Proceeding for International Conference

on

Emerging Trends

in

Engineering and Technology

Bengaluru

8th November'15

Institute for Engineering Research and Publication

(A Unit of VVERT)

4A, Girija Apartment, MMDA,

Arumbakkam,Chennai-600106,India

www.iferp.in

Publisher: IFERP Explore

Editorial:

We cordially invite you to attend the International Conference on Emerging Trends in Engineering and Technology (ICET-2015), which will be held in Hotel Pai Vaibhav, Bengaluru on November 8, 2015. The main objective of ICET-2015 is to provide a platform for researchers, engineers, academicians as well as industrial professionals from all over the world to present their research results and development activities in Electrical, Electronics, Mechanical, Civil, Computer Science and Information Technology. This conference provides opportunities for the delegates to exchange new ideas and experience face to face, to establish business or research relations and to find global partners for future collaboration.

These proceedings collect the up-to-date, comprehensive and worldwide state-of-art knowledge on software engineering, computational sciences and computational science application. All accepted papers were subjected to strict peer-reviewing by 2-4 expert referees. The papers have been selected for these proceedings because of their quality and the relevance to the conference. We hope these proceedings will not only provide the readers a broad overview of the latest research results on Electrical, Electronics, Mechanical, Computer Science and Information Technology but also provide the readers a valuable summary and reference in these fields.

The conference is supported by many universities and research institutes. Many professors plaid an important role in the successful holding of the conference, so we would like to take this opportunity to express our sincere gratitude and highest respects to them. They have worked very hard in reviewing papers and making valuable suggestions for the authors to improve their work. We also would like to express our gratitude to the external reviewers, for providing extra help in the review process, and to the authors for contributing their research result to the conference.

Since April 2015, the Organizing Committees have received more than 120 manuscript papers, and the papers cover all the aspects in Electrical, Electronics, Computer Science and Information Technology. Finally, after review, about 11 papers were included to the proceedings of ICET- 2015.

We would like to extend our appreciation to all participants in the conference for their great contribution to the success of International Conference 2015. We would like to thank the keynote and individual speakers and all participating authors for their hard work and time. We also sincerely appreciate the work by the technical program committee and all reviewers, whose contributions make this conference possible. We would like to extend our thanks to all the referees for their constructive comments on all papers; especially, we would like to thank to organizing committee for their hard work.

Editor-In-Chief
Dr. Nalini Chidambaram
Professor
Bharth University

Acknowledgement

IFERP is hosting the International Conference on Emerging Trends in Engineering and Technology this year in month of November. Technical advantage is the backbone of development and nanoelectronics has become the platform behind all the sustainable growth. International Conference on Emerging Trends in Engineering and Technology will provide a forum for students, professional engineers, academician, scientist engaged in research and development to convene and present their latest scholarly work and application in the industry. The primary goal of the conference is to promote research and developmental activities in Electrical, Electronics, Mechanical, Civil, Computer Science and Software, Information Technology and to promote scientific information interchange between researchers, developers, engineers, students, and practitioners working in and around the world. The aim of the Conference is to provide a platform to the researchers and practitioners from both academia as well as industry to meet the share cutting-edge development in the field.

I express my hearty gratitude to all my Colleagues, staffs, Professors, reviewers and members of organizing committee for their hearty and dedicated support to make this conference successful. I am also thankful to all our delegates for their pain staking effort to travel such a long distance to attain this conference .

Er. R. B. Satpathy
Secretary
Institute for Engineering Research and Publication(IFERP)

CONTENTS

ORGANIZATION COMMITTEE

MANAGING DIRECTOR
Dr. P. C. Srikanth
Head of the Department,
Department of ECE,
Malnad College of Engineering

PRESIDENT:
Dr. P A Vijaya
Professor, Department of ECE,
BNM Institute of Technology

ORGANIZING SECRETARY
Er. Rajesh Babu
Er. A. Siddharth

KEY NOTE SPEAKER
Prof.G P Ramesh
Head of the Department,Department of ECE,
st.Peter's University

PUBLICATIONS COMMITTEE
Dr. Shankar Narayanan
Dr.S. Sangeetha

PROGRAM CHAIR
Dr. Nalini Chidambaram
Professor
Bharth University

Sensing vulnerabilities and multiple spoofing adversaries in wireless LAN

[1] S.karthika [2] A.kanagalakshmi
[1] PG student, ME Communication Systems, Sree Sastha institute of engg & tech,
Chennai-123, [1] karthika.isro@gmail.com
[2] Assistant Professor ,Department of ECE, Sree Sastha institute of engg & tech,Chennai-123

Abstract- **Wireless spoofing attacks easy to launch and can significantly impact the performance of networks. The identity of a node verified through cryptographic authentication, conventional security approaches are not always desirable because of their overhead requirements. The spatial information of physical property associated with each node, hard to falsify and not reliant on cryptography, as the basis for detecting spoofing attacks, determining the number of attackers when multiple adversaries masquerading as the same node identity and localizing multiple adversaries. The formulation of determining the number of attackers as a multiclass detection problem. This project requires Request Storms (RS) algorithm to determine the number of attackers. This RS algorithm used for sending and receiving continuous packet transmission storms and detect malicious intruder using intensity based localization. The RS algorthim detect the unauthorized Internet Protocol / Medium Access Control (IP / MAC) and copy to the Access Control List (ACL), easy to detect and localize the intruder in the network. The integrated detection and localization system that can localize the positions of multiple attackers.**

Key words-**Spoofing,Internetprotocol,Medium access control protocol, Access control list.**

I. INTRODUCTION

A Wireless Local Area Network (WLAN) is a flexible data communications system that can use either infrared or radio frequency technology to transmit and receive information over the air. In 1997, Institute of Electrical and Electronics Engineers (IEEE) 802.11 was implemented as the first WLAN standard. It is based on radio technology operating in the 2.4 GHz. frequency and has a maximum throughput of 1 to 2 Mbps.

A.Overview

WLAN has been widely used in many sectors ranging from corporate, education, finance, healthcare, retail, manufacturing and warehousing. According to a study by the gartner group, approximately 74 percent of company laptops around the world will be equipped for WLAN by the end of 2013. It has increasingly becoming an important technology to satisfy the needs for installation flexibility, mobility, reduced cost of ownership and scalability.

Wireless networks are vulnerable to identity based attacks, including spoofing attacks, significantly impact the performance of networks. The generalized spoofing attack detection model generate unique identifier for each wireless nodes and a physical property associated with each node, as the basis for detecting spoofing attacks, finding the number of attackers when multiple adversaries masquerading as a same node identity and localizing multiple adversaries. Cluster based mechanisms are developed to determine the number of attackers.

In identity based spoofing attacks, an attacker can forge its identity to masquerade as another device or even create multiple illegitimate identities in the networks by masquerading as an authorized wireless Access Point (AP) or an authorized client. An attacker can launch Denial of Service (DoS) attacks, bypass access control mechanisms, or falsely advertise services to wireless clients. Therefore, identity based attacks will have a serious impact to the normal operation of wireless and sensor networks. Spoofing attacks can further facilitate a variety of traffic injection attacks such as attacks on access control lists, rogue AP attacks, and eventually DoS.

II. SECURITY THREATS OF WIRELESS LOCAL AREA NETWORK

Despite The Productivity, Convenience And Cost Advantage That Wlan Offers, The Radio Waves Used In Wireless Networks Create A Risk Where The Network Can Be Hacked. This Section Explains Three Examples Of Important Threats :Dos, Spoofing, And Eavesdropping.

A.*Denial Of Service*

In this kind of attack, the intruder floods the network with either valid or invalid messages affecting the availability of the network resources. Due to the nature of the radio transmission, the WLAN are very vulnerable against DoS attacks. The relatively low bit rates of WLAN can easily be overwhelmed and leave them open to DoS attacks. By using a powerful enough transceiver, radio interference can easily be generated that would enable WLAN to communicate using radio path. In computing, a DoS is an attempt to make a machine or network resource unavailable to its intended users. The target of a DoS attack vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend service of a host connected to the Internet. DoS attacks typically target sites or services hosted on high profile web servers such as banks, credit card payment gateways and even root nameservers.

B.Spoofing And Session Hijacking

This Is Where The Attacker Could Gain Access To Privileged Data And Resources In The Network By Assuming The Identity Of A Valid User. This Happens Because Ieee 802.11 Networks Do Not Authenticate The Source Address, Which Is Medium Access Control (Mac) Address Of The Frames. Attackers May Therefore Spoof Mac Addresses And Hijack Sessions. Moreover, Ieee 802.11 Does Not Require An Ap. This Facilitates Attackers Who May Masquerade As Ap. In Eliminating Spoofing, Proper Authentication And Access Control Mechanisms Need To Be Placed In The Wlan.

C.Eavesdropping

Eavesdropping involves attack against the confidentiality of the data that is being transmitted across the network. By their nature, WLAN intentionally radiates network traffic into space. This makes it impossible to control who can receive the signals in any WLAN installation. In the wireless network, eavesdropping by the third parties is the most significant threat because the attacker can intercept the transmission over the air from a distance, away from the premise of the company.Eavesdropping can also be done over telephone lines, email, instant messaging and other methods of communication considered private. The communications is also vulnerable to electronic eavesdropping via infections such as trojans.

III. SPOOFING ATTACKS

More wireless networks are deployed, they will increasingly become tempting targets for malicious attacks. Due to the openness of wireless networks, they are especially vulnerable to spoofing attacks where an attacker forges its identity to masquerade as another device, or even creates multiple identities. Spoofing attacks are a serious threat as they represent a form of identity compromise and can facilitate a variety of traffic injection attacks, such as evil twin AP attacks. Attacker can easily break the wireless AP security and easily enter using some tools like cain and abel, wireshark and ethereal etc. When attacker entry is possible, then attacker wants to get some user credentials like username, password, balance amount, credit card number and other valuable information.

A.Possible Spoofing Attacks

Spoofing occurs when a hacker inside or outside a network impersonates the conversations of a trusted computer. Two general techniques are used during spoofing :

A hacker uses an Internet Protocol (IP) address that is within the range of trusted IP addresses.A hacker uses an authorized external IP address that is trusted.Spoofing is a technique an attacker send fake spoofed Address Resolution Protocol (ARP) messages onto a Local Area Network (LAN). Generally, the aim is to associate the attacker's MAC address with the IP address of another host (such as the default gateway) causing any traffic meant for that IP address to be sent to the attacker instead. A hacker uses an authorized external IP address that is trusted. ARP spoofing may allow an attacker to intercept data frames on a LAN, modify the traffic, or stop the traffic altogether. Often the attack is used as an opening for other attacks, such as DoS, man in the middle or session hijacking attacks.Session hijacking occurs in the context of a user, whether human or computer. The user has an on going connection with a server. Hijacking is said to occur when an attacker causes the user to lose connection and the attacker assumes identity and privileges for a period.Spoofing attacks are broadly classified into two types resource depletion attacks and masquerading attacks.

B.Resource Depletion Attack

In resource depletion attacks, an attacker sends high rate of request messages using random MAC values in order to emulate a high number of clients and consume scarce resources in the network.An attackerdepletes a resource to the point that the target’s functionality is affected as shown in fig. 3.2. Virtually any resource necessary for the target’s operation can be targeted in this

attack. The result of a successful resource depletion attack is usually the degrading or denial of one or more services offered by the target. Resources required will depend on the nature of the resource to be depleted, the amount of the resource the target has access to and other mitigating circumstances such as the target's ability to shift load, detect and mitigate resource depletion attacks.

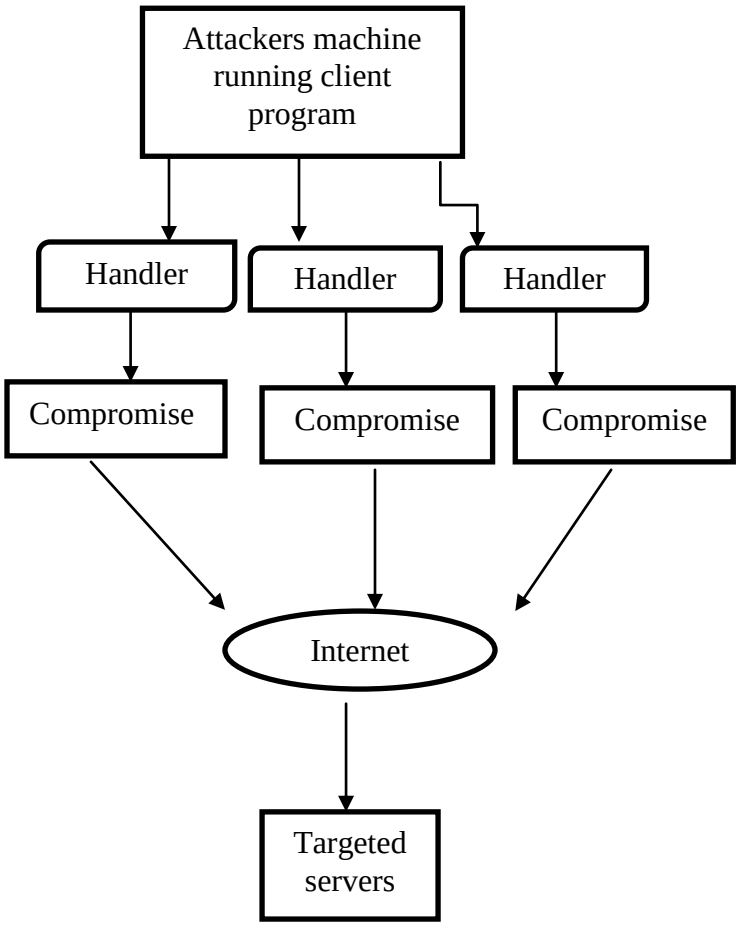


Fig. 1Resource Depletion Attack

Resource depletion can target endpoint hosts like servers and workstations as well as network resources like processing capability or memory consumption for normal operation. Resource depletion can also target exhaustion of bandwidth capabilities but the final goal is to make a DoS attack to the service. Virtually any resource necessary for the target's operation can be targeted in this attack. The more protected the resource and the greater the quantity of it that must be consumed, the more resources the attacker will need to have at their disposal.To prevent resource depletion monitor normal network activity and disable unnecessary services that could be used for undesired network device utilization. To avoid bandwidth exhaust should configure Quality of Service (QoS) at the perimeter of Wide Area Network (WAN) network to prioritize important traffic. If the network is at the edge of its capabilities because of bottlenecks in network should consider upgrading the weakest nodes or increasing the available bandwidth.

The result of a successful resource depletion attack is usually the degrading or denial of one or more services offered by the target. Resource depletion can target endpoint hosts like servers and workstations as well as network resources like processing capability or memory consumption for normal operation. The successful resource depletion attack is usually the degrading or denial of one or more services offered by the target. Vulnerable authentication is one of the other factors that can trigger a attack, as it helps the attacker to gain access much more easily.

C.Masquerading Attack

In masquerading attacks, an attacker targets a specific client by cloning its MAC address or the address of its AP. A masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification. If an authorization process is not fully protected, it can become extremely vulnerable to a masquerade attack.The attack can be triggered either by someone within the organization or by an outsider if the organization is connected to a public network.The amount of access masquerade attackers get depends on the level of authorization they have managed to attain. The target has access to, and other mitigating circumstances such as the target's ability to shift load. As such, masquerade attackers can have a full smorgasbord of cybercrime opportunities if they have gained the highest access authority to a business organization. Personal attacks, although less common, can also be harmful.

Masquerade attacks may happen in a number of ways. In case of an insider attack, a masquerade attacker gains access to the account of a legitimate user. Vulnerable authentication is one of the other factors that can trigger a masquerade attack, as it helps the attacker to gain access much more easily. Once the attackers gain access, they can get into all of the organization's critical data and can delete or modify it. For example, although a unique IP address is assigned to each individual computer, a hacker can convince another system that it is the authorized user through spoofing, essentially convincing the target computer that the hacker's computer has the same IP.

IV. PROPOSED SYSTEM

The proposed system will lead to develop Request Storms (RS) algorithm. In RS algorithm, the ARP duplicate IP address detection is already turned on by default and it have features to uncover the detect ARP, RS function. This

function can also provide summaries of ARP flooding and ARP spoofing attack events as shown in fig 2. ARP flooding and spoofing attack is even capable of indicating which frames should be further investigated because they were involved in an attack.

A.System Requirements

The requirements specification is a technical specification of requirements for the software products. It is the first step in the requirements analysis process it lists the requirements of a particular software system including functional, performance and security requirements. The hardware requirements consist of processor type, speed, Random Access Memory (RAM) and hard drive. The purpose of software requirements specification is to provide a detailed overview of the software project, its parameters and goals. This describes the project target audience and its user interface, hardware and software requirements.

B.Java

Java programming language was originally developed by Sun Microsystems which was initiated by James Gosling and released in 1995 as core component of Sun Microsystems' Java platform (Java 1.0). In java, everything is an object. Java can be easily extended since it is based on the object model.With Java's secure feature it enables to develop virus-free, tamper-free systems. Authentication techniques are based on public key encryption.Java is designed to be easy to learn.Java enables high performance.Java is designed for the distributed environment of the internet.

C.Java Swing

Swing is an advanced Graphical User Interface (GUI) toolkit. It has a rich set of widgets.Swing is a part of Java Foundation Classes (JFC). It is a collection of packages for creating full featured desktop applications. JFC consists of Abstract Window Toolkit (AWT), swing, accessibility, java 2Dimensional (2D) and drag and drop. The java platform has java2D library, which enables developers to create advanced 2D graphics and imaging.

There are basically two types of widget toolkits. Light weight and Heavy weight.

A heavyweight toolkit uses Operating Systems (OS) Application Programming Interface (API) to draw the widgets. For example Borland's Visual Computing Library (VCL), is a heavyweight toolkit.

V. ESTABLISHING WIRELESS NETWORK AND MONITORING

WPA is a mechanism provides pre shared key between AP and nodes. So using that key only, anyone can enter into the network. It also uses data integrity check. It is possible to easily analyze integrity of the received data. Establishing secure wireless networks is very important, because any intruder can poison the network at any time. Two kinds of authentication mechanisms used in Wired Equivalent Privacy (WEP). WPA provides pre shared key between AP

and nodes. So anyone can enter into the network. It is possible to easily analyze integrity of the received data.The status of system as shown in fig. 2 Establishing secure wireless networks is very important, because any intruder can poison the network at any time.

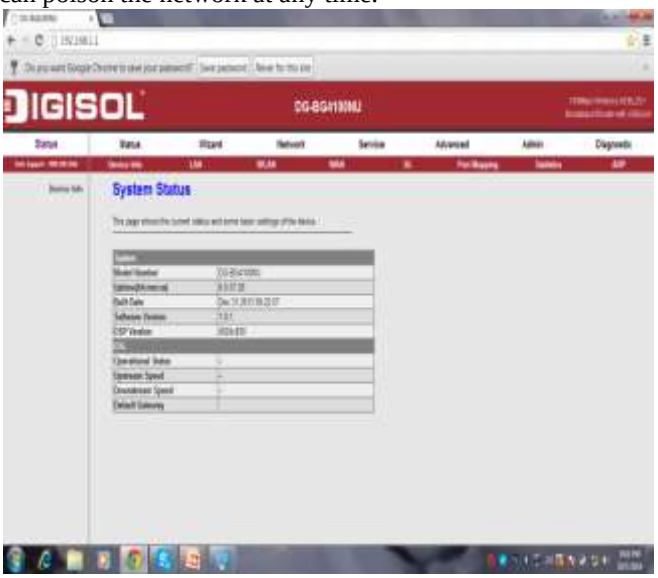


Fig.2 System Status

A. Cracking Wired Equivalent Privacy

A password and cryptography attack that does not attempt to decrypt any information, but continue to try a list of different passwords, words or letters. For example, a simple brute force attack may have a dictionary of all words or commonly used passwords and cycle through those words until it gains access to the account as shown in fig. 3.Although a brute force attack may be able to gain access to an account eventually, these attacks can take several hours, days, months and even years to run. The amount of time it takes to complete these attacks is dependent on the complexity of the password, the strength of the encryption, how well the attacker knows the target and the strength of the computers being used to conduct the attack.

Fig.3 Wireless Basic Settings

B. Attack Detection

The RS algorithm is used for sending and receiving continuous packet transmission storms and detects the malicious intruder using intensity based localization. From RS algorithm can get ARP flooding or ARP spoofing attack events. Using this, it is possible to add this detected IP / MAC to ACL. In this way, it is easy to detect and localize the intruder.

C. LOCALIZATION

In this phase, attacking the network using some tools, like wireshark, cain&abel. When anyone tries to intrude this secure network, the RS algorithm will detect the unauthorized IP / MAC and copy it to the ACL. So, it is very easy to detect and localize the intruder in a network as shown in fig. 4.

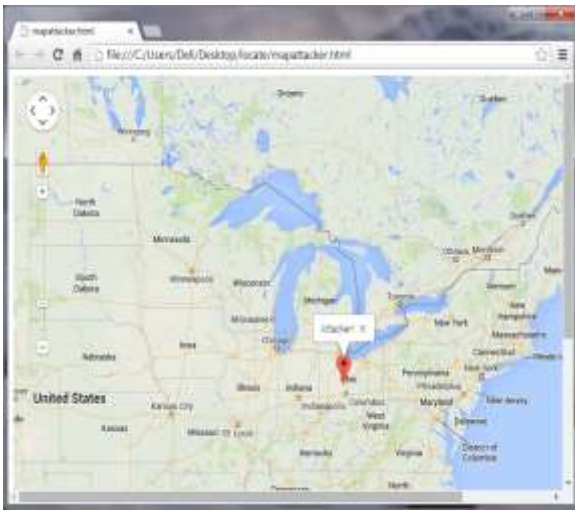


Fig.4Localization Attacker Using Internet Protocol

Based on the work the sensor energy levels at the individual nodes to calculate target object localizations and show that this does not add excessive amounts of computation or communication compared to a plain tracking algorithm such as envirotrack. On the contrary, knowing the current and past locations of the target objects also helped them with the tracking aspect as it enable to predict the object's future path.

CONCLUSION AND FUTURE WORK

As wireless networks are integrated with our daily social lives and there is an increasing need to support emerging mobile wireless applications. One serious class of threats that will affect the successful deployment of mobile wireless applications are spoofing attacks. In this work, proposed an unique approach to detect spoofing attacks in mobile wireless environments, which is a problem that has not been addressed in previous work. This approach can detect the presence of attacks as well as determine the number of adversaries, spoofing the same node identity, so that it is possible to localize any number of attackers and eliminate them. Determining the number of adversaries is a particularly challenging problem. By developing a strong algorithm it will be possible to spoof vulnerabilities and detect number of adversaries in wireless LAN. Further, based on the number of attackers will be determined by this mechanism. The integrated detection and localization system can localize any number of adversaries even when attackers using different transmission power levels. The performance of localizing adversaries achieves similar results as those under normal conditions, thereby, providing strong evidence of the effectiveness of the approach in detecting wireless spoofing attacks, determining the number of attackers and localizing adversaries.This project can also be extended to applications such as military application and organization.

REFERENCES

1. Abu A. and Abed R. (2010) 'Enhancement of Passive MAC Spoofing Detection Techniques', (IJACSA) International Journal of Advanced Computer Science and Application, Vol. 1, No. 1, pp. 11-18.
2. Chandrasekaran and Francisco (2009) 'Detecting Identity Spoofs in IEEE 802.11e Wireless Networks', Global Telecommunications Conference, Vol. 1, No. 1, pp. 1-6.
3. Jieyang, Yingying and Trappe (2009) 'Detecting Spoofing Attacks in Mobile Wireless Environments', IEEE trans. Communications

Society Conference on Digital Object Identifier, Vol. 2, No. 1, pp. 1-9.

4. Lifeng S. and Arora (2008) 'Spatial Signatures for Lightweight Security in Wireless Sensor Networks', IEEE International Conference on Computer Communications, Vol. 4, No. 1, pp. 17-23.
5. Misra and Gosh (2007) 'Detection of Identity Based Attacks in Wireless Sensor Networks Using Signal Prints', IEEE International Conference on Cyber, Physical and Social Computing, Vol. 7, No. 1, pp. 35-41.
6. Quing L. and Trappe (2007) 'Detecting Spoofing and Anomalous Traffic in Wireless Networks via Forge-Resistant Relationship', IEEE trans. Information on Forensics and Security, Vol. 2, No. 1, pp. 4-9.
7. Wool (2005) 'Lightweight Key Management for IEEE 802.11 WLAN With Key Refresh and Host Revocation', Springer Wireless Networks, Vol. 11, No. 2, pp. 677-686.
8. Yang and Trappe (2013) 'Detection and Localization of Multiple Spoofing Attackers in Wireless Networks', IEEE trans. Parallel and Distributed System, Vol. 9, No. 1, pp. 44-58.
9. Ying and wade T. (2013) 'Detecting and Localizing Identity Based Attacks in Wireless and Sensor Networks', IEEE trans. Vehicular Technology, Vol. 59, No. 1, pp. 62- 68.

Machining zone Area in Single Point Diamond Turning

[1]Venkatraman. B, [2]Om Kumar. M, [3]Ganesan. G, [4]Balaji .R , [5]Neha Khatri, [6]Ramagopal V Sarepaka
[1][2][3][4] College of Engineering Guindy, Anna University Chennai, India-600025
[5][6] CSIR-Central Scientific Instruments Organisation, Chandigarh, India-160030
[1] vramb13@gmail.com,[2]omkumar2000@yahoo.com

Abstract: **Heat is generated during most of the machining process. The generated heat causes the physical changes in the workpiece such as phase transformation, micro-crack formation, residual stresses, deviation in surface texture etc. These changes cause failure in getting the required shape and size of the component. In some cases workpiece dimension deviates from the required tolerance limit. Hence, the material will deviate from its functionalities. The heat generated should be analysed and it should be minimised by optimizing the field parameters. The major factors that cause heat to be generated are feed, depth of cut and speed. These parameters cause local plastic deformation and the chips to form from the machining zone. In most of the cases, the chip will take the maximum of heat generated during machining. The remaining heat will transferred in to the material as a residue. The calculation of heat affected zone and the machining area helps us to optimize the amount of heat transferred through the material by knowing the Volume of material removal. This proposed paper aids to calculate the machining zone area in Single Point Diamond Turning (SPDT). The shear stress acting in this area causes the plastic deformation of the material and thereby let to heat generation.**

Keywords— **Diamond Turning, Heat generation zone, Surface Finish in Nano Level, shear failure**

I. INTRODUCTION

The ultra precision Single Point Diamond Turning (SPDT) technology has been developed for over 40 years and has been successfully applied to numerous fields [1]. At present, the ultra precision single point diamond turning technology already expanded to Single Point Diamond Machining (SPDM) technology, which includes several related processes in addition to the more conventional single point diamond turning [2]. The related technologies have undergone significant renovations with features such as high resolution glass scales, high speed CNC controls, high speed spindle, DC linear motor, Fast Tool Servo (FTS), Slow Tool Servo (STS), broaching, and fly cutting and high precision on-machine measurement technique [3]. The primary objective in diamond turning operations is to produce products with low cost and high quality, with a lower number of cuts. Parameter optimization plays an important role in achieving this goal. It can be classified into two types. There are controlled parameters and uncontrolled parameters. Controlled parameters are called as machining parameters .Uncontrolled parameters are Temperature, vibration and material homogeneity [4]. Machining parameters optimization in a diamond turning operation usually involves the optimal selection of cutting speed, feed rate, depth of cut, number of passes , tool over hang, spindle speed, tool nose radius, etc[5,6]. Thermal issues are generally taken care by application of coolant. Alcohol based coolant is generally used in diamond turning to ensure surface finish. In some materials it has been observed experimentally that the use of coolant in case of polycarbonates hampers the surface quality, so dry cutting is preferable. Even after use of coolant the surface roughness profile (Ra) and surface waviness profile (Pt) deteriorates to some extent [7]. Hence, there may be some issues due to residue heat component transferred into the material. So, there is a need to find a relation of temperature distribution, residue heat going into the workpiece during machining as a function of machining parameters, material property. Such that the optimum combination of these parameters would result in minimal residue heat transfer for next machining cycles [8]. In this study, the area where the heat is being generated is identified and the proposed mathematical modeling is also provided.

II. MATHEMATICAL MODELLING

The mathematical modelling for heat generation zone in the machining operation by considering two distinct cases are given as follows,

A. Case I

Depth of cut is equal to the tool nose radius

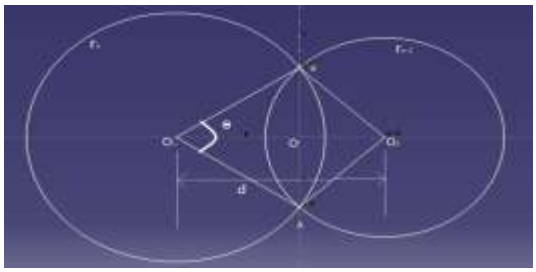


Figure 1. Formation of lens like shape between intersections of two circles

In conventional machining process the depth of cut can be assign a value equal to the tool nose radius.

The area of lens segment is given by,

$$A = \pi r_n^2 \sin^{-1}\left(\frac{d}{2r_n}\right) - \frac{1}{2}bh + \pi r_{n-1}^2 \sin^{-1}\left(\frac{d}{2r_{n-1}}\right) - \frac{1}{2}bh \quad (1)$$

$$A = \pi r_n^2 \sin^{-1}\left(\frac{d}{2r_n}\right) - \frac{1}{2}(2OB).d_1 + \pi r_{n-1}^2 \sin^{-1}\left(\frac{d}{2r_{n-1}}\right) - \frac{1}{2}(2OB).d_2 \quad (2)$$

$$A = \pi r_n^2 \sin^{-1}\left(\frac{d}{2r_n}\right) - OB.d_1 + \pi r_{n-1}^2 \sin^{-1}\left(\frac{d}{2r_{n-1}}\right) - OB.d_2 \quad (3)$$

Figure 2. Hatched portion shows the common material to be machined during subsequent feed cycle

Thus, the area of one of the hatched portion is given by,

$$A = \frac{1}{2}\left(\pi r_n^2 \sin^{-1}\left(\frac{d}{2r_n}\right) - OB.d_1 + \pi r_{n-1}^2 \sin^{-1}\left(\frac{d}{2r_{n-1}}\right) - OB.d_2\right) \quad (4)$$

$$A = \frac{1}{2}\left(\pi r_n^2 \sin^{-1}\left(\frac{d}{2r_n}\right) + \pi r_{n-1}^2 \sin^{-1}\left(\frac{d}{2r_{n-1}}\right)\right) - \frac{OB}{2}[d_1 + d_2] \quad (5)$$

Here,

$$d_1 = \frac{r_n^2 - r_{n-1}^2 + d^2}{2d}$$

$$d_2 = d - d_1$$

$$OB = \sqrt{r_n^2 - d_1^2}$$

For 'n' number of circles, the value of 'r' differs,

$r = r_n, r_{n-1}, r_{n-2}, r_{n-3}, \dots, r_n$

$$A = \frac{1}{2}\left(\pi r_n^2 \sin^{-1}\left(\frac{d}{2r_n}\right) + \pi r_{n-1}^2 \sin^{-1}\left(\frac{d}{2r_{n-1}}\right)\right) - \sqrt{(r_n^2 - d_1^2)}.[d_1 + d - d_1] \quad (6)$$

$$A = \frac{1}{2}\left(\pi r_n^2 \sin^{-1}\left(\frac{d}{2r_n}\right) + \pi r_{n-1}^2 \sin^{-1}\left(\frac{d}{2r_{n-1}}\right)\right) - \sqrt{(r_n^2 - d_1^2)}.[d] \quad (7)$$

In machining operation, the consecutive tool nose radius will be the same, irrespective of tool wear.

Thus, $r_n = r_{n-1}$

The equation (7) becomes,

$$A = \frac{1}{2}\left(\pi r_n^2 \sin^{-1}\left(\frac{d}{2r_n}\right) + \pi r_n^2 \sin^{-1}\left(\frac{d}{2r_n}\right)\right) - \mathrm{d}.\sqrt{(r_n^2 - d_1^2)} \quad (8)$$

$$A = \frac{r_n^2}{2}\left(\pi.\sin^{-1}\left(\frac{d}{2r_n}\right) + \pi.\sin^{-1}\left(\frac{d}{2r_n}\right)\right) - \mathrm{d}.\sqrt{(r_n^2 - d_1^2)}$$

$$A = \frac{r_n^2}{2}\left(2.\pi.\sin^{-1}\left(\frac{d}{2r_n}\right)\right) - \mathrm{d}.\sqrt{(r_n^2 - d_1^2)}$$

$$A = r_n^2\pi.\sin^{-1}\left(\frac{d}{2r_n}\right) - \mathrm{d}.\sqrt{(r_n^2 - d_1^2)} \quad (9)$$

Figure 3. Sectional view of volume of material removal

The volume of material removal follows the series of hemispherical path gives rise to surface roughness profile, the volume of material removal can be calculated by the following relation,

$$V = A \times 2\pi r_n$$

$$V = 2\pi^2.r_n^3.\sin^{-1}\left(\frac{d}{2r_n}\right) - 2\pi r_n.\mathrm{d}.\sqrt{(r_n^2 - d_1^2)} \quad (10)$$

The machining of materials follows the spiral coil path, thus the length of spiral should be calculated.

The spiral coil path is shown in the figure 4.

Figure 4. Tool-movement along Spiral coil path

The Calculation of the length of spiral at given feed and specimen size is as follows.

Number of turns, $N = \frac{D_0}{2.f}$

Calculation of length of coil

$L_1\ at\ D_1 = f;$

$L_2\ at\ D_2 = \pi(D_1 + 2.f);$

$L_3\ at\ D_3 = \pi(D_1 + 4.f); \dots$

$L_n at\ D_n = (D_1 + 2.(N-1)f)$

Total Length of coil,

$$L = L_1 + L_2 + L_3 + \cdots + L_n$$

$$L = f + \pi(D_1 + 2.f) + \pi(D_1 + 4.f) + \cdots + \pi(D_1 + 2.(N-1)f) \quad (11)$$

[∵ D1 changes for hollow specimens, it should be written as it is]

Here $D1 = f$

$$L = f + \pi.\{N.f + 2.f.[1 + 2 + 3 + \cdots + (N-1)]\}$$

$$L = f + \pi.\left[N.f + 2.f.\left(\frac{N.(N-1)}{2}\right)\right]$$

$$L = f.[1 + \pi.N^2] \quad (12)$$

Thus the volume of material removed will be,

$$V = L.A$$

$$V = f.[1 + \pi.N^2].r_n^2\pi.\sin^{-1}\left(\frac{d}{2r_n}\right) - \mathrm{d}.\sqrt{(r_n^2 - d_1^2)} \quad (13)$$

The above relation is used only when the depth of cut is equal to the tool nose radius. It is noted in the case of conventional lathe operations. In the case of diamond turning, the machining occurs is in the ductile regime zone. For that condition, the depth of cut will be only a proportion of tool nose radius.

B. Case II

Depth of cut - not equal to the tool nose radius

For brittle materials, crack propagation is more during machining. To reduce this crack propagation and the associated failure, Ductile Regime Machining has been chosen. In ductile regime machining, the plastic flow of material occurs in the form of severely sheared machining chips. This is possible due to High Pressure Phase Transformation (HPPT) or direct amorphization. The plastic deformation caused from highly localized contact pressure and shear stresses. For this, High pressure (metallic) phase could be used to improve manufacturing processes and ductile response during machining.

Area at the machining zone is given in the Figure 5.

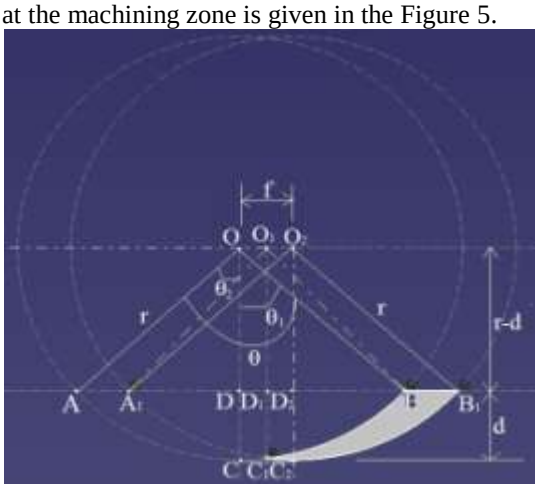


Figure 6. Heat generation Area with respect to tool nose radius and depth of cut

The shaded portion in the figure (5) is the area at the machining zone. To calculate this area, following steps are used,

In segment, AOB,

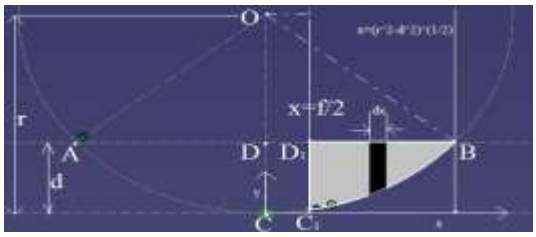


Figure 7. Element 'dx' along 'x' direction

The element 'dx' changes from the line passing through C_1 and B; traces the curve boundary of radius 'r'.

The equation of line passing through the point C_1 is $x = \frac{f}{2}$.

The equation of curve with radius 'r' from origin is given by,

$$x^2 + y^2 = r^2 \quad (14)$$

Thus,

$$x = \sqrt{r^2 - y^2}$$

$$x = \sqrt{r^2 - d^2} \ [\because y = d]$$

Thus the equation of line passing through the point B is $x = \sqrt{r^2 - d^2}$ ant the point of intersection of the curve and this line is given by, $(\sqrt{r^2 - d^2}, d)$

To calculate the area of the shaded portion,

$$A = \int_{\frac{f}{2}}^{\sqrt{r^2-d^2}} \left(\sqrt{r^2 - x^2} - \frac{f}{2}\right) dx \quad (15)$$

$$A = \left[\frac{x.\sqrt{r^2-x^2}}{2} + \frac{r^2}{2}.\sin^{-1}\left(\frac{x}{r}\right) - \frac{f.x}{2}\right]_{\frac{f}{2}}^{\sqrt{r^2-d^2}} \quad (16)$$

$$A = \left[\frac{\sqrt{r^2-d^2}.\sqrt{r^2-\left(\sqrt{r^2-d^2}\right)^2}}{2} + \frac{r^2}{2}.\sin^{-1}\left(\frac{\sqrt{r^2-d^2}}{r}\right) - \frac{f.\sqrt{r^2-d^2}}{2} - \frac{\frac{f}{2}.\sqrt{r^2-\left(\frac{f}{2}\right)^2}}{2} - \frac{r^2}{2}.\sin^{-1}\left(\frac{f}{2.r}\right) + \frac{f^2}{4}\right] \quad (17)$$

$$A = \left[\frac{d.\sqrt{r^2-d^2}}{2} + \frac{r^2}{2}.\sin^{-1}\left(\frac{\sqrt{r^2-d^2}}{r}\right) - \frac{f.\sqrt{r^2-d^2}}{2} - \frac{f.\sqrt{4r^2-f^2}}{8} - \frac{r^2}{2}.\sin^{-1}\left(\frac{f}{2.r}\right) + \frac{f^2}{4}\right] \quad (18)$$

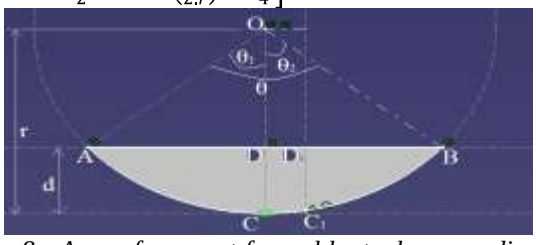


Figure 8. Area of segment formed by tool nose radius with respect to depth of cut

To find the area of the segment ACBA,

$$\theta_1 = \cos^{-1}\left[\frac{r-d}{r}\right] \quad (19)$$

$$\sin\theta_1 = \frac{BD}{OB}$$

$$BD = r\sin\theta_1 \ [\because OB = r] \quad (20)$$

Since, orthogonal cutting in diamond turning gives better surface finish for ductile materials. We can say $\theta_1 = \theta_2 ; \theta = \theta_1 + \theta_2; \theta = 2\theta_1$.

$$\theta = 2.\cos^{-1}\left[\frac{r-d}{r}\right] \quad (21)$$

$$A = \frac{\theta}{360}.\pi.r^2 - \frac{1}{2}.AB.OD \quad (22)$$

$$A = \frac{\theta}{360}.\pi.r^2 - \frac{1}{2}.2.r.\sin\theta_1.(r-d) \quad (23)$$

$$A = \frac{\theta}{360}.\pi.r^2 - r.\sin\left(\frac{\theta}{2}\right).(r-d)$$

(or)

$$A = \frac{2.\theta_1}{360}.\pi.r^2 - r.\sin\theta_1.(r-d) \quad (24)$$

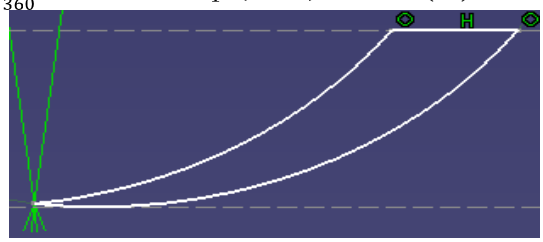


Figure 9. Heat generation Area

Hence, the machining zone area can be given by,

$$\boldsymbol{A = \frac{2.\theta_1}{360}.\pi.r^2 - r.\sin\theta_1.(r-d) - \frac{d.\sqrt{r^2-d^2}}{2} - \frac{r^2}{2}.\sin^{-1}\left(\frac{\sqrt{r^2-d^2}}{r}\right) + \frac{f.\sqrt{r^2-d^2}}{2} + \frac{f.\sqrt{4r^2-f^2}}{8} + \frac{r^2}{2}.\sin^{-1}\left(\frac{f}{2.r}\right) - \frac{f^2}{4}} \quad (25)$$

$$\mathbf{A = r^2\left[\sin^{-1}\left(\frac{f}{2.r}\right) - \sin^{-1}\left(\frac{\sqrt{r^2-d^2}}{r}\right) + \frac{2.\theta_1.\pi}{360} - \sin\theta_1 + r.d.\sin\theta_1 + (f-d).\left(\frac{\sqrt{r^2-d^2}}{2}\right) + \frac{f}{8}.\left(2.f - \sqrt{4.r^2-f^2}\right)\right]} \quad (26)$$

The volume of material removed during one complete machining cycle at given feed, depth of cut, speed and tool nose radius can be calculated from the following relation,

$$\boldsymbol{V = f.[1+\pi.N^2].\left\{r^2\left[\sin^{-1}\left(\frac{f}{2.r}\right) - \sin^{-1}\left(\frac{\sqrt{r^2-d^2}}{r}\right) + \frac{2.\theta_1.\pi}{360} - \sin\theta_1 + r.d.\sin\theta_1 + (f-d).\left(\frac{\sqrt{r^2-d^2}}{2}\right) + \frac{f}{8}.\left(2.f - \sqrt{4.r^2-f^2}\right)\right]\right\}} \quad (27)$$

Where, f = feed, d= depth of cut, r = tool nose radius, N = Spindle speed, the area expressed here is in square units and Volume is in Cubic units.

III. CONCLUSION

The calculation of heat generated area during every machining cycle enables the optimization of parameters to reduce the heat generation rate. The future scope will be optimization of diamond turning parameters with respect to heat transfer and its associated factors that causes failure.

IV. ACKNOWLEDGEMENT

This work was supported by (Council of Scientific and Industrial Research- Central Scientific Instruments Organization, Chandigarh).

REFERENCES

[1] McKeown. P (1987), "The role of precision engineering in manufacturing of the future," *CIRP Annals-Manufacturing Technology*, vol. 36, pp. 495-501

[2] Soo. S and Aspinwall. D (2007), "Developments in modelling of metal cutting processes," *Proceedings of the Institution of Mechanical Engineers, Part L: Journal of Materials Design and Applications*, vol. 221, pp. 197-211Taniguchi. N (1983), "

[3] Current status in, and future trends of, ultraprecision machining and ultrafine materials processing," *CIRP Annals-Manufacturing Technology*, vol. 32, pp. 573-582

[4] Kong. M, W. Lee, C. Cheung, and To.S (2006), "A study of materials swelling and recovery in single-point diamond turning of ductile materials," *Journal of materials processing technology*, vol. 180, pp. 210-215.

[5] Sata. T, Li. M, Takata. S, Hiraoka. H, Li. C, Xing. X, and Xiao. X (1985), "Analysis of surface roughness generation in turning operation and its applications," *CIRP Annals-Manufacturing Technology*, vol. 34, pp. 473-476.

[6] Masuzawa. T (2000), "State of the art of micromachining," *CIRP Annals-Manufacturing Technology*, vol. 49, pp. 473-488

[7] Soo Blok. H (1937), "Theoretical study of temperature rise at surfaces of actual contact under oiliness lubricating conditions," in *Proc. General Discussion on Lubrication and Lubricants*, pp. 222-235.

[8] Ulutan. D, Erdem Alaca. B, and Lazoglu. I (2007), "Analytical modelling of residual stresses in machining," *Journal of materials processing technology*, vol. 183, pp. 77-87..

[9] Venkatraman .B, Jayant Kumar, Omkumar .M, and Ramagopal V Sarepaka, (2014), "Mathematical Formulation for the Estimation of Volumetric Heat Transfer in Precision Machining Operations", *Journal of Material Science and Mechanical Engineering*, vol. 1, pp. 131-134

Low Power CMOS Based Dual Mode Logic Gates

[1]S Sujeetha,[2]Dr. V Renganathan
[1][2]Department of ECE, Sree Sastha Institute of Engineering and Technology, Chennai
[1]sujeetharahul@gmail.com,[2]drvrangan@gmail.com

Abstract— **the advancement in technology and the expansion of mobile applications, power consumption has become a primary focus of attention in Very Large Scale Integration (VLSI) digital design. Recently digital sub-threshold circuit design has become a very promising method for ultra-low power applications. Circuits operating in the sub-threshold region utilize a supply voltage that comes close to or even less than the threshold voltages of the transistors, so it allows significant reduction of both dynamic and static power. A Dual Mode Logic (DML) gate, for selectable operation in either of static and dynamic modes. By scaling down the area there should be a need arise to scale down the supply voltage as well as threshold voltages of the device. It can cause static power dissipation to dominate dynamic power dissipation. To reduce the power consumption and dissipation of the circuit and increase the life time of the battery normally used in mobile phones and personal digital assistants Power Gated Sleep method can be applied. During sleep to active mode transition the stacked sleep transistors connected below the pull-down network are ON after a small duration. During the instant circuit should be experiences the Ground Bounce Noise (GBN). Inserting proper amount of delay which is less than the discharge time of the sleep transistor GBN will be reduced. The output of the circuit should be high enough to drive the another circuit. The simulations were done in TannerEDA 13.0 tool and power consumption of the proposed DML gates compared with Sleep and Dual Sleep methods in the 250-nm process.**

Index Terms—**Dual Mode Logic gates, Ground Bounce Noise, Sub-Threshold Region.**

I. INTRODUCTION

In recent years the demand for low power devices has been increases tremendously. Low power consumption, speed of the system and the small area are the three main factors for increasing the performance. Reducing power dissipation is one of the most important issues in very large scale integration design today. As technology scales into the nanometer regime ground bounce noise and noise immunity are becoming important metric of comparable importance to leakage current, active power and area for the analysis and design of complex arithmetic logic circuits. Static power consumption is a major concern in nanometer technologies. Along with technology scaling down and higher operating speeds of CMOS VLSI circuits, the leakage power is getting enhanced. Reduction in leakage power has become an important concern in low-voltage, low power, and high performance applications. This demand may be due to fast growth of battery operated portable applications such as cell phones, laptops and other handheld devices. There are three major components of power dissipation in complementary metal oxide circuits such as switching power, short circuit power and static power. Reducing any of these components will end up with low power consumption of the whole work.

DUAL MODE LOGIC GATES

Dual mode logic (DML), designed to operate in the subthreshold region. The DML logic can be operated in two modes: static CMOS-like mode and dynamic np-CMOS-like mode (which will be referred to as a dynamic mode). In the static mode, the DML gates feature very low power dissipation with moderate performance, while in the dynamic mode, they achieve much higher performance with increased power dissipation. This unique feature of the DML provides the option to control system performance on-the-fly and thus support applications in which a flexible workload is required.

The basic DML gate architecture is composed of a standard CMOS gate and an additional transistor M1, whose gate is connected to a global clock signal, as shown in Fig. 1. The DML aims to allow operation in two functional modes: static mode and dynamic mode. To operate the gate in the dynamic mode, the Clock is assigned an asymmetric clock, allowing two distinct phases: precharge and evaluation. During the precharge phase, the output is charged to high/low, depending on the topology of the DML gate. In the consequent evaluation phase, the output is evaluated according to the values at the gate inputs. The DML topologies, marked Type A and Type B, are illustrated in Fig. 1.

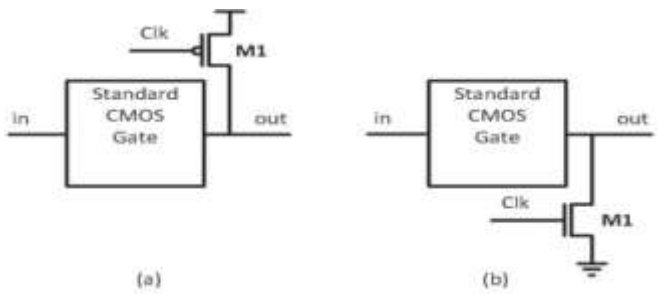


Fig. 1. Proposed basic DML gate. (a) Type A topology. (b) Type B topology.

Type A has an added p-MOS transistor that precharges the output to a logical "1" during the precharge phase. Type B has an added n-MOS that precharges the output to a logical "0". Dynamic logic gates are often implemented using a footer, which requires an additional transistor. The footer is used to decrease precharge time by eliminating the ripple effect of the data advancing through the cascaded nodes and allowing faster precharge. This is the key attribute to the immunity to process variations, temperature fluctuations, and solving some of the domino's well known drawbacks such as charge sharing, crosstalk noise, and susceptibility to glitches, which intensify with process and voltage scaling. DML shows high immunity to process variations, making it possible to operate DML gates from a supply voltage as low as 300 mV while operating in the dynamic mode, subthreshold DML achieves an improvement in speed of up to 10× compared to a standard CMOS, while dissipating 1.5× more power. In the static mode 5× reduction of power dissipation is achieved, compared to a basic domino, at the expense of a magnitude decrement in performance.

As the CMOS technology moved below sub-micron levels the power consumption per unit area of the chip has risen tremendously. There are three major components of power dissipation in CMOS circuits: switching power, short circuit power and static power. Reducing any of these components will end up with low power consumption of the whole system. The first two components are referred to as dynamic power. Dynamic power accounts for the majority of the total power consumption in digital CMOS VLSI circuits. The current pulse from VDD to GND results in a short circuit dissipation. Static CMOS gates are very power efficient because they dissipate nearly zero power when idle. The total power is given by the following equation

$$P_{total}=V_{dd}^2.F_{clk}.C_{load}+V_{dd}.\Sigma I_{isc}+V_{dd}.I_l \quad \ldots\ldots\ldots (1)$$

where, Vdd is the power supply voltage, Fclk is the system clock frequency, Cload is the load capacitance, Iisc is the short-circuit current at node I and Il is the leakage current.

II. GROUND BOUNCE NOISE

Ground bounce defines a condition when a device's output switches from high to low and causes a voltage change on other pins. It is usually seen on high density VLSI where insufficient precautions have been taken to supply a logic gate with a sufficiently low resistance connection to ground. Ground bounce is a voltage oscillation between the ground pin on a component package and the ground reference level on the component die. Essentially it is caused by a current surge passing through the lead inductance of the package. This voltage drop on the ground line creates two main problems: first it raises the chip off ground potential which in turn increases the devices input threshold level, and secondly increases the voltage level on an output pin which is not switching. This is also called Simultaneous Switching Noise. Fig. 2 shows the graphical representation of ground bounce noise.

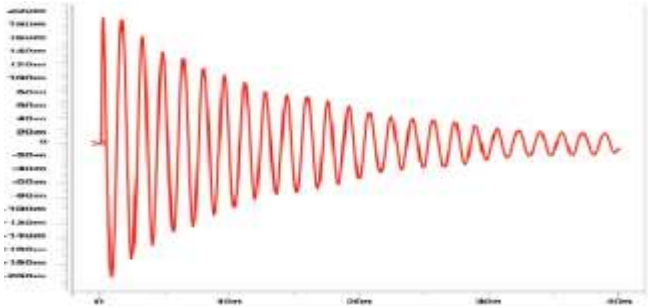


Fig. 2. Ground bounce noise

In this phenomenon, when the gate is turned on, enough current flows through the emitter-collector circuit that the silicon in the immediate vicinity of the emitter is pulled high, sometimes by several volts, thus raising the local ground, as perceived by the transistor, to a value significantly above true ground. Relative to this local ground, the base voltage can go negative, thus shutting off the transistor. Otherwise it is the large sudden current that flows through the power and ground rails during standby-to-active mode transition. This results in long period of power and ground rails' fluctuation, due to the inductance of the off-chip packaging and the on-chip power grids. This noise occurs in both power networks during mode transition, and the fluctuation in the power network. This GBN effect can be reduced by inserting proper amount of delay which is less than the discharge time of the sleep transistor.

III. POWER GATING TECHNIQUES

Power gating uses low-leakage PMOS transistors as header switches to shut off power supplies to parts of a design in standby or sleep mode [15]. NMOS footer switches can also be used as sleep transistors. Inserting the sleep transistors splits the chip's power network into a permanent power network connected to the power supply and a virtual power network that drives the cells and can be turned off.

Techniques for leakage power reduction can be grouped into two categories: state-preserving techniques where circuit state is retained and state destructive techniques where the current Boolean output value of the circuit might be lost. A state preserving technique has an advantage over a state destructive technique in that with a state-preserving technique the circuitry can resume operation at a point much later in time without having to somehow regenerate state. There are several VLSI techniques for reducing leakage power. Each technique provides an efficient way to reduce leakage power. They are:

- Sleep method
- Dual sleep method

Each technique has its own merits and demerits. Based on the application, the technique which is best suited can be utilized.

Sleep Method

In the sleep approach, a "sleep" PMOS transistor is placed between VDD and the pull-up network of a circuit and a "sleep" NMOS transistor is placed between the pull-down network and Ground. The sleep transistors are turned on when the circuit is active and turned off when the circuit is idle. By cutting off the power source, this technique can reduce leakage power effectively. However, output will be floating after sleep mode, so the technique results in destruction of state plus a floating output voltage. The circuit is connected as shown in Fig. 3.

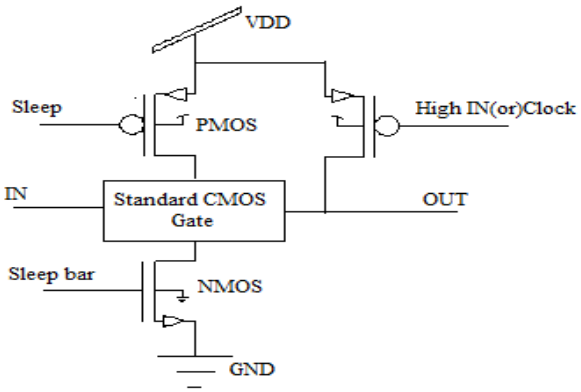


Fig. 3. DML Sleep method (Type A topology)

Dual Sleep Method

Another technique called Dual sleep approach uses the advantage of using the two extra pull-up and two extra pull-down transistors in sleep mode either in OFF state or in ON state. Since the dual sleep portion can be made common to all logic circuitry, less number of transistors is needed to apply a certain logic circuit. The sleep state attained due to the voltage headroom effect. The circuit is connected as shown in Fig. 4. The logic gates NAND, NOR and Inverter are implemented in these two methods and their average power consumption is measured for power comparison.

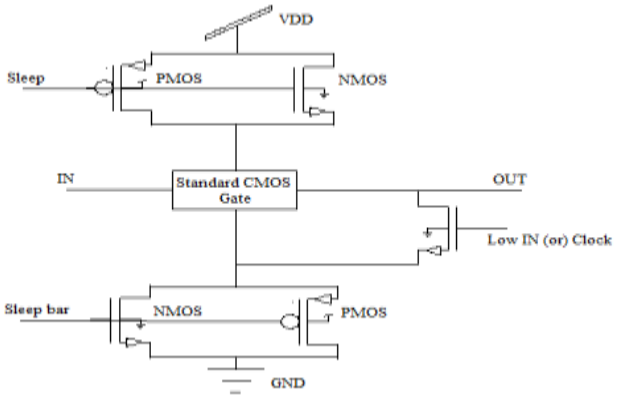


Fig. 4. DML Dual Sleep method (Type B topology)

IV. PROPOSED POWER GATED SLEEP METHOD

To reduce the power consumption of the circuit and increase the life time of the battery normally used in the devices, the sleep transistors are added. The PMOS sleep transistor is added in between V_{dd} power rail and PMOS Logic network, NMOS sleep transistor is added in between NMOS logic network and ground. The sleep stacking is applied to sleep transistors. There are several benefits of combining stacked sleep transistors. First the magnitude of power supply fluctuations sleep mode during mode transitions will be reduced because these transitions are gradual. Second, while conventional power gating uses a high- threshold device as a sleep transistor to minimize leakage. Power gated sleep circuit has three modes of operations. They are,

- Active mode
- Standby mode
- Sleep to active mode transition

In active mode, the sleep signal is held at '0' and sleep bar is '1'. In this case both transistors offer very low resistance and virtual ground (VGND) node potential is pulled down to the ground potential, making the logic difference between the logic circuitry approximately equal to the supply voltage. In standby mode operation sleep signal is held at '1' and the sleep bar signal is '0'. In this case both transistors offer very low resistance and virtual ground (VGND) node potential is pulled down to the ground potential, making the logic difference between the logic circuitry approximately equal to the supply voltage and leakage current is reduced by the stacking effect.

During sleep to active mode transition, the sleep transistor at the bottom side is turned ON after a small duration of time. According to the effect of GBN the output gets oscillated. To make the circuit output stable desirable delay is applied to the sleep transistors by turning it off for a while. The GBN can be greatly reduced by controlling the intermediate node voltage VGND2 and operating the sleep transistor in triode region.

In stacking of transistors vary the threshold voltage of the transistors by providing bulk to source biasing negative. This increase the threshold voltage of the device, more threshold voltage means less sub threshold current, this cause less total leakage power. The threshold voltage of a device is given as,

$$V_{th} = 2\varphi_f + \left(\frac{\sqrt{2q\varepsilon N_a(2\varphi_f + |V_{bs}|}}{C_{OX}}\right) \quad \ldots\ldots\ldots (2)$$

where, V_{th} is threshold voltage, φ_f is built-in surface potential, V_{bs} is body bias voltage, q is charge of an electron, N_a is doping concentration and Cox is oxide capacitance.

Inverter

In the DML Type A Power Gated Sleep Static Inverter topology, the switching element is a PMOS transistor connected parallel to the pull-up network. The input to the switching element is a constant high voltage is shown in Fig.5.

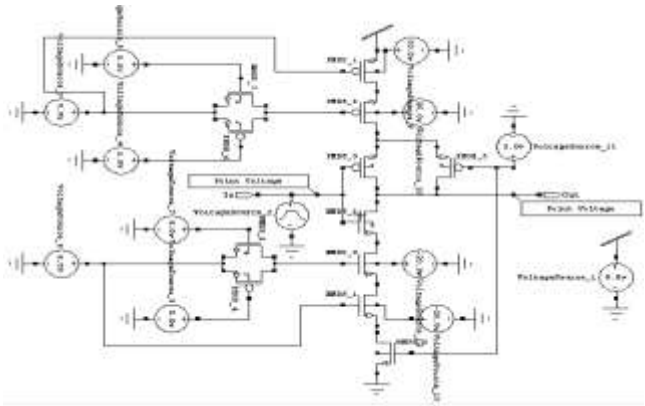


Fig. 5. Type A Power Gated Sleep Static Inverter

The footer is used to decrease pre-charge time by eliminating the ripple effect of the data advancing through the cascade and allowing faster pre- charge. The only difference when designing DML Type-A Power Gated Sleep Dynamic Inverter is that the input to the switching element is a clock signal.

In the DML Type B Power Gated Sleep Dynamic Inverter topology, the switching element is a NMOS transistor connected parallel to the pull-down network. The input to the switching element is a clock signal is shown in Fig. 6.The only difference when designing DML Type-B Power Gated Sleep Static Inverter is that the input to the switching element is a constant low voltage.

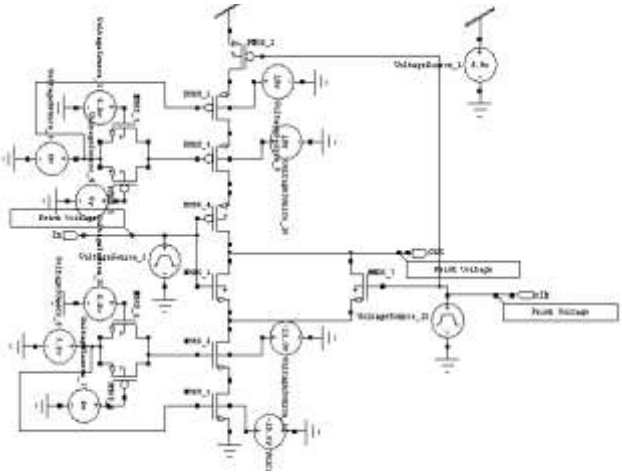


Fig. 6. Type B Power Gated Sleep Dynamic Inverter

NAND Gate

In the DML Type-A Power Gated Sleep Dynamic NAND topology, the switching element is a PMOS transistor connected parallel to the Pull-up network. The input to the switching element is a clock signal is shown in Fig. 7. The only difference when designing DML Type-A Power Gated Sleep Static NAND is that the input to the switching element is a constant HIGH voltage.

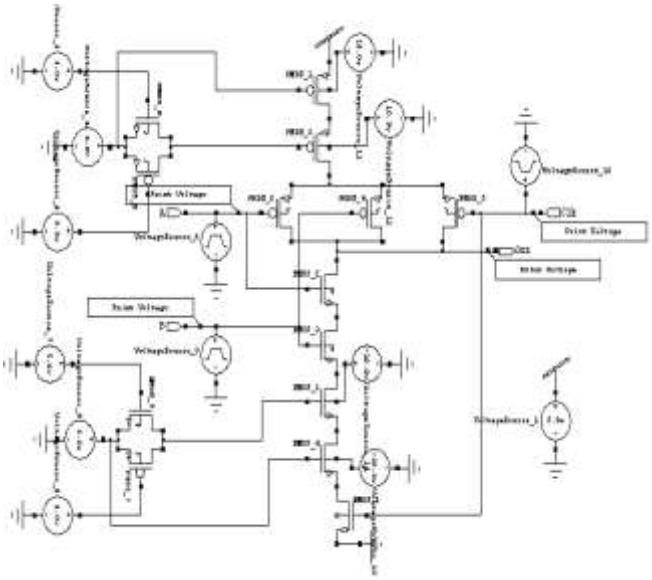


Fig. 7. Type A Power Gated Sleep Dynamic NAND Gate

In the DML Type B Power Gated Sleep Static NAND topology, the switching element is a NMOS transistor connected parallel to the pull-down network. The input to the switching element is a constant low voltage is shown in Fig.8. The only difference when designing DML Type-B Power Gated Sleep Dynamic NAND Gate is that the input to the switching element is a clock signal.

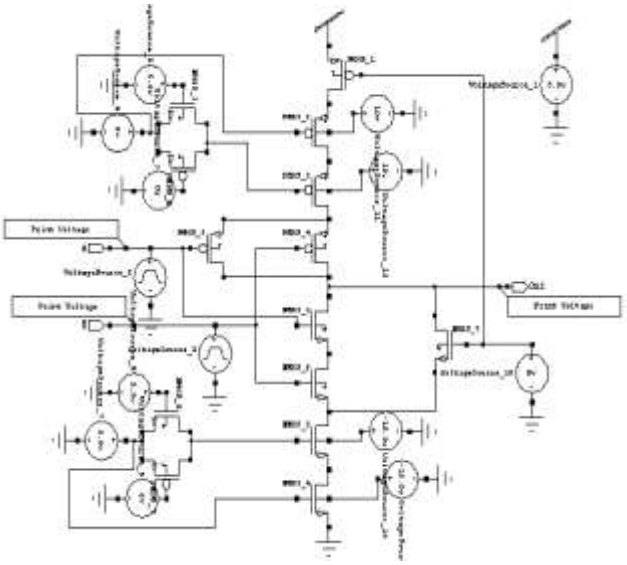


Fig. 8. Type B Power Gated Sleep Static NAND Gate

NOR Gate

In the DML Type A Power Gated Sleep Static NOR topology, the switching element is a PMOS transistor connected parallel to the pull-up network. The input to the

switching element is a constant high voltage is shown in Fig.9. The only difference when designing DML Type-A Power Gated Sleep Dynamic NOR Gate is that the input to the switching element is a clock signal.

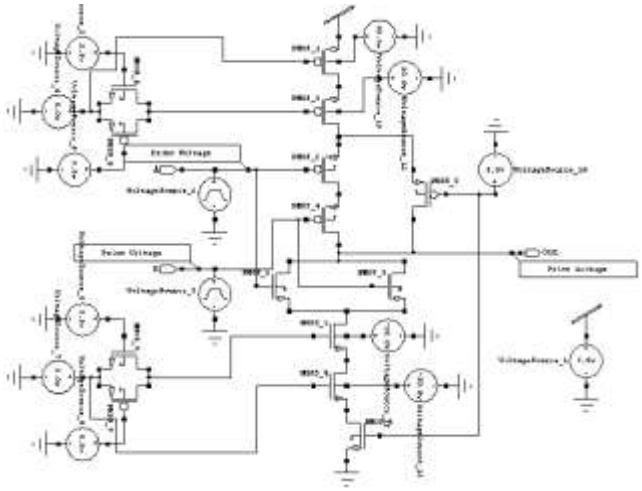


Fig. 9. Type A Power Gated Sleep Static NOR Gate

In the DML Type B Power Gated Sleep Dynamic NOR topology, the switching element is a NMOS transistor connected parallel to the pull-down network. The input to the switching element is a clock signal is shown in Fig. 10.The only difference when designing DML Type-B Power Gated Sleep Static NOR Gate is that the input to the switching element is a constant low voltage.

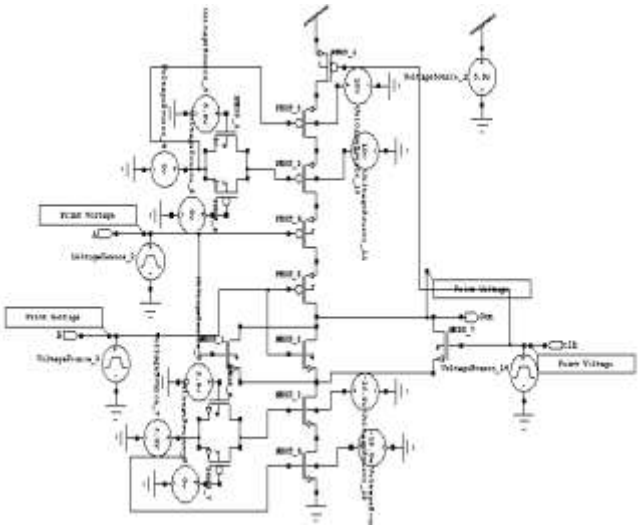


Fig. 10. Type B Power Gated Sleep Dynamic NOR Gate

SIMULATION RESULTS

The simulation is performed in Tanner EDA 13.0 at 250 nm technology. The operating temperature was maintained at 25ºC.The Output of Type A Power Gated Sleep Static Inverter is shown in Fig. 11.

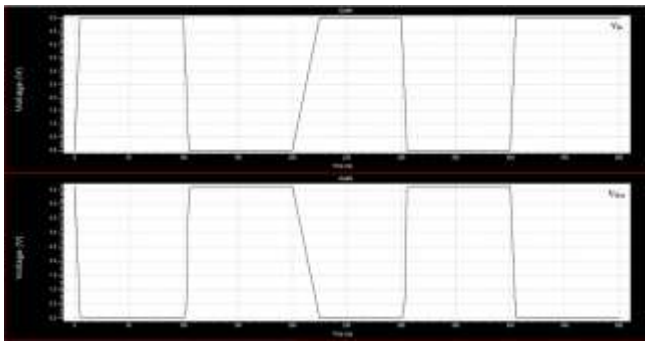


Fig. 11. Output of Type A Power Gated Sleep Static Inverter

The power gated sleep technique provides the output and the observed average power consumption is 5.546µW. For a supply voltage of 5V, the output of Type B Power Gated Sleep Dynamic Inverter is shown in the Fig. 12.

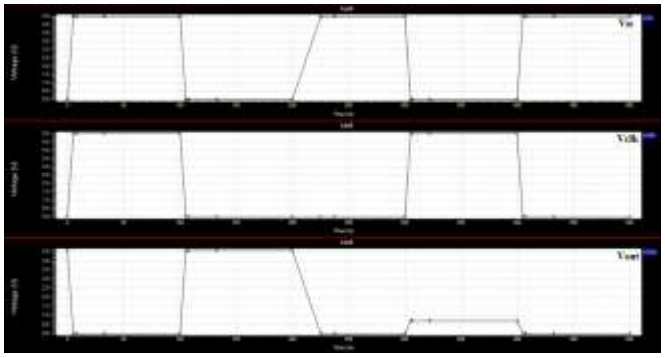


Fig. 12. Output of Type B Power Gated Sleep Dynamic Inverter

The power gated sleep technique provides the output and the observed average power consumption is 9.875µW. The Output of Type A Power Gated Sleep Dynamic NAND gate is shown in Fig. 13.

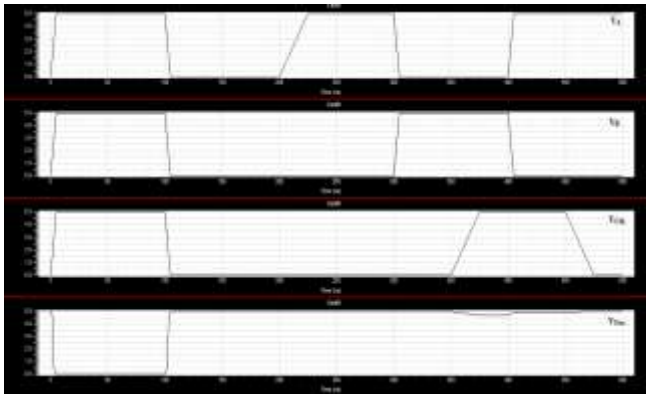


Fig. 13. Output of Type A Power Gated Sleep Dynamic NAND gate

The power gated sleep technique provides the output and the observed average power consumption is 14.347µW. For a supply voltage of 5V, the output of Type B Power Gated Sleep Static NAND is shown in the Fig. 14.

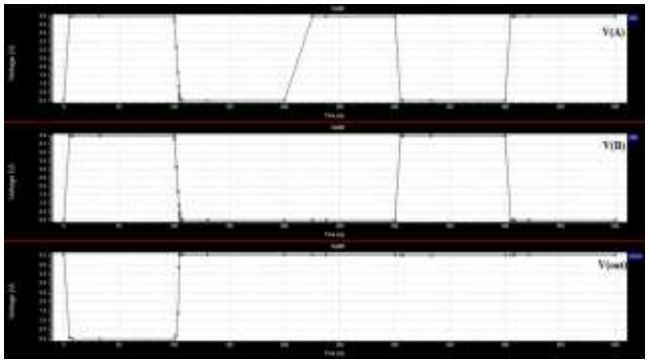


Fig. 14. Output of Type B Power Gated Sleep Static NAND gate

The power gated sleep technique provides the output and the observed average power consumption is 7.012µW. The Output of Type A Power Gated Sleep Static NOR gate is shown in
Fig. 15.

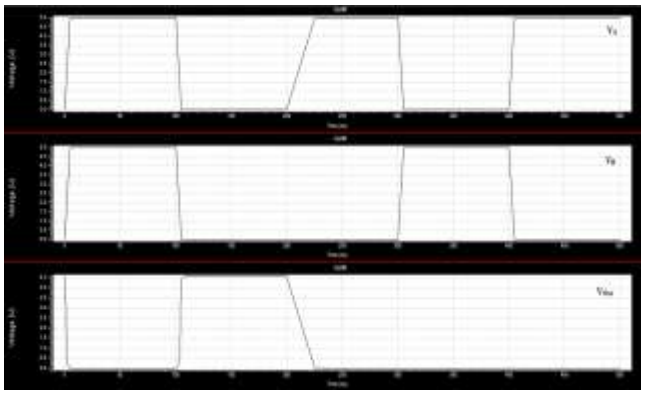


Fig. 15. Output of Type B Power Gated Sleep Static NOR gate

The power gated sleep technique provides the output and the observed average power consumption is 4.733µW. The Output of Type A Power Gated Sleep Static NOR gate is shown in Fig. 16.

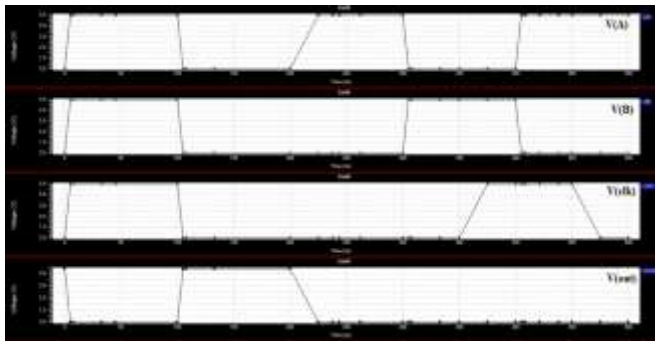


Fig. 15. Output of Type B Power Gated Sleep Dynamic NOR gate

The power gated sleep technique provides the output and the observed average power consumption is 12.080µW. Comparison of power consumed by Inverter, NAND and NOR gate are shown in Table I.II and III

TABLE I
POWER COMPARISON OF INVERTER

Type	**Sleep Method (µW)**	**Dual sleep method (µW)**	**Power gated sleep method (µW)**
Type A Static	4078.17	15.564	5.546
Type A Dynamic	77.451	17.451	9.173
Type B Static	17.754	16.785	9.653
Type B Dynamic	18.953	17.785	9.875

TABLE II
POWER COMPARISON OF NAND GATE

Type	**Sleep Method (µW)**	**Dual sleep method (µW)**	**Power gated sleep method (µW)**
Type A Static	44.64	44.52	13.529
Type A Dynamic	49.10	49.06	14.347
Type B Static	20.276	16.083	7.012
Type B Dynamic	22.626	17.240	9.437

TABLE III

POWER COMPARISON OF NOR GATE

Type	Sleep Method (µW)	Dual sleep method (µW)	Power gated sleep method (µW)
Type A Static	14.511	14.541	4.733
Type A Dynamic	16.104	16.130	5.202
Type B Static	14.212	13.414	10.485
Type B Dynamic	15.386	14.915	12.080

The power comparison of three methods tells us that the power gated sleep method provides optimal power consumption compared to other two methods.

CONCLUSION

In nanometer scale CMOS technology, sub threshold leakage power consumption is a great challenge. This paper presents a novel circuit structure named "power gated sleep method" as a new remedy for designer in terms of power products. The power gated sleep method shows the least speed power product among all methods. Therefore, the power gated sleep method provides new ways to designers who require ultra-low leakage power consumption with much less speed power product. Especially it shows nearly 50-60% of power than the existing methods. So, it can be used for future integrated circuits for power Efficiency.

REFERENCES

1. Athira P.K. and Mahalakshmi M. (2014) 'Low Power Design of Dual Mode Logic using Stacking Power Gating', International Journal of Review in Electronics & Communication Engineering, Vol. 2, No. 2, pp. 63-67.
2. Kaizerman A., Fisher S. and Fish A. (2013) 'Subthreshold Dual Mode Logic', IEEE transaction on VLSI systems, Vol. 21, No. 5, pp.979-983.
3. Kumar M., Hussain A.Md. and Paul S.K. (2013) 'New Hybrid Digital Circuit Design Techniques for Reducing Subthreshold Leakage Power in Standby Mode', Circuits and Systems, Vol. 4, No. 1, pp.75-82.
4. Lakshmisree P. V. and Raghu M.C. (2014) 'Design of Subthreshold Logic Gates with Power Gating Techniques', International Journal of Research in Engineering and Technology, Vol. 3, No. 4, pp. 174-180.
5. Levi I., Belenky A. and Fish A. (2014) ';Logical Effort for CMOS Based Dual Mode Logic Gates', IEEE transaction on VLSI Systems, Vol. 22, No. 5, pp. 1042-1053.
6. Nigam K.K. and Tiwari A. (2012) 'Zigzag Keeper: A New Approach for Low Power CMOS Circuit', International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, No. 9, pp. 694-699.
7. Reddy A.K. and Kumar S. (2013) 'A Novel Technique for Ground Bounce Noise Reduction in Deep Sub Micron Circuits', International Journal of Innovative Technology and Research, Vol. 1, No. 5, pp.485-490.

Dynamic Secure System For Detecting and Eliminating Fraudulence In Cloud Storage

[1]Kalaivani A,[2]Ranjith Kumar M,[3]Sabarish M,[4]Sai Kishore R
[1][2]Assistant Professor, Dept. of CSE, R.M.K College of Engineering and Technology, Puduvoyal, Chennai.
[3][4]Third Year , Dept. of CSE, R.M.K College of Engineering and Technology, Puduvoyal, Chennai.

Abstract— **the advancement in technology and the expansion of mobile applications, power consumption has become a primary focus of attention in Very Large Scale Integration (VLSI) digital design. Recently digital sub-threshold circuit design has become a very promising method for ultra-low power applications. Circuits operating in the sub-threshold region utilize a supply voltage that comes close to or even less than the threshold voltages of the transistors, so it allows significant reduction of both dynamic and static power. A Dual Mode Logic (DML) gate, for selectable operation in either of static and dynamic modes. By scaling down the area there should be a need arise to scale down the supply voltage as well as threshold voltages of the device. It can cause static power dissipation to dominate dynamic power dissipation. To reduce the power consumption and dissipation of the circuit and increase the life time of the battery normally used in mobile phones and personal digital assistants Power Gated Sleep method can be applied. During sleep to active mode transition the stacked sleep transistors connected below the pull-down network are ON after a small duration. During the instant circuit should be experiences the Ground Bounce Noise (GBN). Inserting proper amount of delay which is less than the discharge time of the sleep transistor GBN will be reduced. The output of the circuit should be high enough to drive the another circuit. The simulations were done in TannerEDA 13.0 tool and power consumption of the proposed DML gates compared with Sleep and Dual Sleep methods in the 250-nm process.**

Index Terms—**Dual Mode Logic gates, Ground Bounce Noise, Sub-Threshold Region.**

LIST OF TABLES

I. LITERATURE SURVEY

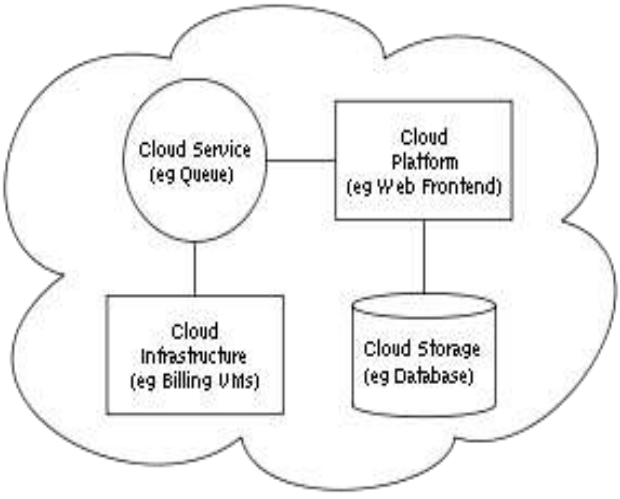
LITERATURE SURVEY	EXISTING SYSTEM	PROPOSED SYSTEM
Secure Untrusted Data Repository (SUNDR)	SUNDR is a network file system designed to store data securely on untrusted servers. SUNDR lets clients detect any attempts at unauthorized file modification by malicious server operators or users.	SUNDR's protocol achieves a property called *fork consistency*, which guarantees that clients can detect any integrity or consistency failures as long as they see each other's file modifications. An implementation is described that performs comparably with NFS (sometimes better and sometimes worse), while offering significantly stronger security.
A View of Cloud Computing	The interesting thing about cloud computing is that we've redefined	This article is to reduce that confusion by clarifying terms,

	cloud computing to include everything that we already do.I don't understand what we would do differently in the light of cloud computing other than change the wording of some of our ads.	providing simple figures to quantify comparisons between of cloud and conventional computing, and identifying the top technical and non-technical obstacles and opportunities of cloud computing.
Efficient Byzantine-tolerant erasure-coded storage	Survivable storage systems spread data redundantly across a set of distributed storage-nodes in an effort to ensure its availability despite the failure or compromise of storage-nodes. Such systems require some protocol to maintain data consistency in the presence of failures and concurrency.	A decentralized consistency protocol for survivable storage that exploits local data versioning within each storage-node is described. Such versioning enables the protocol to efficiently provide linearizability and wait-freedom of read and write operations to erasure-coded data in asynchronous environments with Byzantine failures of clients and servers.
The Complexity of Online Memory Checking	We consider the problem of storing a large file on a remote and unreliable server. To verify that the file has not been corrupted, a user could store a small private (randomized) finger-print" on his own computer. This is the setting for the well-studied authentication problem in cryptography, and the required fingerprint size is well understood.	It was previously shown that when the adversary is computationally bounded, under the assumption that one-way functions exist, it is possible to construct much better online memory checkers. T he same is also true for sub-linear authentication schemes.
Efficient Remote Data Possession Checking in Critical Information Infrastructures	Checking data possession in networked information systems such as those related to critical infrastructures (power facilities, airports, data vaults, defense systems, and so forth) is a matter of crucial importance	In this paper, we present a new remote data possession checking protocol such that 1) it allows an unlimited number of file integrity verifications and 2) its maximum running time can be chosen at set-up time and traded off against storage at the verifier.

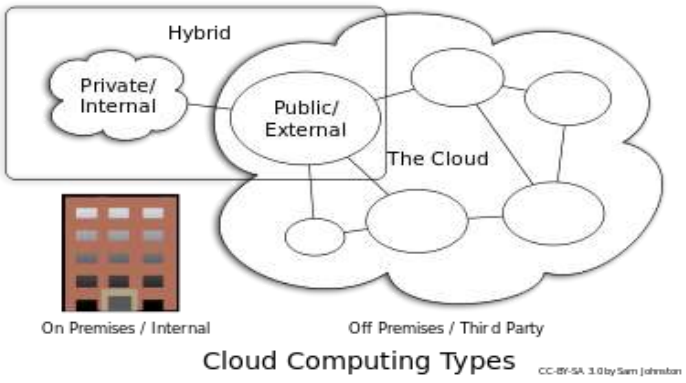
Securing Distributed Storage: Challenges, Techniques, and Systems	The rapid increase of sensitive data and the growing number of government regulations that require longterm data retention and protection have forced enterprises to pay serious attention to storage security.	we discuss important security issues related to storage and present a comprehensive survey of the security services provided by the existing storage systems. We cover a broad range of the storage security literature, present a critical review of the existing solutions, compare them, and highlight potential research issues

II. LIST OF FIGURES

Cloud Architecture



CLOUD COMPUTING TYPES



III. SYSTEM REQUIREMENT SPECIFICATION

Analysis

System Analysis

Existing System

The data owners host their data on cloud servers and users (data consumers) can access the data from cloud servers. Due to the data outsourcing, however, this new paradigm of data hosting service also introduces new security challenges, which requires an independent auditing service to check the data integrity in the cloud. Some existing remote integrity checking methods can only serve for static archive data and, thus, cannot be applied to the auditing service since the data in the cloud can be dynamically updated. Thus, an efficient and secure dynamic auditing protocol is desired to convince data owners that the data are correctly stored in the cloud. Here we first design an auditing framework for cloud storage systems and propose an efficient and privacy-preserving auditing protocol. Then, we extend our auditing protocol to support the data dynamic operations, which is efficient and provably secure in the random oracle model.

Drawbacks In Existing System:

- In dynamic auditing protocol cloud server have threat for security for data storage.
- When any system is suspected that will be under tracked only under complaint.
- There is no link between all the databases where an individual have different accounts.

Proposed System

A monitoring tool that detects fraudulent using link analysis and checks for similar details among multiple databases will be created. As there is no interlinking between different banks database an individual can create many accounts with different identity proofs So

that they can do malicious activities in the network. To avoid this we use link analysis for finding similarity link in the entire combined cloud stored database. It uses Joint Threshold Administrative Model (JTAM) for authenticating database storage and handles fault tolerance effectively using the monitoring tool.

Advantages In Proposed System

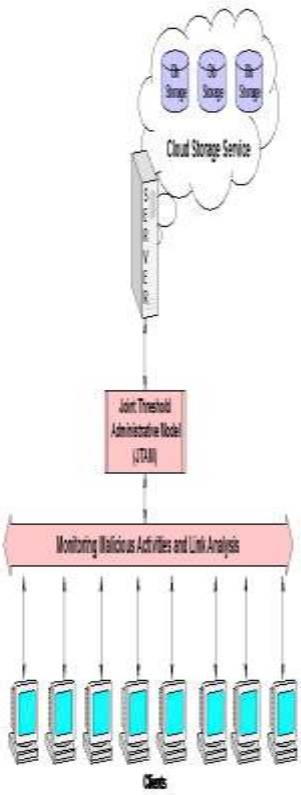
- Creating monitoring tool that tracks fraud account creation using link analysis.
- Monitors and handles all the suspected system involved in malicious activities.
- Joint Threshold Administrative Tool (JTAM) is used for permitting privileges for data storage.
- Handles fault tolerance effectively.

Function

- It uses link analysis algorithm for similarity details.
- Joint Threshold Administrative Tool (JTAM) is used for permitting privileges for data storage.
- A monitoring tool is created for monitoring malicious activities on database.

System Design Specification

Architecture

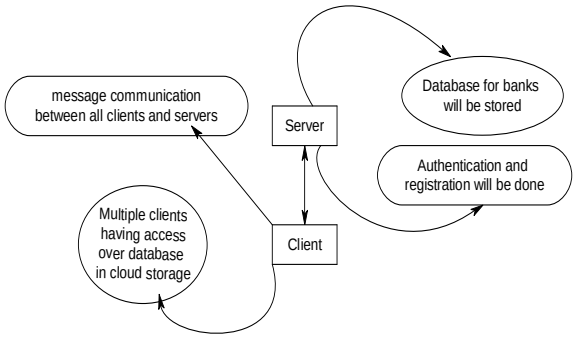


Modules

- SERVER/CLIENT ESTABLISHMENT
- CLOUD STORAGE
- MONITORING TOOL CREATION
- JTAM IMPLEMENTATION

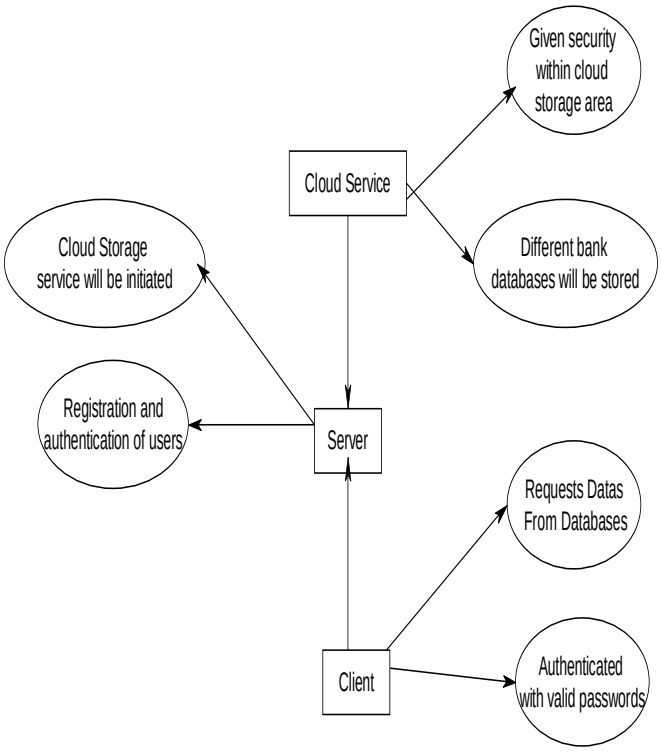
Server/Client Establishment

In this module we create server & client systems. We create different databases denoting different bank data. These all will be given strong security thus no one can hack any message communication in terms of money. We thus create many client systems with some system having secured database. . Here we create a single server and multiple client systems which have intermediate communications between each other. Thus they can be easily pass messages between server and client and the message communications between clients to client is also possible.



IV. CLOUD STORAGE

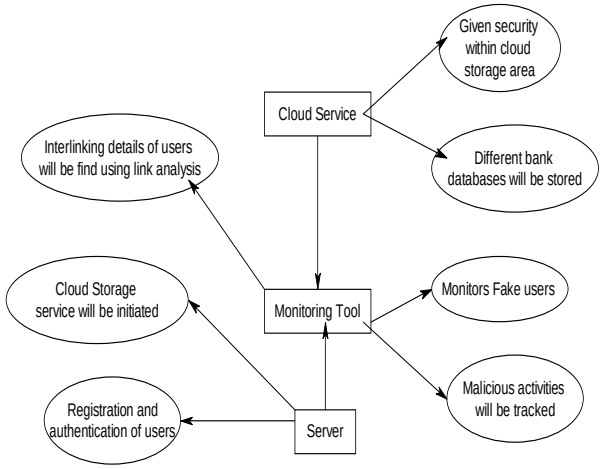
Data from the different databases combined and implemented in cloud storage for linking all the data for further data storage and retrieval. Cloud storage will be online storage system that provides secured space for storing data for different banks. Thus every bank will have individual memory space for storing their authenticated secured user information and their money transactions between bank and their customers. Cloud computing concept of storage as a service will be implemented in this module for storing databases for different banks.



V. MONITORING TOOL CREATION

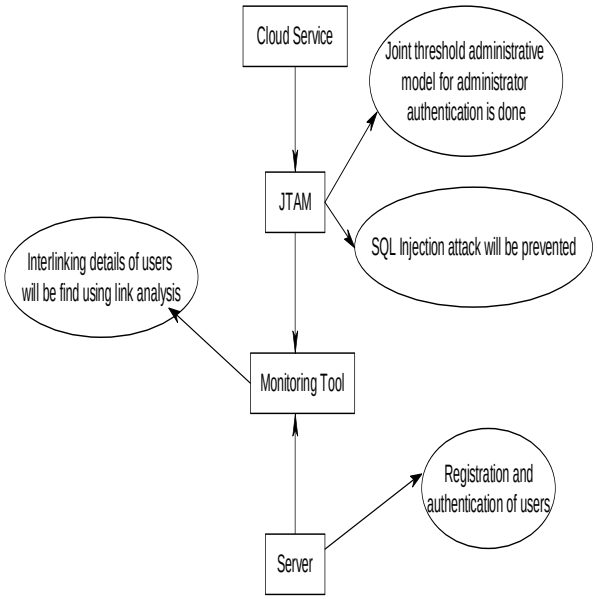
In this module we create a monitoring tool in the cloud database which monitors the stored data for their similarity interlinking details. It helps to monitor the details of users who is trying to create fake database or even the users having multiple accounts. The similarity details of a particular user will be kept track so that the user's malicious activity on the network using their different account databases. Such users will be caught and informed about their malicious

database activity. The interlinking activities will be handled using link analysis mapping for all the possible similarity details.



VI. JTAM IMPLEMENTATION

Joint Threshold Administrative Model (JTAM) tool is created with different administrators implied in different databases. Admin gives authentication for storage of data and subsequently analyse similarity details in cloud storage database. This JTAM model will ask for authentication to each and every administrator all the time. Only when all the administrators given authentication to that particular task then only that task will be proceeds otherwise it will wait until every admin given authentication. This handles SQL injection attack at any database from the secured database.



System Requirements

Software Requirement:

- Front End : Jdk 1.7
- Back End : Oracle 10g (Server Edition)
- IDE :NetBeans
- Operating System :Windows Xp,Windows 7

Hardware Requirement:

- Processor :Pentium 4 or above
- Ram :512mb or above
- Hard disk
- :80gb

VII. SYSTEM IMPLEMENTATION

At first the node topology is created using server socket program .the client module uses the socket and the server module uses the server socket. Java swing is used to design the front end. Quaqua look and feel is used to enhance the design part of the project.

The encryption algorithm of aes is implemented using java code .the system port number and the dsn details in the network are gathered so that the message is transferred through the specified path. The back end is sql server where we are storing data and retrieving from there. The node connected in the network topology and the dsn of all nodes and the port number of all nodes is retrieved from this sql server database 2000. we are creating table in sql server for storing this details . The front end and the backend is connected with the help of jdbcodbc driver.

Modules implement procedure

Link Analysis

TRADITIONAL statistical, machine learning, pattern recognition, and data mining approaches usually assume a random sample of independent objects from a single relation. Many of these techniques have gone through the extraction of knowledge from data (typically extracted from relational databases), almost always leading, in the end, to the classical double-entry tabular format, containing features for a sample of the population. These features are therefore used in order to learn from the sample, provided that it is representative of the population as a whole. However, real-world data coming from many fields (such as World Wide Web, marketing, social networks, or biology; see) are often multirelational and interrelated. The work recently performed in statistical relational learning, aiming at working with such data sets, incorporates research topics, such as link analysis, web mining social network analysis or graph mining. All these research fields intend to find and exploit links between objects (in addition to features—as is also the case in the field of spatial statistics), which could be of various types and involved in different kinds of relationships.

The focus of the techniques has moved over from the analysis of the features describing each instance belonging to the population of interest (attribute value analysis) to the analysis of the links existing between these instances (relational analysis), in addition to the features. This paper precisely proposes a link-analysis-based technique allowing to discover relationships existing between elements of a relational database or, more generally, a graph. More specifically, this work is based on a random walk through the database defining a Markov chain having as many states as elements in the database. Suppose, for instance, we are interested in analyzing the relationships between elements contained in two different tables of a relational database. To this end, a two-step procedure is developed. First, a much smaller, reduced, Markov chain, only containing the elements of interest typically the elements contained in the two tables and preserving the main characteristics of the initial chain, is extracted by stochastic complementation. An efficient algorithm for extracting the reduced Markov chain from the large, sparse, Markov chain representing the database is proposed. Then, the reduced chain is analyzed by, for instance, projecting the states in the subspace spanned by the right eigenvectors of the transition matrix or by computing a kernel principal component analysis, on a diffusion map kernel computed from the reduced graph and visualizing the results. Indeed, a valid graph kernel based on the diffusion map distance, extending the basic diffusion map to directed graphs, is introduced. The motivations for developing this two-step procedure are twofold. First, the computation would be cumbersome, if not impossible, when dealing with the complete database.

Second, in many situations, the analyst is not interested in studying all the relationships between all elements of the database, but only a subset of them. Moreover, if the whole set of elements in the database is analyzed, the resulting mapping would be averaged out by the numerous relationships and elements we are not interested in for instance, the principal axis would be completely different. It would therefore not exclusively reflect the relationships between the elements of interest. Therefore, reducing the Markov chain by stochastic complementation allows to focus the analysis on the elements and relationships we are interested in. Interestingly enough, when dealing with a bipartite graph (i.e., the database only contains two tables linked by one relation), stochastic complementation followed by a basic diffusion map is exactly equivalent to simple correspondence analysis.

On the other hand, when dealing with a starschema database (i.e., one central table linked to several tables by different relations), this two-step procedure reduces to multiple correspondence analysis. The proposed methodology therefore extends correspondence analysis to the analysis of a relational database. In short, this paper has three main contributions. A two-step procedure for analyzing weighted graphs or relational databases is proposed. . It is shown that the suggested procedure extends correspondence analysis. . A kernel version of the diffusion map distance, applicable to directed graphs, is introduced.

JTAM (Joint Threshold Administrative Model)

Our interactive response policy language makes it very easy for the database administrators to specify appropriate response actions for different circumstances depending upon the nature of the anomalous request. The two main issues that we address incontext of such response policies are that of policy matching, and policy administration. For the policy matching problem, two algorithms that efficiently search the policy database for policies that match an

anomalous request. We also extend the PostgreSQL DBMS with our policy matching mechanism, and report experimental results. The experimental evaluation shows that our
techniques are very efficient. The other issue that we address is that of administration of response policies to prevent malicious modifications to policy objects from legitimate users. We propose a novel Joint Threshold Administration Model (JTAM) that is based on the principle of separation of duty. The key idea in JTAM is that a policy object is jointly administered by at least k database administrator (DBAs), that is, any modification made to a policy object will be invalid unless it has been authorized by at least k DBAs. We present design details of JTAM which is based on a cryptographic threshold signature scheme, and show how JTAM prevents malicious modifications to policy objects from authorized users.

VIII. TESTING

Systemtesting

System testing of software or hardware is testing conducted on a complete, integrated system to evaluate the system's compliance with its specified requirements. System testing falls within the scope of black box testing, and as such, should require no knowledge of the inner design of the code or logic.

Software Testing

Software Testing is an empirical investigation conducted to provide stakeholders with information about the quality of the product or service under test, with respect to the context in which it is intended to operate. Software Testing also provides an objective, independent view of the software to allow the business to appreciate and understand the risks at implementation of the software. Test techniques include, but are not limited to, the process of executing a program or application with the intent of finding software bugs. Software Testing can also be stated as the process of validating and verifying that a software program/application/product (1) meets the business and technical requirements that guided its design and development; (2) works as expected; and (3) can be implemented with the same characteristics.

Unit Testing

The primary goal of unit testing is to take the smallest piece of testable software in the application, isolate it from the remainder of the code, and determine whether it behaves exactly as you expect. Each unit is tested separately before integrating them into modules to test the interfaces between modules. Unit testing has proven its value in that a large percentage of defects are identified during its use.

Integration Testing

Integration testing (sometimes called Integration and Testing) is the activity of software testing in which individual software modules are combined and tested as a group. It occurs after unit testing and before system testing. Integration testing takes as its input modules that have been unit tested, groups them in larger aggregates, applies tests defined in an integration test plan to those aggregates, and delivers as its output the integrated system ready for system testing.

Acceptance Testing

Acceptance testing by the system provider is often distinguished from acceptance testing by the customer (the user or client) prior to accepting transfer of ownership. In such environments, acceptance testing performed by the customer is known as user acceptance testing (UAT). This is also known as end-user testing, site (acceptance) testing, or field (acceptance) testing.

CONCLUSION:

From this Cloud storage all the dynamic auditing details and data storage system will be analysed for similarity and interlinking between different individual databases. Joint Threshold Administrative tool implies authenticated and secured database management.

FUTURE WORK:

Recommending this proposal to the world bank to control black money . Then the bank should increase the speed of uploading the registration process in cloud.

REFERENCE:

1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," technical report, Nat'l Inst. of Standards and Technology,2009.

[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, 2010.

[3] T. Velte, A. Velte, and R. Elsenpeter, Cloud Computing: A PracticalApproach, first ed., ch. 7. McGraw-Hill, 2010.

[4] V. Kher and Y. Kim, "Securing Distributed Storage: Challenges, Techniques, and Systems," Proc. ACM Workshop Storage Security and Survivability (StorageSS), V. Atluri, P. Samarati, W. Yurcik, L. Brumbaugh, and Y. Zhou, eds., pp. 9-25, 2005.

[5] Y. Zhu, H. Wang, Z. Hu, G.-J.Ahn, H. Hu, and S.S. Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds," Proc. ACM Symp.

Applied Computing, W.C. Chu, W.E. Wong, M.J. Palakal, and C.-C.Hung, eds., pp. 1550-1557, 2011.

[6] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.

[7] M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," Proc. 11th USENIX Workshop Hot Topics in Operating Systems (HOTOS), G.C. Hunt, ed., 2007.

[8] G. Ateniese, S. Kamara, and J. Katz, "Proofs of Storage from Homomorphic Identification Protocols," Proc. Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology, M. Matsui, ed., pp. 319-333, 2009.

[9] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.

[10] M. Naor and G.N. Rothblum, "The Complexity of Online Memory Checking," J. ACM, vol. 56, no. 1, article 2, 2009.

[11] J. Li, M.N. Krohn, D. Mazie`res, and D. Shasha, "SecureUntrusted Data Repository (SUNDR)," Proc. Sixth Conf. Symp. Operating Systems Design Implementation, pp. 121-136, 2004.

[12] Y. Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage," IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 12, pp. 2231-2244, Dec. 2012.

[13] K. Yang and X. Jia, "Data Storage Auditing Service in Cloud Computing: Challenges, Methods and Opportunities," World Wide Web, vol. 15, no. 4, pp. 409-428, 2012.

[14] B. Schroeder and G.A. Gibson, "Disk Failures in the Real World: What Does an MTTF of 1,000,000 Hours Mean to You?" Proc. USENIX Conf. File and Storage Technologies, pp. 1-16, 2007.

[15] C. Wang, K. Ren, W. Lou, and J. Li, "Toward Publicly Auditable Secure Cloud Data Storage Services," IEEE Network, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.

Implementation of Low Power Dynamic Logic CMOS Circuits

[1]J Mercy, [2] Priya Stalin
[1]PG student, ME VLSI Design, Sree Sastha institute of engg. & tech, Chennai-123,
[2]Assistant Professor, Department of ECE, Sree Sastha institute of engg. & tech, Chennai-123
[1]sajmercy@gmail.com, [2]priyastalinme@gmail.com

Abstract—**Today in Very Large Scale Integration (VLSI) technology several applications require high speed operation. To achieve this dual output dynamic logic using Source Coupled Logic (SCL) topology was designed and it provides high speed operation with area and power over head. In order to reduce the power in dual output dynamic logic with optimizable speed of operation half swing is introduced. With the help of half swing without altering the operation of the logic function power is reduced. The half swing technique is applied to clock as well as input level. The existing system NMOS (N- type Metal Oxide Semiconductor) differential tree logic is applied to NAND, NOR, Exclusive -NOR (EX-NOR), half adder, and full adder. Due to the usage of NMOS differential tree logic this circuit gives true and complementary outputs. The power dissipation of NMOS differential tree logic is 80% greater than Complementary Metal Oxide Semiconductor (CMOS). Compared to the existing system the power dissipation is reduced by 46% in the proposed half swing. The delay achieved with existing system is 0.2 ns. The delay in the proposed system increases by 33% which is less compared to power dissipation reduction that is achieved. Advantages of dual output dynamic logic circuit is it increases the speed, avoids noise, no charge sharing problem, no short circuit power dissipation and it eliminates monotonicity problem.**

Index Terms— **Dual output dynamic logic, SCL, NMOS differential tree, Half swing**

I. INTRODUCTION

Among many logic circuit design techniques, CMOS is widely used because of high noise margin and ease of implementation. The conventional static CMOS circuits are intrinsically slow, because each gate must drive both NMOS and PMOS (P-type Metal Oxide Semiconductor) transistors. When the input is high, NMOS transistor will conduct, when the input is low, PMOS transistor will conduct as in [4]. Domino logic circuits drive only NMOS transistors and thus have the advantage of faster operation and smaller area compared to conventional CMOS circuits. Domino logic circuits have been widely used for high-performance microprocessors and other logic chips. However, their drawbacks include the non-inverting nature, strict timing constraints and charge sharing problems. Several dynamic logic circuits have been proposed for practical applications. Dynamic logic families offer more advantages than the traditional CMOS logic.

The main problem with dynamic circuit is its low susceptibility to noise. Dual output dynamic logic using SCL topology was proposed to overcome the noise problem in dynamic logic. Source coupled logic used in ultra - low power applications [9].It also has the following additional advantages like,

1) Increased speed
2) Low noise due to differential nature
3) No short circuit power dissipation
4) No charge sharing problem
5) No monotonicity problem
6) Dual output (True and complementary outputs)

The drawback of existing system is that it consumes more power. To overcome the drawback three techniques have been proposed. The three techniques are: i) clock half swing ii) input half swing iii) clock and input half swing. In each technique considerable amount of power is reduced maintaining the same area.

II. DIFFERENTIAL NMOS TREE REALIZATION

In integrated circuits dynamic logic design is mostly preferred. The difference between static and dynamic logic is that, in dynamic logic it has temporary storage, less surface area, they are faster than static logic and uses a clock signal for implementing combinational logic circuits but they are more difficult to design.

Dynamic logic consists of two phases. They are, 1) precharge phase 2) evaluation phase. During precharge phase the clock is low and the outputs are driven high irrespective of the input. During evaluation phase the clock is high and the output depends on the input combination. Dual output dynamic logic considers the two main techniques are: (1) using keeper, (2) precharging internal nodes as in [8]. Keeper circuit improves the noise immunity as in [7]. When all nodes are precharged, able to eliminate the charge sharing problem as in [3].

The NMOS block used in dynamic logic is based on static CMOS type realization. For which, a new type of realization is used for Boolean function, with which dual output can be obtained. This type of realization is used for SCL based logic gates design. There are several ways of realizing NMOS tree network. The most useful is Variable Entered Mapping (VEM) method. SCL topology avoids tedious simulation iterations as in [1].

VEM is an efficient method to obtain the most compact form of Boolean equation. It is not only suitable for two variable Boolean equations but also suitable for large variable Boolean equations. It can be utilized in various application areas of Boolean equations.

This technique reduces the input decision tree which gives minimized logic expression for all possible ordering of input variable. It is recommended to choose the realization which gives equal number of branches on the two output (i.e., normal and complementary) terminals. For example, the NMOS tree realization of Boolean function f (A, B) = A.B as shown in Fig. 1.

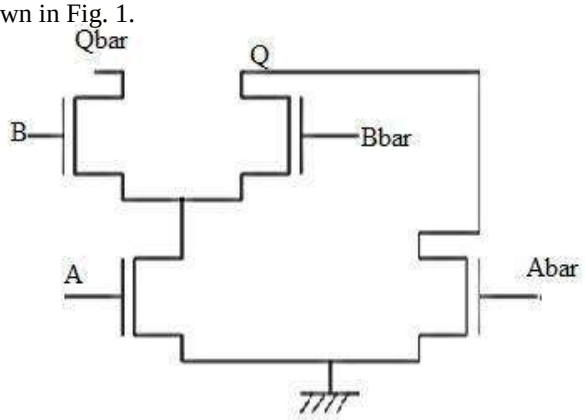


Fig. 1. Differential tree realization of NAND gate

Dual output dynamic logic AND/NAND circuit consists of basic dynamic logic structure with NMOS differential tree and two cross coupled keepers provides dynamic operation. Based on the two cross coupled connections it can operate in two phase.

(i) Precharge phase
(ii) Evaluation phase

During precharge phase the clock signal is always LOW. Therefore both outputs Q and Qbar are always connected to V_{dd} irrespective of the inputs, because there is no path exists between V_{dd} and ground. Since the clock is LOW, the NMOS transistor of the dynamic logic resides in high impedance state.

During evaluation phase the clock signal is HIGH. Therefore the PMOS transistors of dynamic logic turn OFF. The output depends on logical inputs given to the circuits.

Dual output dynamic logic has many advantages like increased speed and avoids noise. The additional advantages are there is no charge sharing problem, no short circuit power dissipation. It also eliminates the monotonicity problem. But due to the usage of NMOS differential tree concept, the number of transistor increases. This in turn increases the area and power. So to reduce the power, half swing technique is introduced.

III. HALF SWING TECHNIQUE

Reducing power consumption without sacrificing processing speed is a critical factor in VLSI design, especially for hand-held devices. In CMOS circuits, dynamic power consumption is proportional to the transition frequency, capacitance and square of supply voltage that is $P = CV^2$. Consequentially, reducing supply voltage provides significant power savings at the expense of speed.

This technique employs high performance architectures to achieve the specified speed and is quite effective for Application Specific Integrated Circuits (ASIC). In general purpose processors, however, it is more difficult to employ high performance architectures, because the architecture is already a part of the specifications. It is therefore very important to reduce power consumption without reducing supply voltage or sacrificing performance.

The drawback of dual output dynamic logic is overcome by the half swing technique. The NMOS and PMOS transistor turns ON when the gate voltage is greater than the threshold voltage. For example if the threshold voltage of NMOS is

0.8 V the transistor starts conduction if the gate voltage is greater than 1V. But 5 V is given to make it ON. So the power consumption increases. To reduce the power the input voltage swing is made half that is instead of 0 V to 5 V, 0 V to 2.5 V is given.

If the swing of the N-transistor input signal is limited from 0 to 2.5 V (half swing) the on-off characteristics of all N-transistors remain digitally identical. Similar observation can be made for clock signal. The input signal feeding p-transistor where the swing limited from 2.5 V to 5 V. The power can be reduced by the following three half swing techniques. They are,

- Clock half swing
- Input half swing
- Clock and input half swing

A. Clock half swing

The half swing clock is especially attractive in the two phase non overlapping clocking design where a sequential element requires two out-of-phase clock signals. The power saved from the reduced swing is 75% on the clock signal. The penalty incurred is the reduced speed of sequential element. In general the sequential delay is expressed in terms of propagation delay and setup/hold time delay. This is due to the on resistance of a transistor is inversely proportional to the voltage difference between its gate and source and the reduced clock swing increases the on-resistance of transistors. The clock swing of 5 V is reduced to half that is to 2.5 V and it is shown in Fig. 2. Dual output dynamic logic NAND/AND gate

using half swing technique is shown in Fig. 3.

Fig. 2. Clock half swing

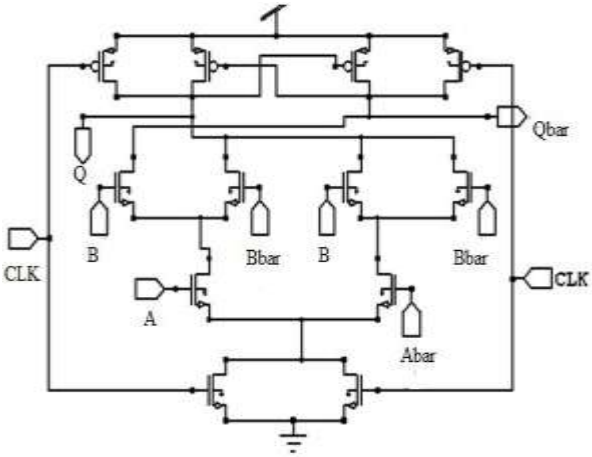


Fig. 4. Input half swing

Dual output dynamic logic NOR/OR gate using half swing is shown in Fig. 5.

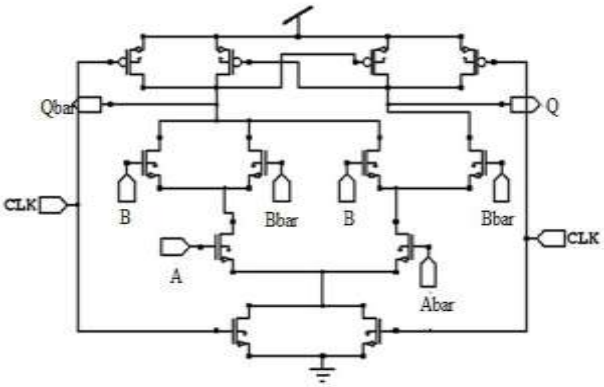


Fig. 5. Dual output dynamic logic NOR/OR gate using half swing

C. Input and clock half swing

The input and clock voltage is made half swing to reduce the power. The clock and input half swing is shown in Fig. 6

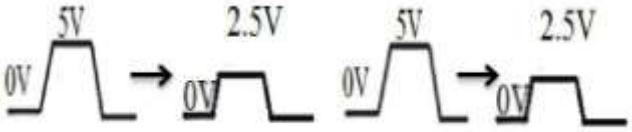


Fig. 6. Input and clock half swing

Dual output dynamic logic EXNOR/EXOR gate using half swing is shown in Fig. 7.

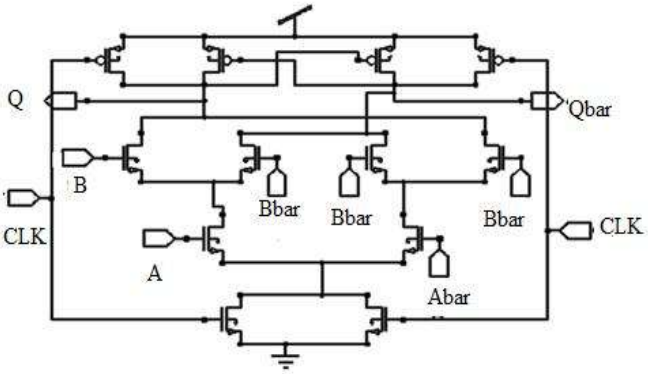


Fig. 7. Dual output dynamic logic EXNOR/EXOR gate using half swing

IV. HALF ADDER

The half adder consists of two inputs and produces two output sum and carry. Dual output dynamic logic half adder has two inputs (both in true form and in complement form) and the two outputs sum and carry (both also in true form and in complement form). The sum output corresponds to a logic EX-OR function while the carry output corresponds to an AND function. So, the half adder circuit can be implemented using EX-OR, AND gates. While compared to conventional CMOS technique the speed increases in this technique with optimized power and area. The half adder sum using half swing is shown in the Fig. 8.

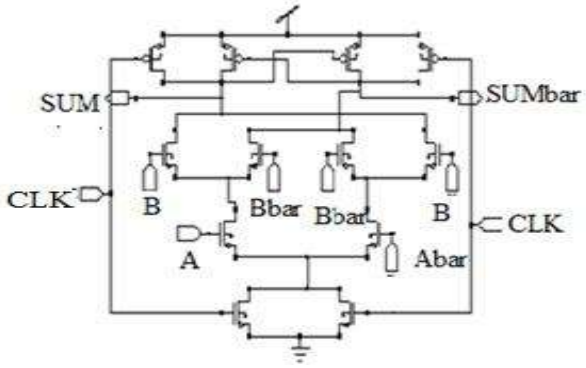


Fig. 8. Dual output dynamic logic half adder sum using half swing

The half adder carry using half swing is shown in the Fig. 9.

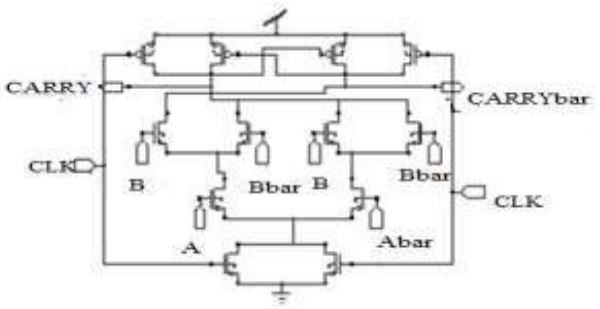


Fig. 9. Dual output dynamic logic half adder carry using half swing

V. FULL ADDER

The full adder consists of A, B and carry as inputs (both true and complementary) and produces sum and carry as outputs (both true and complementary). This carry is given to next adder as input. The full adder sum using half swing is shown in the Fig. 10.

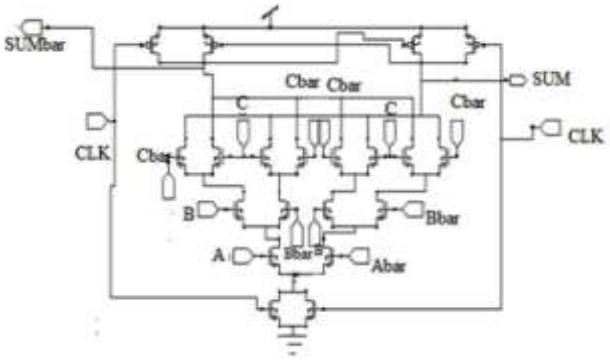


Fig. 10. Dual output dynamic logic full adder sum half swing

The full adder carry using half swing is shown in the Fig. 11.

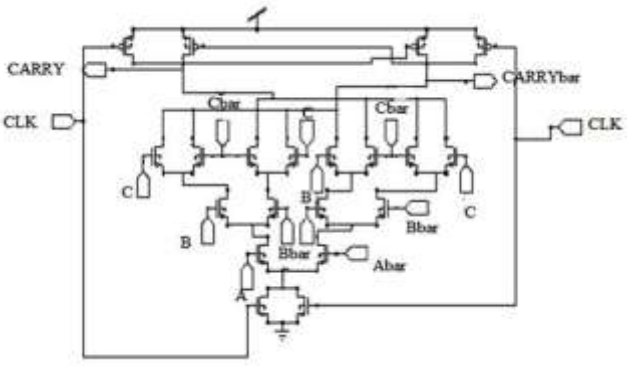


Fig. 11. Dual output dynamic logic half adder carry using half swing

VI. SIMULATION RESULTS

The simulation is performed in Tanner EDA at 250 nm technology. The operating temperature was maintained at 25ºC.The output of NAND gate using clock half swing is shown in Fig. 12.

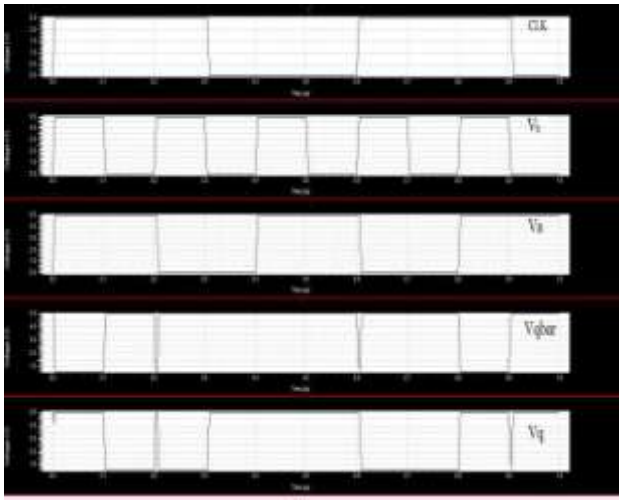


Fig. 12. Output of NAND gate using clock half swing

The clock half swing technique for NAND/AND gate provides the output waveform with the delay of 0.24 ns and the power consumption is 1.08 mW.

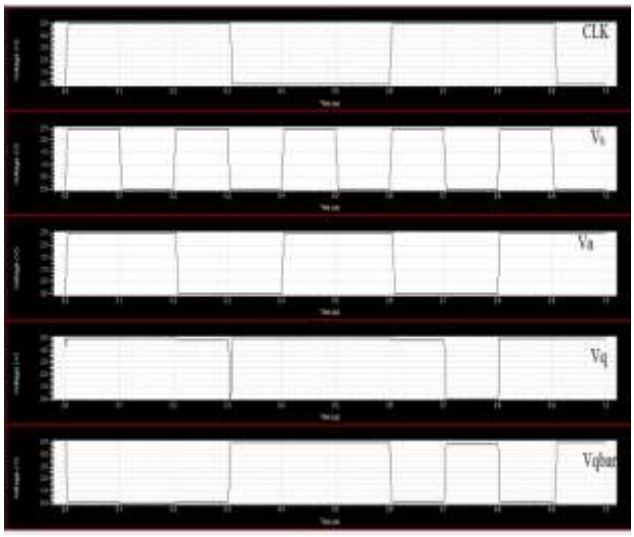


Fig. 13. Output of NOR gate using input half swing

The input half swing technique for NOR/OR gate provides the output waveform with the delay of 0.305 ns and the power consumption is 0.684 Mw.

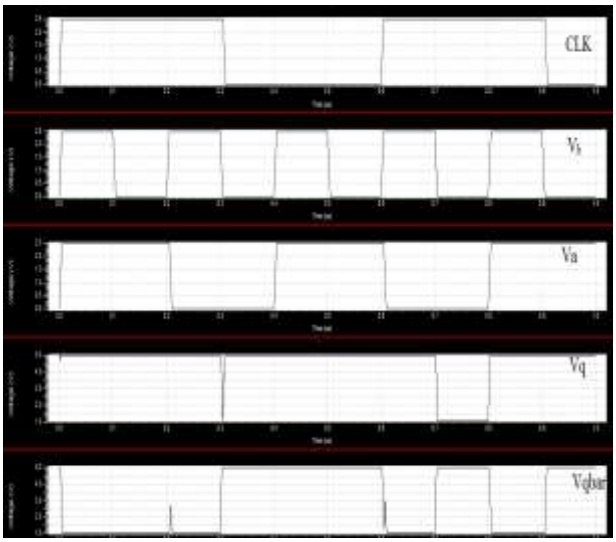


Fig. 14. Output of NOR gate using input and clock half swing

The clock and input half swing technique for NOR/OR gate provides the output waveform with the delay of 0.32 ns and the power consumption is 0.632 mW.

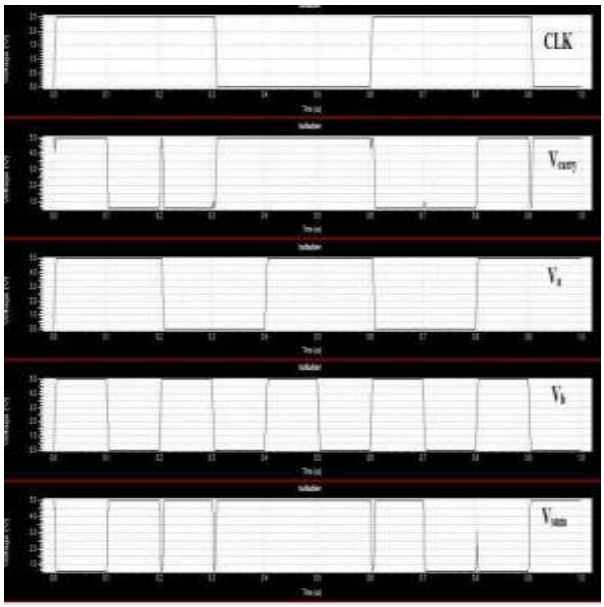


Fig. 15. Half adder using clock half swing

The clock half swing technique for half adder provides the output waveform with the delay of 0.262 ns and the power consumption is 1.57 mW.

Fig. 16. Full adder using clock and input half swing

The clock and input half swing technique for full adder provides the output waveform with the delay of 0.9 ns and the power consumption is 1.37 mW.

TABLE I

Performance analysis of NMOS differential tree logic with other half swing techniques

Logic Type	NMOS Differential Tree Logic		Clock Half Swing		Input Half Swing		Clock and Input Half Swing	
	Power (mW)	Delay (ns)	Power (mW)	Delay (ns)	Power (mW)	Delay (ns)	Power (mW)	Delay (ns)
NAND	1.33	0.21	1.08	0.24	0.72	0.312	0.6784	0.325
AND	1.33	0.21	1.08	0.24	0.72	0.312	0.6784	0.325
NOR	0.99	0.206	0.73	0.241	0.68	0.305	0.632	0.32
OR	0.99	0.206	0.73	0.241	0.68	0.305	0.632	0.32
EX-NOR	1.36	0.210	1.24	0.23	0.72	0.314	0.684	0.331
EX-OR	1.36	0.210	1.24	0.23	0.72	0.314	0.684	0.331
HALF ADDER	1.77	0.24	1.57	0.262	1.21	0.320	1.105	0.34
FULL ADDER	2.84	0.5	2.18	0.64	1.49	0.75	1.37	0.9

CONCLUSION

Dual output dynamic logic gives two outputs (true and complementary outputs) which is required for both combinational and sequential circuits. Dual output dynamic logic is more suitable for implementing flip-flops and latches.

The logic gates such as AND/NAND gate, OR/NOR gate, EX-OR/EX-NOR gate and adders are half adder and full adder uses dual output dynamic logic concept. This logic avoids the short circuit power dissipation and eliminates the noise and monotonicity problems. Dual output dynamic logic reduces the delay in circuit but increases the power and area. This increase in power is reduced by half swing technique. Thus this technique reduces the power than dual output dynamic logic with full swing. Future work involves reduction of area in this circuit.

REFERENCES

1. M. Alioto and G. Palumbo, "Design Strategies for Source Coupled Logic," *IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications",* vol. 50, no. 5, pp. 640-653, May 2003.
2. G. Diaz , L. Aranda and M. Hernaindez "A Comparison between Noise- Immunity Design Techniques for Dynamic Logic Gates', *IEEE International Symposium on Circuits and Systems*," vol. 1, pp. 484-488, 2006.
3. L. Ding and P. Mazumder "On Circuit Techniques to Improve Noise Immunity of Dynamic Logic", *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 12, no. 9, pp. 910-924.
4. HARRY J.M. VEENDRICK, "Short-Circuit Dissipation of Static CMOS Circuitry and Its Impact On the Design OF Buffer Circuits**,**" *IEEE journal of solid state circuits, vol 19, no 4, August 1984*.
5. C. Kim, S. Ookjung , K. H. Baek and S. M. Kang (2002) "High Speed CMOS Circuits with Parallel Dynamic Logic and Speed-Enhanced Skewed Static Logic*," IEEE Transactions on circuits and systems II*: *Analog and digital signal processing*, vol. 49, no. 6, pp. 434-439, May 2002.
6. J.H. Lou and J.B. Kuo "A 1.5-V CMOS All-N-Logic True-Single-Phase Bootstrapped Dynamic-Logic Circuit Suitable for Low Supply Voltage and High-Speed Pipelined System Operation," *IEEE Transactions on Circuits and Systems*, vol. 46, no. 5, pp. 628-631.
7. A. Rao, TH. Haniotakis, Y. Tsiatouhas and H. Djemil "The Use of Pre- Evaluation Phase in Dynamic CMOS Logic", *IEEE Computer Society Annual Symposium on VLSI New Frontiers in VLSI Design*, pp. 270-271, 2005.
8. Shamim Akhtar and Saurabh Chaturvedi, "A Novel method for Dual Output Dynamic Logic Using SCL Topology", *International Conference on signal Processing and Integrated Networks (SPIN), 2014.*
9. A. Tajalli and Y. Leblebici "Leakage Current Reduction using Sub-Threshold Source Coupled Logic", *IEEE Transactions on Circuits and Systems*, vol. 56, no. 5, pp. 374-378, May 2009.

Deep Web Mining Formulated with Information Administration Systems

[1]Dr. Brijesh Khandelwal,[2]Dr. S. Q. Abbas,[3]Dr. Parul Verma,[4]Dr. Shahnaz Fatima,[5]Dr. Ina Kapoor Sharma

[1]Research Scholar, Shri Venkateshwara University, Merut, UP., India, bbrijeshlko@yahoo.com
[2]Research Supervisor, Shri Vinkateshwara University, Merut, U.P. India, qrat_abbas@yahoo.com
Director, Ambalika Institute of Management & Technology, Lucknow, U.P.
[3]Asst. Professor, Amity University, Lucknow, UP., India, pverma1@lko.amity.edu
[4]Asst. Professor, Amity University, Lucknow, UP., India, sfatima1@lko.amity.edu
[5]Asst. Professor, SAMA Degree College, Lucknow, UP., India, ina_kapoor@yahoo.co.in

Abstract - **Most of the Web's information is buried far down on sites, and standard search engines do not find it. Traditional search engines cannot see or retrieve content in the deep Web. The portion of the Web that is indexed by standard search engines is known as the Web. Most Web structures are large and complicated and users often miss the purpose of their inquiry, or get ambiguous results when they try to navigate through them. Internet is enormous compilation of multivariate data. Several problems prevent effective and efficient information discovery for required better information administration systems it is important to retrieve accurate and complete data. The deep Web, also known as the deep invisible web has given rise to a novel issue of deep web mining research. An enormous amount of documents in the hidden web, as well as pages hidden behind search forms, specialized databases, and dynamically generated Web pages, are not accessible by universal Deep web mining application. In this research paper we have proposed a system that has an ability to access the deep web information using web structured mining systems for better intelligent information administration system resulting for effective and efficient information retrieval.**

Keywords— **Deep web, Information administration, information collection, information work model, web mining.**

I. INTRODUCTION

It is impossible to measure or put estimates onto the size of the deep web as the majority of the information is hidden or locked inside databases. Early estimates suggested that the deep web is around 5,000 times larger than the surface web. However, since more information and sites are always being added, it can be assumed that the deep web is growing exponentially at a rate that cannot be quantified. The deep Web, also known as the Dark web, dark net and invisible web, consists of web pages and data that are beyond the reach of search engines. Deep Web data integrative structure will categorize web database by domain, to provide users with a integrated query interface, called the integrated interface. Web database query interface itself, is called the local interface. Through the query interface, users can submit queries to several local structured interfaces of Web databases at the same time. Mapping queries of user uniform interface to the local interface, the key issue is pattern matching. The purpose of pattern matching is to find the attribute-pairs with logical association in different query structured interfaces. Due to the diversity of the local interface, the Deep Web pattern matching becomes a very challenging work.[7]

II. LITERATURE REVIEW-

Several research groups have focused on the problem large scale applications of intelligent deep web integration and information retrieval. Much of the research is in the context of a database system, and the focus is on wrappers that translate a database query to a Web request and parse the resulting HTML page. Deep web crawling aims to harvest data records as many as possible at an affordable cost Barbosa, 2004) [1], whose key problem is how to generate proper queries. Presently, a series of researches on Deep Web query has been carried out, and two types of query methods, namely prior information-based methods and nonprior information methods, have been proposed. The prior information-based query methods need to construct the information base beforehand, and generate queries under the guidance of prior information. In (Raghavan, 2001) proposed a task-specific Deep Web crawler and a corresponding query method based on Label Value Set table; the Label Value Set table as prior information is used for passing values to query forms. (Alvarez, 2007)[4] brought forward a query method based on domain definitions which increased the accuracy rate of filling out query forms. Such methods automate deep crawling to a great extent (Barbosa, 2005), The non-prior information methods are able to overcome the above deficiencies. These methods generate new candidate query keywords by

analyzing the data records returned from the previous query, and the query process does not rely on prior information.. However, queries with the most frequent keywords in hand do not ensure that more new records are returned from the Deep Web database. (Ntoulas, 2005) proposed a greedy query selection method based on the expected harvest rate. In the method, candidate query keywords are generated from the obtained records, and then their harvest rates are calculated; the one with the maximum expected harvest rate will be selected for the next query. (Wu P, 2006) modeled each web database as a distinct attribute-value graph, and under this theoretical framework, the problem of finding an optimal query selection was transferred into finding a Weighted Minimum Dominating Set in the corresponding attributed-value graph; according to the idea, a greedy link-based query selection method was proposed to approximate the optimal solution.[2]

Compared with the prior information-based methods, the non-prior information methods improve the query capability on Deep Web crawling Information Acquisition, Query processing module, Information work model, Information work model, Information acquisition from web structured interfaces and web database representation, Information representation, Information storage and reasoning.

queries to web databases. Every web database manages to capture its distribution and characteristics. Second Query translation try to translate the query on integrated interface equivalently into a set of local queries on the query structured interfaces of Web databases after extracting and mapping attributes, we get valid attributes for the query translation. This step is to generate valid query predicates from valid attributes. In the source query form, user can use four attributes to describe a book, which means that the more attributes we have the more restrictive query predicate we can get. When it comes to the target query form, user can use one of all the attributes to describe one facet of the book each time. To get translation of the different query forms, we have to get more valid predicates as we can. If we have some domain information about book, we will find the 'price' is the least important attribute when describing a type of book. In the other domain, there are the same situations. When translating queries, it is better to make numeric attributes useless, because we have found the numeric attributes are not more important than the other text attributes. Third part Query submission whereby analyzing the submission approaches of local query structured interfaces, and submit automatically each local query.[5]

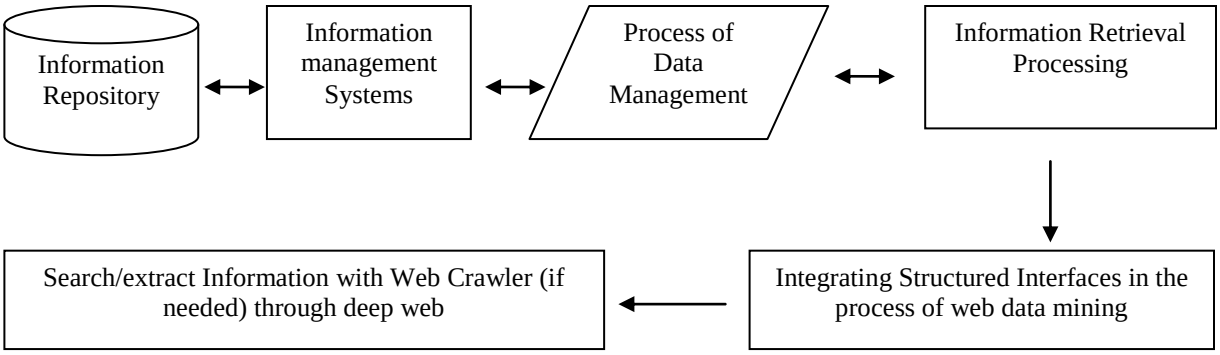


Figure 1. Information work model- Information Retrieval with Deep Web Mining

III. INFORMATION YIELDING QUERY PROCESSING SYSTEM- A STUDY

Process a user's query filled in integrated interface, and submit the query to each Web databases. There are three components in this module. The functions of them are described as follows: First one Web database selection Select appropriate Web databases for a user's query in order to get the satisfying results at minimal cost. When a query is submitted to the Web Database Selection, it will analyze the characteristics of the query, select the top web databases according to statistical data in Sampling Base, fill in query structured interfaces of these web databases, and submit

A. INFORMATION WORK MODEL

Its logical constrains relation and elements and among representation component parts are usually involved in deep web information processing. So information of data relation model and representation concept structure is useful. In addition, most Deep Web information is text document.

Lexical and logical analysis is needed and relative grammar information is necessary. Besides, there are the problem of hetero-generation among different web databases and the lack of universal logical concepts set for different dark Web. On the basis of the analysis above, a domain information work model for special domain Deep Web is put forward. The model describes entity of structured representation and its related information retrieval besides the attributes and relation of domain concept as shown in figure 1.

B. INFORMATION RETRIEVAL

Information retrieval from web structured interfaces and web database representation- With this process we collect and analyze web database representations and Deep Web query structured interface information. We obtain representation structure feature by taking statistics and analyzing pre-processed Representation samples.

Information representation- Our information-base will compose of a series of frames of several levels. Each structure can be treated as an information chunk or information unit. There are different levels of information units. Domain representation frame are constructed based on relational data model and structure fields based on database representation fields and concept logical dictionary.

Discovering Occurrences for Input Attributes- For a deep web data source, sample outputs can only be obtained when we can query the input interface by finding valid occurrences of input attributes. Furthermore, occurrences of input attributes and output attributes can efficiently suggest the logical matching between them. We combine two different ideas for finding such valid occurrences. [7]

1) Occurrences from Input Structured Interface: We have developed a new approach for automatically finding occurrences for input attributes using the information that is typically available from web pages related with the input interface provided by the data source. The key observation is that the webpage of input interface and web pages linked by the input interface always contain informative examples that help user to learn how to query the data source.

2) Obtaining occurrences from Output Web pages: Besides help web pages of the interface, another type of informative source that provides occurrences for an input attribute is the output web pages from other data sources in the same domain. The occurrences of output attributes might be able to query input attributes of other data sources if they are similar to each other, resulting in more output web pages and occurrences of output attribute that can further provide occurrences for input attributes.

CONCLUSION-

The study has provided a fundamental resources construction system which is helpful to the Deep Web intelligent integration and information retrieval. We showed how the systems can be used in the Deep Web interface matching systems. Extensive experiments over three real world domains show the utility of our approach. The results show that domain information can help improve matching accuracy. It may be valuable to large scale applications of the real-world Deep Web. Information-base construction is indispensable to web information processing from information engineering point of view. Hence information retrieval is longer a challenge with deep web in framed domain.

REFERENCES

[1] Manuel Álvarez, Alberto Pan+, Juan Raposo, Angel Viña: Client-Side Deep Web Data Extraction, Proceedings of the IEEE International Conference on E-Commerce Technology for Dynamic E-Business (CEC-East'04), IEEE

[2] Dheerendranath Mundluru, Jayasimha Reddy Katukuri, Saygin Celebi: Automatically Mining Result Records from Search Engine Response Pages, Proceedings of the Fifth IEEE International Conference on Data Mining (ICDM'05), IEEE

[3] Robert Baumgartner, Michal Ceresna, Gerald Ledermuller: Deep Web Navigation in Web Data Extraction, Proceedings of the 2005 International Conference on Computational Intelligence for Modeling, Control and Automation, and International Conference on Intelligent Agents, Web Technologies and Internet Commerce (CIMCAIAWTIC'05), IEEE

[4] Yoo Jung An, James Geller, Yi-Ta Wu and Soon Ae Chun: Automatic Generation of Ontology from the Deep Web, Proceeding of 18th International Workshop on Database and Expert Systems Applications 2007, IEEE

[5] Isabelle Guyon, Amir Saffari, Gideon Dror, and Gavin Cawley: Agnostic Learning vs. Prior Knowledge Challenge, Proceedings of International Joint Conference on Neural Networks, Orlando, Florida, USA, August 12-17, 2007

[6] Jufeng Yang Guangshun Shi Yan Zheng Qingren Wang: Data Extraction from Deep Web Pages, 2007 International Conference on Computational Intelligence and Security, IEEE

[7] Anand Singh Rajawat, Gopalkrushna Patel and Dr. Prashant R. Makwana: Web Mining through Advanced Knowledge Management Techniques: International Conference on Intelligent Computational Systems (ICICS'2012) Jan. 7-8, 2012 Dubai

ITBUZZ.CO
A collaborative Academic Portal

[1]Dr D S Adane,[2]Nayan Goenka,[3]Sneha Virwani,[4]Pooja Kulwal
[1][2][3][4]Department of Information Technology, Shri Ramdeobaba College of Engineering and Management Nagpur, India
[1]hodit@rknec.edu,[2]ping@nayangoenka.me, [3]snehavirwani76@gmail.com, [4]pooja.kulwal15@gmail.com

Abstract— **ITBUZZ.CO is an attempt to bridge the gap between academic and social life. ITBUZZ.CO thus is an academic social networking portal with an advanced and comprehensive feature list to compete some of the hit social networking websites of our age. ITBUZZ.CO is a secured online portal which grants access to only those personnel which are verified by the Department of IT, RCOEM. ITBUZZ.CO is a one stop communication channel for everyone in IT Department to share resources, knowledge have a healthy discussion for various topics, ,manage departmental activities, maintain personal profile and communicate freely through the website itself. ITBUZZ.CO is a portal which boasts a continuous, reliable and cross device network. ITBUZZ.CO has an extensive outreach to all the internet users through devices and platforms of their choice, may it be through desktops or laptops, mobile devices on Android, IOS or Windows phone/tablets.**

Keywords— **ITBUZZ, Socio-Academic Portal, Xenforo, Academic and Social Networking, Discussion Forums, Department Management, Academic Modernization**

I. INTRODUCTION

Collaborative learning is a buzz word in the education system today. Rapid developments in new technologies coupled with slow pace of reforms and updates in the university curriculum and increasing awareness levels of the students, it has become necessary for the teachers to fine tune their teaching skills so that relevant education is imparted to the students. It is necessary to go beyond the usual chalk-duster teaching to make teaching more effective. [1]

ITBUZZ.CO is a social and academic networking portal which bridges the gap between academic and social life of teaching and non-teaching staff as well as the students of Department of IT, RCOEM. ITBUZZ.CO is a platform in which academic resources as well as personal conversations find an excellent symphony to co-exist and provide the best of user experience at current technological as well as aesthetic sense colluding with the ominous delivery of the platform to user's disposal anytime, anywhere through its cross platform flexibility and cross gadget support throughout Windows, Linux, IOS, Android and other engines.

ITBUZZ.CO is needed in today's time in order to keep-in-touch with the daily happenings in the department. In the age of marvelous gadget coolness, referring to a notice board seems out of style. Thus ITBUZZ.CO is a modern day literally keep-in-touch platform. Ranging its expanse from hand held device support to anywhere-internet-deployed access to a cool digital notice board. ITBUZZ.CO is needed to bridge the tedious and traditional ways of information relay methods and modern day infrastructure. ITBUZZ.CO is scaled to behave as a self-dependent and comprehensive web portal. It provides inbuilt news relay, resource and file sharing, instant and reliable communication network as well as a social networking support to keep the users clung to the department and all the activities in and around it. ITBUZZ.CO can be scaled at an institute level and owing to its availability across the internet through various approaches. ITBUZZ.CO can easily grow up to be the campus connect-all portal. Just like Facebook started out.

II. PLATFORM SPECIFICATIONS AND DEPENDENCIES

A. Platform

ITBUZZ.co uses Xenforo version 1.3.2. Version 1.3.2 is a stable version and has many bug fixes and performance improvements. MySQL remains to be the primary database tool and it uses PHP version 5.5.3+.

B. Platform Features and Scale across various devices

ITBUZZ.CO being developed using Xenforo community software, it inherits all of its inbuilt features. Some of the namely features being Discussion forums, User accounts, User profile pages, User preferences, Inbox, Alert and Notification system, Member directory, Recent activity and administrator module for each level. XENFORO has been supplemented with various add-ons to enhance the

user experience. One of the add-ons being Tapatalk forum integration in order to render support on mobile devices on Android, IOS and Windows phones and tablets engines.

III. FEATURES

Below is the list of features of ITBUZZ.CO which are provided so as to give the users a state-of-the-art experience.

A. Discussion Forums

Users have a Forum Board available at link http://itbuzz.co/forums/ which has various categories, forums and sub forums. All the forums and sub forums are mapped against the various user groups and their access levels. Users have been mapped to accordingly view, comment and edit/access the threads. Moderator and Administrator level access have been given to specific user and user groups to monitor the forum board. Specific posts made by the management can be marked as Official posts and the users who have seen the thread are displayed in the bottom so that the administrators can know which users have read the thread. Also, certain threads can be marked sticky so that they appear first in listing always as well as locked so that further discussion or commenting on the same can be restricted. Similar or redundant threads can be merged, moved by the moderators and even deleted. The messages posted in threads can be specifically liked by other users or marked as spam via various post ratings. The user with more likes, earn more ratings. Thus trophies are awarded to users at specific milestones and earn points for the same which later results in distinguished recognition throughout the community. The threads can be specifically appended by premade thread prefixes which mark similarity of topics. This also provides a good search tag. Drafts of content are saved every 20 seconds in case the connection with the user fluctuates.

B. Resource Sharing

Users can share resources with others through this link http://itbuzz.co/resources/ which can be in downloadable, link or textual format. The resource categories are mapped against user groups just like forum discussions to facilitate level wise access to resources. Also, the users can upload revisions to the same resource and rate and review the same. This creates a healthy discussion on the resources there itself. The upload resources cannot be more than 5MB in size, the size can be later customized and there are restrictions on which extension of file that can be uploaded based on security and threat protocols. The extensions which are not supported can be zipped and uploaded.

C. Gallery

Users can share their pictures or videos or other media through this feature which can be located at http://itbuzz.co/media/. Gallery feature lets the users create their own albums and photo/video diaries to share with others and give a personal and social touch to their experience on ITBUZZ.

D. Events

Events can be created and managed right from http://itbuzz.co/events/. This feature allows the users to create events as they need and share and invite others. The access to view events can be selected while creating them and RSVP feature is made available for all members to let the event host know if they are attending the event.

E. User Profiles and Member Directory

All users have a personalized profile page which displays social information about them as specified. It shows personal information, recent activity information, medals, trophies, ribbons and other achievements information and

status updates. The status updates work similar to that in Facebook where users can like and comment on the same. Users can follow or ignore each other depending on their choice and the feeds from the users followed can be seen at http://itbuzz.co/account/news-feed. The personal account settings can be set from http://itbuzz.co/account/personal-details which includes password, signature privacy and other settings. Users can display their mood and avatar when and as they like and also have their own personalized signatures.

The complete Member directory can be accessed from http://itbuzz.co/members/ and a sorted list can also be access using the various criteria listed. Members can be tagged into conversations or forum posts or media by user tagging features which works by appending '@' before the username.

F. Inbox and Chat

ITBUZZ.CO also diminishes the use of separate email accounts by providing an Inbox right in the portal. The users can communicate among themselves on a personal level or within a specific group of users using this feature. Attachments and other similar features are inherited from the Forums and Resource sharing facilities. The Administrators can also send newsletters or group emails to all/some users through the Admin Panel.

Adding to it, ITBUZZ.CO provides a real-time char shout box or one may call it an IRC at http://itbuzz.co/chat/

G. Blogs

[1] The definition says that a blog is an online journal where users post thoughts, comments or news in a chronological format. Updates are often frequent and done on a regular basis.

Users who love to write and share their views, ITBUZZ.CO acts as a ready platform for them. Users can create their Blogs and manage them more efficiently which is much better and easier than maintaining personal blog website. It gives the author a ready fan base and encourages writing and sharing views and data among a trusted community.

H. Quizmaster and Subjective Tests

Quizmaster is another feature on ITBUZZ.CO which provides a rapid fire objective as well as subjective test to be conducted for the users. This becomes instrumental while preparing for competitive exams or interviews.

Apart from this, a subjective exam can also be converted on the portal which is one of its kind transforming the way exams are conducted all over.

I. Media Embeding

The messages posted in the community can hold attachments as well as embed of various types like images, videos, documents etc. These embeds can be live videos, video lectures, live streaming of lectures from the classes, presentations, documents etc.

J. User Discipline and Web Traffic Monitoring

Users can be disciplined by moderators or administrators by regularly issuing warnings, handing out community bans

or user discouragement if needed. Various usage restrictions and discouraged service by website is thus managed so as to keep the discipline and integrity of the website inline.

Recent website activity can be seen by all users. The sidebar shows users online list and also specifically shows recent status updates, total website statistics and other important alerts from the website. Recent activity of specific users can be seen from their profile pages. Also the website traffic, diagnosis and other logs and statistics can be viewed from the admin panel by the administrators. Also the users' IP address can be traced and IP based settings and specifications can be set accordingly.

K. Mobile Support

ITBUZZ.CO has a personalized mobile application for Android, IOS and Windows phones and Windows 8 tablets. This has been achieved by integrating ITBUZZ.CO with Tapatalk mobile app. The Tapatalk mobile app should be installed on the device, search for ITBUZZ in the forums and login using the appropriate credentials. A comprehensive UI and excellent UX can be obtained while using ITBUZZ.CO from anywhere, anytime. Tapatalk control panel can be used to send push notifications to all users using the app for ITBUZZ.CO to give important and urgent updates. This can only be done by the administrators as many times required

L. Medals, Trophies, Ribbons and Titles

ITBUZZ.CO has an extensive range of Medals, Trophies and other Honorary Titles which can be awarded to users based on their achievements and performances. Medals are manually awarded to the members on their specific achievements. Trophies are automatically awarded to the users when they achieve particular number of ratings collected via likes or other up-votes on their content from the community. The Titles can be automated or user generated. These titles are thus displayed on the profiles. Ribbons and Moods are other decorative aspect which reflect on the user account which adds to the charm of socializing on ITBUZZ.CO

CONCLUSION

ITBUZZ.CO has tremendous potential to be the ERP lay for the entire Information Technology community right at the academic level. ITBUZZ.CO is extremely flexible and easily configurable portal for any and all interested organizations since the back end of the software makes it useful in a wide range of applications and purposes. ITBUZZ.CO has a successful and stable performance on Laptops, Desktops, Tablets, Mobile devices and all other hand-held devices on a real time scale.

ACKNOWLEDGMENT

We wish to avail this opportunity to acknowledge our profound indebtedness and extend our deep sense of gratitude to our guide and Head of Department of Information Technology, Dr. D. S. Adane for his valuable advice, endless support, co-operation and encouragement that has led to successful execution of this project. We express our sincere gratitude to the Principal and Vice-Principal and all the staff of the college in striving continuously to provide us the stature to take up the project and execute it. Finally we would like to express deepest gratitude and reverence to our parents, their steadfast encouragement throughout progress of this work.

REFERENCES

1. D.S Adane, "Effective Teaching-Learning Using Web Tools", The
Indian Journal of Technical Education, Volume 31. No.2 , April-June 2008. ISSN 0971-3034.

Review on Design of Hand Gesture based Wheelchair Controller using MEMS Technology

[1]Ms. Nupur Jaiswal,[2]Ms Ashlesha S Nagdive
[1]Department of Computer Science & Engineering, G. H. Raisoni College of Engineering, Nagpur, Maharashtra, India
[2]Assistant Professor Department of Information Technology, G. H. Raisoni College of Engineering, Nagpur, Maharashtra, India
[1]jaiswal_nupur.ghrcees@raisoni.net,[2]ashlesha.nagdive@raisoni.net

Abstract - **This paper describes an automatic wheelchair for physically disabled people. The aim is to design and develop a system that allows the user to robustly interact with the wheelchair at different levels of control and sensing. The wheelchair will be controlled via gestures. Sensors integrated with wheelchair will perform gesture recognition. Sensors give x-axis and y-axis output independently which is fed to ADC & then microcontroller which decides the movement of wheelchair. On chair obstacle sensors will be installed. Total 4 sensors will be installed for detection of obstacle in the forward, backward, left & right direction. We propose to build an automatic wheelchair using various technologies, which are discussed in this paper.**

Index Terms – **Gesture recognition, obstacle detection, automatic wheelchair.**

I. INTRODUCTION

The overall framework of this project is to restore autonomy to severely disabled people by helping them use a wheelchair independently. An automatic wheelchair is an electric wheelchair fitted with infrared sensors, obstacle sensors and controller to help less able drivers achieve some independent mobility. Just by detecting the gesture wheelchair can be moved in four directions. The obstacle sensor can help the rider control the wheelchair by taking over some of the responsibility for steering and avoiding objects until he or she is able to handle the job. The amount of work that the rider chooses to do and how much control will be taken by the chair will be decided by the rider. Obstacles in the way can be determined by the wheelchair and wheelchair will stop automatically.

In recent times there have been a wide range of guidance systems available in wheelchair. Also various control systems are being developed, specialized for people with various disorders and disabilities. The systems that are developed are highly competitive in replacing the old traditional systems. In order to increase the quality of life for handicap people and facilitate their integration into the working world, we intend to build a wheelchair with embedded intelligence.

There are many assistive systems using visual aids like smart wheelchair systems, using joystick and much more. There are systems based on voice recognition too. The basic aim is to detect basic commands using joystick or tactile screen. These applications are quite popular among people with limited upper body mobility. But still there are certain drawbacks in these systems. They cannot be used by people of higher disability because they require fine and accurate control which is most of the time not possible.

This paper reports the preliminary work in developing a wheelchair system that involves gesture recognition. The system enables the person to have command over the wheelchair and its direction of movement and will also tell the user about the obstacles in the path, to avoid collision. The aim is to design and develop a system that allows the user to robustly interact with the wheelchair at different levels of control and sensing

II. ADVANTAGES

Increased mobility, for disabled people who cannot use their arms to power a manual wheelchair, or for people who do not have the upper body strength to self-propel a manual wheelchair. Increased manoeuvrability, automatic wheelchairs use casters that swivel a full 180 degrees to provide more manoeuvrability, especially in small areas. According to the Electric Wheelchairs Centre, manoeuvrability is one of the key problems associated with use of wheelchair. Automatic wheelchairs allow a disabled individual to get around tight spaces and move through smaller areas, which is especially beneficial at home. Increased physical support, a power wheelchair can have the option to allow for more physical support, including adjustable seating such as tilt and recline. Increased ability to live independently – to enjoy the same choice, control and freedom as any other citizen –at home, at work, and as members of the community. Enable young disabled children and their families to enjoy ordinary lives. Increase the number of disabled people in employment and providing

support for those unable to work.

III. PROPOSED SYSTEM

Issues with the existing wheelchair systems are: Existing system is unable to adapt to the external conditions. Accuracy of identification is less. Complex classification techniques employed. Time consuming. So to overcome all these issues, we propose a methodology based on following assumptions: To use wheelchair automatically for moving forward, backward, left & right through head movements. Our system basically works on the principle of acceleration, using accelerometer. When person tilt his hand in forward direction chair will move in forward direction.

If person tilt his hand in backward direction chair will move in backward direction. If person tilt his hand in left direction chair will move in left direction, and if person tilt his hand in right direction chair will move in right direction.

IV. IMPLEMENTATION PLATFORM

A] Hardware requirements:

AT89C51 microcontroller

MAX232 for protocol conversion Acceleration sensor

L293D driver IC

12v DC power supply

Obstacle sensors
Motors

LM7805

B] Software Requirements:

Kiel uVision4 for Embedded C programming Flash Magic for burning program to IC

Xpress PCB software for PCB design

V. ARCHITECTURE

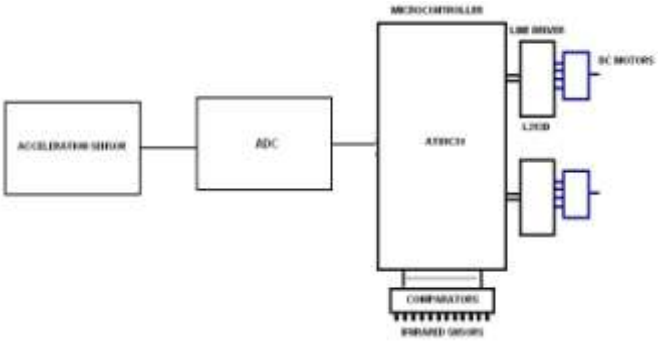


Fig.1. Block diagram of automated wheelchair

Our project basically works on the principle of acceleration; one accelerometer sensor provides two axes. This sensor, whose output is analog, varies according to acceleration applied to it. By applying simple formula we can calculate the amount of tilt & output of tilt will decide the direction in which to move. Sensor gives x-axis & y-axis output independently, which is fed to ADC & then microcontroller & depending on the pulse width it decides to move or not. On chair obstacle sensors are installed. Total 4 sensors will be installed for detection of obstacle in the forward, backward, left & right direction. The aim is to design and develop a system that allows the user to robustly interact with the wheelchair at different levels of control and sensing.

VI. CIRCUIT DIAGRAM

From circuit diagram, it is clear that we have used microcontroller 89C51, and the accelerometer sensor is connected to the port 3 of microcontroller. Depending on the movement of hand, the motor moves in any of the four directions (i.e. forward, backward, left or right).

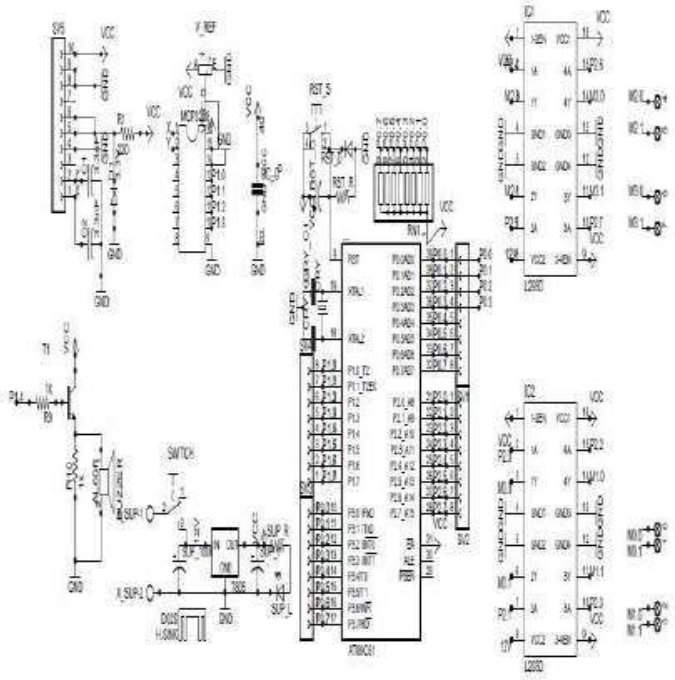


Fig.2. Circuit diagram of automated wheelchair

When person tilt his hand in forward direction chair will move in forward direction. If person tilt his hand in backward direction chair will move in backward direction. If person tilt his hand in left direction chair will move in left direction. If person tilt his hand in right direction chair will move in right direction. Depending on the width of pulse width modulation, microcontroller will generate a count

value. So, depending on the value of the count it will give the signal to the motor to move in corresponding direction

VII. FUTURE SCOPE

We can make a wheelchair which can be operated by a wireless remote. Output of sensor can be applied to wireless transmitter circuit and can received at wheelchair circuit by receiver circuitry. So wireless operation will reduce wiring arrangements. Instead of using acceleration motion (hand movement) we can use eye retina using optical sensor to move wheelchair in different direction. Using retina movement we would be able to drive a wheelchair. We can use voice command IC to interface our voice signals with controller. So computer interfacing may not be needed. The voice stored in IC will be sufficient to analyze speaker's voice command. Research is going on development of wheelchair using nervous system of humans.

CONCLUSION

Automated wheelchair can be used to help handicapped people, especially those who are not able to move. Our project is a combination of electronic circuits, implemented by hardware designing & software programming. We have achieved the aim of removing the limitations of existing systems. The system was successfully implemented and tested to move in left, right, forward and backward direction. There are several barriers that must be overcome before smart wheelchairs can become widely used. A significant technical issue is the cost versus accuracy.

REFERENCES

[1] Bourhis G, Moumen K, Pino P, Rohmer S, Pruski A. *"Assisted navigation for a powered wheelchair. Systems Engineering in the Service of Humans"*, Proceedings of the IEEE International Conference on Systems, Man and Cybernetics; 2013 Oct 17–20; Le Touquet, France. Piscataway (NJ): IEEE; 2013. p. 553–58.

[2] Boy ES, Teo CL, Burdet E. *"Collaborative wheelchair assistant"* Proceedings of the 2012 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS); 2012 Sep 30–Oct 5; Lausanne, Switzerland. Piscataway (NJ):IEEE; 2012. p. 1511–16.[3]B. Rebsamen, C. L. Teo, Q.

[3] Zeng, M. H. Ang Jr., E. Burdet, C. Guan, H. Zhang, and C. Laugier. *"Controlling a wheelchair indoors using thought"* IEEE Intelligent Systems, 22(2):18–24, 2012.

[4] Keating D, Warwick K. *"Robotic trainer for powered wheelchair users"* Proceedings of the IEEE International Conference on Systems, Man and Cybernetics; 2012 Oct 17–20; Le Touquet, France. Piscataway (NJ): IEEE; 2013. p. 489–93.

[5] Masato Nishimori, Takeshi Saitoh and Ryosuke Konishi, *"Voice controlled intelligent wheelchair,"* 2011.

[6] SICE Annual Conference 2007, International onference on Instrumentation, Control and Information Technology, 2007, pp.336–340.

[7] Moon, M. Lee, J. Chu, and M. Mun, *"Wearable EMG-based HCI for Electric-Powered Wheelchair Users with Motor Disabilities,"* Proc. of the 2005 IEEE Int. Conf. on Robotics and Automation, pp. 2649-2654, 2005.

[8] R. Simpson, Takeshi Saitoh, D. Poirot, and M. F. Baxter. "*Evaluation of the Hephaestus smart wheelchair system. in Intemational Conference on Rehabilitation Robotic",* 2004.

SECURITY ISSUE IN CLOUD COMPUTING

[1]Ms Sonal N.Gamey,[2]Ms.MonalN.Gamey,[3]Mrs.Neha A. Khatri
[1][2][3]M.E.(CSE)Aurangabad Maharashtra Mumbai
[1]sonalgamey@gmail.com,[2]monal_2525@yahoo.co,[3]innehakhatri123@gmail.com

Abstract- Cloud Computing is an Internet-based computing technology, where shared resources such as software, platform, storage and information are provided to customers on demand. It is a computing platform for sharing resources that include infrastructures, software, applications, and business processes. It is a virtual pool of computing resources. It provides computing resources in the pool for users through internet .Examples are it Google Docs or Google Apps ,YouTube Video sharing or Picasa Image sharing, Amazon's EC2. cloud Computing presents an added level of risk because essential services areoften outsourced to a third party, which makes it harder to maintain data security and privacy, support data and service availability, and demonstrate compliance. Cloud Computing leverages many technologies (SOA, virtualization, Web 2.0); it also inherits their security issues, which we discuss here, identifying the main vulnerabilities in this kind of systems and the most important threats found in the literature related to Cloud Computing and its environment as well as to identify and relate vulnerabilities and threats with possible solutions This seminar provides a concise but all-round analysis on data security and privacy protection issues associated with cloud computing. Then this seminar discusses some current solutions & describes future research work about data security and privacy protection issues in cloud

***Index Terms*- Cloud Computing, Utility computing, Risk ,IaaS, PaaS, SaaS, Security, Quality Assurance, Threats,CIA.**

I. INTRODUCTION:

It is an Internet-based computing technology, where shared resources such as software, platform, storage and information are provided to customers on demand.Cloud Computing is a computing platform for sharing resources that include infrastructures, software, applications, and business processes.Cloud Computing is a virtual pool of computing resources.It provides computing resources in the pool for users through internet.Cloud computing, as an emerging computing paradigm aiming to share storage, computation, and services transparently among a massive users. Current cloud computing systems pose serious limitation to protecting users' data confidentiality. Since users' sensitive data is presented in unencrypted forms to remote machines owned and operated by third party service providers, the risks of unauthorized disclosure of the users' sensitive data by service providers may be quite high. There are many techniques for protecting users' data from outside attackers. an approach is presented to protecting the confidentiality of users' data from service providers, and ensures service providers cannot collect users' confidential data while the data is processed and stored in cloud computing systems. Cloud computing systems provide various Internet-based data storage and services. Due to its many major benefits, including cost effectiveness and high scalability and flexibility, cloud computing is gaining significant momentum recently as a new paradigm of distributed computing for various applications, especially

for business applications. Along with the rapid growth of the Internet. With the rise of the era of "cloud computing", concerns about"Internet Security" continue to increase. How will customers of the "cloud" know that their information will be available to them,as well as secure and safe from others? To address this problem we propose the design of a system that will capture the movementof information on the cloud. We will be identifying whether thereis a need for some type of security capture device/measure on the cloud, which will allow users to know whether their information is secure and safe without comprising from threats and attacks.

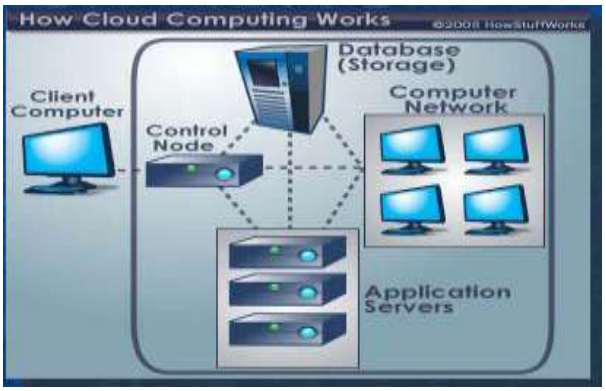
II. LITERATURE SURVEY:

The term "cloud" in cloud computing is the communications network or a network combined with computing infrastructure. It is an Internet-based computing technology, where shared resources such as software, platform, storage and information are provided to customers on demand.Cloud Computing is a computing platform for sharing resources that include infrastructures, software, applications, and business processes.Cloud Computing is a virtual pool of computing resources.It provides computing resources in the pool for users through internet.

III. CLOUD ARCHITECTURE

The architecture of Cloud involves multiple cloud components communicating with each other over the application programming interfaces (APIs), usually web services. The two most significant components of cloud computing architecture are known as the front end and the back end. The front end is the part seen by the client, i.e. the

customer. This includes the client's network or computer, and the applications used to access the cloud via a user interface such as a web browser. The back end of the cloud computing architecture is the 'cloud' itself, which comprises of various computers, servers and data storage devices.



IV. WORKING OF CLOUD COMPUTING:

Cloud Computing system can be divided it into two sections: the **front end** and the **back end**. They connect to each other through a network, usually the Internet. Thefront end is the side the computer user, or client, sees.**The back end** is the "cloud" section of the system. On the back end there are various computers,servers and data storage systems that create the "cloud" ofcomputing services.A central server administers the system, monitoring traffic and client demands to ensure everything runs smoothly. It followsa set of rules called protocols Servers and remote computers do most of the work and store the data.

cloud model provides three types of services [21,28,29]:

Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. Theapplications are accessible from various clientdevices through a thin client interface such as a webbrowser (e.g., web-based email).

Platform as a Service (PaaS). The capability providedto the consumer is to deploy onto the cloudinfrastructure his own applications without installingany platform or tools on their local machines. PaaSrefers to providing platform layer resources,including operating system support and softwaredevelopment frameworks that can be used to buildhigher-level services._ Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing,storage, networks, and other fundamentalcomputing resources where the consumer is able todeploy and run arbitrary software, which caninclude operating systems and applications.WithSaaS, the burden of security lies with the cloudprovider. In part, this is because of the degree ofabstraction, the SaaS model is based on a high degree ofintegrated functionality with minimal customer control or extensibility. By contrast, the PaaS model offers greaterextensibility and greater customer control. Largely becauseof the relatively lower degree of abstraction, IaaS offersgreater tenant or customer control over security than doPaaS or SaaS [10].Before analyzing security challenges in Cloud Computing,we need to understand the relationships anddependencies between these cloud service models. PaaS as well as SaaS are hosted on top of IaaS; thus, anybreach in IaaS will impact the security of both PaaS andSaaS services, but also it may be true on the other wayaround. However, we have to take into account thatPaaS offers a platform to build and deploy SaaS applications,

V. CLOUD SECURITY ISSUE

The world of computation has changed from centralized (client-server not web-based) to distributed systems and now we are getting back to the virtual centralization (Cloud Computing). Location of data and processes makes the difference in the realm of computation.we have the cloud

computing wherein, the service and data maintenance is provided by some vendor which leaves the client/customer unaware of where the processes are running or where the data is stored. So, logically speaking, the client has no control over it. The cloud computing uses the internet as the communication media. When we look at the security of data in the cloud computing, the vendor has to provide some assurance in service level agreements (SLA) to convince the customer on security issues.Organizations use cloud computing as a service infrastructure, critically like to examine the security and confidentiality issues for their business critical insensitive applications. What are the "security" concerns that are preventing companies from taking advantage of the cloud? In this section we present a taxonomy of the "security" concerns. Traditional security Availability Third-party data control

VI. TRADITIONAL SECURITY

These concerns involve computer and network intrusions or attacks that will be made possible or at least easier by moving to the cloud. Cloud providers respond to these concerns by arguing that their security measures and processes are more mature and tested than those of the average company.It could be easier to lock down information if it's administered by a third party rather than in-house, if companies are worried about insider threats… In addition, it may be easier to enforce security via contracts with online services providers than via internal controls.Availability These concerns center on critical applications and data being available. Well-publicized incidents of cloud outages include Gmail.As with the Traditional Security concerns, cloud providers argue that their server uptime compares well with the availability of the cloud user's own data centers.Cloud services are thought of as providing more availability, but perhaps not – there are more single points of failure and attack.Third-party data control The legal implications of data and applications being held by a third party are complex and not well understood. There is also a potential lack of control and transparency when a third party holds the data. Part of the hype of cloud computing is that the cloud can be implementation independent, but in reality regulatory compliance requires transparency into the cloud.The architecture of Cloud involves multiple cloud components communicating with each other over the application programming interfaces (APIs), usually web services. The two most significant components of cloud computing architecture are known as the front end and the back end. The front end is the part seen by the client, i.e. the customer. This includes the client's network or computer, and the applications used to access the cloud via a user interface such as a web browser. The back end of the cloud computing architecture is the 'cloud' itself, which comprises of various computers, servers and data storage devices.

VII. THREATS IN CLOUD COMPUTING

3.1 Threats Cloud computing faces just as much security threats that are currently found in the existing computing platforms, networks, intranets, internets in enterprises. These threats, risk vulnerabilities come in various forms.

The Cloud Security Alliance (Cloud Computing Alliance, 2010) did a research on the threats facing cloud computing and it identified the flowing major threats:

- Failures in Provider Security
- Attacks by OtherCustomers
- Availability and Reliability Issues
- Legal and Regulatory Issues
- Perimeter Security Model Broken
- Integrating Provider and Customer Security Systems
- Abuse and Nefarious Use of Cloud Computing
- Insecure Application Programming Interfaces
- Malicious Insiders
- Shared Technology Vulnerabilities
- Data Loss/Leakage
- Account, Service & Traffic Hijacking
- Unknown Risk Profile

VIII. NEED FOR SECURITY IN CLOUD

A user's dependence on cloud is analogous to a person's dependence on public transportation as it forces one to trust over which one have no control, limits what one can transport, and subjects us to rules and schedules that wouldn't apply if one had their own vehicles. On the other hand, it is so economical that one doesn't realistically have any alternative.Users of the cloud aren't aware about the location of the data and ultimately have to rely on the cloud service provider for exercising appropriate security measures. Therefore cloud security issue is the most important and elicited topic amongthe IT professionals.

Security in cloud computing is of two types:-

1. Data Security:-

It focuses on protecting the software and hardware associated with the cloud. It deals with choosing an apt location for data centers so as to protect it from internal threats, different types of weather conditions, fire and even physical attacks that might destroy the center physically and external threats – avoiding unauthorized access and break ins.

2. Network Security :-

Protecting the network over which cloud is running from various attacks – DOS, DDOS, IP Spoofing, ARP Spoofing and any novel attacks that intruders may device. Attack on data affects a single user whereas a successful attack on Network has the potential to affect multiple users. Therefore network security is of foremost importance.

1) the service provider has privilege to access and collect the users' confidential data in cloud.
2) the service provider can understand the meaning of the users' data.

Our approach makes sure that any of these entities in a cloud computing system does not satisfy the three conditions simultaneously.Software Cloud: A Software Cloud provides software as a service upon users' requests. Each software cloud may contain multiple software services, and each software service can be discovered and accessed by users through Software Service Broker.

IX. SOLUTION OF SECURITY ISSUES

Find Key Cloud Provider First solution is of finding the right cloud provider. Different vendors have different cloud IT security and data management. A cloud vendor should be well established, have experience, standards and regulation. So there is not any chance of cloud vendor closing.

ii. Clear Contract with cloud vendor should be clear. So if cloud vendor closes before contract, enterprise can claim.

iii. Recovery Facilities Cloud vendors should provide very good recovery facilities. So, if data are fragmented or lost due to certain issues, they can be recovered and continuity of data can be managed.

iv. Better Enterprise Infrastructure Enterprise must have infrastructure which facilitates installation and configuration of hardware components such as firewalls, routers, servers, proxy servers and software such as operating system, thin clients, etc. Also should have infrastructure which prevents from cyber attacks.

v. Use of Data Encryption for security purpose Developers should develop the application which provides encrypted data for the security. So additional security from enterprise is not required and all security burdens are placed on cloud vendor

X. FUTURE WORK

We are investigating in the cloud security management problem. Our objective is to block the hole arise in the security management processes of the cloud consumers and the cloud providers from adopting the cloud model. To be able to resolve such problem we need to Capture different stakeholders security requirements from different perspectives and different levels of details map security requirements to the cloud architecture, security patterns and security enforcement mechanisms and Deliver feedback about the current security status to the cloud providers and consumers.

CONCLUSIONS

Although Cloud computing can be seen as a new phenomenon which is set to revolutionizethe way we use the Internet, there is much to be cautious about. There are many new technologiesemerging at a rapid rate, each with technological advancements and with the potential of makinghuman's lives easier. However, one must be very careful to understand the security risks andchallenges posed in utilizing these technologies. Cloud computing is no exception. In this paperkey security considerations and challenges which are currently faced in the Cloud computing are
highlighted. Cloud computing has the potential to become a frontrunner in promoting a secure,virtual and economically viable IT solution in the future.

References

[1]Stephen S. You and Ho G, "Protection of users' data confidentiality "from ACM digital library.
[2] J. Heister and M. Nicolet, "Assessing the security risks of
cloudcomputing, "from ACM digital library.
[3] La'Quata Sumter," Cloud Computing: Security Risk" from ACM digital library.
[4] Gary Anthes,"Security in the Cloud" november 2010 | vol. 53 | no. 11 | communications of the acm 11.
F. Gens. (2009, Feb.). "New IDC IT Cloud Services Survey: Top Benefits and Challenges",
[5] IDC exchange, Available: <http://blogs.idc.com/ie/?p=730> [Feb. 18, 2010].International Conference and Workshop on Emerging Trends in Technology (ICWET 2011) – TCET,Mumbai, India.

A survey of big data analysis its issues and Challenges

[1]Dr. Vikash K Singh,[2]Devendra Singh Kushwaha,[3]Shaibya Singh,[4]Sonal Sharma
Assistant Professor, Dept. of Computer Science, Indira Gandhi National Tribal University, Amarkantak
[1]drvksingh76@gmail.com,[2]devendra2904@gmail.com,[3]shaibyaigntu@gmail.com,[4]Sonal_sdl@yahoo.co.in

Abstract- **Now a day's everyone has been speaking about Big Data for some time, but there is a lot of rumor and tire kicking by many in the industry. We wanted to evaluate how people are viewing Big Data today, how important it is, how to deal with it, what returns can be had from it…**

Big data is the term for data sets so large and complicated that it becomes difficult to process using traditional data management tools or processing applications. It is already true that Big Data has drawn huge attention from researchers in information sciences, policy and decision makers in governments and enterprises. As the speed of information growth exceeds, excessive data is making great troubles to human beings. However, there are so much potential and highly useful values hidden in the huge volume of data. A large number of fields and sectors, ranging from economic and business activities to public administration, from national security to scientific researches in many areas, involve with Big Data problems. On the one hand, Big Data is extremely valuable to produce productivity in businesses and evolutionary breakthroughs in scientific disciplines, which give us a lot of opportunities to make great progresses in many fields. There is no doubt that the future competitions in business productivity and technologies will surely converge into the Big Data explorations. On the other hand, Big Data also arises with many challenges, such as difficulties in data capture, data storage, and data analysis and data visualization. This paper is aimed to demonstrate a close-up view about Big Data, including Big Data applications, Big Data opportunities and challenges, as well as the state-of-the-art techniques and technologies we currently adopt to deal with the Big Data problems.

I. INTRODUCTION

Big data is a popular term used to describe the exponential growth and availability of data, both structured and unstructured. And big data may be as important to business – and society – as the Internet has become. Data that is so large in volume, so assorted in variety or moving with such velocity, that traditional modes of data capture and analysis are insufficient The declining cost of collection, storage, and processing of data, combined with new sources of data like sensors, cameras, geospatial and other observational technologies, means that we live in a world of near-ubiquitous data collection. The volume of data collected and processed is unparalleled. This explosion of data from web-enabled appliances, wearable technology, and advanced sensors to monitor everything from vital signs to energy use to a jogger's running speed will drive demand for high-performance computing and push the capabilities of even the most sophisticated data management technologies.[1]

There is not only more data, but it also comes from a wider variety of sources and some data is "born digital," meaning that it is created specifically for digital use by a computer or data processing system. Examples include email, web browsing, or GPS location. Other data is "born analog," meaning that it emanates from the physical world, but increasingly can be converted into digital format. Examples of analog data include voice or visual information captured by phones, cameras or video recorders, or physical activity data, such as heart rate or perspiration monitored by wearable devices. With the rising capabilities of "data fusion," which brings together disparate sources of data, big data can lead to some remarkable insights.[2]

II. WHAT ARE THE SOURCES OF BIG DATA?

The sources and formats of data continue to grow in variety and complexity. A partial list of sources includes the public web; social media; mobile applications; and local records and databases; commercial databases that aggregate individual data from a spectrum of commercial transactions and public records; geospatial data; surveys; and traditional offline documents scanned by optical character recognition into electronic form. The advent of the more Internet-enabled devices and sensors expands the capacity to collect data from physical entities, including sensors and radiofrequency identification (RFID) chips. Personal location data can come from GPS chips, cell-tower triangulation of mobile devices, mapping of wireless networks, Furthermore, data collection and analysis is being conducted at a velocity that is increasingly approaching real time, which means there is a growing potential for big data analytics to have an immediate effect on a person's surrounding environment or decisions being made about his or her life. Examples of high-velocity data include click-stream data that records users' online activities as they

interact with web pages, GPS data from mobile devices that tracks location in real time, and social media that is shared broadly.[3] Customers and companies are increasingly demanding that this data be analyzed to benefit them instantly, a mobile mapping application is essentially useless if it cannot immediately and accurately identify the phone's location, and real-time processing is critical in the computer systems that ensure the safe operation of our cars.[4]

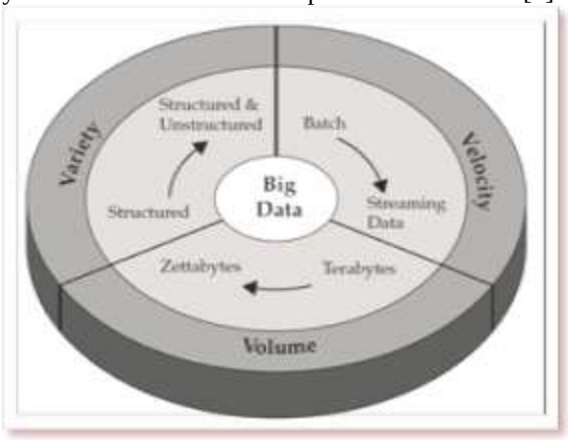


Figure: Big Data Image

III. OPPORTUNITIES AND CHALLENGES

Big data technologies can derive value from large datasets in ways that were previously impossible in fact, big data can generate insights that researchers didn't even think to seek. But the technical capabilities of big data have reached a level of complexity and popularity that demands consideration of how best to balance the opportunities afforded by big data against the social and ethical questions these technologies raise. Used well, big data analysis can boost economic productivity, Examples include:

- Big data and the growing "Internet of Things" have made it possible to merge the industrial and information economies. Jet engines and delivery trucks can now be outfitted with sensors that monitor hundreds of data points and send automatic alerts when maintenance is needed. This makes repairs smoother, reducing maintenance costs and increasing safety.
- The Centers for Medicare and Medicaid Services have begun using predictive analytics software to flag likely instances of reimbursement fraud before claims are paid. The Fraud Prevention System helps identify the highest risk health care providers for fraud, waste and abuse in real time, and has already stopped, prevented or identified.
- One big data study synthesized millions of data samples from monitors in a neonatal intensive care unit to determine which newborns were likely to contract potentially fatal infections. By analyzing all of the data not just what doctors noted on their rounds the project was able to identify factors, like increases in temperature and heart rate, that serve as early warning signs that an infection may be taking root. These early signs of infection are not something even an experienced and attentive doctor would catch through traditional practices.

Big data technology also holds tremendous promise for better managing demand across electricity grids, improving energy efficiency, boosting agricultural productivity in the developing world, and projecting the spread of infectious diseases, among other applications. Unstructured text documents, email, video, audio, stock ticker data and financial transactions, managing, merging and governing different varieties of data.[5,6]

IV. WHY BIG DATA SHOULD MATTER TO US

The real issue is not that we are acquiring large amounts of data. It's what we do with the data that counts. The hopeful vision is that organizations will be able to take data from any source, bind relevant data and analyze it to find answers that enable 1) cost reductions, 2) time reductions, 3) new product development and optimized offerings, and 4) smarter business decision making. For instance, by combining big data and high-powered analytics, it is possible to:

- Determine root causes of failures, issues and defects in near-real time, potentially saving billions of dollars annually.
- Optimize routes for many thousands of package delivery vehicles while they are on the road.
- Analyze millions of SKUs to determine prices that maximize profit and clear inventory.
- Generate retail coupons at the point of sale based on the customer's current and past purchases.
- Send tailored recommendations to mobile devices while customers are in the right area to take advantage of offers.
- Recalculate entire risk portfolios in minutes.
- Quickly identify customers who matter the most.
- Use click stream analysis and data mining to detect fraudulent behavior.

V. BIG DATA AND HEALTH CARE DELIVERY

Data has long been a part of health care delivery. In the past several years, legislation has created incentives for health care providers to transition to using electronic health records, vastly expanding the volume of health data available to clinicians, researchers, and patients. Big data can identify diet, exercise, preventive care, and other lifestyle factors that help keep people from having to seek care from a doctor. Big data analytics can also help identify clinical treatments, prescription drugs, and public health interventions that may not appear to be effective in smaller samples, across broad populations, or using traditional research methods. From a payment perspective, big data can be used to ensure professionals who treat patients have strong performance records and are reimbursed on the

quality of patient outcomes rather than the quantity of care delivered.

The emerging practice of predictive medicine is the ultimate application of big data in health. This powerful technology peers deeply into a person's health status and genetic information, allowing doctors to better predict whether individuals will develop a disease and how they might respond to specific therapies. Though medicine is changing, information about our health remains a very private part of our lives.

VI. BIG DATA AND EDUCATION

Students now access class materials, watch instructional videos, comment on class activities collaborate with each other, complete homework, and take tests online. Technology-based educational tools and platforms offer important new capabilities for students and teachers. After only a few generations of evolution, these tools provide real-time assessment so that material can be presented based on how quickly a student learns. Education technologies can also be scaled to reach broad audiences, enable continuous improvement of course content, and increase engagement among students. Beyond personalizing education, the availability of new types of data profoundly improves researchers' ability to learn about learning. Data from a student's experience in massive open online courses (MOOCs) or other technology-based learning platforms can be precisely tracked, opening the door to understanding how students move through a learning trajectory with greater fidelity, and at greater scale, than traditional education research is able to achieve. The big data revolution in education also raises serious questions about how best to protect student privacy as technology reaches further into the classroom.[7]

VII. PROTECTING CHILDREN'S PRIVACY IN THE ERA OF BIG DATA

Children today are among the first generation to grow up playing with digital devices even before they learn to read. Now a day's most of the children and teenagers are active users of mobile apps and social media platforms. As they use these technologies, granular data about them some of it sensitive is stored and processed online. This data has the potential to dramatically improve learning outcomes and open new opportunities for children, but could be used to build an invasive consumer profile of them once they become adults, or otherwise pose problems later in their lives. Although youth on average are typically no less, and in many cases more, cognizant of commercial and government use of data than adults, they often face scrutiny by parents, teachers, college admissions officers, military recruiters, and case workers.[8] Vulnerable youth, including foster children and homeless youth, who typically have little adult guidance, are also particularly susceptible to data misuse and identity theft. Struggling to find some privacy in the face of tremendous supervision, many youth experiment with various ways to obscure the meaning of what they share except to select others, even if they are unable to limit access to the content itself.

VIII. ANALYSIS OF BIG DATA

At the simplest level, advanced analytics allows us to develop models and then use them to ask what-if questions about your data. For example, developing a statistical model that associates buying behavior with customer profiles can then be applied to future behavior of customers. The application of that model is referred to as "scoring" and is the basis for predictive analytics.

That type of analysis is worlds away from traditional business intelligence, which is more about asking simple questions about data in one or two dimensions (e.g., how many clothes of Brand X do we have in stock?). That kind of analysis is fairly simple using a traditional database, needing only a small pipe to get the data in and out and a software component on the client to manage the interface.

Combining big data with predictive analytics can be a challenge for many industries, but high-performance analytics, which speeds the process of scoring and reporting, is helping customers in many areas like.

IX. DETECT, PREVENT AND REMEDIATE FINANCIAL FRAUD

Every day around the world, criminals are busily at work trying to defraud companies through a constantly evolving portfolio of schemes and strategies. As the volume and sophistication of these schemes increases, many organizations are turning to powerful analytics to sift through massive data volumes and uncover hidden patterns, trends and suspicious events that can indicate criminal fraud. In most instances, fraud detection involves analyzing the various attributes of transactions and making a determination about whether those orders should be flagged for further review.[9,10]

X. CALCULATE RISK ON A LARGE CROWD OF LOANS

In the past few years, it's been anything but smooth sailing for financial services firms that have struggled to effectively manage their extensive consumer home loan portfolios. An industry wide failure to properly assess the latent risks lurking in thousands of substandard loans led to billions of dollars of losses,

XI. EXECUTE HIGH-VALUE MARKETING CAMPAIGNS

The same financial services company faced similar big data challenges in its marketing operations as well. Financial services segments are increasingly competitive as institutions seek to offset the loss of fee income and minimize their own churn.[11]

CONCLUSION

We are living in the midst of a social, economic, and technological revolution. How we communicate, socialize, spend leisure time, and conduct business has moved onto the Internet. The Internet has in turn moved into our phones, into devices spreading around our homes and cities, and into the factories that power the industrial economy. The resulting explosion of data and discovery is changing our world. Big data technologies will be transformative in every sphere of life. The knowledge discovery they make possible raises considerable questions about how our framework for privacy protection applies in a big data ecosystem. Big data also raises other concerns. A significant finding of this report is that big data analytics have the potential to eclipse longstanding civil rights protections in how personal information is used in housing, credit, employment, health, education, and the marketplace.

REFRENCES

[1] Source: META Group. "3D Data Management: Controlling Data Volume, Velocity, and Variety." February 2001.

[2] http://quantumcomputers.com.

[3] http://www.gigaspaces.com

[4] C.L. Philip Chen ⇑, Chun-Yang Zhang Data-intensive applications, challenges, techniques and technologies: A survey on Big Data Department of Computer and Information Science, Faculty of Science and Technology, University of Macau, Macau, China

[5]Karmasphere Studio and Analyst, 2012. <http://www.karmasphere.com/>.

[6]Pentaho Business Analytics, 2012. <http://www.pentaho.com/explore/pentaho business-analytics/>.

[7] Laurila, Juha K., et al. The mobile data challenge: Big data for mobile computing research. Proceedings of the Workshop,10th International Conference on Pervasive Computing. 2012.

[8] F. Shull,"Getting an Intuition for Big Data," IEEE Software, vol. 30, no. 4, pp. 3-6, 2013.

[9] V. Marx, "The Big Challenges of Big Data," Nature, vol. 498, no. 7453, pp. 255-260, 2013.

[10] James Ahrens, Kristi Brislawn, Ken Martin, Berk Geveci, C. Charles Law, Michael Papka, Large-scale data visualization using parallel data streaming,

[11] Chris Anderson, The End of Theory: The Data Deluge Makes the Scientific Method Obsolete, 2008. <http://www.wired.com/science/discoveries/ magazine/16-07/pb-theory>.

● ● ●

Elimination of brake fade in vehicles by altering the brake disc size(A concept)

[1]Gowtham.S, Manas M Bhat
[1] Mechanical engineering PES Institute of Technology,
[1] Bangalore , India.
[1]gauthamgreat10@gmail.com

Abstract: **Brakes are one of the most important control components of the vehicle. They contribute very much in the movement of the vehicle. . Brakes are generally applied to rotating axles or wheels. The momentum or kinetic energy to stop the vehicle when in motion is converted to heat energy by the friction of brake pads and the rotors which is dissipated into the surrounding air. The main functions of brakes are mainly to stop the vehicle in shortest possible time and to help in controlling the speed of the vehicle. However, with long term use of brakes many problems occur which results in brake failure, leading to a fatal injury caused to the driver and co-passengers. One of the most important causes of brake failure are brake fades. Vehicle braking system fade, or brake fade, is the reduction in stopping power that can occur after repeated or sustained application of the brakes, especially in high load or high speed conditions. For elimination of brake fade, it is necessary for maximum temperature to be less than fade stop temperature. So, to have lesser temperature we alter the parameters dependent on it. Since, stopping time, density of material, specific heat capacity, thermal conductivity and ambient temperature are constants, it is possible to alter heat flux. . If the value of fade stop temperature is higher than maximum temperature , then fade doesn' t occur. So for a higher fade temperature, we should have the volume of disc minimum. Thus, in here we prove that fade stop temperature is higher than maximum temperature. So, theoretically proving fade is not possible. Advantages- Low-fade brakes such as disc brakes in steered wheels can do more braking without causing brake steer, Elimination of brake fading provides a larger leverage and mechanical advantage to resist the turning of the rotor itself and It also provides a longer life time for the braking system, thus reducing the maintenance cost of the vehicle.**

Index Terms: **brake disc, fade temperature, heat flux, maximum temperature of disc.**

I. INTRODUCTION

Brakes are one of the most important control components of the vehicle. They contribute very much in the movement of the vehicle. Most brakes commonly use friction between two surfaces pressed together to convert the kinetic energy of the moving object into heat, though other methods of energy conversion may be employed. Brakes are generally applied to rotating axles or wheels, but may also take other forms such as the surface of a moving fluid. [1]

In an automobile, if the pressure from the accelerator is removed, the vehicle tends to slow due to wind resistance, drag of engine and road friction. These forces of course would stop the vehicle, but in modern day traffic, this would be quite unpractical and dangerous. The braking system provides added friction, to overcome motion and to slow up or stop the vehicle. The momentum or kinetic energy to stop the vehicle when in motion is converted to heat energy by the friction of brake pads and the rotors which is dissipated into the surrounding air. The main functions of brakes are mainly to stop the vehicle in shortest possible time and to help in controlling the speed of the vehicle. It is also used to reduce the speed at turnings and other crowded places. [2] Thus making brakes an important control system of the car.

However, with long term use of brakes many problems may occur which results in brake failure, leading to a fatal injury caused to the driver and co-passengers. One of the most important causes of brake failure is brake fade. Vehicle braking system fade, or brake fade, is the reduction in stopping power that can occur after repeated or sustained application of the brakes, especially in high load or high speed conditions. [3] Brake fade occurs when the brake pad and the brake rotor no longer generate sufficient mutual friction to stop the vehicle at its preferred rate of deceleration and can happen on motorcycles cars and trucks. [4]

The brake pad in any brake system is designed to work at certain operating temperatures. Being made of many different formulations brake pads perform in very different ways under temperature. This certainly indicates the fitness of a brake pad for application and its general quality.

II. TERMINOLOGIES

Brake disc material- Most of industrial automobiles companies produced the brake rotor part from a grey cast iron. The cast iron material differs from standard steels by having significantly higher carbon (C) and silicon (Si) contents. So, for best reduction of fade, we can use grey cast iron or carbon ceramic materials. Since, the cost of carbon ceramic materials is too high we use grey cast iron. Also, modern automobile sector uses grey cast iron in their disc brakes.

Deceleration of vehicle- If the speed of the car decreases, this is an acceleration in the opposite direction of the direction of the vehicle, sometimes called deceleration.[5] It is given by, coefficient of friction * acceleration due to gravity(g).

Stopping distance- Stopping distance refers to the distance a vehicle will travel from the point when its brakes are fully applied to when it comes to a complete stop. It is given by, (velocity of vehicle)²/(2*coefficient of friction*g)

Stopping time- It is the time required for a vehicle to completely stop, when brakes are applied. It is given by, (stopping distance)/ (acceleration).

Average power (P) - It is the ratio of kinetic energy to stopping time.

It is given by, [kinetic energy (E])/ [stopping time (T)]

Heat flux (Q) - Heat flux or thermal flux is the rate of heat energy transfer through a given surface, per unit time. Heat flux density is the heat rate per unit area. In SI units, heat flux density is measured in [W/m²]. [6]

It is given by, [4*P*]/ [(D²-d²)]*3.14]

Where, ‘P’ is the Average power.

‘D’ is the outer diameter on the rotor disc.

‘d’ is the inner diameter on the rotor disc.

Maximum temperature- It is the maximum temperature experienced by the rotor disc when brakes are applied.

It is given by, {(0.527*Q*√T)/ [√ (density of the material* specific heat capacity*thermal conductivity)]} +T (amb)

Where, ‘Q’ is the heat flux

‘T’ is the stopping time

‘T (amb)’ is the ambient temperature. It is defined as the temperature of the surroundings.

Fade stop temperature rise- The reduction of friction termed brake fade is caused when the temperature reaches the "knee point" on the temperature-friction curve and gas builds up between disc and pad. This temperature is called as ‘fade temperature’.

It is given by, (P*T)/ (Density of material* specific heat capacity*volume of rotor disc.)

Where, ‘P’ is the average power.

‘T’ is the stopping time.

III. DESIGN FOR ELIMINATION of fade

For elimination of fade, it is necessary for maximum temperature to be less than fade stop temperature. So, to have less maximum temperature we alter the parameters dependent on it. Since, stopping time, density of material, specific heat capacity, thermal conductivity and ambient temperature is constant; it is possible to alter heat flux. Heat flux is dependent on average power and inner and outer diameter of the rotor disc. Since, average power is constant; we should have a rotor disc of minimal value for a lesser maximum temperature. Also, ensuring that maximum temperature is not too minimum, otherwise resulting in fatal injury of the passengers. If the value of fade stop temperature is higher than maximum temperature, then fade doesn’t occur. So for a higher fade temperature, we should have the volume of disc minimum, since other quantities like average power, stopping time, density of material and specific heat capacity are constants.

IV. CALCULATIONS

Mass of vehicle – 250kg.
Coefficient of friction – 0.75
Outer diameter of brake disc- 200mm
Inner diameter of brake disc- 90mm
Speed of vehicle (V) - 50km/hr (13.89m/s)
Volume of brake disc-125663.70mm³
Density of brake disc material- 7250(kg/m³)-grey cast iron
Specific heat capacity of grey cast iron – 0.5 (kJ/kg/k)
Thermal conductivity of grey cast iron – 54(W/m K)
Ambient temperature- 22° Celsius.
Acceleration due to gravity- 9.81(m/s).

Deceleration of vehicle-

=coefficient of friction * acceleration due to gravity (g)

=0.75*9.81

=7.35(m/s²)

Stopping distance-

= (velocity of vehicle) ²/ (2*coefficient of friction*g)

= (13.89)²/ (2*0.75*9.81)

=13.125m.

Kinetic energy of the vehicle-

=.5*m*V²

=.5*250*13.89²

=24.116KJ.

Stopping time-

= (stopping distance)/ (acceleration)

=13.125/7.35

=1.89 seconds.

Average power-

= [kinetic energy (E])/ [stopping time (T)]

=24116.51/1.89

=12760.05W.

Heat flux-

= [4*P*]/ [(D^2-d^2)]*3.14]

= [4*12760.05]/ [(.2^2-.09^2)*3.14]

=509500(W/m^2)

Maximum temperature-

= {(0.527*Q*√T)/ [√ (density of the material* specific heat capacity*thermal conductivity)]} +T (amb)

= {(.527*509500*1.38)/[7250*500*54]}+22

=48.48° Celsius.

Fade stop temperature rise-

= (P*T)/ (Density of material* specific heat capacity*volume of rotor disc.)

= (12760.05*1.89)/ (7250*500*0.000125)

= 53.22° Celsius.

Thus, in here we see that fade stop temperature is higher than maximum temperature. So, theoretically proving fade is not possible.

V. ADVANTAGES

Low-fade brakes such as disc brakes in steered wheels can do more braking without causing brake steer. [7]

Elimination of brake fading provides a larger leverage and mechanical advantage to resist the turning of the rotor itself.

It also provides a longer life time for the braking system, thus reducing the maintenance cost of the vehicle.

It also helps in ensuring that the brake pads have a sustained and longer life time.

CONCLUSION

In this research paper, we have discussed the various terminologies involved in the braking system and their relation with respect to brake fade. We have also seen their dependence on temperature and heat flux. We also proved theoretically the elimination of brake fade in vehicles. Thus, ensuring that vehicles can experience a longer and sustained braking system.

REFERENCES

[1] *Nice, Karim (2000-08-22).* "How Power Brakes Work". *Howstuffworks.com*. Retrieved 2011-03-12.S

[2] A Text Book of Automobile Engineering by R K.Rajput Spartan Engineering 1959;

[3] Disk Brake, accessed 2007-02-26

[4] Spicer Trailer Axles & Brakes; Application Guide AXAG-0300 March 2006; See "Brake Fade" in glossary; accessed 2007-02-26

[5] Raymond A. Serway, Chris Vuille, Jerry S. Faughn (2008). College Physics, Volume 10. Cengage. p. 32. ISBN 9780495386933.

[6] The NIST Reference on Constants, Units, and Uncertainty

[7] Gary Ganaway, Air Disc Brake Production, Use & Performance, NDIA Tactical Wheeled Vehicles Conference, Monterey California, 28 January 2002. Accessed 2010/01.