.G. Student [1], Associate Professor [2]
Email:[1]desaiutkarsh1992@gmail.com, [2]dapatel.mech@spcevng.ac.in
Department of Mechanical Engineering [1,2]
Sankalchand Patel College of Engineering, Visnagar, Gujarat

Abstract-
Spur gear is the simplest & widely used in power transmission system. A spur Gear is generally subjected to bending stress which causes teeth failure. However it is observed that performance of the spur gear is not satisfactory in certain applications and therefore it is required to explore some alternate materials to improve the performance of the spur gears. Composite materials provide adequate strength with weight reduction and they are emerging as a better alternative for replacing metallic gears. In this work, A metallic gear of Alloy Steel is replaced by the composite gear of 30% Glass filled Poly-ether-ether- Ketone (PEEK). Such Composites material provides much improved mechanical properties such as better strength to weight ratio, more hardness, and hence less chances of failure. In this work, an analysis is made with replacing metallic gear with composite material such as PEEK so as to increase the working life of the gears to improve overall performance of machine. Finally the Modeling of spur gear is carried out using SOLID WORK and bending stress analysis of spur gear is carried out using ANSYS V14.

Keywords- Composite Material, Modeling, Bending stress, Static Load, Finite element analysis.

INTRODUCTION

Composite materials are engineered materials made from two or more constituent materials with significantly different physical or chemical properties which remain separate and distinct on a macroscopic level within the finished structure. The upcoming requirement of power saving and efficiency of mechanical parts during the past few years increased the use of composite materials.

Composite materials are preferred in place where lighter materials are desired or required without sacrificing strength. nowadays, composite materials are used in large volume in various engineering structures including spacecrafts, airplanes,automobiles, boats, sports' equipments, bridges and buildings. Widespread use of composite materials in industry is due to the good characteristics of its strength to density and hardness to density

Parameters	GF 30 PEEK	NICKEL CHROME STEEL
DENSITY	1320 kg/m^3	7800 kg/m^3
MODULUS OF ELASTICITY	4000-4200 Mpa	200000 Mpa
TENSILE STRENGTH	90-100 N/mm^2	413.61 N/mm^2

Table 1. Properties of Materials

BACKGROUND

The spur gear transmits mechanical energy from a prime mover to an output device. The spur gears are used in heavy and low duty mechanical devices. But in this study we have emphasized on the low duty application like Textile machines, Printing press machines, Robotic mechanism etc. The major problems observed with existing metallic Spur gear are

- Existing gear is made of metal component provides poor weight to strength ratio.
- Metallic parts lead to corrosion so need to properly shielded.
- More wear in between the gears so required proper lubrication.
- Gears are getting costly due to increasing metal prices.
- Due to poor weight to strength ratio power losses in gear are higher.

Thus gear needs to be redesigned providing energy saving by weight reduction, providing internal damping, reducing lubrication requirements without increasing cost. Such a scope is provided by application of composite material providing solution to other existing problems in current gears available. Therefore this work is concerned with the replacement of existing metallic gear with composite material gear in order to make it lighter and increasing the efficiency of mechanical machines

LITERATURE REVIEW

R. Yakut et al. The purpose of the paper is to examine the load capacity of PC/ABS spur gears and investigation of gear damage. Further in this study usability of PC/ABS composite plastic material as spur gear was investigated and was defined that PC/ABS gears were tested by applying three different loading at two different numbers of revolutions on the FZG experiment set.The experiment result summarized that the usage of PC/ABS materials brings an advantage in many industrial area because such materials are durable against flame, air, ultraviolet lights and holding lower moister than PA66 GFR 30 materials. The another result of this study was that good operating condition are comprised at low numbers of revolution and the tooth loads. Further the suitable environmental condition must be revolutions and the tooth load for gears. PC/ABS gear should be preferred at low tooth and unwanted high power transmission.[1]

V. Siva Prasad et al. This paper describes design and analysis of spur gear and it is proposed to substitute the metallic gears of sugarcane juice machine with polymer gears to reduce the weight and noise. A virtual model of spur gear was created in PRO-E, Model is imported in ANSYS 10.0 for analysis by applying normal load condition. The main purpose of this paper to analysis the different polymer gears namely nylon, polycarbonate and their viability checked with counterpart metallic gear like as cast iron. Concluding the study using the FEA methodology, it can be proved that the composite gears, if well designed and analysed, will give the useful properties like as a low cost, noise, Weight, vibration and perform its operation similar to the metallic gears. Based on the static analysis Nylon gear are suitable for the application of sugarcane juice machine under limited load condition in comparison with cast iron spur gears.[2]

Vivek Karaveer et al. This paper presents the stress analysis of mating teeth of the spur gear to find maximum contact stress in the gear tooth. The results obtained from finite element analysis are compared with theoretical Hertz equation values. The spur gear are modeled and assembled in ANSYS DESIGN MODELER and stress analysis of Spur gear tooth is done by the ANSYS 14.5 software. It was found that the results from both Hertz equation and Finite Element Analysis are comparable. From the deformation pattern of steel and grey cast iron, it could be concluded that difference between the maximum values of steel and grey CI gear deformation is very less.[3]

Mahebub Vohra et al. In this paper, Metallic material Cast iron and Non Metallic material Nylon are investigated. The stress analysis of the lathe machine headstock gear box are analyzed by finite element analysis. Analytical bending stress is calculate by two formula Lewis formula and AGMA formula. Analytical results is compared with the finite element method result for validation. Concluding the study, we observed that finite element method software ANSYS have values of stress distribution were in good agreement with the theoretical results. Besides non metallic material can be used instead of metallic material because non metallic material provide extra benefits like as less cost, self lubricating, low noise, low vibration and easy manufacturing.[4]

M. Patil et al. The objective of this paper is to study the free vibration behavior of composite spur gear using finite element method which is also known as first order shear deformation plate theory (FSDT). The finite element analysis has been carried out for composite gear as a 4 nodded and 8 nodded quadrilateral element with each nodes has five degree of freedom. Finite element formulation of composite gear is modeled and coded using MATLAB. Based on the numerical analysis which is carried out for of spur gear the following important conclusion can be drawn. The developed MATLAB code is validated with the available result and it can be concluded that the present FE code result are in good agreement with those of reference. Fundamental frequencies obtained for composite spur gear using MATLAB are presented. It is found that natural frequency increases with increase in fiber orientation.[5]

Nitin Kapoor et al. In this paper the parametric model of differential gear box is developed using some parameters i.e. (number of teeth, Pressure angle, helix angle, tooth thickness, module) in CATIA-V5 and weight analysis of differential gear box for different material (aluminium alloy, alloy steel, cast iron, Glass filled Polyamide) under static loading condition using FEA. The case study shows that the composite material can be used effectively in place of metallic material because the weight of Glass filled Polyamide composite material of differential is reduced by 60% Comparing with the traditional materials (Aluminium alloy, Alloy Steel, Cast iron). So, we conclude that Glass filled Polyamide Composite material is selected as a best material for differential gear box.[6]

A.D. Dighe et al. In this study the comparative performance spur gear of 30% Glass filled PA66 and 30% Glass filled PEEK was investigated at different torque and speed. Wear test of the spur gear pairs and the experiment spur gear tooth were performed on a FZG test machine. A weight loss is measured by 0.0001g sensitive weighing machine and the tooth temperature of gear is measured by Impact infrared thermometer. After summarized the experimental result of PA66 GF30 gears and PEEK GF30 gears are at different torque and speeds. The tooth temperature increases with increase in torque and increased temperature resulted into thermal softening of gear tooth which further increases specific wear rate. The comparative results of PA66 GF30 and PEEK GF30 gears show that the specific wear rate of PA66 GF30 is much higher than PEEK GF30 at all torque and speeds. Therefore the torque transmission capacity of PEEK GF30 is higher than PA66 GF30.[7]

Pradeep Kumar singh et al. In this paper using ANSYS workbench software, bending stress, contact stress and static load on the tooth of spur gear drive is found. The Hertz theory and Lewis formula also are used for theoretical calculation of contact stress and bending stress of spur gear. We observed that Theoretically results obtained by Lewis formula and Hertz equation are comparable with finite element analysis of spur gear, keeping in mind the comparison we can conclude that the finite element analytical result can be better as a problem solving software and used for other analyzing purpose.[8]

MODELING OF THE SPUR GEAR

By the design calculation, the modeling of the spur gear is done using SOLID WORK premium 2013.

The input parameter for modeling of spur gear are given in Table 2.

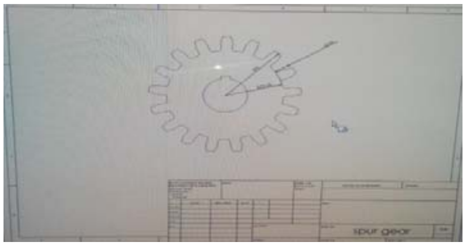
Description	Symbol	Values
Number of teeth	Z	17
Pressure angle	α	20°
Module	m	10mm
Pitch circle diameter	d	170mm
Face width	b	100mm

Addendum circle dia.	d_a	190mm
Dedendum circle dia.	d_f	145mm

Table 2. Geometry of spur gear

SOLID MODEL OF SPUR GEAR

FIG 1. 2-D Part design of Spur Gear



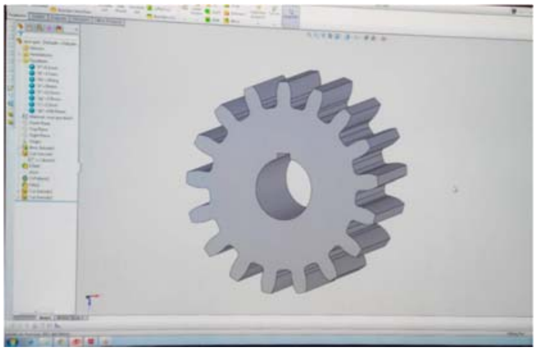


Fig 2. Part design of Spur Gear

FINITE ELEMENT ANALYSIS OF SPUR GEAR

Bending stress of spur gear teeth is generally calculated by analytically and finite element method. In this chapter, static finite element method is applied on the spur gear teeth for a different material of a spur gear. Analytical bending stress is calculated by AGMA formula. Analytical result is compared with the finite element method result for validation

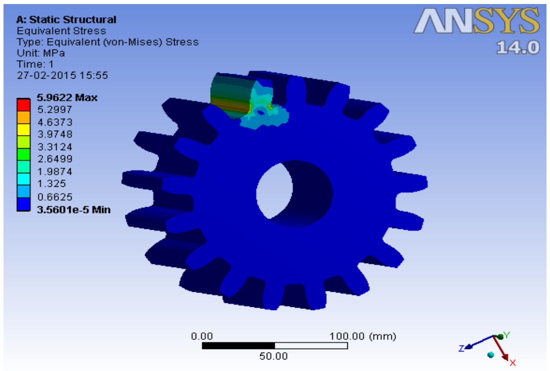


Fig 3. von-Mises stress for GF 30 PEEK

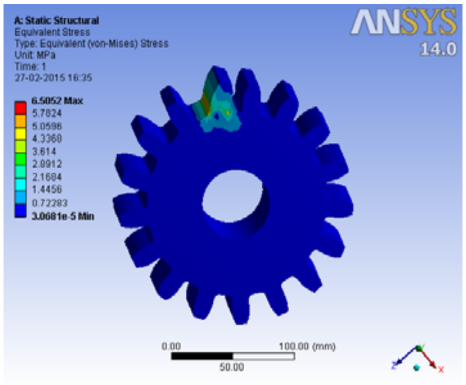


Fig 4. von-Mises stress for ALLOY STEEL

RESULT

Material	Maximum stress induced(MPa)	
	Analytical Procedure	FEM Procedure
Alloy Steel	2.77	6.5052
GF 30 PEEK	2.77	5.9622

CONCLUSION

The objective of current work is to replace the alloy steel spur gear with GF 30 PEEK composite spur gear. For that, analytical and finite element method are applied for determining bending stress of gear tooth. The obtained FEA result is compared with the analytical result and found that both result are comparable. Result shows that by stress analysis the strength of the GF 30 PEEK spur gear is more when compared with alloy steel spur gear.

Also the density of the GF 30 PEEK is very less when compared with alloy steel. So we can conclude that the alloy steel spur gear canbe replaced by GF 30 PEEK(composite) spur gear due to its high strength, low weight and damping characteristics.

REFERENCES

[1] R. Yakut, H. Duzcukoglu, M. T. Demirci, " The load capacity of PC/ABS spur gears and investigation of gear damage", Archives of Materials science and Engineering, November 2009, 40/1, page 41-46.

[2] V. Siva Prasad, Syed Altaf Hussain, V. Pandurangadu, K. PalaniKumar, " Modeling and Analysis of spur gear for Sugarcane Juice Machine under Static Load Condition by Using FEA",July-Aug 2012,International Journal of Modern Engineering Research,Vol-2/4, pp-2862-2866.

[3] Vivek KaraveerȦ*, Ashish MogrekarȦ and T. Preman Reynold JosephȦ, " Modelling and Finite Element Analysis of Spur Gear", Dec 2013, International Journal of Current Engineering and Technology, Vol 3.

[4] Mahebub Vohra, Prof. Kevin Vyas, "Comparative Finite Element Analysis of Metallic and non Metallic spur gear", May-June 2014, IOSR Journal of Mechanical and Civil Engineering, Vol-11/3,pp- 136-145.

[5] M. Patil, S.Herakal, S. B. Kerur, "Dynamic Analysis of Composite spur gear", May- 2014, Proceeedings of 3rd IRF International Conference.

[6] Nitin Kapoor, Pradeep Kumar, Rahul Garg and Ram Bhool, " Parametric Modeling and Weight Analysis of Glass Filled Polyamide Composite Differential Gearbox", June-2014, International Journal of Science, Engineering and Technology Research, Vol-3/6

[7] A. D. Dighe, A. K. Mishra, V. D. Wakchaure," Investigation of Wear Resistance and Torque Transmission Capacity of Glass Filled Polyamide and PEEK composite spur gears", Feb-2014, International Journal of Engineering and Advance Technology, Vol-3/3.

[8] Pradeep Kumar Singh, M. Gautam, Gangasagar and Shyam Bihari Lal," July-2014, International Journal of Mechanical Engineering and Robotics Research, Vol-3.

CRYPTOSCANF: CRYPTOSYSTEM USING CFG

[1]Aishwarya R Parab, [2]Celroy A Ratos, [3]Fiola Carvalho, [4]R. Nageshwar,
[5]Shambhavi S Paradkar
Department of computer engineering, Don Bosco College of engineering, Goa
Email:[1]aishwaryaparab94@gmail.com , [2]celroyratos@gmail.com , [3]fiolacarvalho@gamil.com,
[4]r.nagesh21@gmail.com, [5]paradkar34@gmail.com

Abstract— There is no theoretical study which proves that, given a set of strings from a language how difficult it is to generate another string which belongs to the same language. The fascinating property of CFG is that it is hard to identify the grammar given only the strings generated by it, however it is easy to generate and validate strings from a given grammar.

Due to this property of CFG the idea is to develop a CFG based cryptosystem to provide security for text files. This cryptosystem is a symmetric key encryption technique which consists of various levels of encryption and decryption at sender and receiver side.

***Index Terms*— grammar, cryptosystem, symmetric, CFG, encryption, decryption.**

I. INTRODUCTION

Data security is a challenging issue of data communications today that touches many areas including secure communication channel, strong data encryption technique and trusted third party to maintain the database. The rapid development in information technology, the secure transmission of confidential data herewith gets a great deal of attention. The conventional methods of encryption can only maintain the data security. The information could be accessed by the unauthorized user for malicious purpose. Therefore, it is necessary to apply effective encryption/decryption methods to enhance data security Strong cryptography or cryptographically strong is general terms applied to cryptographic systems or components that are considered highly resistant to cryptanalysis.

Transmission of sensitive data over the communication channel have emphasized the need for fast and secure digital communication network to achieve the requirements for secrecy, integrity and non-reproduction of exchanged information. Cryptography provides a method for securing and authenticating the transmission of information over secure channels. It enables us to store sensitive information or transmit it across insecure network so that unauthorized persons cannot read it.

Cryptography refers to encryption, the process of converting ordinary information (plaintext) into unintelligible cipher text Decryption is the reverse, moving from unintelligible cipher text to plaintext. A cipher is a pair of algorithms which creates the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and, in each instance; by a key .This is a secret parameter for a specific message exchange context. Keys are important, as ciphers without variable keys are trivially breakable and therefore less than useful for most purposes. Historically, ciphers were often used directly for encryption or decryption, without additional procedures such as authentication or integrity checks.

Cryptography is the methods that allow information to be sent in a secure from in such a way that the only receiver able to retrieve this information. Presently continuous researches on the new cryptographic algorithms are going on. However, it is a very difficult to find out the specific algorithm, because we have

already known that they must consider many factors like: security, the features of algorithm, the time complexity and space complexity.

II. GRAMMAR

A. *Context-Free Grammars*

Many cryptographic algorithms use one-way functions to provide their security against adversaries, but still be useful for authorized parties. A one-way function is a function that given x, it is easy to find f(x). However, given f(x) it is hard to find x. An algorithm that uses context free grammars is proposed in this paper

A context-free grammar (CFG) is a set of recursive rewriting rules (or *productions*) used to generate patterns of strings.

A CFG consists of the following components:

- a set of *terminal symbols*, which are the characters of the alphabet that appear in the strings generated by the grammar.
- a set of *nonterminal symbols*, which are placeholders for patterns of terminal symbols that can be generated by the nonterminal symbols.
- a set of *productions*, which are rules for replacing (or rewriting) nonterminal symbols (on the left side of the production) in a string with other nonterminal or terminal symbols (on the right side of the production).
- a *start symbol*, which is a special nonterminal symbol that appears in the initial string generated by the grammar.

Context-free grammars are strictly more powerful than regular expressions.

- Any language that can be generated using regular expressions can be generated by a context-free grammar.
- There are languages that can be generated by a context-free grammar that cannot be generated by any regular expression.

As a corollary, CFGs are strictly more powerful than DFAs and NDFAs.

III. CURRENT SYSTEM

The most straight-forward attack on an encrypted message is simply to attempt to decrypt the message with every possible key. Most of these attempts will fail. But one might work. At which point you can decrypt the message.

Most encryption algorithms can be defeated by using a combination of sophisticated mathematics and computing power. The results are that many encrypted messages can be deciphered without knowing the key. A skilled cryptanalyst can sometimes decipher encrypted text without even knowing the encryption algorithm.

AES is a new cryptographic algorithm that can be used to protect electronic data. Specifically, AES is an iterative, symmetric-key block cipher that can use keys of 128, 192, and 256 bits, and encrypts and decrypts data in blocks of 128 bits (16 bytes). Unlike public-key ciphers, which use a pair of keys, symmetric-key ciphers use the same key to encrypt and decrypt data. Encrypted data returned by block ciphers have the same number of bits that the input data had. Iterative ciphers use a loop structure that repeatedly performs permutations and substitutions of the input data.

AES is the successor to the older Data Encryption Standard (DES).The AES algorithm is based on permutations and substitutions. Permutations are rearrangements of data, and substitutions replace one unit of data with another. AES performs permutations and substitutions using several different techniques

The AES encryption routine begins by copying the 16-byte input array into a 4×4 byte matrix named State. The encryption algorithm performs a preliminary processing step that's called AddRoundKey in the specification.

AddRoundKey performs a byte-by-byte XOR operation on the State matrix using the first four rows of the key schedule, and XORs input State[r,c] with round keys table w[c,r].

The main loop of the AES encryption algorithm performs four different operations on the State matrix, called Sub Bytes, Shift Rows, Mix Columns, and AddRoundKey in the specification. The AddRoundKey operation is the same as the preliminary Add Round Key except that each time AddRoundKey is called; the next four rows of the key schedule are used. The SubBytes routine is a substitution operation that takes each byte in the State matrix and substitutes a new byte determined by the Sbox table. ShiftRows is a permutation operation that rotates bytes in the State matrix to the left. The Mix Columns operation is a substitution operation that is the trickiest part of the AES algorithm to understand. It replaces each byte with the result of mathematical field additions and multiplications of values in the byte's column.

The addition and multiplication are special mathematical field operations, not the usual addition and multiplication on integers.

The four operations SubBytes, ShiftRows, MixColumns, and AddRoundKey are called inside a loop that executes Nr times—the number of rounds for a given key size, less 1. The number of rounds that the encryption algorithm uses is 10, 12, or 14 and depends on whether the seed key size is 128, 192, or 256 bits.

The new AES will certainly become the de facto standard for encrypting all forms of electronic information, replacing DES. AES-encrypted data is unbreakable in the sense that no known cryptanalysis attack can decrypt the AES cipher text without using a brute-force search through all possible 256-bit keys.

IV. PROPOSED SYSTEM

The algorithm makes cryptanalysis even more difficult because of the use of "Random Number Generator" function which further decides order of encryption rounds and keys to be used to encrypt the plain text. This eliminates the overhead of defining a fixed key by the user and makes algorithm secure also. With secret key cryptography, a single key is used for both encryption and decryption. The key selection mechanism and the encoding methodology express the efficiency of the cipher text generated.

Context free grammars present the desirable cryptographic property that it is easy to generate and validate strings from a given grammar; however it is hard to identify a grammar given only the strings generated by it. The project aims at developing a CFG-based cryptosystem that will encrypt a text file to protect from various security attacks.

This cryptosystem will use a symmetric algorithm that will have a secret key. The text file will be converted into a cipher text which will be sent to the receiver who will decrypt it.

```
Procedure Key Generation ()
Input: text
Output: secret key
Begin
Enter text
Generate secret key
End
```

Figure 1: Algorithm for key generation

```
Procedure Encryption ()
Input: plain text file
Output: cipher text
Begin
Key stuffing in plain text file
Reassigning ASCII
Count the number of characters in the text file
If c mod 16= =0
Generation of matrices
Generate reverse productions
Generate ASCII and binary values
Stuffing of the bits
Else
Stuff space characters
Generate cipher text
End
```

Figure 2: Algorithm for encryption

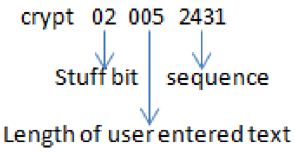
```
Procedure decryption ()
Input: cipher text, secret key
Output: plain text file
Begin
Generate binary
Unpacking the bits
Generate ASCII values
Generate reverse productions
Reverse even odd method
Generate matrices
Key extraction
Key matching
If secret key = = key in text file

Display plain text
Else
Display garbage value
End
```

Figure 3: Algorithm for decryption

Considering an example:
Plain text file: this is the text to be encrypted
User entered text: crypt
Generated key (secret key): crypt020052431
The first level is **KEY GENERATION** where the following processes will occur:
-user will enter text
-the secret key will be generated

The secret key is divided into 4 parts



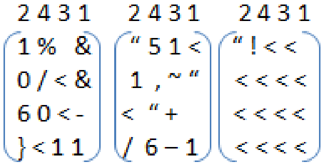
02 in the secret key indicates after how many places to stuff the key, 005 is the length of the user entered text, 2431 is he matrix sequence which is randomly generated.

The next level is **ENCODE** where the following processes will occur:
-The user will input the text file
-Stuffing of the key into the file
-Reassigning ASCII values
-count the number of characters in the text file
-generate 4 X 4 matrices

After stuffing the key we get:
Thcisr iys pa ttext to be encrypted
The algorithm reassigns the ASCII values to generate the following string:
1% &0/<&60<-}<11”51<1,~”<”+ /6-1”!

It will then count the number of characters in the text file
Let ‘c’ be the count
c = 34
Now compute c mod 16
34 mod 16 = 2
16-2=14
Thus, 14 space characters will be stuffed in the text file

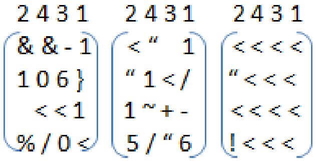
The next step is to generate the 4 x 4 matrices:



2	4	3	1	2	4	3	1	2	4	3	1
1	%		&	“	5	1	<	“	!	<	<
0	/	<	&	1	,	~	“	<	<	<	<
6	0	<	-	<	“	+		<	<	<	<
}	<	1	1	/	6	–	1	<	<	<	<

(Note: “<“ is used to indicate the stuffed space characters in the above matrices just for understanding)

Shuffling of matrices:



2	4	3	1	2	4	3	1	2	4	3	1
&	&	-	1	<	“		1	<	<	<	<
1	0	6	}	“	1	<	/	“	<	<	<
	<	<	1	1	~	+	-	<	<	<	<
%	/	0	<	5	/	“	6	!	<	<	<

Hence we get the string:
1}1<&1
%-6<0&0</1/-6<”15<+””1~/<<<<<”<!<<<<<<
<<

The third level is the **ENCRYPT** level which begins by generating reverse productions using context free grammar (CFG)

1}1<&1 % **-6<0&0</** **1/-6<”15**
A1->%1 A2 } A4->/- A5 <6 A7->51
A8 1/
A2->11 A3 &< A5->0< A6 &0
A8->”-A9<6
A3->E A6->E A9->E

<+””1~/ **<<<<<”<!**
<<<<<<<<
A10->/ A11~< A13->!<A14<<
A16-><<A17<<
A11->1+ A12 “” A14->”< A15<<
A17->< < A18<<

A12->E A15->E A18->E

After eliminating the non-terminals we get the string:
%1
}11&</-<60<&0511/”-<6/~<1+”””!<<<”<<<<<<
<<<<<<

The algorithm then generates the ASCII and binary values of each character in the text file.

After stuffing of the bits we get:
0110001001000001111110100110001001100011010011000111100101011010011110010110110001100000101111001010011010110000101100010011000110101111101000100101101101111000011011010100000011111101011110000110001101010111010001010100010101111000011110010111100001000100011110000111100001111001011110000111100101111001011110010111100101111000011111000

This file is then converted to the cipher text:
bAúbcLyZylayMabc_D¶ðÚ úðÆ®ŠŠðòðˆððò ðòòòòð

This cipher text file will then be sent to the receiver who will decrypt it using the same secret key.
The decryption process consists of the **DECRYPT** and the **DECODE** level which is exactly opposite to encryption except that key matching will occur at the end of the algorithm. If the key is matched only then the plain text will be displayed to the receiver.

V. DESIGN

The flowcharts explain the flow of the algorithm and its different levels of processing, both for encryption and decryption.

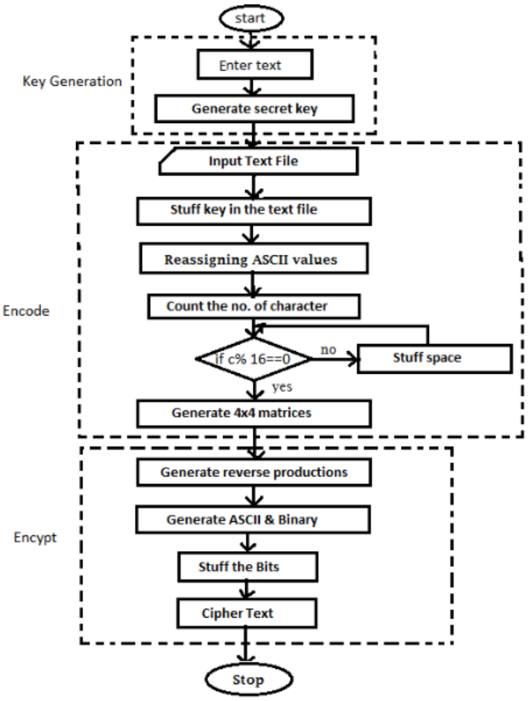


Figure 4: Flowchart for Encryption

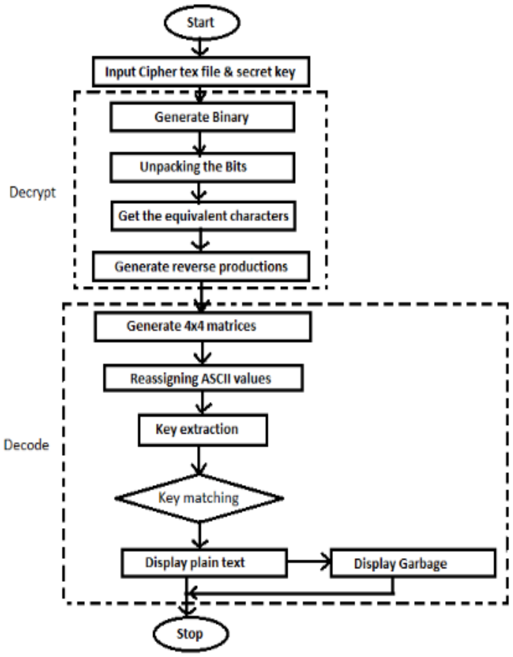


Figure 5: Flowchart of Decryption

VI. SECURITY ATTACKS

Brute force

In cryptography, a brute-force attack, or exhaustive key search, is a cryptanalytic attack that can, in theory, be used against any encrypted data. Such an attack is not possible on our algorithm because of two reasons firstly, since we are using context free grammar it is very easy to generate productions but very difficult to get back the grammar. Secondly, we are using 128 bit key so it will require 2^{128} combinations which is a very big number for the attacker to try.

Cryptanalysis

Most encryption algorithms can be defeated by using a combination of sophisticated mathematics and computing power. The results are that many encrypted messages can be deciphered without knowing the key. A skilled cryptanalyst can sometimes decipher encrypted text without even knowing the encryption algorithm.

A cryptanalytic attack can have two possible goals. The cryptanalyst might have ciphertext and want to discover the plaintext, or the cryptanalyst might have ciphertext and want to discover the encryption key that was used to encrypt the message. The following attacks are commonly used when the encryption algorithm is known. These may be applied to encrypted files or Internet traffic:

Known Plaintext Attack

The goal of a known plaintext attack is to determine the cryptographic key and possibly the algorithm which can then be used to decrypt other messages. Since we are using random key generation algorithm every time the key will be different therefore the attacker won't be able to determine the key.

VII. Conclusion

A powerful cryptosystem has been proposed in this paper. The protocol discussed provides security without requiring additional layer of encryption like SSL. The protocol's use of context free grammar provides its security.

The salient features of the algorithm include no large overheads, user friendliness and independent of any other cryptographic protocol. The described cryptosystem makes use of interesting issues regarding context free grammars that until now have only been used to design programming languages. It's desirable cryptographic property that it is easy to generate and validate strings from a given grammar but it is hard to identify the grammar given only the strings generated by it. The proposed system does not rely on any other cryptographic protocols. This paper presents and analyzes the protocol with respect to its robustness against malicious attacks.

Acknowledgment

The authors are grateful to the anonymous reviewers for their valuable advices. The authors also wish to express their thankfulness to Prof. Manisha G. Fal Dessai and Prof. Amey Kerkar for their invaluable suggestions.

References

[1] Abhishek Singh, Andre L M dos Santos, "*Context Free Grammar for the Generation of a One Time Authentication Identity*"

[2] Abhishek Singh, Andre L M dos Santos, "*Grammar Based Off line Generation of Disposable*
Credit Card Numbers"

TEXTBOOK

1. Cryptography and Network security 4th ed. William Stallings PEA, ISBN:978-81-7758-774-6.

SECURING SINGLE SIGN-ON MECHANISM

[1]Yash Kedia [2]Amit Agrawal, [3]K. Chandrasekaran
Department of Computer Science& Engineering, NITK, Surathkal, Mangalore, India
Email:[1]yash.kedia2694@gmail.com, [2]amitagrawal1612@gmail.com, [3]kchnitk@ieee.org

Abstract- Nowadays the importance of authentication has increased for accessing your accounts registered for various applications on the internet. Due to increase in popularity of internet, people have started using internet for various purposes such as social networking, banking, e-commerce and many more activities in masses. The Single Sign-On (SSO) technology is increasing in demand as it is a benevolence for the users requiring multiple accounts. SSO has a schema with incorporated one-password based confirmation component at SSO server and local verification and approval at application's side. These activities require highly secure transmission due to involvement of confidential information. The main vulnerability point in this framework is authentication at the centralized server. This paper intends to propose a model which will reduce the vulnerability to maximum extent. This model merges the concepts of TPV (Third Party Verification), Diffie-Hellman key exchange and centralized authentication.

Keywords- SSO, Security and Third Party Verification

I. INTRODUCTION

A web service is a business application, which has a unique address on the Internet that can be accessed globally. World is shifting towards the use of internet for every need possible, so for these purposes one needs to authenticate himself on N number of web portals which can be stressful as remembering multiple strong passwords is not a piece of cake. Single sign-on (SSO) is a system whereby a solitary activity of client validation and approval can allow a client to get to all the web administrations where he has entry in all actuality as a user, without the necessity of giving his certifications once more.Thus Single Sign-On minimizes the effort of remembering multiple login credentials, a significant part of frameworks failure and is hence exceedingly alluring.

With the increase in number of users on web portals, the number of threats are also increasing which reduces the efficiency of the system and in some cases even results in loss of confidential data and wealth in case of financial transactions, thus increasing the vulnerability of SSO systems. So to secure the web services, we need to identify a mechanism which is least susceptible to attacks. Authentication is required to access the web services that are secure in which the user needs to provide identification. The primary concern after valid authentication is authorization. Authorization is used to establish connections between clients and web services providing them the permissions needed to perform various transactions.

SSO is the new development in this scenario to solve the work of multiple authentications and reducing the risk of attack on each web service authentication. This paper tends to give such a model which will provide secure transmission of user credentials at the centralized master level resulting in secure transmission of user's confidential data. This model will be able to detect threats such as man in the middle attack (MIM). This paper focuses on the secure establishment of connection between valid client and server and detecting any unauthorized attacker in the middle. After successful authentication, a service token will be generated for each session, which when terminated can't be accessed to access any information.

The paper is organized in the form of following sections. Section II consists of related work. Section III consists of proposed model. Section IV deals with attacks and system analysis. The subsequent sections consists of conclusion and references.

II. RELATED WORK

SSO is being developed and researched to provide ways of securing web services. Microsoft's Passport convention was the first endeavor at making a Web SSO framework, but it was never substantially put in use by non-Microsoft vendors. The adoption of this protocol was hindered as many security flaws were identified in it. Passport is by all account not the only Web SSO convention that had vulnerabilities. MDSSO alludes to the situation where SSO happens between security spaces worked by dissimilar associations. Rather than MDSSO electronic frameworks, some Web SSO frameworks give SSO inside a solitary association. They are called Web Initial Sign-On (WebISO) frameworks. WebISO frameworks normally give a web based part to an association's current single sign-on SSO schema, which in present state can't help online confirmation. Likewise remarkable is an alternate Internet2 venture called Shibboleth. Shibboleth handles both the online MDSSO and SSO inside an association, and implements SAML v1.1 [17].

SAML (Security Assertion Markup Language) is a standard that encourages the trade of security data. SAML is a XML-based system which empowers diverse associations (with distinctive security spaces) to safely trade validation and approval data. Numerous SSO administration suppliers like Google, Webex support SAML. The standard has risen as the go-to SSO convention for such applications. SAML got on rapidly with cloud-based suppliers, for example, Google, Webex and once conventional organizations, for example, IBM and Microsoft advocated SAML, it turned into the go-to SSO convention for some applications [16].

Kerberos based- Initial sign- on prompts the client to give username and password, which on check will deliver a ticket-granting ticket (TGT). Extra programming applications obliging validation, for example, email web administrations like yahoo mail utilize the ticket-granting ticket to claim their administration tickets, giving the client's credentials to the mailserver, without inciting the client to get re-authorized [4].

Smart card based- Firstly, it approaches the client for the smart card. Other web benefits likewise utilize this card, without hinting the client to re-enter details. It deals with the qualifications of the client put away on the smart card [4].

III. PROPOSED MODEL

The primary idea is to articulate a SSO model that provides credential management for all the web services on single server. The process of authentication in this model is built on password authentication scheme. This gives the benefits of simple usability in most web services that still use passwords for authentication.

Model Components
Following are the participants which make up our model:

1. Client (C): The web browser of the user acts as client on the behalf of user to access web services.

2. Centralized Authentication Server (AS): It is responsible for handling authentication and authorization services.

3. Web Service Provider (WS): It is the web service provider that requires client authentication before giving the client authorization.

4. Third Party (TP): It is responsible for generating random prime number P and random base G for securing the transmission.

The SSO model presented in this paper is the summation of the following steps:

1. The client requests for a web service (WS).

2. This service is redirected to an authentication service (AS).

3. AS requests client for username (UID) for validation of existence of such user in Database.

4. Client sends the UID for verification.

5. After successful verification, AS invokes Third Party (TP) and publically transports a dummy value of P and G.

6. TP sends P and G to AS and C.

7. C and AS generate random number and create the secret keys.

8. AS requests for password from C.

9. Then C sends H_1 -> password hashed with the secret key for validation.

10. After successful verification of H_1 with the local copy H_2 of AS, it authenticates C to WS and sends P and G to WS.

11. Then the connection is established between C and WS, and authorization privileges are provided to C accordingly by WS. The data is exchanged in encrypted form with the help of secret key.

IV. ANALYSIS OF THE SYSTEM

There are certain threats to user's confidential data that may occur while sending it over the network.

Man in the Middle Attack

The man in the middle attack (MIM) in machine security is a manifestation of dynamic listening in which the assailant makes autonomous associations with the exploited people and transfers messages between them, making them accept that they are talking specifically to one another over a private association, when truth be told the whole discussion is controlled by the aggressor [4].

MIM basically occurs during the process of establishing secure connection that is the key exchange process. As given in Diffie-Hellman's algorithm, when TP is not present, the numbers P and G is publically transported and the attacker may know it.

The secret key generated by the client and web service is as follows:
C-> $[(P)^a \bmod G] = L_1$ (Lets Say) AS-> $[(P)^b \bmod G] = L_2$ (Lets Say) Now

C-> $[(L_2)^a \bmod$
$G] = X_1$ AS->
$[(L_1)^b \bmod G]$
$= X_2$

Now $X_1 = X_2$ as we know by
mathematical fundamentals: $X_1 = ((P)^a$
$\bmod G)^b \bmod G = ((P)^a)^b \bmod G$
$X_2 = ((P)^b \bmod G)^a \bmod G =$
$((P)^b)^a \bmod G$ Thus
$X_1 = X_2 = X$ acts as the secret
key.

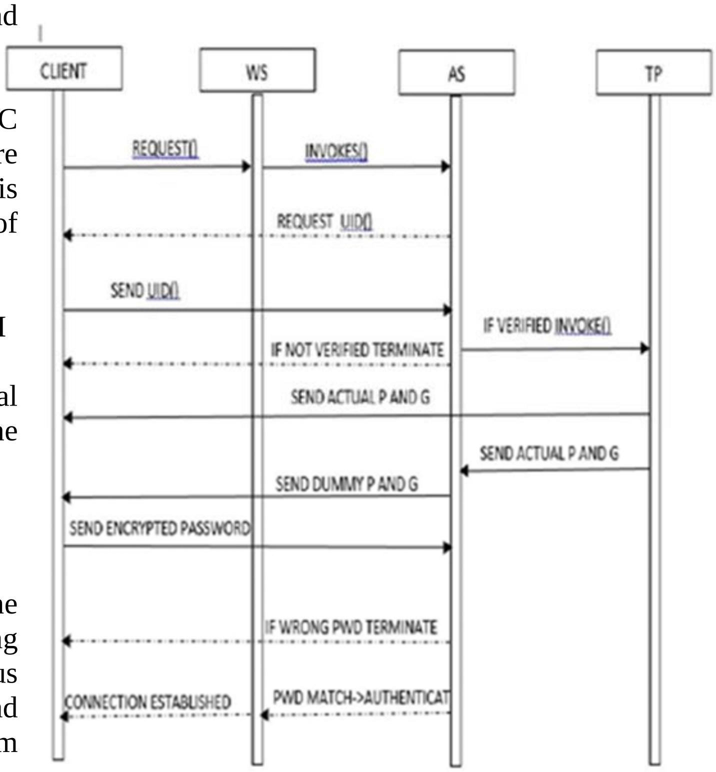


Fig. 1 Secure Connection Sequence Diagram

If P and G is known by the attacker, then value of a and b does not matter as attacker will choose a random number c and use it for generating two sets of secret keys one for client and another for authentication server, thus fooling the client and server in believing that the connection is secure.

As with the introduction of TP and the dummy values, the original G and P are not known by the attacker as TP send the value of G and P privately to C and AS.

Without knowing the actual values of G and P, the attacker cannot generate the right sets of keys. With the dummy values of G and P, attacker generates two sets of keys for C and AS respectively. These sets of keys are sent by him to C and AS which cannot be verified by them as they are wrong. This results in termination of connection which prevents the unsecure transmission of confidential data.

At present the most popular mechanism for securing SSO is SAML as it is faster and cheaper than other SSO mechanisms like OpenID and OAUTH2 which we have concluded after various researches on the Internet. It depends on "statements" about identities. It is expected that an AS is making a statement and that the AS is in charge of keeping up client credentials, confirming clients and deciding authorities. Our model uses TP(Third Party), that fools the attacker in believing that the TP does not exist [because of dummy values], thus reducing the chance of connection being compromised.Since our additive inclusion of dummy values leads the attacker to believe that he is hacking the correct link, it makes it very difficult for the attacker to try hacking our link with TP which send the actual values of p & g.

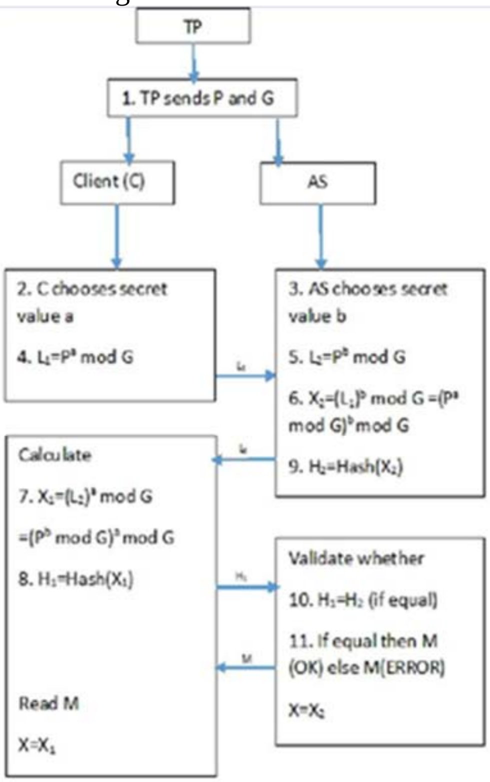


Fig. 2 Secure Key Exchange with the Help of Third Party

Our model aims to provide a secure transmission by adding this feature in pre-existing SAML model. Our model looks at the problem from the layman point of view, and tries to come up with a very simple and elegant solution for providing SSO security at minimal cost. Our models main focus is to remove MIM attack with minimal resources. This solution does not require any high order thinking, as it goes on a very basic way to solve the problems by fooling the attacker with dummy values without his knowledge.

V. CONCLUSION AND FUTURE WORK

In this paper we have proposed a Secure Single Sign on System to improve SAML with respect to the threat of Man in the Middle Attack. Our model uses the concept of Diffie-Hellman algorithm for secret key exchange with the additive inclusion of Third Party generation of P and G and transferring of dummy values of P and G between Client and Centralized Authentication Server for detection of Man in the Middle. The transmission of message takes place in encrypted form to maintain message layer integrity after securing the link by confirming the absence of MIM. Thus, our model provides a simple and cost-effective solution especially for smaller networks. In future, this model can be added with an efficient algorithm for selecting the TP server randomly to further minimize the possibility of attacker even knowing where to try to hack. Thus, it will provide an even more secure model which is already secured.

REFERENCES

[1] Yebin Chen, Bing Xia, Lianghong Shi and Baozhu Wu"Design of Web Service Single Sign On Based on Ticket and Assertion" Artificial Intelligence, Management Science and

Electronic Commerce (AIMSEC), 2011,pp297-300

[2] Web Single Sing-On Systems, [Online]. Available:http://www.cse.wustl.edu/~jain/cse571-07/ftp/websso/

[3]Diffie-Hellman-Key-exchange, [Online]. Available:http://searchsecurity.techtarget.com/definition/Diffie-Hellman-key-exchange

[4] L.Wrage, S.Simanta, G.A.Lewis, and S.Jaspan, “T-check in Technologies for Interoperability: Web Services and Security-Single Sign-On”, Software Research Institute Carnegie Mellon, 2007, pp 1-53

[5] Microsoft. net passport review guide

[6] J.Gantner, A.G.Schulz and A.Thede, “A Single Sign-On Protocol for Distributed Web Applications Based On Standard Internet Mechanisms”, e-business and telecommunications networks Springer Netherland, 2006

[7] C.-C. Chang and C.-Y. Lee, “A secure single sign-on mechanism for distributed computer networks,” IEEE Trans. Ind. Electron, Jan. 2012

[8] C.-L. Hsu and Y.-H. Chuang, “A Novel User Identification Scheme with Key Distribution Preserving User Anonymity for Distributed Computer Networks”, Inf. Sci., 2009

[9] C.P. Schnorr, “Efficient Signature Generation by Smart Cards”, J. Cryptology, 1991

[10] K. Lauter, “The advantages of elliptic curve cryptography for wireless security,” Wireless Commun., 2004

[11] R. L. Rivest, A. Shamir, and L. M. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,”Commun. ACM, 1978

[12] Single Sign-On, [Online], Available:http://www.replicon.com/customer-zone2/kb-2834

[13]Secure Authentication Blog for mobile SSO, [Online]. Available: https://www.secureauth.com/Resources/Blog.aspx?page=15

[14]Tivoli Software Information Center, [Online]. Available: http://www.publib.boulder.ibm.com

SETUP TIME REDUCTION OF MACHINE USING SMED TECHNIQUE AND LEAN MANUFACTURING

[1]N. S. Jagtap, [2]V. D. Ugale, [3]M. M. Kadam, [4]S. S. Kamble, [5]A. V. Salve
UG Student, UG Student, UG Student, UG Student, Asst. Professor
Vishwakarma Institute of information Technology, Pune
Email:[1]nageshsjagtap@gmail.com, [2]vishal.ugale31@gmail.com, [3]mayurkdm07@gmail.com, [4]kshri3512@gmail.com, [5]aniket.salve@gmail.com

Abstract— Growth of an industry and its productivity ultimately depends on its ability to systematically and continuously respond to the market changes for enhancing the product value. Value addition process is necessary to achieve this perfection; hence implementing a lean manufacturing system and its tools is becoming a core competency. Since setup time is a major cause for production downtime, minimum setup time is always desirable. Single Minute Exchange of Dies (SMED) as proposed by Shingo is a tool which aims to reduce excessive setup time, but not effective when used alone. SMED can be effectively implemented with the help of additional tools like ECRS (Eliminate, Combine, Reduce and Simplify). This paper presents a procedure for organizing and implementing SMED along with other useful tools. It is based on teamwork which allows a gradual reduction of machine setup time to less than 10 minutes accompanied by continuous improvement system. This paper also presents the case study of bearing manufacturing industry suggesting improvements that will significantly reduce machine setup time by 30%-35%. The methodology explained is this paper is applicable to most of the batch manufacturing industries.

INDEX TERM- GRINDING MACHINE, PARETO, SETUP TIME, SMED

I. INTRODUCTION

"One of the most noteworthy accomplishments in keeping the price of products low is the gradual shortening of the production cycle. The longer an article is in the process of manufacture and the more it is moved about, the greater is its ultimate cost."- Henry Ford 1926. In an industry, time is money. The product cycle time directly reflects in cost. Due to flexibility in market demand and competitiveness, many manufacturers are opting to reduce machine setup time and down time. Machine setup is to be changed according to customer requirements. Set up time is the time passed between the completion of the last product of the old batch and the completion of the first good product of the new batch. There is always a need to change set up of equipment, unfortunately with the production loss accompanied with it. In the past two decades, setup time reduction and quality improvement programs have become prevalent in manufacturing industry. These programs had contributed towards higher efficiency and agility needed by manufacturers. At present manufacturers must be able to manufacture a wide variety of high quality products in a cost-effective manner with reduced inventories and respond quickly to changes in the product volumes in order to sustain in the market. [1], [2]

One of the significant losses is equipment setup or a tooling changeover. The principles pioneered by Shigeo Shingo, known as SMED or Single Minute Exchange of Dies, can be used to dramatically reduce this time. Also known as “quick changeover,” or “rapid changeover”, this method can be applied any time equipment is “changed” from one physical state to another. This may include tool changes, material changes, or changing to a different product or configuration. [3]

Fig. 1 shows the relations between setup time and costs with three strategies. It can be seen that a reduction of setup time using the SMED method is cheaper, but reduction in time achieved is not significant. Replacing an existing machine is most effective strategy, unfortunately cost associated with it is higher and generally industries are reluctant for such a change. So optimum solution is to use SMED along with other tools and some improvements in the existing design of machine. [4]

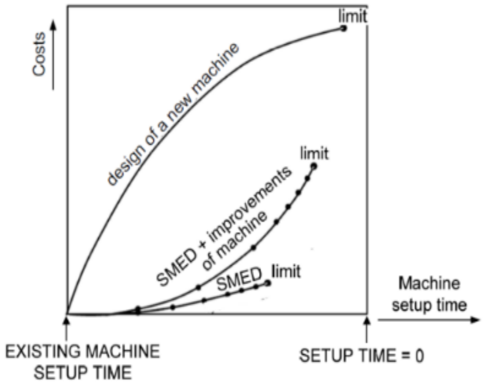


Fig-1.Dependency between machine set up time and cost(4).

STEP I: PRIORITIZE MACHINES

The selection of machine is done by consideration of factors such as setup time, frequency of setup, bottleneck machines, efficiency loss, and complexity of operation and on the basis of ABC analysis. In materials management, the ABC analysis (or Selective Inventory Control) is an inventory categorization technique. ABC analysis divides an inventory into three categories- "A items" with very tight control and accurate records, "B items" with less tightly controlled and good records, and "C items" with the simplest controls possible and minimal records. [4]

STEP II: DOCUMENTATION OF MACHINE TOOLS AND PROCESSES

SMED team must have thorough knowledge of machine and process. The current process data and working methodology is collected from machines’ operators, line supervisors and managers. Plenty of tools and components have to be replaced during machine setup which is a complex activity in batch manufacturing. So as to simplify the analytical data, check sheets are designed according to specification of product. It will help in finding the tools and parts in short time and hence ultimately reducing the overall setup time.

STEP III: TIME AND MOTION STUDY

Time and motion study is a work measurement and business efficiency technique for recording the times of performing a certain specific job or its elements carried out under specified conditions. For analyzing the data so as to obtain the time necessary for an operator to carry it out at a defined rate of performance. [7]

Purpose of time and motion study:

1. To eliminate unnecessary motions
2. Identify the best sequence for maximum efficiency
3. Standardization of work

STEP IV: DESCRIBE STEPS IN DETAIL WITH TIME FOR EACH

From Time and Motion Study all processes are to be divided in sub processes, with the time required for the same. It will provide a base for initial prioritizing of activities which will ultimately decide the workflow.

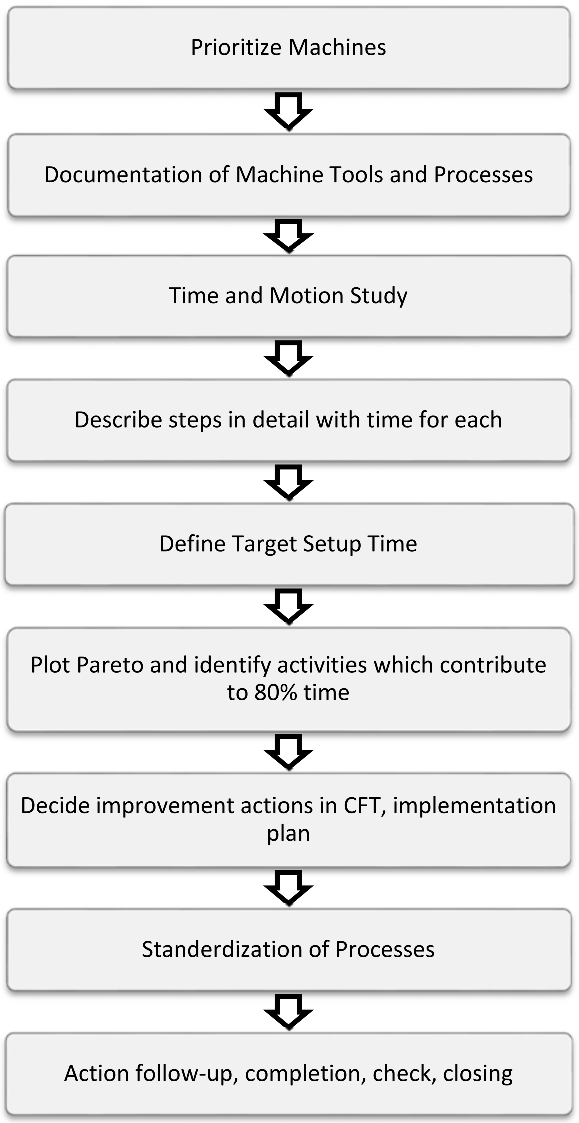

Prioritize Machines
Documentation of Machine Tools and Processes
Time and Motion Study
Describe steps in detail with time for each
Define Target Setup Time
Plot Pareto and identify activities which contribute to 80% time
Decide improvement actions in CFT, implementation plan
Standerdization of Processes
Action follow-up, completion, check, closing

Fig. 2. Steps in organization and execution of SMED workshop

STEP V: DEFINE TARGET SETUP TIME

The motivation of team members gets influenced by the definition of target setup time. It should be optimum and practical to achieve, otherwise it will demotivate the team members. It is generally taken as 20% to 30% less than the current setup time. [3]

STEP VI: PLOT PARETO AND IDENTIFY ACTIVITIES WHICH CONTRIBUTE TO 80% TIME

Pareto analysis is a formal technique useful where many possible courses of action are competing for attention. In essence, the problem-solver estimates the benefit delivered by each action, then selects a number of the most effective actions that deliver a total benefit reasonably close to the maximal possible one. Basically it helps in prioritising the activities. [6]

STEP VII: DECIDE IMPROVEMENT ACTIONS IN CFT, IMPLEMENTATION PLAN

Cross Functional Team (CFT): A cross-functional team is a small group of individuals that cross formal departmental boundaries and levels of hierarchy. The group is committed to a common purpose or goal of improvement; it acts and works as a unit-communicating frequently, cooperating and providing mutual support, coordinating activities, drawing upon and exploiting the skills and capabilities of the team while considering the needs of individual members.

CFT will decide the plan for improvement on the basis of prioritization of activities which is done by considering factors such as complexity and frequency of operation.

STEP VIII: STANDARDIZATION

Developing standardized work is the first step in waste elimination. The analytical process will reveal waste that should be eliminated for developing the standardized work. Operators should be encouraged to suggest changes that will improve the process and be reflected in revisions to the standardized work. [3]

STEP IX: ACTION FOLLOW-UP, COMPLETION, CHECK, CLOSING

When standard work is developed and with skilled manpower, regular audits are needed to check on whether the standards are being followed, and if not, why. But this is continuous and time consuming process as regular assessment is necessary. [3]

IV. CASE STUDY

Case study is carried out on bore grinding machine at bearing manufacturing industry. This Machine is used for bore grinding of inner ring (IR) of taper roller bearing (TRB). Frequency of setup is high because of batch production. SMED technique and ECRS principle are used to reduce machine setup time.

I. Prioritize Machines

Main criteria for machine selection is frequency of setup. Also bottleneck and average setup changeover time obtained from previous data is considered. Hence 1st bottleneck machine i.e. IR bore grinding machine is selected.

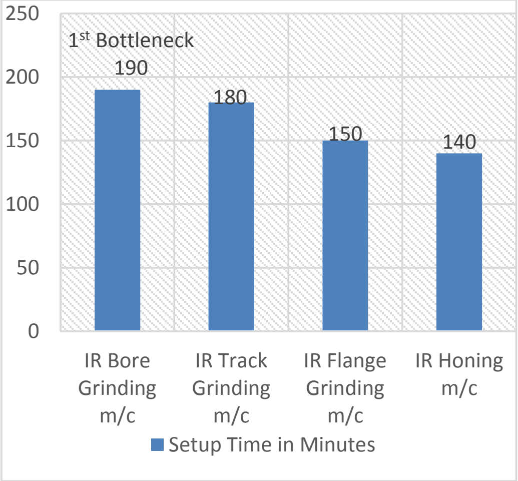
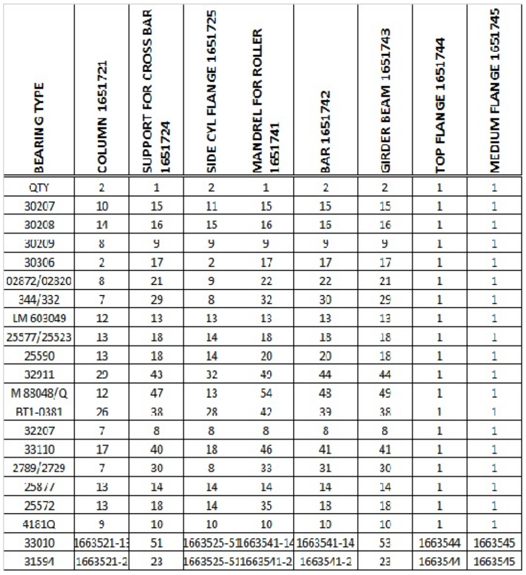


Fig. 3. Average Setup Time for Machines

Table I. Check Sheet Format



BEARING TYPE	COLUMN 1651721	SUPPORT FOR CROSS BAR 1651724	SIDE CYL FLANGE 1651725	MANDREL FOR ROLLER 1651741	BAR 1651742	GIRDER BEAM 1651743	TOP FLANGE 1651744	MEDIUM FLANGE 1651745
QTY	2	1	2	1	2	2	1	1
30207	10	15	11	15	15	15	1	1
30208	14	16	15	16	15	16	1	1
30209	8	9	9	9	9	9	1	1
30306	2	17	2	17	17	17	1	1
02872/02320	8	21	9	22	22	21	1	1
344/332	7	29	8	32	30	29	1	1
LM 603049	12	13	13	13	13	13	1	1
25577/25523	13	18	14	18	18	18	1	1
25590	13	18	14	20	20	18	1	1
32911	29	43	32	49	44	44	1	1
M 88048/Q	12	47	13	54	48	49	1	1
BT1-0381	26	38	28	42	39	38	1	1
32207	7	8	8	8	8	8	1	1
33110	17	40	18	46	41	41	1	1
2789/2729	7	30	8	33	31	30	1	1
25877	13	14	14	14	14	14	1	1
25572	13	18	14	35	18	18	1	1
4181Q	9	10	10	10	10	10	1	1
33010	1663521-13	51	1663525-51	1663541-14	1663541-14	53	1663544	1663545
31594	1663521-2	23	1663525-51	1663541-2	1663541-2	23	1663544	1663545

II. Documentation of Machine Tools and Processes:

Data collection is done with the help of operators, supervisors and managers. It includes listing down all components which are to be replaced and required tooling. Each process is to be defined separately and divided in small sub processes if possible. This will help in implementing ECRS principle and prioritizing activities at later stage. To reduce the complexity in analysis, special types of check sheets are formed which is shown in table I.

III. Video Shooting of Setup Changeover Activities:

Video shooting and analysis is one of the effective methods of Time and Motion study. With very little knowledge also one can understand the procedure of changeover which is essential.

IV. Describe Steps in detail with time for each:

Video Analysis involves reviewing recorded setup process and simultaneously defining each sub process. These activities are classified into internal (done when machine is offline) and external (performed as the machine is running) activities [8]. Critical and lengthy activities are further subdivided into simpler ones. Then the time required for each process is mentioned as shown in table II. (a), (b) and table III.

V. Define Target Setup Time:

After getting an idea about the current procedure and total time required for individual activity, the target setup time is defined. It should be optimum i.e. not too low and not too high. Very low setup time makes team members feel that it is impossible to achieve. On the other hand, very lesser reduction in setup time will not improve the productivity substantially.

There is no standard procedure to define the target setup time. It will be variable depending upon activities and their complexity. After brainstorming session between all the team members, 30%-35% reduction in current setup time is targeted.

VI. Plot Pareto and Identify activities which contributes to 80% time:

The basic principle of Pareto analysis is 80% activities consumes 20% time and 20% activities consumes 80% time. The Pareto chart for internal and external activities is shown in fig. 4 and fig. 5 respectively.

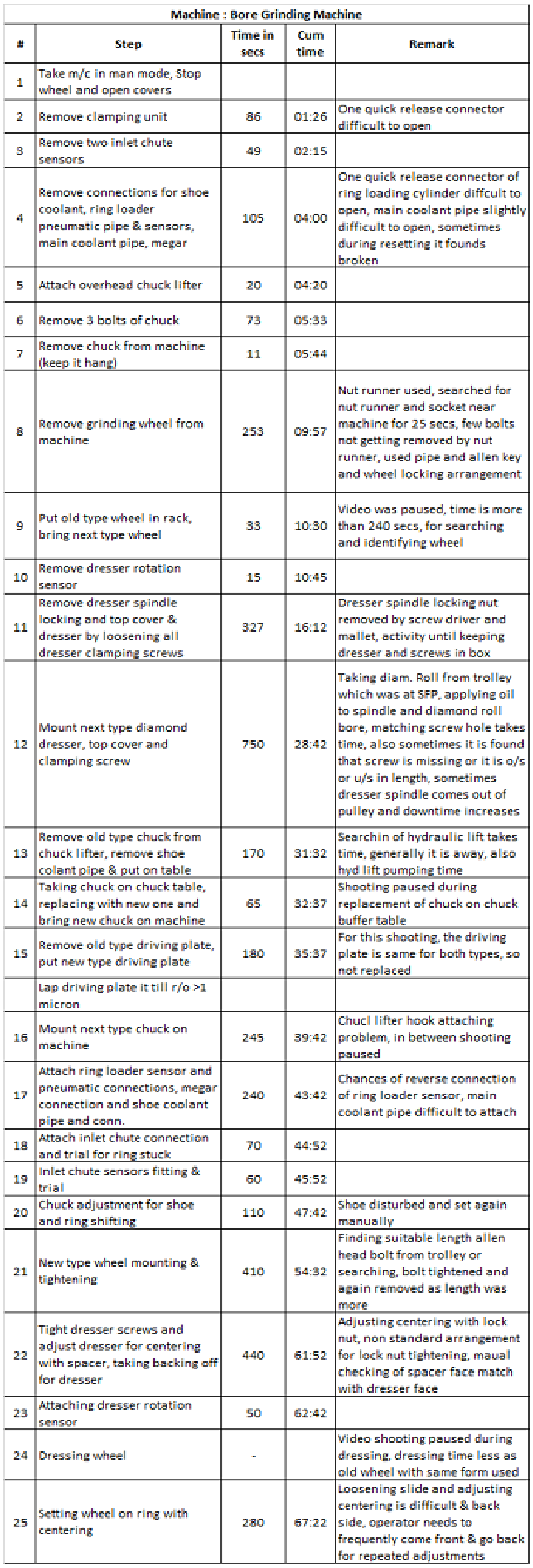
VII. Decide improvement actions in CFT, implementation plan:

Cross Functional Team (CFT) will form action plan for setup time reduction. For internal as well as external activities ECRS (Eliminate, Combine, Rearrange & simplify) principle is applied. Refer remarks in table II. (a) and II. (b).

VIII. Standardization:

Standardization is mostly applicable to external activities e.g. Shoe Setting, Ring Chucking which consumes more time than internal activities. It also includes defining standardization of procedures (SOP) for driving plate rework, shoe setting. SOP made the rework process simpler from supplier point of view which ensures specifications as per the requirement.

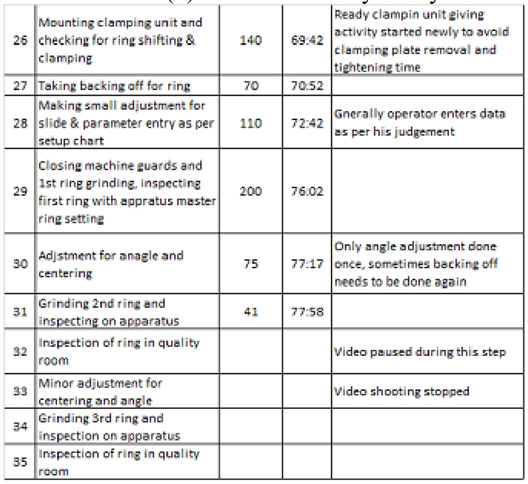
Table II. (a). Internal Activity Analysis



Machine : Bore Grinding Machine

#	Step	Time in secs	Cum time	Remark
1	Take m/c in man mode, Stop wheel and open covers			
2	Remove clamping unit	86	01:26	One quick release connector difficult to open
3	Remove two inlet chute sensors	49	02:15	
4	Remove connections for shoe coolant, ring loader pneumatic pipe & sensors, main coolant pipe, megar	105	04:00	One quick release connector of ring loading cylinder diffcult to open, main coolant pipe slightly difficult to open, sometimes during resetting it founds broken
5	Attach overhead chuck lifter	20	04:20	
6	Remove 3 bolts of chuck	73	05:33	
7	Remove chuck from machine (keep it hang)	11	05:44	
8	Remove grinding wheel from machine	253	09:57	Nut runner used, searched for nut runner and socket near machine for 25 secs, few bolts not getting removed by nut runner, used pipe and allen key and wheel locking arrangement
9	Put old type wheel in rack, bring next type wheel	33	10:30	Video was paused, time is more than 240 secs, for searching and identifying wheel
10	Remove dresser rotation sensor	15	10:45	
11	Remove dresser spindle locking and top cover & dresser by loosening all dresser clamping screws	327	16:12	Dresser spindle locking nut removed by screw driver and mallet, activity until keeping dresser and screws in box
12	Mount next type diamond dresser, top cover and clamping screw	750	28:42	Taking diam. Roll from trolley which was at SFP, applying oil to spindle and diamond roll bore, matching screw hole takes time, also sometimes it is found that screw is missing or it is o/s or u/s in length, sometimes dresser spindle comes out of pulley and downtime increases
13	Remove old type chuck from chuck lifter, remove shoe colant pipe & put on table	170	31:32	Searchin of hydraulic lift takes time, generally it is away, also hyd lift pumping time
14	Taking chuck on chuck table, replacing with new one and bring new chuck on machine	65	32:37	Shooting paused during replacement of chuck on chuck buffer table
15	Remove old type driving plate, put new type driving plate	180	35:37	For this shooting, the driving plate is same for both types, so not replaced
	Lap driving plate it till r/o >1 micron			
16	Mount next type chuck on machine	245	39:42	Chucl lifter hook attaching problem, in between shooting paused
17	Attach ring loader sensor and pneumatic connections, megar connection and shoe coolant pipe and conn.	240	43:42	Chances of reverse connection of ring loader sensor, main coolant pipe difficult to attach
18	Attach inlet chute connection and trial for ring stuck	70	44:52	
19	Inlet chute sensors fitting & trial	60	45:52	
20	Chuck adjustment for shoe and ring shifting	110	47:42	Shoe disturbed and set again manually
21	New type wheel mounting & tightening	410	54:32	Finding suitable length allen head bolt from trolley or searching, bolt tightened and again removed as length was more
22	Tight dresser screws and adjust dresser for centering with spacer, taking backing off for dresser	440	61:52	Adjusting centering with lock nut, non standard arrangement for lock nut tightening, maual checking of spacer face match with dresser face
23	Attaching dresser rotation sensor	50	62:42	
24	Dressing wheel	-		Video shooting paused during dressing, dressing time less as old wheel with same form used
25	Setting wheel on ring with centering	280	67:22	Loosening slide and adjusting centering is difficult & back side, operator needs to frequently come front & go back for repeated adjustments

Table II. (b). Internal Activity Analysis



26	Mounting clamping unit and checking for ring shifting & clamping	140	69:42	Ready clampin unit giving activity started newly to avoid clamping plate removal and tightening time
27	Taking backing off for ring	70	70:52	
28	Making small adjustment for slide & parameter entry as per setup chart	110	72:42	Gnerally operator enters data as per his judgement
29	Closing machine guards and 1st ring grinding, inspecting first ring with appratus master ring setting	200	76:02	
30	Adjstment for anagle and centering	75	77:17	Only angle adjustment done once, sometimes backing off needs to be done again
31	Grinding 2nd ring and inspecting on apparatus	41	77:58	
32	Inspection of ring in quality room			Video paused during this step
33	Minor adjustment for centering and angle			Video shooting stopped
34	Grinding 3rd ring and inspection on apparatus			
35	Inspection of ring in quality room			

Sr. No.	Activity	Setup Time Before implementation of SMED (min)	Setup Time After implementation of SMED (min)
1	Ring checking (Shoe Setting) i. DK Chucking ii. Track Chucking	28	19
2	Driving plate lapping	10	5
3	Dresser spindle adjustment	37	23
4	Driving plate face matching	15	10
5	Tool Search	10	3
6	Idle Time	5	2
	Total Time	105	62

Table III. External Activity Analysis

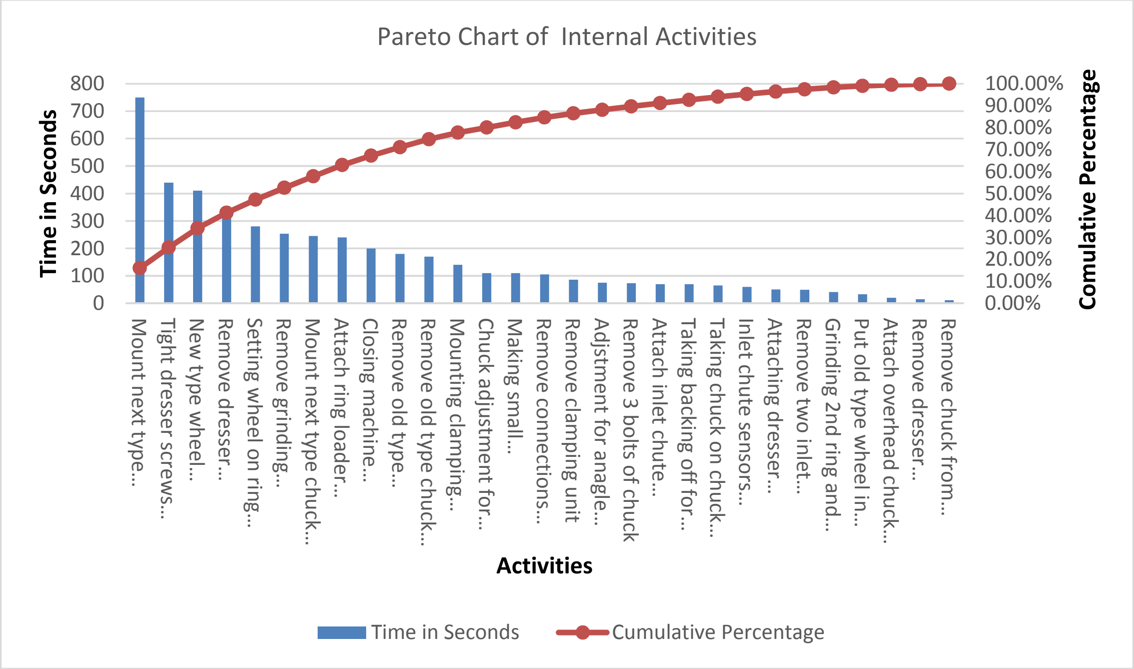


Fig. 4. Pareto chart of internal activities of bore grinding machine

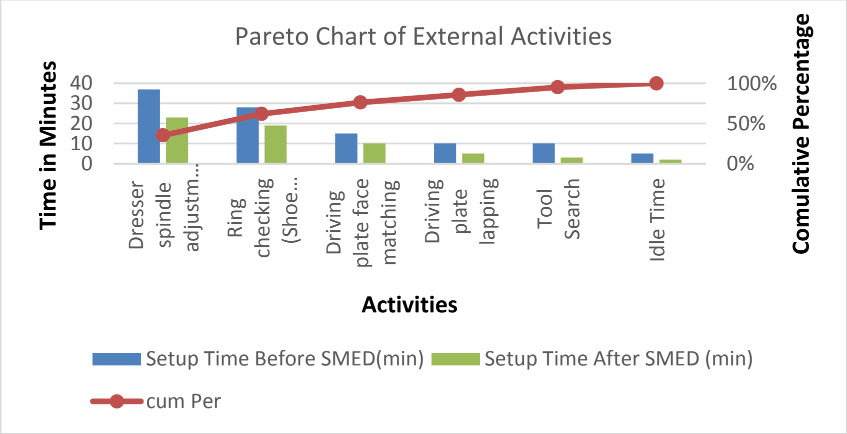
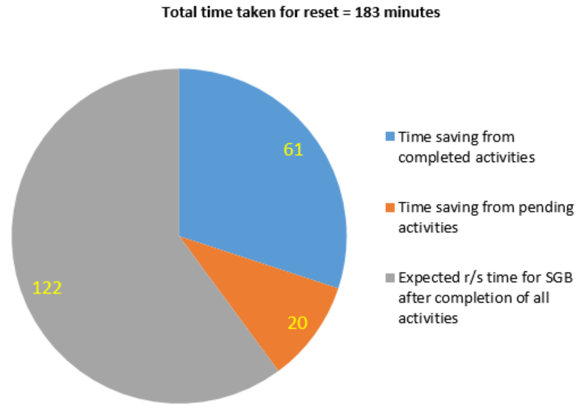


Fig. 5. Pareto chart of External activities of bore grinding machine

IX. Action Follow-Up, Completion, Check, Closing:

Whether the action plan is executed or not is to be verified by taking feedback from operators and changeover department.

The time for internal activities is reduced from 78 minutes to 60 minutes. For external activities, time is reduced from 105 minutes to 62 minutes. Therefore total time is reduced from 183 minutes to 122 minutes i.e. about 33% reduction in previous setup time as shown in fig. 6.



V. Conclusion

New approach for setup time reduction is proposed for effective utilization of SMED by combining it with tools of lean manufacturing like ECRS. The results illustrate that 33% setup changeover time reduction can be achieved with above methodology

VI. References

[1] R. Sundara, A. N. Balajib, R. M. SatheeshKumar, "A Review on Lean Manufacturing Implementation Techniques", 12th GLOBAL CONGRESS ON MANUFACTURING AND MANAGEMENT, GCMM 2014, Procedia Engineering 97 (2014) 1875 – 1885

[2] Pablo Guzmán Ferradás, Konstantinos Salonitis, "Improving changeover time: a tailored SMED approach for welding cells", Forty Sixth CIRP Conference on Manufacturing Systems 2013, Procedia CIRP 7 (2013) 598 – 603

[3] Liker J. K. and David Meier, The Toyota Way Field book, McGraw-Hill, New York, pp. 70-80,163, 2006

[4] Janez Kušar, Tomaž Berlec, Ferdinand Žefran, Marko Starbek, "Reduction of Machine Setup Time", Strojniški vestnik, Journal of Mechanical Engineering 56(2010)12, 833-845

[5] Yash Dave, Nagendra Sohani, "Single Minute Exchange of Dies: Literature Review", International Journal of Lean Thinking Volume 3, Issue 2 (December 2012)

[6] M. Kemal Karasu, Mehmet Cakmakci, Merve B. Cakiroglu, Elif Ayva, Neslihan Demirel-Ortabas, "Improvement of changeover times via Taguchi empowered SMED/case study on injection molding production", Measurement 47 (2014) 741–748

[7] Mohammed Ali Almomani, Mohammed Aladeemy, Abdelhakim Abdelhadi, Ahmad Mumani, "A proposed approach for setup time reduction through integrating conventional SMED method with multiple criteria decision-making techniques", Computers & Industrial Engineering 66 (2013) 461–469

[8] James R. Freeland, John P. Leschke, Elliott N. Weiss, "Guidelines for Setup-Cost Reduction Programs to Achieve Zero Inventory", Journal of Operations Management Vol. 9, No. 1, January 1990

STRESS ANALYSIS OF CRANE HOOK USING FEA

B Nagaraju [1], M RajaRoy[1] , P Venkatesh Reddy[1] , K Satyanarayana[1]
[1] Department of Mechanical Engg, Anil Neerukonda Institute of Technology and Sciences,
Sangivalasa, Visakhapatnam-531162,Andhra Pradesh.
Email: [1]anitsnagaraju@gmail.com, [2]anitsrajaroy@gmail.com,
[3]venkateshreddy348@gmail.com,

Abstract— Crane hook is very significant component used for lifting the load with the help of chain or wire ropes. Crane hooks are highly liable components and are always subjected to bending stresses which leads to the failure of crane hook. To minimize the failure of crane hook, the stress induced in it must be studied. A crane is subjected to continuous loading and unloading. This may causes structural failure of the crane hook. In the present work, an attempt has been made by considering four different type's of cross sections of crane hooks and are designed theoretically by using curved beam concept. CATIA software is used for modeling the crane hook and ANSYS software used to find out the stresses. As a conclusion, the results obtained from ANSYS and theoretical calculations are compared.

***Index Terms*—crane hook, static analysis , FEA.**

1. INTRODUCTION

Crane Hooks are highly liable components that are typically used for industrial purposes. It is basically a hoisting fixture designed to engage a ring or link of a lifting chain or the pin of a shackle or cable socket and must follow the health and safety guidelines. Thus, such an important component in an industry must be manufactured and designed in a way so as to deliver maximum performance without failure. Thus, the aim of the work is to study the stress distribution pattern of a crane hook using finite element method and to verify the results using caustic method.

The lifting of objects generally occurs on construction sites, in factories and other industrial situations. Correct lifting can move large objects efficiently and reduce manual handling operations. Incorrect lifting however, can lead to disastrous accidents. Every year, incorrect lifting procedures cause injuries, loss of work time and property. People, machinery, loads, methods and the work environment, are all important factors for correct lifting. Provided that enough safety measures are fully implemented, lifting accidents can be reduced. The Fig 1.1 as shows the general diagram of crane hook.

Fig 1.1 Crane Hook

2. LITERATURE REVIEW

Crane hooks are the components which are generally used to elevate the heavy load in industries and constructional sites. Recently, excavators having a crane-hook are widely used in construction works site. *M. Shaban et al [1]* studied the stress pattern of crane hook in its loaded condition, a solid model of crane hook is prepared with the help of ABAQUS software. Real time pattern of stress concentration in 3D model of crane hook is obtained. The stress distribution pattern is verified for its correctness on an acrylic model of crane hook using shadow optical method (Caustic method) set up. By predicting the stress concentration area, the shape of the crane is modified to increase its working life and reduce the failure rates. *E. Narvydas et al* [2] investigated circumferential stress concentration factors with shallow notches of the lifting hooks of trapezoidal cross-section employing finite element analysis (FEA). The stress concentration factors were widely used in strength and durability evaluation of structures and machine elements. The FEA results were used and fitted with selected generic equation. This yields formulas for the fast engineering evaluation of stress concentration factors without the usage of finite element models. The design rules of the lifting hooks require using ductile materials to avoid brittle failure; in this respect they investigated the strain based criteria for failure, accounting the stress triaxiality . *SpasojeTrifkovic' et al* [3] analyzes the stress state in the hook using approximate and exact methods. They calculated stresses in various parts of the hook material firstly by assuming hook as a straight beam and then assuming it as a curved beam. Analytical methods were used with the help of computers, using FEM. *Bhupender Singh et al* [4] presented the solid modeling and finite element analysis of crane boom has been done using PRO/E WILDFIRE 2.0 and ALTAIR HYPER MESH with OPTISTRUCT 8.0 SOLVER*Y. Torres et al* [5] studied the probable causes which led to a failure of the crane hook in service. The study of accident includes: details of the standards governing the manufacturing and use of lifting hooks, experimental analysis, mechanical behavior of steel of reported hook and simulation of the thermal history of the hook. From the literature survey it is understood by this author that there is a lot of scope for studying the stress analysis with different cross sections. Taking into this consideration, the author has embarked on studying the stress analysis of crane hook with four different cross sections such as rectangle, trapezoidal, triangle and circular cross sections.

3 DESIGN OF CRANE HOOK

Machine frames having curved portions are frequently subjected to bending or axial loads or to a combination of bending and axial loads. With the reduction in the radius of curved portion, the stress due to curvature become greater and the results of the equations of straight beams when used becomes less satisfactory. For relatively small radii of curvature, the actual stresses may be several times greater than the value obtained for straight beams. It has been found from the results of Photo elastic experiments that in case of curved beams, the neutral surface does not coincide with centroidal axis but instead shifted towards the Centre of curvature. It has also been found that the stresses in the fibers of a curved beam are not proportional to the distances of the fibers from the neutral surfaces, as is assumed for a straight beam.

The design of crane hook was done by assuming the data pertaining to load(w), C.S.A and curvatures which are used in industrial applications of crane hook as shown in Figs 3.1 to 3.4

3.1 Theoretical Design of Crane Hook with Rectangular C.S.A

W = 20 KN = 20 × 10^3N; Ri= 50 mm; R_o= 150 mm; h = 100 mm; b = 60 mm

ri = Distance of inner fibre from centre of curvature, C

ro = Distance of outer fibre from centre of curvature

rc = Distance of centroidal axis (CG axis) from centre of curvature
rn = Distance of neutral axis from centre of curvature
The neutral axis is shifted towards the centre of curvature by a distance called eccentricity
'e'. The value 'e' should be computed very accurately since a small variation in the value of 'e'

causes a large variation in the values of stress.
e = rc – rn
ci = Distance between neutral axis and inner fibre = rn – ri
co = Distance between outer fibre and neutral axis = ro – rn

Resultant stress at the inside fibre,
σ_t +σ_{bi}= 3.33+30.66 = 33.99MPa (tensile)
∴ Resultant stress at the outside fibre,

$\sigma_t - \sigma_{bo}$ = 3.33-14.66 = -11.33MPa (compressive)

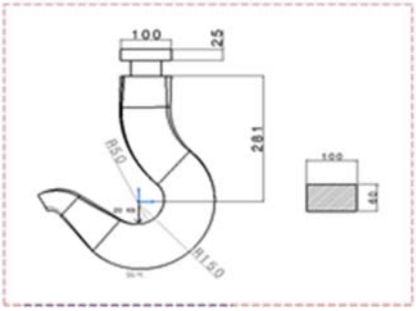


Fig 3.1 Design of Crane Hook with rectangular C.S.A

3.2 Theoretical Design of Crane Hook with Trapezoidal C.S.A

W = 20 KN = 20 × 10^3N; R_i= 50 mm ; R_o= 150 mm ; h = 100 mm ; b_i=90 mm; b_o=30 mm

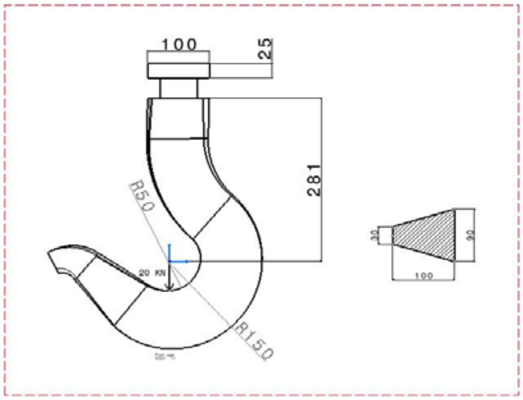


Fig 3.2Design of Crane Hook with Trapezoidal C.S.A

∴ Resultant stress at the inside fibre
σ_{bi}= 3.33+25.169 = 28.499 MPa (tensile)
Resultant stress at the outside fibre
$\sigma_t - \sigma_{bo}$ = 3.33-16.63 = -13.3MPa (compressive)

3.3 Theoretical Design of Crane Hook with Triangular C.S.A

W = 20 kN = 20 × 10^3N; R_i= 50 mm ;R_o= 150 mm ; h = 100 mm ; b_i =90 mm;

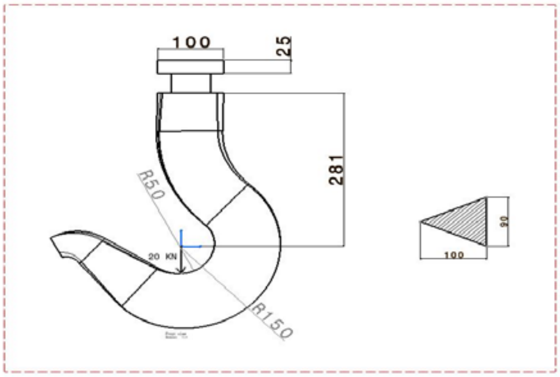


Fig 3.3 Design of Crane Hook with Triangular C.S.A
∴ Resultant stress at the inside fibre

σ_t+ σ_{bi}= 6.163+32.654 = 38.817MPa (tensile)

∴ Resultant stress at the outside fibre
$\sigma_t - \sigma_{bo}$ = 6.163-29.177 = -23.014 MPa (compressive)

3.4 Theoretical Design of Crane Hook with circular C.S.A

W = 20 KN = 20×10^3N;R_i= 60 mm ; R_o= 150 mm; d=90mm

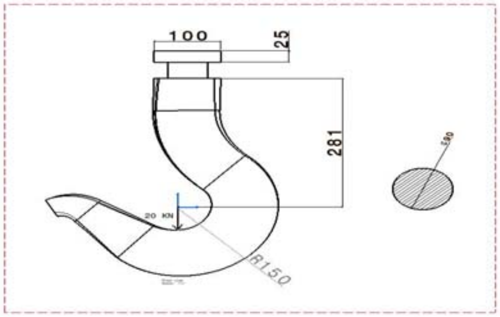


Fig 3.4 Design of Crane Hook with circular C.S.A

∴ Resultant stress at the inside fibre

$\sigma_t + \sigma_{bi}$= 3.143+43.31 = 46.461MPa (tensile)

∴ Resultant stress at the outside fibre

$\sigma_t - \sigma_{bo}$ = 3.143-21.73 = -18.587 MPa (compressive)

4. MODELLING OF CRANE HOOK USING CATIA

CATIA serves the design tasks by providing different workbenches. A workbench is defined as a specific environment consisting of a set of tools, which allows the user to perform specific design tasks in a particular area. The basic workbenches in CATIA V5 are Part design workbench, Wireframe and Surface Design workbench, Assembly Design workbench, and Drafting workbench.

.

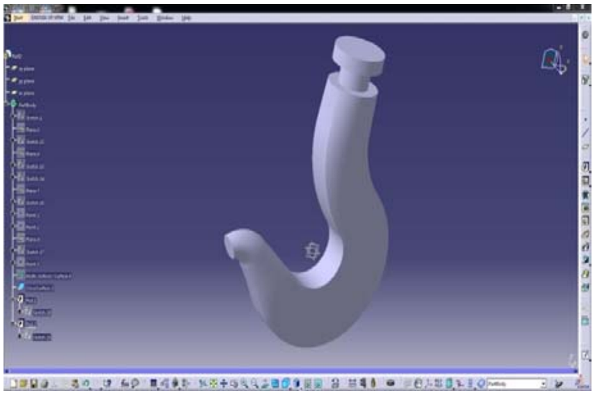


Fig 4.1 CATIA Model of Crane Hook with Rectangular C.S.A

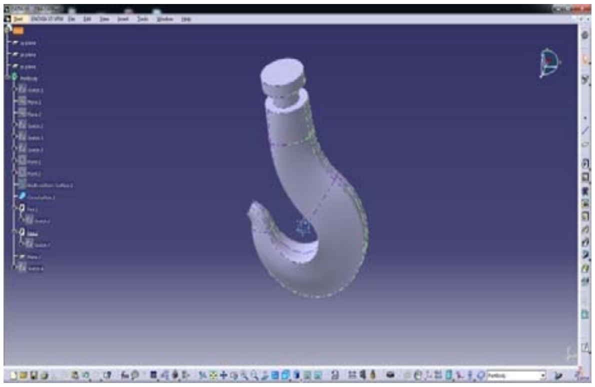


Fig 4.2 CATIA Model of Crane Hook with Trapezoidal C.S.A

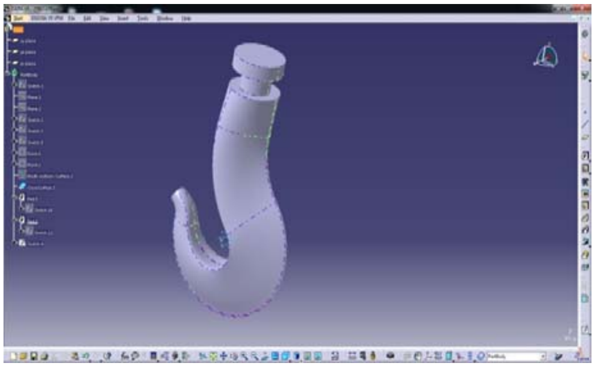


Fig 4.3 CATIA Model of Crane Hook with Triangular C.S.A

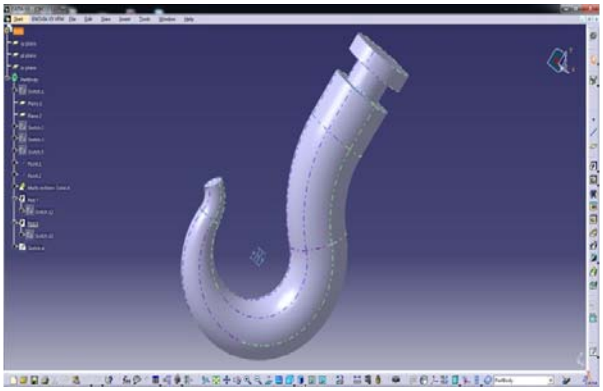


Fig 4.4 CATIA Model of Crane Hook with circular C.S.A

5 FINITE ELEMENT ANALYSIS OF CRANE HOOK USING ANSYS

The finite element method has become a powerful tool for the numerical solution of wide range of engineering problems. Applications range from deformation and stress analysis of automotive aircraft, building, and bridge structures to field analysis of heat flux, seepage and other flow problems, with advances in computer technology and CAD systems, complex problems can be modeled with relative ease.

In this method of analysis, a complex region defining a continuum is discretized into simple geometric shapes called finite elements. The material properties and the governing relationships are considered over these elements and considering the loading and constraints, results in a set of equations. Solution of these equations gives us the approximate behavior of the continuum.

6 RESULTS AND DISCUSSION

In this work, four different types of sections of crane hook are designed successfully by using curved beam concept. The induced Stresses are determined for a load of 20 KN using curved beam concept.

The solid modal was prepared using CATIA V5 R20 version and exported to ANSYS using IGES format. The hook is fixed at the top end in x,y and z directions and are fully constrained. The inner curvature of hook is subjected 20 KN load and is applied on nodes. The results of stresses obtained for a crane hook which is made up of steel material are plotted in the Figs 6.1 to 6.4. The results obtained through analytical and theoretical methods are good in agreement with minor deviation and shown in Table 6.1.

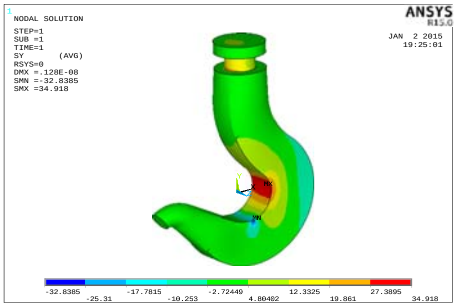


Fig 6.1 variation of Stresses for a crane hook made of steel with Rectangular C.S.A along Y-Direction

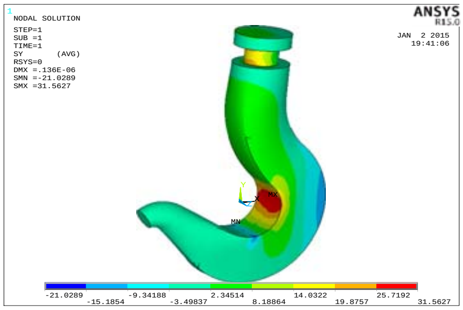


Fig 6.2 variation of Stresses for a crane hook made of steel with Trapezoidal C.S.A along Y-Direction

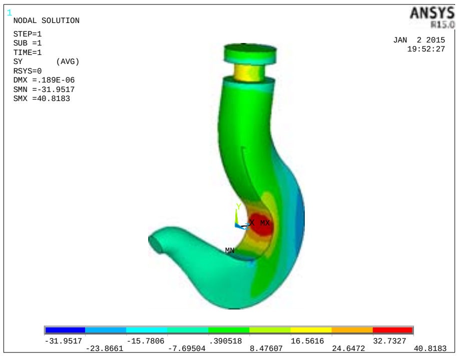


Fig 6.3 variation of Stresses for a crane hook made of steel with Triangular C.S.A along Y-Direction

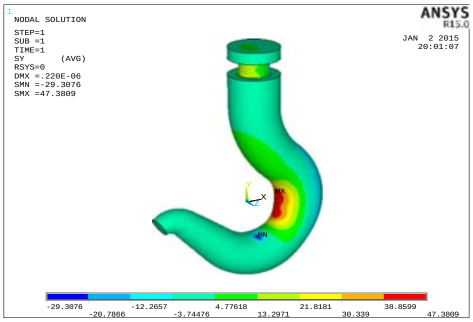


Fig 6.4 variation of Stresses for a crane hook made of steel with Circular C.S.A along Y-Direction

Table 6.1 Comparison of Stresses obtained in Theoretical and analytical methods

SECTION	THEORITICAL		ANSYS	
	COMPRESSIVE	TENSILE	COMPRESSIVE	TENSILE
RECTANGLE	11.3	33.99	10.25	34.91
TRAPEZOIDAL	13.3	28.49	15.18	31.56
TRIANGULAR	23.01	38.81	23.86	40.81
CIRCULAR	18.58	46.46	20.78	47.38

7.CONCLUSION

1. The crane hooks are successfully designed for four different cross sections such as rectangular, trapezoidal, triangular and circular by using curved beam concept.
2. The model was prepared using CATIA software and analysis has been carried out using ANSYS.
3. The trapezoidal cross section gives better results in comparison with other three cross sections as because stresses induced are less in trapezoidal cross section.
4. The stresses obtained in theoretical and analytical methods are in good agreement. The model prepared is used for further studied with different loads and also for different materials.

REFERENCES

[1] M. Shaban, M. I. Mohamed, A. E. Abuelezz and T. Khalifa, “Determination of Stress Distribution in Crane Hook by Caustic”, International Journal of Innovative Research in Science, Engineering and Technology, Vol. 2, Issue 5, May 2013.

[2] E. Narvydas, N. Puodžiūnienė, “Circumferential stress concentration factors at the asymmetric shallow notches of the lifting hooks of trapezoidal cross-section”, ISSN 1392 - 1207. MECHANIKA. 2012 Volume 18(2): 152-157.

[3] SpasojeTrifković, NebojšaRadić et. al, “Stress analysis of crane hook using FEM”, INFOTEH-JAHORINA Vol. 10, Ref. C-2, p. 244- 248, March 2011.

[4]Bhupender Singh, Bhaskar Nagar, B.S. Kadam and Anuj kumar, “Modeling and Finite Element Analysis of Crane Boom”, International Journal of Advanced Engineering Research and Studies, Vol. I/ Issue I/October-December, 2011/ 51-52.

[5] Y. Torres , J.M. Gallardo , J. Domínguez , F.J. Jiménez E, “Brittle fracture of a crane hook”, Engineering Failure Analysis 17 (2010) 38–47.

[6] Takuma Nishimura, Takao Muromaki et. al, “Damage Factor Estimation of Crane Hook (A Database Approach with Image, Knowledge and Simulation)”, 4th International Workshop on Reliable Engineering Computing (REC 2010).

[7] C. Oktay AZELOĞLU, Onur ALPAY, Investigation Stress of A Lifting Hook with Different Methods, “Verification of The Stress Distribution with Photo elasticity Experiments”, Electronic Journal of Machine Technologies, Vol: 6, No: 4, 2009 (71-79).

[8] Yu Huali, H.L. and Huang Xieqing, “Structure-strength of Hook with Ultimate Load by Finite Element Method”, Proceedings of the International Multi-Conference of Engineersand Computer Scientists, 2009 Vol II IMECS 2009, March 18 - 20, 2009, Hong Kong.

MECHANICAL BEHAVIOUR OF GROUNDNUT SHELL POWDER/ CALCIUM CARBONATE /VINYL ESTER COMPOSITE

R. Pragatheeswaran[1], S. Senthil Kumaran[2]
[1]PG Student, [2]Associate professor, College of Engineering, Guindy, Anna University
Email:[1]pragathees92@gmail.com, [2]metrosenk@gmail.com

Abstract— In recent years, natural fiber along with mineral fillers is used to fabricate hybrid composite which shows improved mechanical properties. In this study the effect of calcium carbonate on the mechanical properties of groundnut shell powder based composite was investigated. To meet this objective, groundnut shell powder(GNP) and calcium carbonate(CC) reinforced vinyl ester(VE) were prepared by hand lay-up process. The effects of calcium carbonate on tensile and flexural properties of the composites were investigated. The test result shows that increase in calcium carbonate increases the tensile and flexural properties of composites.

Index Terms— Groundnut shell powder, Calcium Carbonate, Vinyl ester, Natural Fiber Composite

I. INTRODUCTION

Natural fibers have become alternative reinforcement for synthetic fibers in polymer composites, due to their advantages like low density, less tool wear during processing, low cost, non-toxic, easy to process, environmental friendly, and biodegradability[1,8].

The natural fiber-containing composites are more environmentally friendly, and are used in various applications like automobiles, aerospace, railway coaches, military applications, building and construction industries and ceiling paneling, partition boards, packaging, consumer products, etc [2].

Several studies have been carried out on the composites made of groundnut, calcium carbonate and vinyl ester

G.C. Onuegbu et al(2013) [3] investigated the mechanical properties of polypropylene composites with ground nut husk powder at different particle sizes and found that the presence of ground nut husk improved the tensile strength, modulus, flexural strength and impact strength of the composites.

Behzad Kord (2011) [4] studied the effect of calcium carbonate as mineral filler on the physical and mechanical properties of wood based composites and found that the mineral filler loading had significant effects on the mechanical properties of wood based composites Vasanta V Cholachagudda et al (2013) [5] found that coir fiber as the major reinforcement and rice husk as an additional fiber improves the mechanical property of polymer composites were prepared by hand lay-up process according to ASTM standards, he also found that there is an increase in tensile and flexural.

II. MATERIALS AND PROCESSING

Lignin binds individual fiber cells together, the lignin content of groundnut shell fiber is much greater than that of banana, baggase, rice husk, jute, hemp, kenaf and sisal fibers and the hemicellulose influence moisture absorption of composites, the hemicellulose content of groundnut shell is less than rice husk, banana, wood, baggase and kenaf fibers[6]. Groundnut shell treated properly to remove impurities and it crushed to powder. Groundnut shell powder and calcium carbonate are mixed in different composition.

Table.1. shows the Chemical composition of various natural resources [6]

Species	Cellulose (wt%)	Hemi cellulose (wt%)	Lignin (wt%)
Pine (softwood)	40-45	25-30	26-34
Maple (hardwood)	45-50	22-30	22-30
Banana	63-64	19	5
Coir	32-43	0.15-0.25	40-45
Sisal	63-64	12	10-14
Jute	61-71.5	12-20.4	11.8-13
Kenaf	31-39	21.5	15-19
Hemp	70.2-74.4	17.9-22.4	3.7-5.7
Bagasse	40-46	24.5-29	12.5-20
Groundnut shell	**35.7**	**18.7**	**30.2**
Rice husk	31.3	24.3	14.3
Pineapple	81	-	12.7

Table.2. shows the volume and mass fraction of reinforcement and polymer used in the work.

	% of volume fraction			%mass (gram)		Volume (ml)
S.No	GNP	CC	VE	GNP	CC	VE
1	35	0	65	21.546	0	175.5
2	30	5	65	18.468	36.585	175.5
3	25	10	65	15.39	73.17	175.5
4	20	15	65	12.312	109.755	175.5

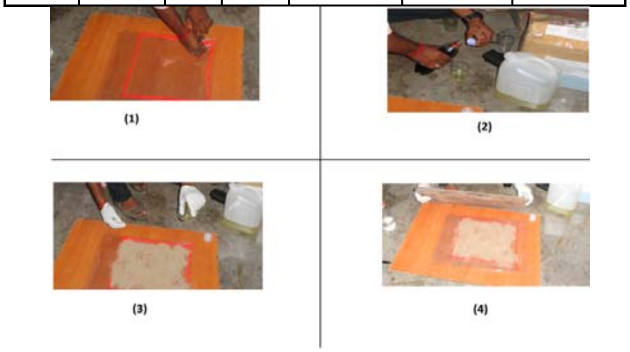


Figure.1. Shows the hand lay-up technique

(1) Placing the bottom mould plate with silicon rubber

(2) Adding catalyst, accelerator, promoter to resin

(3) Mixing resin to the fiber

(4) Closing with the top mould plate

The composite fibre is prepared by hand lay-up technique. A mould with the dimension of 300 mm × 300mm × 3mm was used to prepare the composite specimen[7]. Measured quantities of groundnut shell powder, calcium carbonate and vinyl ester resin were taken in a glass beaker and stirred thoroughly to get homogeneous mixture. Methyl Ethyl Ketone Peroxide is used as a catalyst to support the moulding process. Cobalt Naphthenate is used as an accelerator to speed up the reaction[9]. Dimethyl Acetamide is used as promoter to increase adhesion between a polymer and reinforcement. After adding the suitable quantity of resin, catalyst, accelerator and promoter, the mixture was again stirred for 10 minutes and thoroughly mixed mixture was placed in the mould and compressed uniformly. This set up allowed for curing and then the composite specimen was taken out from the mould.

III. Cutting Of Laminates Into Samples Of Desired Dimensions

A Wire Hacksaw blade was used to cut each laminate into smaller pieces, in accordance with ASTM standard.

The tensile test was generally performed on flat composite sample. The length of the test specimen was as per ASTM D638. The dimension of the specimen is 250 mm x 25 mm x 3 mm.

Flexural test is a 3-point bend test, which generally promotes failure by inter-laminar shear. This test is conducted as per ASTM standard D790 using Universal Testing Machine. The dimension of the specimen is 20mm x 150mm x 5mm.

IV. EXPERIMENTAL RESULTS

A. Tensile Test

The tensile strength of a material is the maximum amount of tensile stress that it can take before failure. The commonly used specimen for tensile test is the flat type. During the test a uniaxial load is applied through both the ends of the specimen. The results are tabulated in the table.3.

B. Flexural Test

Flexural strength is defined as a material’s ability to resist deformation under load. It is a 3-point bend test, which generally promotes failure by inter-laminar shear. The results are tabulated in the table.4.

Table.3. shows tensile load of specimen

Sample no.	Percentage of volume fraction			Maximum load (N)
	Ground nut powder	Calcium carbonate	Vinyl ester	
1	35	0	65	443
2	30	5	65	535
3	25	10	65	580
4	20	15	65	650

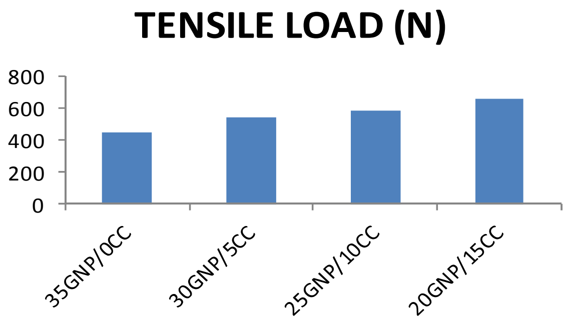


Figure.2. shows graph of tensile load of specimens

Table.4.shows flexural load of specimen

Sample no.	Percentage of volume fraction			Maximum load (N)
	Ground nut powder	Calcium carbonate	Vinyl ester	
1	35	0	65	20
2	30	5	65	40
3	25	10	65	42
4	20	15	65	48

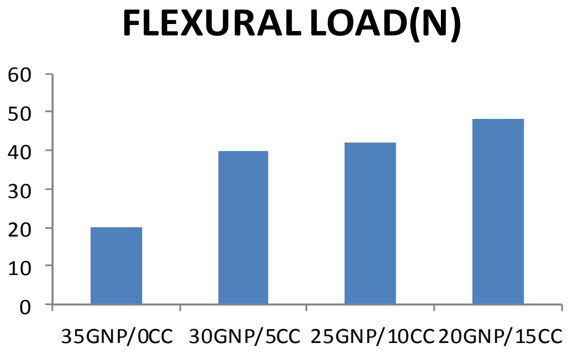


Figure.3.shows graph of flexural load of specimens

V. CONCLUSION

A new class of natural fiber based polymer composites groundnut shell powder and calcium carbonate reinforcement in the vinyl ester polymer is developed.

The experimental investigation on mechanical properties ie Tensile strength and flexural strength, groundnut shell powder/ calcium carbonate /vinyl ester composite ,material is greatly influenced by the groundnut shell powder/ calcium carbonate composition.

The maximum tensile load is obtained for the composite prepared With 20%GNP/15%CC. The tensile load graph (See Figure.2) shows an increase of calcium carbonate volume, increases the tensile load.

The maximum flexural load is obtained for the composite prepared with 20%GNP/15%CC. The flexural load graph (See Figure.3) shows an increase of calcium carbonate volume, increases the flexural load.

REFERENCES

[1] S.V.Joshia, L.T. Drzal, A.K.Mohanty, S.Arorac "Are natural fiber composites environmentally superior to glass fiber reinforced composites?", Composites Part A: Applied Science and Manufacturing, Vol.35(3), pp371-376, 2004

[2] D. Chandramohan,K.Marimuthu "A review on natural fibers", International Journal of

Research and Reviews in Applied Sciences, Vol.8(2),2011

[3] G.C. Onuegbu, S.C. Nwanonenyi, M.U.Obidiegwu "The Effect of Pulverised Ground Nut Husk on Some Mechanical Properties of Polypropylene Composites", International Journal of Engineering Science Invention, Vol.2(6), pp.79-83, 2013.

[4] Behzad Kord "Effect Of Calcium Carbonate As Mineral Filler On The Physical And Mechanical Properties Of Wood Based Composites", World Applied Science Journal, Vol. 13(1) pp 129-132, 2011.

[5] Vasanta V Cholachagudda , Udayakumar.P.A , Ramalingaiah "Mechanical characterisation of coir and rice husk reinforced hybrid polymer composite", International Journal of Innovative Research in Science, Engineering and Technology ,Vol. 2(8),2013.

[6] G. U. Raju, V. N. Gaitonde, S. Kumarappa, "Experimental Study on Optimization of Thermal Properties of Groundnut Shell Particle Reinforced Polymer Composites", International Journal of Emerging Sciences, Vol .2(3), pp 433-454, 2012.

[7] S.Muthukumar, K.Lingadurai "Investigating the mechanical behaviour of coconut shell and groundnut shell reinforced polymer composite", Global Journal Of Engineering Science And Researches, Vol.1(3) pp 2348 – 8034, 2014.

[8] N.P.G. Suardana, Yingjun Piao, Jae Kyoo Lim "Mechanical properties of hemp fibers and hemp/pp composites: effects of chemical surface treatment" Materials Physics and Mechanics , 2011.

[9] Afroz mehar, S.Irfan Sadaq, Sameer Mohammed, "Experimental Study and the Effect of Alkali Treatment with Time on Jute Polyester Composites", International Journal of Engineering Research, Vol.2(2), pp : 23-28, 2013.

A REVIEW OF SCHEDULING AND OPTIMIZATION TECHNIQUES

[1] INDU S. JAISWAR, [2]VINAY B.HARSORA
[1,2] R K UNIVERSITY
Email:[1]indujaiswar@gmail.com,[2]vinay.harsora@rku.ac.in

ABSTRACT:

Scheduling is repetitious process. To find optimal solution become complex one. This paper gives review of various scheduling and optimization techniques, this includes basic Local Search, Simulated Annealing, Greedy randomized constructive search procedure,Tabu search, Genetic Algorithm and Branch & bound.In this paper we presented this techniques in detail with their issues. Simulated Annealing does not provide guaranteed for the optimal solution. Tabu search is impractical in case of continuous neighborhood movement. Genetic Algorithm is Randomized Algorithm that provide different solutions for Each Independent Run. Various Variants of genetic Algorithm provide Optimal as well as feasible Solution for Scheduling Problems.

KEY WORDS: Scheduling and optimization, Simulated annealing, Greedy Randomized Constructive Search Procedure, Tabu Search, Genetic Algorithm

1. Introduction

Scheduling is allocation of resources over time to execute set of tasks. Scheduling carries two meanings, First Scheduling is process of forming the schedule. Second, collection of techniques and principles that gives perception into the scheduling function. In general, Scheduling invloves order of perfroming collection of tasks at predefine time slots using fiexd resources.Due to development and expansion, Scheduling problem exists in Educational Institutions, manufactoring and production systems,Trasportaion distribution system and many service situations.Educational Institutions Scheduling is alloction of particular course with respect to time schedule. I.e. course time tabling, exam time tabling.Production scheduling deals with actual implementation according to the time schedule for all jobs to be processed. Any Organization or System, Scheduling process interface with many other functions.

In general, to obtain fruitful results, effective scheduling of tasks and proper allocation of resources becomes mandotory. There are several methods, principles and techniques has been developed for solving such kind of problems. This paper gives brief introduction of optimization techniques, like Local Search Algorithm, Simulated Annealing, Greedy Randomized Constructive Search Procedure, Tabu Search, Genetic algorithms. All such techniques have different application area according to the problem definition. Flow shop schduling can be effectively solved with simulated annealing and university time tabling can be solved with Genetic algorithms

2. OPTIMIZATION TECHNIQUES

LOCAL SEARCH ALGORITHM (LSA)

Local Search algorithm need initial solution to begin. It process number of times and search the solution using neighbor generation method. LSA checks whether new solution is better than familiar one then use the better one.

Searching procedure will be stopped based on following criteria

- Quality of familiar solution fulfill the need.
- Algorithm processes fixed times
- No improvement in the results during last n iterations

LSA proceeds as follwing

- Load initial Solution
- Generate neighbor solution check if it is better solution, if better solution then remember the solution and check ending criteria else generate the neighbor solution.
- Now check current solution satisfies the needs and ending criteria are satisfied then store the current soltution and terminate.One of the drawback of the LSA is sometime it reach to the local optimum. Local optimum is point where all neighbor solutions have same value.

SIMULATED ANNEALING (SA)

The idea of SA comes from a paper published by Metropolis in 1953.SA is Analogous to physical annealing process. The annealing is a process of heating and controlled cooling of material to improve quality. During the annealing process, high temperature changes the atom positions, as temperature decreases changes likely to happen. SA does the same, SA overcomes the drawback of Local search algorithm.it allows Local search algorithm to pick a worse solution. The probability that every time worse solution is accepted is diminish with the time of algorithm. This is the main concept of annealing. The local search algorithm begins with initial temperature and it is slowly decreased. Once some criteria is satisfied the temperature is changed. The criteria that change the temperature level is same as ending criteria of LSA.Problem with the SA is it can not tell whether it has found optimal solution [3]

Greedy Randomized Constructive Search Procedure

GRCP creates initial solution for local search heuristic.it use dynamic algorithm for implementation. GRCP generate the solution step by step. At each step it generate the candidate list. Candidate list stores the element that may be used in soltution. Parameter p ∈ (0, 1) defines the length of the list. For 0, list contains only one solution. For 1, No restriction at all and algorithm may choose one of the solution from number of possible solution. An urgency indicator is computed for each candidate, lower value means more urgent the candidate. Urgency indicator is evaluated using the number of possible time slots that each elements can be assigned to.

```
GRCP implementation
Result=Nil
do
  {
   Candidate List=generateCandidateList ()

RestrictedCandidateList=restrictCandidateList()

Candidate=pickRandomly(restrictedCandidateList)
   Result = result + candidate
  Return result
 } while is Complete (result):
```

TABU SEARCH (TS)

Tabu search was invented by idea proposed by Fred Glover between 1977 and 1986.TS is one type of local search Meta heuristic.it is improvement over the Local Search algorithm by decreasing chances of local minima. TS use the memory structure that store visited solutions and user provided rules .if potential solution has been visited early and if it violates the rule then it marked as ‘tabu’. So that algorithm does not consider that solution again. TS is impractical in case of continuous neighborhood movement in search space.[4]

BRANCH AND BOUND

All the optimization problems can be solved with the group of algorithms. This algorithms search and evaluate the possible solution .In most of the cases,the number of solution is too large,so it cosume much time to assess every solution.More advanced technique available that minimize amount of solution require to evaluate.One such method is Branch and bound. As the name suggest, the concept of B&B includes Branching and bounding.

- In Branching Scheme, It makes group solution in one set and provide possibility to evaluate entire collection at once.
- In Bounding Scheme, It gives way of approximation of lower and upper bound of objective function value.

If lower bound of set of solution is higher than the value of known solution, the entire collection may be discarded, else set is split into smaller one and bounding of them take place. Considering the fact that lower bound is not higher than the already known solution if set holds only one optimal solution, such set will be split until it holds only one optimal solution. One of the issue of this B&B, it is hard to implement.it is insignificant to write an algorithm that use it.

GENETIC ALGORITHM (GA)

Genetic algorithm research launch in the late 1960 to the early 1970s by professor john holland, the University of Michigan. Genetic Algorithms works on principle of natural evolution and survival of fittest.GA use past information to explore the best solution from the previous searches, known as generations. GA includes three steps selection, crossover and random mutations.

GA works as follows.

1. Construct Initial Population.
2. Evaluate fitness value of Individuals.
3. Check Fitness value of Individual Satisfies the all Constrains. If Yes then it is ‘Best Individual’ else Perform Selection, Crossover and Mutation operation and generate the new population continue the procedure until the ‘Best Individual’ is found.

- **Crossover**
  Crossover is method that takes two solutions and mixes them to obtain new solution. Fitness function obtained by this operation may or may not be higher than the old solution.

- **Mutation**
  Mutation add or update the information random way to the search procedure and help to avoid the local minima.

VARIANTS OF GENETIC ALGORITHM

Simple Genetic Algorithm (SGA)

SGA is the simplest form of all other Variants. It maintain two pools of individuals. One is Parent pool and second is Child Pool. Size of both the pool kept same. Initially, Parent pool contains Initial Populations and Child Pool contain empty population. Two Individual from Parent Pool is Selected and Genetic Operations is applied which generate new Individual which are now placed in Child pool if it is better than their parents.

One of the drawback of the algorithm is child pool always start with null population. Child pool is replaced with the parent pool when it becomes full therefore old generation will not survived. So we may loss some good solutions. More resources are needed as it has to maintain two pools.

Generation Genetic Algorithm (GGA)

GGA also uses two pools. It resolve the Problem with SGA, first best parents copied into the second pool. So it makes the group of best solution.

Although it makes group of best solution, it does not provide the feasible solution. [1]

Steady State Genetic Algorithm (SSGA)

It uses only one pool. In SSGA, Two Individual from population is selected and GA operations are applied which produces new Individual which may or may not be better than their parents. If the fitness value of new Individual is less than their parents than it is discarded

otherwise, worst individual from the population is replaced with the new one.
It uses single pool. So need less resources. Algorithm may stuck to local minima and does not come out from that point. It does not provide feasible solution. [2]

Enhanced Steady State Genetic Algorithm (ESSGA)

ESSGA is Enhancement over the SSGA. It applies Fuzzy Logic on Crossover and Mutation Operation. It introduce new parameter "age" to determine weather crossover or mutation applicable or not. Age of the new Individual is Zero and it is gradually incremented depending on its survival in Schedule Process.

To Perform Crossover and Mutation Operation, Crossover Probability (Pc) and Mutation Probability (Pm) Determined. [1]

Age € [Young, Middle-age, Old]

TABLE I. FUZZY LOGIC FOR CROSSOVER PROBABILITY

	Individual I		
Individual II	Young	Mid-Age	Old
Young Mid-Age Old	Low Medium Low	Medium Medium Medium	Low Medium High

TABLE II. FUZZY LOGIC FOR MUTATION PROBABILITY

Individual			
Age	Young	Mid-Age	Old
Pm	High	Medium	Low

Modified Enhanced Genetic Algorithm (MESSGA)

MESSGA is Enhancement over the ESSGA, Enhancement is achieved by Introducing Fuzzy Logic during "Insertion" Process.

In Shiburaj's paper [1], It is proved that Fuzzy Logic during the Insertion Process has better convergence time compared to SSGA and ESSGA.

TABLE III. FUZZY LOGIC FOR INSERTION

Individual			
Age	Young	Mid-Age	Old
Pi	High	Medium	Low

MESSGA takes more time compared to SSGA and ESSGA due to additional steps in Insertion Process.

REFERENCES:

1. Shiburaj Pappu, K. T. Talele and K. V. Mehul, "Modified Enhanced Steady State Genetic Algorithm for Scheduling Optimization," 2013 Annual IEEE India Conference
2. AlSharafat W. S.; and AlSharafat M. S.;. Adaptive steady state genetic algorithm for scheduling university exams. In International Conference on Networking and Information Technology (ICNIT), pages 70–74, June 2010. Doi: 10.1109/ICNIT.2010.5508555.
3. M. König1 and U. Beißert2, "Construction Scheduling Optimization by Simulated Annealing", 26th International Symposium on Automation and Robotics in Construction (ISARC 2009)
4. Marek E. Skowro´nski, Paweł B. Myszkowski, Marcin Adamski, Paweł Kwiatek,"Tabu Search approach for Multi–Skill Resource–Constrained Project Scheduling Problem" Proceedings of the 2013 Federated Conference onComputer Science and Information Systems pp. 153–158
5. Arjun.K.R Dr. M. S Jayamohan, "Application of Simulated Annealing in Flow Shop Scheduling", International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization, Volume 2, Special Issue 1, December 2013
6. M. O. Odim, 2B. O. Oguntunde, 3O. O. Alli, "On the Fitness Measure of Genetic Algorithm for Generating Institutional Lecture Timetable," in Journal of Emerging Trends in Computing and Information Sciences April 2013.