jims
Sector-5,Rohini,Delhi
(IP Department)

INSIGHT

TECHBYTE 2020

HIGH TECH COMPUTATING

ARTICLES

- Green Computing
- Security issue in Cloud Computing
- 5G Wireless technologies
- Performance in Blockchain Implementation
- Smart Eye Technology
- Vehicle monitoring and security surveillance
- Virtual surgery
- Web mining
- Data Breaches and its prevention
- Wireless integrated network sensors

TECHBYTE 2020

17th Annual IT Symposium

"High Performance Computing"

Department of Information Technology

Jagan Institute of Management Studies,
Sector-5 Rohini,
New Delhi-110085

CHAIRMAN
Mr. Manish Gupta

DIRECTOR
Dr. Pooja Jain

PATRON
Dr. Praveen Arora
Dean, IPU-Affiliated Programmes

CONVENERS
Dr. Manjot Kaur Bhatia
Dr. Chetna Laroiya

EDITOR
Dr. Chetna Laoriya

STUDENT EDITORS
Mr. Manav Bansal (MCA – 2nd Year)
Ms. Varsha Saxena (MCA – 2nd Year)
Mr. Deepanshu Solanki (MCA – 2nd Year)

DATE
Saturday, 7th November 2020

VENUE
Online Mode
(ZOOM)

Editor's Desk

Wisdom is not the product of schooling but is sum of all the learning attempt to acquire it. To attain knowledge, we try to add something every day to our knowledge pool.

Today's world is booming with exciting and innovative technologies and new learning challenges. We at JIMS encourage students to move beyond curriculum in order to meet industry expectations through workshops on latest technologies. Learning new skills is a life-long gig now.

Though INSIGHT we try to accumulate articles from students on various technological corners touched in our Annual IT Symposium TECHBYTE 2020.

We would like to manifest our gratefulness to the management of JIMS and faculty members for their incredible endowment.

Dedicated effort of our students is much appreciated.

Editorial Team

CHAIRMAN'S MESSAGE

JIMS has been working to develop highly skilled and professional human resource for industry and business. We have created a niche in 26 years in the fields of Management and Information Technology.

We had started JIMS, keeping some of the leading institutions as our benchmarks but today we take this pride to be a benchmark for other institutions to follow. We have evolved and developed extensive modern teaching methodologies that transform ideological thinking to practical thinking and lead to ideas that are out of the box which trigger creativity. Our students explore ample opportunities of learning with us which prepares them to face the industry challenges and meet corporate expectations.

We understand that both information technology as well as management education are ever-changing and ever-evolving. On these lines we focus and frequently interact with the industry to understand our employer expectations. This has enabled repeated arrival of companies for campus recruitments year after year. The feedback received from the industry is regularly incorporated to update and upgrade our academic deliverables which has made our students highly competent. Moreover, our rich alumni base has also proved our 26 years of fruitful interactive existence. Our Alumni are present in all parts of the world and have earned reputation for them and as well as for the institute. The content of Information technology courses is designed and revised to meet up with the demands of qualified professionals in the IT Industry by including latest technologies and concepts.

Our determination, conviction and perseverance have helped us to keep our roots intact. On the completion of our 26th year of academic excellence, we renew our commitment to uplift the standards of education and we welcome all the students to join JIMS with high spirits, right focus and vision to excel. We look forward to serve the society in our endeavour of imparting quality education.

Manish Gupta

DIRECTOR'S MESSAGE

One thing that's remarkable about today's business environment is the sheer number of technologies that exist and the number of directions an enterprise can take. It's not a question of whether a business will adopt various emerging technologies, it's how, when, where, and in what combination will they adopt technologies to gain competitive advantage in the Industry.

Technology stands still for no one. Undoubtedly, it is our educational institutions, which are the source of most scientific advances, scholarly discoveries, creative processes and innovations.

High Performance Computing helps solve people's most complex glitches. As an Educational Institution, we adapt to prepare students learn the latest technologies including advanced robotics, artificial intelligence, cloud computing; the Internet of Things; data analytics; and so on.

The high-performance computing is marked by a strong dynamic with a continuous appearing and disappearing of manufacturers, systems, and architectures. Different applications of high-performance computing will emerge, not only in science and engineering, but also in commerce.

I wish the entire team of Tech byte 2020 best of luck for undertaking such initiative and create a knowledge enhancing platform for students on the emerging technologies.

Dr. Pooja Jain

CONTENTS

DISCLAIMER

Great care has been taken in the compilation of information and every effort has been made to ensure that all Information is up-to-date at the time of going to press. The responsibility of the authenticity of articles lies with student writers. The institute or the editorial team is not responsible for error, if any, and their consequences.

BLOCKCHAIN IMPLEMENTATION

Faculty Mentor:
Dr. C Komalavalli

Student Authors:
Varun Mangla (MCA-2nd Year)
Paramjeet Singh (MCA-2nd Year)

1. INTRODUCTION

Blockchain is an emerging technology was invented by Satoshi Nakamoto in 2008. It was first emerged as a platform to provide a tamper-proof and transparent way of exchange of cryptocurrencies without the involvement of any intermediaries. Blockchain is the technology behind the Bitcoin.

But what actually Blockchain is? In short, Blockchain is a technology which is used to make **decentralized applications**. Blockchain is a decentralized, distributed ledger technology of chain of records, called as Blocks, which are linked cryptographically. This technology was introduced in late 90s but gained attention since Bitcoin was introduced as Cryptocurrency.

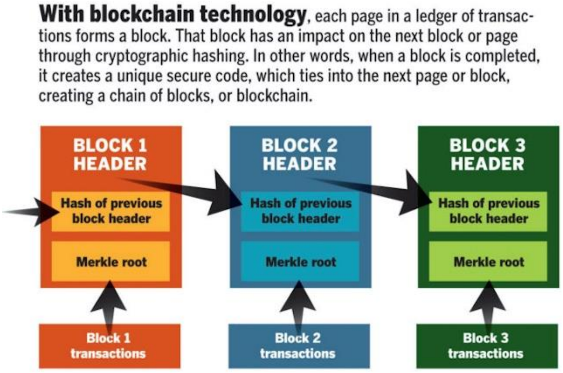
2. WHAT ARE CENTRALIZED AND DECENTRALIZED SYSTEMS?

There are many technologies, machines, industries that used to rely on centralized system. That means all of the confidential data is stored under one system only. That particular system has all the authority of the data. This led to the security concerns of the confidential data. Moreover, if that system crashes, whole of the data would be lost. The operators of that system have access to the whole data. We all are dependent on that central authority only.

Decentralized System means **networked system**. No single node is given the full authority. None of the node is given more privileges than the other. Each node has same authority and changes made to blockchain data needs to be validated by each of the block (node).

3. ROLE OF BLOCKCHAIN ON DECENTRALIZED SYSTEM

Here comes the role of Blockchain which implements Decentralized System i.e., it implements peer-to-peer network. It is a chain of many blocks where each block can be divided into 3 parts:
First is the **Hash**. It is the unique identifier. Same data has same Hash and it connects one
block to its next block. Hash is like a fingerprint of a block. Each block has different hash. It helps us to detect the changes made to the data of the particular block.



With blockchain technology, each page in a ledger of transactions forms a block. That block has an impact on the next block or page through cryptographic hashing. In other words, when a block is completed, it creates a unique secure code, which ties into the next page or block, creating a chain of blocks, or blockchain.

Fig 1: Blockchain Blocks

Second is the **Data**, which can be in any form. For ex. In Bitcoins, the Transactions are referred to as Data. By Transactions we mean the name of sender, receiver and amount of coins sent.

Third is the **Previous Block Hash**. As its name suggests, it stores the unique code for its previously connected block in the chain. These 3 components make up the Blockchain.

4. SECURITY IMPLEMENTATION WITH BLOCKCHAIN

Security Phase 1

Let me explain Blockchain security through an example.

Let's say we are on Block X. Since each data has its Hash code, so if we try to change one data block (Block X), then its Hash code will automatically be changed (since Hash and Data are interconnected). Now since Block X is connected to Block X + 1, we would need to change the Previous Hash of Block X + 1, which in turn changes the data of Block X + 1.

Again, this will change the Hash of this block and it would require us to change the Previous Hash of Block X + 2 (because X + 1 is connected to X + 2). And this chain will keep on going like this which makes it impossible to change all the data. It makes the data immutable because once the data is recorded into a block, it cannot be changed without changing all of the following blocks in the blockchain.

Whenever a new block is added to the network Blockchain, all the involving systems need to validate that particular block's data. We keep that data in Blockchain which we want to prevent from any alterations.

Security Phase 2

Hashing alone is not capable of preventing the changes in blockchain. We have very efficient computer systems now a days that if we change 1 Hash then the system is able to generate new hundreds or thousands of new Hashes per second. To overcome this problem, we have **Proof-of-work algorithm.** In this mechanism, it slows down the process of creating new blocks or new hashes. In this algorithm, the prover or changer appeals to the verifiers that I want to change or add this new block in the chain. The verifiers take some time in doing computations. This prevents the sudden changes in the blockchain.

For ex. In bitcoins, it takes about 10 minutes to calculate the new proof-of-work and add a new block to the chain. So, if we add 1 new block, it would take 10 mins to recalculate the proof-of-work of its next block X, 10 mins again for block X + 1, and so on, which makes it harder to do changes in the following blockchain.

Security Phase 3

To provide more security, no single entity is given the ownership to manage the chain. It uses distributed peer-to-peer network and anyone is allowed to join. Each node is given the full copy of blockchain. Each node can check whether the blockchain is in order or not.

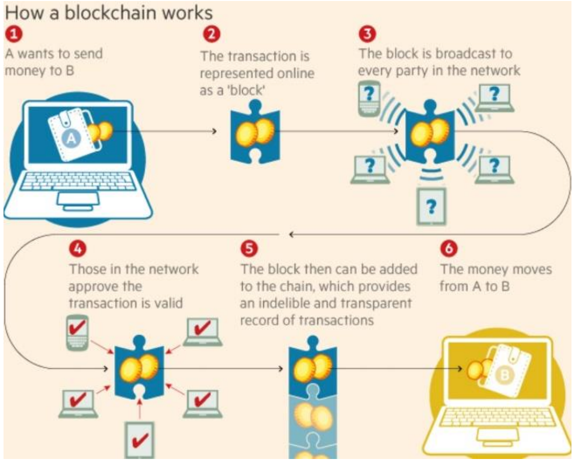

How a blockchain works
1
A wants to send money to B
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
?
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent record of transactions
6
The money moves from A to B
A
B

Fig 2: An example Transaction through Blockchain

If we want to add a new block to the chain, then that block is passed to each of the peer-to-peer node in the network and they verify it whether that particular block is harming the blockchain or not. When that block passes this test, this block is added to each nodes's blockchain. Now if someone want to mislead the blockchain by adding some malicious block, they need to tamper with all the blocks in blockchain and recalculate the proof-of-work for each block again and take control of more than 50% nodes of the network. Once this is done, the malicious block could be added to the blockchain and of course, this is not an easy task to breach all the phases of the chain so easily.

5. BLOCKCHAIN APPLICATION

- **Cryptocurrency:** Most prominent example of this is Bitcoin.
- **Health Care:** For example: Recently in COVID-19 pandemic, blockchain was created to keep a track of the people who were tested with antibody and could be immune to COVID-19.
- **Energy Trading:** Peer-to-peer Energy trading is also done using the basis of Blockchain.
- **Video Games:** A game was launched in November 2017 named CrypoKitties which was based on blockchain. Its character Cryptokitty (a virtual pet) was sold for more than 100,000 US dollars. This game cited the example that how blockchain can be used as a digital asset.

6. BITCOIN INTRODUCTION

Bitcoin is a cryptocurrency, digital currency, or electronic money that is used to transact the amount (Digital currency) from one person to another. Bitcoin was created in 2009 by an unknown group of a developer using the alias "Satoshi Nakamoto". Bitcoin is a peer to peer decentralized Electronic payment system, which means without a central bank or single administrator or there is no middle organization or company keep the log of the transactions. It's also the most widespread and well-substantiated out of all the digital currencies. Bitcoin coin is more secure because it uses an algorithm called SHA256 (Secure Hashing Algorithm) which is nearly impossible to crack.

7. BITCOIN BLOCKCHAIN IMPLEMENTATION

Blockchain can be labelled as the backbone of all crypto-currency system. Blockchain technology not only helps the users with performing transactions using crypto-currencies but also ensures the security and anonymity of the users involved. It is a list of records called blocks, which are linked and secured using cryptographic techniques. A Blockchain can be used as "an open and distributed ledger, that can record transactions between both parties in a confirmable and imperishable way." The ledger that is shared among everyone in the network is public for all to look at. This brings in transparency and trust in the system.

A block is the 'present' part of a Blockchain that stores some or all of the recent transactions, and once finished goes into the blockchain as an imperishable database. Every time a block gets Finished, a new block is set up.

Once recorded, the data in any given block cannot be altered or modified. Transactions once stored in the Blockchain are imperishable. They cannot be hacked or altered.

8. BITCOIN'S BLOCK STRUCTURE

In the Bitcoin network, every block has the same format. All freshly-created block is 'chained' to the previously added block of the blockchain and hoards its digital fingerprint.

- **Magic number:** This is an identifier for the Blockchain network. It has a fixed value of 0xD9B4BEF9. The size of the magic number is 4 bytes**.** It indicates a) Start of block b) Data is from the production network.
- **Block size**: It is of 4 bytes and it specifies the size of the block. each block is fixed to 1 MB. However, a proposal might soon have the consensus of the core development team and this will be expanded to 2 MB. The maximum size is 2

GB so the scalability factor has already been taken care of.

- **Version:** It is of 4 bytes each node running the Bitcoin protocol has to implement the same version and it is mentioned in this field.
- **Previous hash block:** It is a digital fingerprint (hash) of the block header of the previously added block of the blockchain. Its size is 32 bytes. It is obtained by taking all the fields of the header together and applying a cryptographic function (secure hash algorithm) twice by rearranging the bytes of the particular fields.
- **Merkle Root:** It is the hash of all the hashes of all the transactions that are part of a block in a Blockchain network. Its size is 32 bytes.
- **Timestamp:** The actual time the block was produced. Its size is 4 bytes.
- **Difficulty Target:** Bitcoin's difficulty target is a 256-bit number. Difficulty target implies that they are tough to mine. Its size is 4 bytes.
- **Nonce:** The nonce is a random, one-time, whole number. Its size is 4 bytes
- **Transaction Counter:** It is a variable of size 1-9 bytes and it counts all the transactions that are stored within the block.
- **Transaction List:** It is a Variable with a total block size of 1 MB and it Stores the digital finger-print of all the transactions in that block. Every individual transaction has a particular structure.

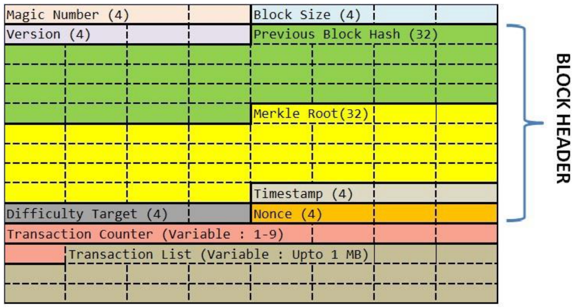
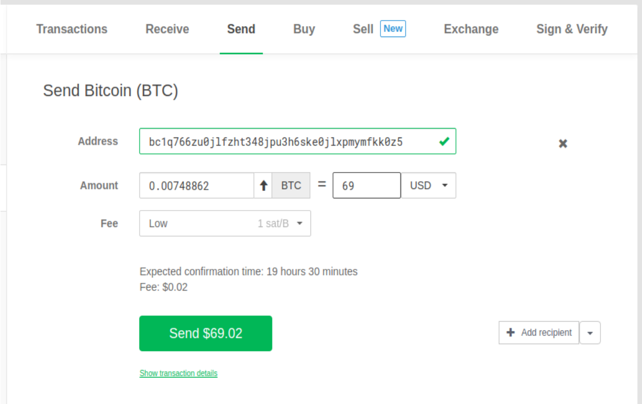


Fig 3: Block Header

9. BITCOIN TRANSACTION

For commencing a Bitcoin transaction between two parties you need to have a Bitcoin wallet and then you're equipped to send Bitcoin anywhere in minutes. In the above diagram, we are using the Trezor hardware wallet. The bitcoin wallet helps us to connect with a network. To send a bitcoin from one party to another party you must have the wallet address of the receiver party. A Bitcoin address consists of inconstantly generated numbers, upper case alphabets, and lower-case alphabets. Bitcoin addresses are between 26 and 35 alphanumeric characters long depending upon the type of address. After entering the wallet address of the receiver, you can now enter the number of bitcoins you want to send and now you have to select how quickly you want to send the bitcoins and then finally click on the send button. After clicking the send button, the transaction is broadcast to other computers on the network, who validate it independently. It is then added to a long list of transactions known as the Blockchain, showing that your Bitcoins now exist in the recipient's wallet.

In the second scenario, if you want to receive Bitcoin, you just need to give your wallet address to the sender so that the sender can send Bitcoin to your wallet. The Wallet can generate as many addresses as you want with no extra cost so no-one can link which payments were made to the same person. It is highly endorsed to use a fresh address for each transaction, for greater anonymity.



Send Bitcoin (BTC)

Address bc1q766zu0jlfzht348jpu3h6ske0jlxpmymfkk0z5 ✓

Amount 0.00748862 BTC = 69 USD

Fee Low 1 sat/B

Expected confirmation time: 19 hours 30 minutes
Fee: $0.02

Fig 4: An example Transaction of Cryptocurrency

10. CONCLUSION

A lot has been emerged and implemented with respect to the Blockchain. While Blockchain is still evolving, lot of applications are emerging using this technology in near future. Today’s digital world concerns data integrity and data security and this can be achieved successfully with Blockchain. The technology can replace the traditional trading system by providing immutable, transparent and distributed system.

11. REFERENCES

[1] https://www.computerworld.com/article/3191077/what-is-blockchain-the-complete-guide.html

[2] http://en.wikipedia.org/wiki/Blockchain

[3] https://www.coindesk.com/

[4] https://en.wikipedia.org/wiki/Payment_system

[5] https://files.stlouisfed.org/files/htdocs/publications/review/2018/01/10/a-short-introduction-to-the-world-of-cryptocurrencies.pdf

WEB MINING: AN OVERVIEW

Faculty Mentor:
Dr. Praveen Kumar Gupta

Student Author:
Keshav Vats (MCA-2nd Year)

1. INTRODUCTION

Web Mining is a part of Data Mining. It is a process to extract information from the internet or World Wide Web which includes page contents, hyperlinks and usage data by using Data Mining techniques. The aim of Web mining is to recognise patterns in the Web data to collect, cleaning of data, analyse, marketing and then decision making according the analyzation of the data.

2. TYPES OF WEB MINING

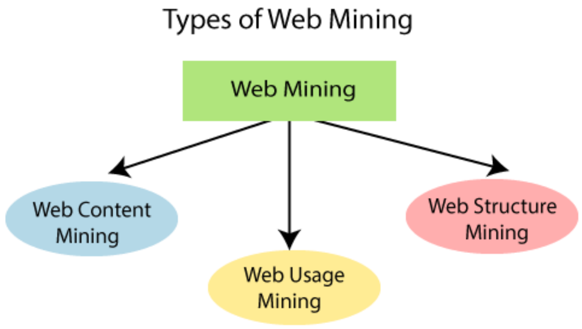


Fig 1: Types of Web Mining

a. **Web Content Mining** – It is an application which is used to extract data and information from the content of web Documents and Web pages. This content can be of many types like audio files, video files, images and text etc. In web content mining the techniques are used from (NLP) natural language processing and the retrieval of information.

b. **Web Structure Mining** – In the web structure mining, Graph theory is used to analyse the connection structure and the nodes. It is a process in which two thing that can be acquire by using this are: the document structure of the website and the structure of the connection of the website and how it is connected to the other websites.

c. **Web Usage Mining** – Web Usage Mining is the process to pull out or extract information, details and patterns from the server logs. This type of web mining is used in social media analytics. Data like how many users are on the website, how many clicks, like and comments are on the website, what are the hours in which there is most traffic on the website and what are the activities being done on the website.

3. HOW THE DATA IS COLLECTED?

In Data Mining the data is collected in many ways. Data can be collected through the server logs, web pages, web documents, connection structure and nodes. And big companies collect data from social media to expand their reach to targeted customers. Social media data refers to all the data collected from different sources and different software. This data helps organization to make changes according to the customers. The main motive to collect data is to give services to customers according their needs.

4. CHALLENGES IN WEB MINING

a. **Size of the web** – Vastness of the web is too huge for data mining and data warehousing. And it's still increasing in a tremendous pace which is almost impossible to keep track**.**

b. **Quality of the Data** – Small portion of data is needed for the analyses and the rest of the data is not relevant. The relevancy of the data is very big challenge in web mining**.**

c. **Source is Dynamic** – Internet is a Dynamic Data Source. The data on the web is rapidly updated so the data can show different results in just a little difference of time.

d. **Complications of the web pages** – Web pages don't have unifying type of the structure. The complexity is too high as compared to the text document. And there are high number of documents on the web and the libraries on the web and these are not sorted in any particular way.

e. **Diversity-** The people on the web are highly diverse. They all have different purposes and different backgrounds. There are hundreds of million workstation which are connected and these are still growing rapidly. That make Data mining Difficult to perform.

5. SOFTWARE USED IN WEB MINING

a) Megaputer PolyAnalyst

It is an analytical system which is used for web mining. But is not designed for the process of web mining particularly. It performs data mining and text mining with the web mining. As Data source nodes, websites can be inputted directly in this analytical system. It has multiple functionalities such as keyword extraction, prediction analyses, pattern discovery, categorization, entity extraction, link analysis and clustering. For performing web mining analyses these different types of functional nodes can be connected to web data source nodes directly. PolyAnalyst can load and integrate data from whatever data sources are used. It can load data from very different types and quality of data sources including spreadsheet systems, statistical systems and major databases.

Fig 2: Megaputer's Logo

b) ClickTracks by Web Analytics

It is a software which is used to perform web mining that makes online behaviour visible. This Software shows the information in context to the user. This software can show that where the visitor clicked and where he goes .it makes it easier to see that what motivates the visitor to take the path they take. By showing these calculations, the site owner can take decision very easily to how to design their website to make the most out of it. Click Tracks can show the movements of how the visitor go through their website and problems they face. You can see what attracts the visitor and what is ignored, the time spend by the visitor and the exit rate.

Fig 3: Click Tracks Logo

c) SPSS Clementine

This software has multiple Data mining capabilities such as propensity modelling, segmentation, affinity analysis and sequence detection. It has number of application modules which are used in web analysis that are activity sequence analysis, search engine optimisation, website activity and user behaviour, propensity analysis, automated user and visit segmentation etc. it can transform simple web data to actionable insights from which the business owner can take decisions very freely and effectively in real time. It can be very beneficial in terms of growth of the company or an organisation. It can also perform prediction analysis from which the business owner can have multiple perspective to a problem.

6. CASE STUDIES

a) **BARCLAYS:** BARCLAY'S launched an application of mobile banking called PingIt. In the following days the launch, Company made notable changes with the help of real-time social media analysis to the application. The sentiment analysis provides that while the app was very well received, a small sector of feedback was negative. It was clearly visible that many users were not happy that the app didn’t work for the age group of under 18’s. It wasn’t only teenagers that were not satisfied, but also guardian's that couldn’t send money to them. This could easily become a PR disaster, but the data information allowed Barclays to act rapidly. Within the week, access was given to the teenagers of the app, showing that Barclays were responsive to the feedback of the customers.

Fig 4: The Pingit Application Logo

b) **ROXY THEATRE:** In West Hollywood ROXY THEATER, located in California where Bruce Springstein, The Clash and Bob Marley, among others, had performed. They software that was used is TweetReach to calculate the number of people and their tweet reach and the quality of the tweets and number of tweets. They also used Klout, which allowed them to compare their efforts to similar businesses. They used the numbers in a TweetReach report to demonstrate to a talent buyer that they could reach a larger potential audience through Twitter so they could stop advertising in certain local publications. AOL City’s Best just named The Roxy as the best live music venue in Los Angeles. They just passed 100,000 Facebook followers and have nearly 50,000 Twitter followers.

Fig 5: The Roxy Theatre Logo

7. CONCLUSION

As the internet presence grows, the amount of data provided by the web will also grow rapidly. The demand and need of web mining are definitely skyrocketed in past few years. It became almost necessary for the websites and online businesses to analyse the data and take action according to the results or prediction. In this article we saw an overview of web mining, categories of web mining, challenges that occurs while performing web mining, how the data is collected, software used in web mining and the related case studies. Now we know Web Mining can save a business and can be very useful to grow their business also.

In this article we saw what are the different functionalities of these web mining software's, like propensity modelling, pattern analysis and discovery, keyword analysis etc.

8. REFERENCES

[1] J. W. Liang, *Introduction to text and web mining*, Seminar at North Carolina Technical University (2003), www.database.cis.nctu.edu.tw/seminars/2003F/TWM/ slides/p.ppt.

[2] Qingyu Zhang∗ and Richard S. Segall, *Web Mining: A Survey of Current Research*, techniques and softwares, Arkansas State University.

[3] *Automatic Tuning of Oracle SGA Parameters – An Overview* , Tecnia Journal of management studies, ISSN 0975-7104 ,TIAS INDIA(2009)

[4] *An Investigate Analysis of Challenges Related to Grid Computing*, The Journal of Computer Science and Information Technology (JCSIT), 0973- 4872, ITM Gurgaon(2007)

[5] *A comparative analysis of temporal data models*, international Journal of advanced Computational engineering and networking, ISSN 2320-2106, IRJ, India (2013) http://ijacen.iraj.in/paper_detail.php?paper_id=88&name=A_Comparative_Analysis_Of_Temporal_Data_Models

[6] *Optimisation of power consumption in VLSI circuit*, IOSR journal of Electrical and Electronics Engineering (double blind peer reviewed), e-ISSN 2278-1676, IOSR India (2014) http://www.iosrjournals.org/iosr-jeee/Papers/Vol9-issue2/Version-3/J09236266.pdf

[7] *Framework for handling uncertainty through temporal databases*, International Journal of Electrical, Electronics and Computer Engineering, e-ISSN 2277-2626, Research TrendIndia(2015)https://www.researchtrend.net/ijeece/ijet21/ijetnew/3%20PRAVEEN%20KUMAR%20GUPTA.pdf

[8] *Temporal fuzzy functional dependencies in temporal databases*, Fuzzy Information and Engineering, ISSN 1616-8658, Elsevier (TnF) Germany, (2017)

[9] *MASTER DATA MANAGEMENT EMERGING ISSUES*, INTERTNATIONAL JOURNAL OF ENGG TECHNOLOGY SCIENCE AND RESEARCH, ISSN2394-3386, IJETSR India (2017)http://www.ijetsr.com/images/short_pdf/1498834486_ieted767.pdf

GREEN COMPUTING

Faculty Mentor:
Ms. Aakanksha Chopra

Student Authors:
Neha Goel (MCA-2nd Year)
Shitij Narang (MCA-2nd Year)

ABSTRACT

Green computing is the study or practice of designing and manufacturing using dispose of computer devices which will create no or minimum impact on our environment. It is an approach to protect our environment from the harmful material and its effects that comes from the computers and related devices. In this research paper we are concerned about the Green computing, need of green computing, and steps towards Green computing by people throughout the world. We all know that computer is the basic need of humans in today's world, but we must be aware of the harmful impacts of computer on the world, it's manufacturing, disposal, and what steps we should take to reduce the harmful impacts to save our environment.

1. INTRODUCTION

In the last few decades, there has been an increase in the greenhouse gasses due to deforestation, burning of fossil fuels and rapid industrialization. This has lead to change in temperature of the air, the ocean and weather in the world. The rise in temperature has led to the increase in sea levels. Over a period of time the rise in the use of computers had also increased enormously. The combined effect of the energy needed to run all these devices and the electricity required for these devices have a huge impact on the environment. This has resulted in the research in the field of Green Computing which is about using computer in an environment friendly way.

Fig 1: Existence of Green Computing

2. WHAT IS GREEN COMPUTING

Green computing is all about designing, manufacturing, using and disposing of computers and its resources efficient, effective and sustainable manner with minimal or no impact on environment. The goals of green computing are power management and energy efficiency, usage of eco-friendly hardware and efficient software and material recycling and increasing the product's life. Information and communication technologies (ICT) has helped green computing in becoming an effective and efficient approach to grow segments that affect carbon emissions.

Fig 2: Environment friendly computing

3. HISTORY OF GREEN COMPUTING

The term "Green computing" came into existence with the launch of Energy Star program in 1992 by the EPA of United States. Computers and other electronics products are awarded by a kind of label that is Energy Star . The first step towards green computing was the introduction of sleep mode function which places a computer on standby mode to a preset period of time.

4. NEED OF GREEN COMPUTING

The basic need of every human is computer nowadays. But there are harmful impacts of the use of computers on the environment which humans are unaware of.

Large amount of CO2 is produced by computer related terms like PC & its peripherals and Network & networking. Only from PC's large amount of CO2 is produced. PC's are harmful for environment because they are not biodegradable and the parts and pieces will be around forever and are very less recyclable. Due to the defects in manufacturing techniques, disposal of computers, components, packaging our environment could be polluted. In the manufacturing of computers toxic chemicals are used and they put harmful impacts on our environment when we use informal disposing. Various reasons are there for the use of green computing and reduce the impacts:

(1) Harmful impact is created on our environment by computers and an electronic device that consumes a lot of Electricity; Air pollution, Land pollution and Water pollution are also produced by these impacts. Air pollution is released by Fossil Fuel power plants and electricity is generated through them.

(2) Emission of CO2 is also caused by most of electronic devices. Warming of the earth's surface to higher temperature by reducing outward radiation is also caused by CO2 which is one of the green house gases.

(3) When computers and its resources are disposed they really damage our environment and a lot of hazardous waste is produced. Heavy metal like mercury (Hg), cadmium (Cd), lead (Pv), are also being releases into the air.

(4) On the use of toxic chemical for electrical insulation, soldering, and fire protection is released by the manufacturing of computers product. Cancer, cause miscarriages can also be caused by expose of comical fumes over the long term.

5. PROS OF GREEN COMPUTING

(1) Green computing can save energy

(2) Reduction of the resource depletion problem

(3) Less pollution

(4) Less greenhouse gas emissions

6. CONS OF GREEN COMPUTING

(1) Significant upfront costs

(2) Plenty of knowledge may be required

(3) Maintenance may be difficult

(4) Lack of awareness among general public

7. ACTIONS FOR GREEN COMPUTING

We have to do some efforts to make environment healthy. The following actions should be taken by us:

(1) *Usage of Energy Star labeled products*: All the energy star labeled products are made keeping in mind the concept of green computing. These products not consume much power and hence they save energy. So

we can use “Energy Star” labeled desktops, monitors, laptops, printers and other computing devices.

(2) *Turn off your computer*: - As stated above, the PC’s and its peripherals consume more power and resultant is the high amount of CO2 emission. So we have to keep it in our mind and never hesitate to turn off our personal computers when they are not in use.

(3) *Sleep Mode*: - Allowing the monitor to fall asleep after idling for some time Period is another easily employed method for improving energy efficiency. It saves 60-70 percent of electricity. The monitor screen will be blank, with no light emitting from it.

8. LATEST TREND IN GREEN COMPUTING

Recycling of computer equipments, reducing the usage of paper, cloud computing and power management are the key initiatives towards Green computing. It is a big challenge to make people understand the importance of green computing and the harmful impacts of computer equipments on environment.

9. CONCLUSION

This research paper shows the importance of Green computing. If we will not take any measure, we will suffer from air pollution, water pollution, soil pollution etc. So with a little sense of understanding the importance and need of Green computing we should take the necessary steps from now onwards.

10. REFERENCES

[1] www.wikipedia.com

[2] http://energystar.gov/

[3] http://www.greencomputing.co.in/

[4] www.youtube.com

[5] www.google.co.in/green_computing_images

VEHICLE MONITORING AND SECURITY SYSTEM

Faculty Mentor:
Dr. Deepti Sharma

Student Authors:
Shivam Bansiwal (MCA-2nd Year)
Sonali Jain (MCA-2nd Year)

1. INTRODUCTION

In India around 1200 road crashes occurs daily and around 40,000 cars have been reported stolen previous year. These numbers could have gone a lot more than they are now but to prevent these accidents and theft Vehicle Monitoring and Security System (VMSS) are used in cars. Tracers has been placed in cars around 1980's which didn't gained popularity until 2000's. As the number of cars increased on the road, number of crashes and theft's increased too, so more advanced vehicle monitoring and security systems were introduced. The technologies that are used in monitoring and security purpose are GPS stands for Global Positioning System and GSM stands for Global System for Mobile Communication.

2. VEHICLE MONITORING AND SECURITY SYSTEM

Vehicle Monitoring and Security System is a GPS based vehicle monitoring system which is used for security. Basically, VMSS uses two main concepts GPS and GMS. The main function of the system is tracking the vehicle by GPS (Global Positioning System) with the help of GPS satellite and GPS module which is connected to the vehicle, which gives the position of the vehicle whenever required. There is a GPS antenna in the GPS module which receives information from the GPS satellite and gives us the location. This information is sent from GPS satellite to GPS antenna, then it is sent to the base station where the information is decoded then is transferred back to GSM module which has an antenna too then we can see the complete information about the vehicle. The GPS Module outputs the vehicle location information such as longitude, latitude, direction, and time. Then this information is received by the vehicle owner through a SMS via GSM module.

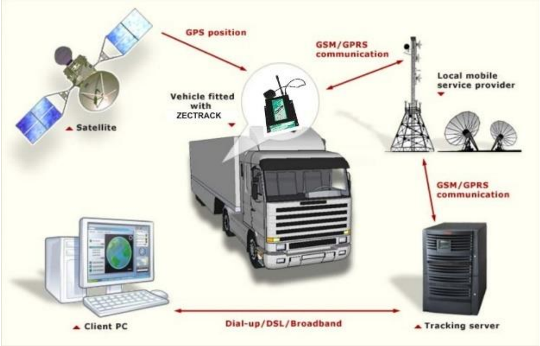


Fig 1: Vehicle monitoring and security system

There are different sensors in vehicle to monitor vehicle working:

Temperature sensor which ensures that the engine is not overheating or caught fire if by means its overheating the owner will get an alert about heating and forcing vehicle to stop.

Fuel level sensor it uses ultrasonic waves to find how empty the tank is and keeps it in memory. It will warn the driver about low fuel.

Collision detection sensor for this an Ultra sonic proximity sensor can used and monitor distance of nearby objects and make sound if they are close or apply automatic brakes if necessary, to prevent collision.

3. ADVANTAGES OF VMSS

- Unauthorized access notification.
- Better customer service.
- Safety of chauffeurs.
- Quick response to theft and quick recovery

- Minimal fuel cost

4. STAGES OF VMSS

The VMSS consists of three stages:

Stage 1: The chauffeur starts his drive from the transport office. VMSS transmits the chauffeur's ID and the commuter ID with the vehicle's location to the base station

Stage 2: Chauffeur picks up the commuter from his location. VMSS transmits the vehicle's location, vehicle's ID and commuter's ID to the base station. So, the commuter and base station will be able to track the vehicle.

Stage 3: Chauffeur drops the commuter to the destination. VMSS transmits the vehicle's position, vehicle ID and commuter ID to the base station.

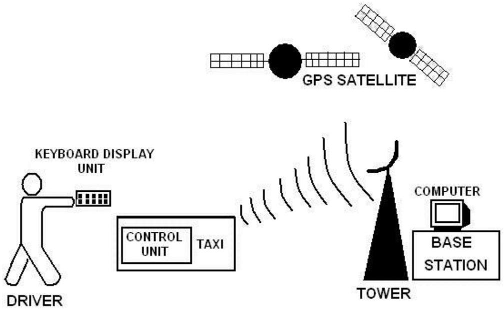


Fig 2: Transmission of Data

5. CONCLUSION

The monitoring of vehicle enhances the safety of vehicle, commuter and chauffeur. This system will help the company to maintain the record of commuters, chauffeur and the movement of the vehicle. This system also enables the car owner to recover the location of their stolen cars. The benefits of VMSS are endless. VMSS not only monitor the vehicle but also guard the vehicle from getting stolen and guard the life's of chauffeur and commuter and many other benefits.

6. REFERENCES

[1] https://krazytech.com/technical-papers/application-of-microcontroller-in-vehicle-monitoring-and-security-system

[2] https://www.researchgate.net/publication/319313720_VEHICLE_MONITORING_CONTROLLING_AND_TRACKING_SYSTEM_BY_USING_ANDROID_APPLICATION

[3] http://azhar-paperpresentation.blogspot.com/2010/04/vehicle-monitoring-and-control-system.html

[4] https://hiphensolutions.com/gps-vehicle-tracking-system/

[5] https://i0.wp.com/krazytech.com/wp-content/uploads/Stage-1-of-Vehicle-Monitoring-and-Security-System.jpg?ssl=1

COMPARATIVE ANALYSIS & EXPERIMENTAL STUDY ON MQ SENSOR SERIES

Faculty Mentor:
Dr. Suman Madan

Student Author:
Prerna Sharma (MCA-3rd Year)

ABSTRACT

Hazardous Gas Leakage Detection is one of the key aspects when the security of a place is considered and it is often treated as an integral element in the security system on the industry level. As a result, there is a growing demand for air quality monitoring and detecting malfunctioning in gas emitting devices for all levels of organisations. One of the emerging sensor technologies for target gas and steam detection is MQ sensor series, which offers a reliable and low cost wireless solution. There are a variety of sensors in the MQ family and each one targets a different set of gases which makes the MQ family suitable for a wide variety of applications. Further, alternatives and limitations of the MQ sensor units have also been discussed along with the proposed solutions for interfacing with prototyping platforms and working for the same (Keywords**:** microcontroller, MQ units, sensors, combustible).

1. INTRODUCTION

Gas leakage detection is the most fundamental and important factor in establishing security measures of premises and the former adds one more quotient strictly for lethal gas detection in compliance with operational efficiency at industry level. Industrial operations increasingly involve the use or manufacture of highly dangerous substances, particularly toxic and combustible gases which inevitably, causes the occasional escapes of gas, creating hazard to the industrial plant, its employees and residents nearby. The advent of the MQ sensor series, as a cost effective and reliable solution to target detection, resolves a need for a standard solution. MQ sensors are MOS type sensors, substantially employed for the detection of combustible gases and flammable steam, some units even capable of detecting smoke. *In this paper, an attempt has been made to* propose a detailed study of various units comprising the MQ family. their target compounds and therefore applications, along with other solutions of gas leakage detection.

2. LITERATURE REVIEW

Evidently, there’s never a single approach to target a problem. There exist multiple algorithms and a number of strategies to get started with and the same go with the wide variety of wireless solutions here. Researchers in the respective fields have developed several strategies to achieve the same throughout this time. Masahiro Maekawa et al.[1] as mentioned in the patent devised a solution for a gas-fueled internal combustion engine which in accordance with the gaseous pressure is capable of detecting even small amounts of gas leakage. Kamarul Ghazali et al.[2] proposed a solution in the field of thermal imaging. The experimental study shows that the system evaluates the severity level of the leakage using infrared image analysis. K. D. Romanak et al.[3] presented a new process-based approach to identify CO2 that has leaked from deep geologic storage reservoirs into the shallow subsurfaces by examining chemical relationships between vadose zones N2, O2, CO2, and CH4 to promptly distinguish a leakage signal from natural vadose zone CO2. Prerna Sharma et al.[4] developed a robust and compact Intrusion Detection and Security System employing various sensor technology for sampling and alarming concerned authorities. Specifically for gas leakage detection, MQ2 sensor was used. Dr. Chetana Tukkoji et al.[5]

proposed an intelligent LPG Gas Leak Detection Tool using MQ6 sensor unit and Arduino for local intelligence.

3. MQ SERIES - A COMPARATIVE STUDY

It is a Metal Oxide Based (MOS) type sensor series, widely accepted standard for gas leakage detection. MOS type sensors are often referred as chemiresistive modules because of their tendency to vary their electrical resistance in consonance with the concentration of target gases in its vicinity. These sensors are highly compatible with microcontrollers and hence with Arduino. Evidently arduinos are very inexpensive and easy solutions to microcontrollers, and the latter is embedded on the Arduino circuit board [6]. The module comes equipped with a potentiometer and thus the sensor can be calibrated as per the requirements. Every sensor in the MQ sensor series is susceptible to a different set of gases and occasionally smoke which makes them an effective and widely adopted standard for target gas detection in households and industry levels. The MQ2 sensor unit is capable of detecting Methane, Butane, Propane, Hydrogen, LPG as well as smoke, which makes it an apt choice for household purposes. MQ6 with target gases (LPG, Butane, and Methane), MQ306A with high sensitivity towards (LPG, Butane), and MQ309A (Carbon Monoxide and Methane) can also be used as an alternative to MQ2. Similar to these sensors, there are other units as well, pertaining to different applications due to variable threshold levels for different sets of target. The following table identifies the applications and sensitive compounds per unit in MQ Series.

Applications and Target gases of MQ units

SNo.	*Module*	*Sensitivity characteristics*	*Applications*
1	MQ135	Alcohol, Benzene, smoke	Air Quality Monitoring, Refineries, Pipelines, Industrial facilities
2	MQ307	Carbon Monoxide (CO)	CO detecting equipment for carbon monoxide at households, vehicles. Portable Gas Detector.
3	MQ2	Methane, Butane, Propane, Hydrogen, LPG, smoke.	LPG gas Detection. Domestic use. Industrial Operations. Fire Detection. Flammable and combustible gas detection.
4	MQ6	LPG and butane	LPG gas Detection. Boilers or Parkings. Detection of explosive vapors.
5	MQ137	Ammonia gas (NH3), trimethylamine, ethanolamine	Toxic Gas Detection, monitoring other organic amines, Safety standard maintenance, Hospitals, Labs
6	MQ138	Volatile and Organic gases, Aromatic compounds, Alcohol, Ketones	Industrial facilities, organic vapour detection, Fire Detection, Aromatic compound detection.

7	MQ9	LPG, Carbon Monoxide (CO), Methane, Propane	LPG gas Detection. Domestic use. Industrial Operations. Fire Detection. Flammable and combustible gas detection.
8	MQ303	Alcohol Sensor	Breath Checker or Automobile’s Ignition locking system, Industrial facilities
9	MQ7	Carbon Monoxide (CO)	CO detecting equipment for carbon monoxide at households, vehicles. Portable Gas Detector.
10	MQ8	Hydrogen (H2), City gas	Domestic use. Industrial Operations.

4. CHALLENGES WITH MQ SERIES

It is evident through various applications that MQ series sensors are now widely accepted as standard for gas leakage detection at various levels of organisation. One of the reasons for this adoption is high efficiency, availability and competitive advantage in cost. However there are other factors that highly affect the production and manufacturing of consumer electronics, and often there is no possibility of trade off with these factors. A considerable amount of MQ sensors are not water resistant, water affects the sensitivity of the sensor. Other natural factors in extreme scenarios like extreme temperature, pollution, humidity for a longer duration cause deformity in general to sensors. Some sensors like MQ303 are subjected to amalgamation by the effect of alkali and halogens yielding undesirable results. Corrosion in the internal structure can also lead to malfunctioning of the unit. Since these sensors have thresholds for different sets of compounds, the existence of some complementary compounds might attenuate the sensitivity and affect the results. Therefore special attention must be given to the conditions of the model environment, and the knowledge of the compounds able to alter the results is prerequisite.

5. CONCLUSION

The goal of this paper was to provide a reference to applications of various sensors of MQ modules. MQ units are MOS based sensors that is conductivity of the sensor is directly proportional to the concentration of target combustible gas or smoke. Each MQ sensor targets a set of gases which makes the MQ series widely accepted solution in terms of gas detection. If a module is susceptible to multiple compounds, the former has different thresholds for different compounds. These sensors can function in both digital and analog mode. Considering the security needs of today with respect to detection of combustible gases and flammable steam MQ units offer robust, portable and cost effective solutions. Despite having competitive advantage in terms of performance and cost, MQ family still poses challenges when it comes to model environment and availability of complementary compounds leading to permanent damage, attenuation of sensitivity and undesirable results. Extreme natural factors like temperature, humidity result in deterioration of the unit. These sensors have found their applicability in the following areas -LPG gas Detection at homes, Industrial Operations, Fire Detection, Lethal gas detection, Medical Institutions, Safety standards Maintenance, Target compound detection, Automobiles etc. Alternative techniques to detect the presence of a particular compound other than sensor technology could be thermal imaging, infrared cameras, with the employment of contrasting chemical compounds etc. MQ Series units are highly compatible with microcontrollers and once interfaced can be installed with negligible changes in the premises and offer long lasting service.

6. REFERENCES

[1] Masahiro Maekawa, Takahiro, Aki, Kohei Igarashi, Hiroki Matsuoka *"Gas leakage detection and fail-safe control method for gas-fueled internal combustion engine and apparatus for implementing the same"* Patent US6467466B1

[2] Mohd Shawal Jadin, Kamarul Hawari Ghazali "*Gas Leakage Detection Using Thermal Imaging Technique*" 2014 UKSim-AMSS 16th International Conference on Computer Modelling and Simulation, Institute of Electrical and Electronics Engineers (IEEE). ISBN: 978-1-4799-4922-9

[3] K. D. Romanak, P. C. Bennett, Changbing Yang, Susan D. Hovorka "*Process-based approach to CO2 leakage detection by vadose zone gas monitoring at geologic CO2 storage sites*" (August, 2012) Geophysical Research Letters, Volume 39, Issue15

[4] Prerna Sharma and Deepali Kamthania, *"Intrusion Detection and Security System"*(2020) Big Data Analytics and Intelligence: A Perspective for Health Care, Emerald Publishing Limited, pp. 139-151, ISBN- 978-1-83909-100-1

[5] Dr. Chetana Tukkoji Mr. Sanjeev Kumar A. N "*LPG Gas Leakage Detection Using IoT* " (April, 2020). International Journal of Engineering Applied Sciences and Technology, Vol. 4, Issue 12, ISSN No. 2455-2143, pp-603-609

[6] Prerna Sharma and Deepali Kamthania, *"Intelligent Object Detection and Avoidance System"*, Two Days *International Conference* on Transforming IDEAS (Inter-Disciplinary Exchanges, Analysis and Search) into Viable Solutions, 29th -30th March, 2019, pp. 342-351, Macmillan Education, ISBN-938882695-7

SECURITY ISSUES IN CLOUD COMPUTING

Faculty Mentor:
Dr. Archana B Saxena

Student Author:
Shivani Singh Tomar (MCA-2nd Year)
Manupriya Gupta (MCA-2nd Year)

1. INTRODUCTION

Cloud means a good range of services that users can access via an online connection. Microsoft, Amazon, Google and many more provides various cloud-based services for which users can pay on the basis of service consumption and subscription. Using these internet enables devices; cloud computing permits the function of application software. It also allows us to perform on an equivalent document for several jobs of various types. Cloud computing makes usage easy by allowing overcoming the limitation of traditional computers. It also provides more services because it allows faster access.

These hosted services are categorized into following categories: Infrastructure-as-a Service (IAAS), Platform-as-a-Service (PAAS), and Software-as-a-Service (SAAS). There are some security threats that have exploited the usage of Cloud Computing. An example of these security threats is BOTNET. Botnet was used to spread spam and malware. Of the 761 data breaches by U.S Secret Service, almost 67% occurred at companies with 100 or fewer employees.

One of the best features of cloud computing is pay-as-you-go model of computing as a resource.

This model of has enabled business and organization in need of computing power to get as many resources as they have without the necessity to place forth an outsized capital investment in IT infrastructure. Cloud is a new trend in evolution of distributed system. The user may not need the knowledge to control the infrastructure of cloud, it provides abstraction.

2. CLOUD COMPUTING MODELS

Cloud hosting deployment models are categorized by size, access and proprietorship.

- **Cloud Computing Deployment Models:**
  - **Public Cloud**: - As the name suggest it is available for general public and data is created and stored in third party servers. This model is best representation of cloud hosting. Customers do not have any control over the location of infrastructure. Public Cloud is fitted to business with low privacy concern because it is economical. It profits the purchasers by achieving economies of scale. It is free deployment model e.g. of a public cloud is Google.
  - **Private Cloud: -** Private cloud deployment model supports all users who want to form use of a computing resource, like hardware (OS, CPU, and memory) or software (Application Server, database) on a subscription basis. It is own by only a specific organization that requires it. Common uses of public clouds are for application development and testing, non-mission-critical tasks like file-sharing, and e-mail service.
  - **Hybrid Cloud: -** This encompass best features of private and public cloud infrastructure. It allows that organization to mix and match features of above two cloud computing methods. Many organizations make use of this model once they got to proportion their IT infrastructure rapidly, like when leveraging public clouds

to supplement the capacity available within a private cloud.

- **Community Cloud**: - This deployment model supports many organizations sharing computing resources that are a part of a community, for example, universities cooperating in certain area of research, or police departments within a country or state sharing computing resources.

➢ **Cloud Computing Service Models**

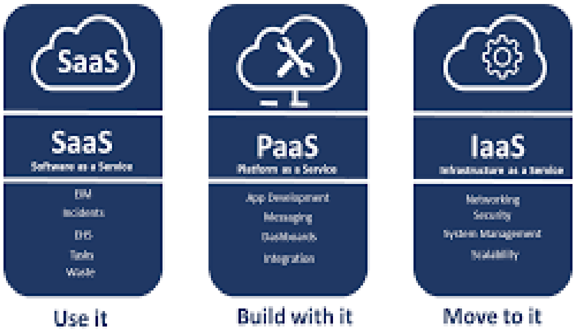


Fig 1: Cloud Computing Service Models

- **Software as a Service (SaaS): -** SaaS, is a way to deliver application as a service over the internet.
  In the software on demand SaaS model, the provider gives customer network-based access to single copy of an application that the provider created specifically for SaaS distribution
  Organizations can integrate SaaS applications with other software using applications programming interfaces.
- **Infrastructure as a Service (IaaS): -** IaaS is an instant computing infrastructure, provisioned and changed over the internet. IaaS quickly scales ups and down with the demand, letting you pay only for what you see. It helps you avoid the expense and complexity of shopping for and managing your own physical servers and other datacenter infrastructure.
- **Platform as a Service (PaaS)**: - Platform as a Service may be a sort of cloud computing offering during which a service provider delivers a platform to clients, enabling them to develop, run, and manage business applications without the need to build and maintain the infrastructure such as software development process typically require.

3. WHAT IS CLOUD SECURITY?

Cloud security is a collective term for the security practices, controls, and technologies that are used to shield cloud's environments. These can be classified into three separate categories:

➢ **Preventative Controls**: These controls try to find and minimize exposure and close possible security gaps in the cloud's infrastructure. This can include things like firewalls and encryption solutions.

➢ **Detection Controls:** These controls work to discover attacks in progress or lately finished attacks so that automated or manual remediation can begin. Things like anti-virus/anti-malware scanning tools, security information and event management (SIEM) solutions (which are frequently delivered via SaaS models), and even managed network security monitoring could be measured examples of detection controls.

➢ **Corrective Controls:** These controls are intended to rectify the damage or adverse effects of an attack after it happens. Things such as virus/malware removal tools, remote data backups (to restore corrupted or damaged files), and managed security incident response services could be examples of corrective controls.

4. SECURITY ISSUES IN CLOUD COMPUTING

There are many threats and challenges involved in cloud computing that one needs to deal with. Some of the biggest issues involved in cloud computing are:

- **Data Breaches:** The no. of attacks on cloud's environment is significantly increased due to cumulative volume of all the data that is stored in cloud. A data breach is always possible to happen unless we take some appropriate measures to secure the cloud's environment from any external attack that may happen. There may be an open port forgotten about or a script with runtime access that someone can increase beyond its anticipated use, and also there can be other trivial holes in the cloud that if we do not handle properly can further turn into a disastrous problem.
- **Insider Threat:**

Web 2.0
Shared Applications
Cloud Computing
The Insider Threat
Monitor Users
Protect Data
Cyber Security

Fig 2: Insider Threat in Cloud Computing

The next security issue is an insider threat. We cannot ignore the possibility of an attack from within our organisation. Access by authorized parties with the intention of damaging the cloud environment is as extremely dangerous as unauthorized access. These types of attacks are even more challenging to detect, and even more tough to prevent. Having a secure cloud storage, no alarm would be raised if someone try to access it under normal circumstances. In fact, it is almost untraceable. Fortunately, if we use exhaustive logging tools and some of the information security's best practices then the damages caused by this type of attack may be regulated efficiently.

- **Account Takeovers:** Impersonators can take over user accounts and roam freely in the environment, carrying out false activities wherever and whenever they want. Successful logins from other counties or IP addresses, mass file downloads, suspicious sharing activity, successful logins from multiple different countries in a short amount of time, phishing emails coming from an internal account are all common examples of an account takeover. Account takeovers are notoriously difficult to detect and even more difficult to find and remediate. One of the best ways to detect attempts and quickly remediate the issue is to use a cloud application account takeover prevention tool.
- **App Vulnerabilities:** A serious security threat can be posed even in a complex web of micro services architecture when we run apps on the cloud environment. Selective port monitoring, multiple firewalls and other security measures will not work if the cause of an attack is from the inside. Sufficient reviews and tests should be performed as part of our development before new codes are deployed.
- **Insufficient Due Diligence Increases Cyber Security Risk:** Organizations when migrating to the cloud often carry out insufficient due diligence. Without understanding the full scope, they often move data to the cloud not understanding the security measures that are used by the CSP.
- **Increased Complexity Strains IT Staff:** Managing, integrating, and operating in the cloud can be tricky and it may require learning of a new model by the existing IT staff as complexity can be increased when migrating to the cloud. IT staff must have proper skill level and have adequate capacity to manage, integrate, and maintain the migration of data to the cloud. More complex services in the cloud are encryption and key management. Due to technology, policies, and implementation methods there may also be evolving threats/risks in hybrid cloud implementations, which further add more complexity. This leads to an amplified potential for security gaps in an organisation's cloud.

- **Data Loss:**

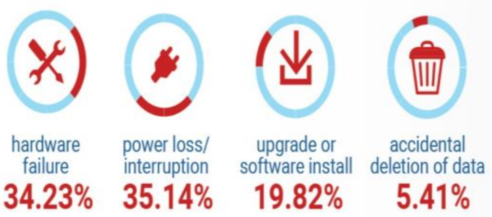


Fig 3: Data Loss figures

  Data loss is another one of the high risks that often doesn't get properly rectified. Servers can fail, power loss can happen, hardware can stop working, and our files may be lost. Creating a backup routine and having a disaster recovery policy is a good practice and can be very helpful in preventing data loss. For maximum security of our cloud's environment maintain online (remote) and offline backups.

- **Risky SaaS Applications:** It's extremely difficult to monitor and block the use of unsanctioned application when end users sign into cloud applications on their systems unbeknownst to the IT department. There are two basic forms in which SaaS risk comes in: malicious SaaS apps and apps that were not developed with proper security controls. These apps can expose a "back door" to our cloud environment. Only allow permissions to well-known and trusted applications through OAuth. SaaS security solutions provide greater visibility and control over cloud applications to protect against data exposure

5. SOLUTIONS TO SECURITY ISSUES

- **Limit Your Cloud Computing Vendors:** It becomes more challenging to manage different cloud-based solutions having various security tools and processes. At this point, finding ways to limit our choice of CSP vendors can be a major help. We should try to restrict ourselves to source from a single vendor.
- **Verify Your Access to Information about the Cloud Environment:**
  Visibility is important to cyber security so it becomes important to verify the information we are going to access about the cloud. With better visibility into the cloud environment, we can effortlessly track and control security.
- **Consult with a Cyber security Expert:**
  Whenever we are not sure about our organisation's security measures, we should consult a cyber-security expert to protect our data. Having an expert's advice can always help us to make more informed decisions.
- **Verify Security SLAs:**
  Before signing an agreement with a cloud service provider, one should check one more thing, that is, what their service level agreements regarding security, like, how long will it take to restore normal service? And how quickly a security breach after detection is resolved? Verifying these SLAs can help ensure that they will protect our industry's information.

6. REFERENCES

[1] https://www.infoworld.com/article/2683784/what-is-cloud-computing.html

[2] https://www.investopedia.com/terms/c/cloud-computing.asp

[3] https://insights.sei.cmu.edu/sei_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html

[4] https://www.akamai.com/us/en/resources/data-security-in-cloud-computing.jsp

[5] https://managedmethods.com/blog/security-issues-in-cloud-computing/

SMART EYE TECHNOLOGY

Faculty Mentor:
Dr. Deepshikha Aggarwal

Student Author:
Harshit Heda (MCA-2nd Year)
Pranav Gupta (MCA-2nd Year)

1. INTRODUCTION

Eye-tracking is the wonders wherein developments of the eye and its gaze is caught. This innovation was established in 1999 by a Swedish cutting-edge organization situated in Gothenburg. In Smart eye innovation, there is a persistent assessment of all social stages which eliminates all the potential measures or methods of the undesirable watcher to jab at your screen.

At the point when we are at a public place and need to see some classified records, the smart eye encourages you to keep its entrance just to your eye. With its biometric screen assurance, it blocks unapproved clients from survey your screen with persistent facial and iris ID, second by second. In this stage, there is an administrator board that permits us to pick report access cut-off points, for example, where they can view and how long they can get to the record.

It likewise gives record following including ongoing notice of alarms for example at the point when the reports have been thought of and marked and whether any endeavours have been made for offering the material to any unapproved clients. A few uses of keen innovation are utilized in the car business for example eye following is utilized in driver observing frameworks and inside vehicle conditions. In medication, eye following is utilized in examination and neuroscience where it can help determine patients to have Alzheimer's and Parkinson's infections. Hardly any results of it are Tobi Pro Spectrum, Tobi Pro Classes, Tobi Pro Fusion, Tobi ace lab.

This kind of innovation will bigly affect figuring. This can help when creating sites or showing data. On the off chance that we take a gander at its negative side, the greatest impediment of eye-following innovation is that not everyone's eyes can be followed for example Contact focal points, glasses, and student tone would all be able to affect the eye-following camera's capacity to record eye developments. Another issue in this innovation is that aligning the instruments/gear requires significant investment which may make the client go astray from utilizing the gadget.

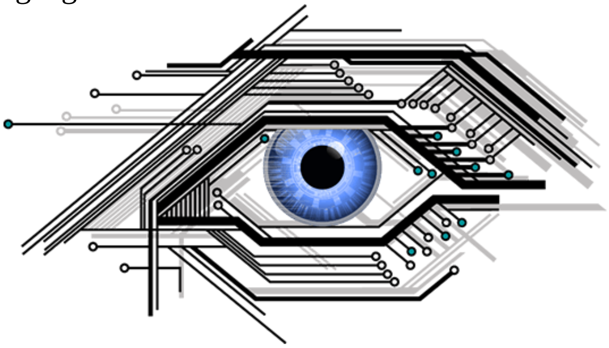


Fig 1: Biometric Security and screen privacy

2. A FUNCTIONING R&D AND PATENT SYSTEM

For over ten years Smart Eye has given progressed eye tracking frameworks to requesting modern clients in the car business and different areas and, in the organization's appraisal, holds a world-driving situation inside cutting-edge multi-camera framework.

Shrewd Eye puts ceaselessly in the further advancement of its eye tracking innovation. Significant assets are additionally put resources into item improvement inside, above all else, the Automotive Solutions business zone, yet in addition inside Research Instruments. By and large, 30 workers are occupied with innovative work.

Brilliant Eye's innovation is ensured by a few licenses and the organization has a functioning patent system to record licenses for new developments. Today, the organization holds two eye tracking licenses. Keen Eye documented eye tracking patent applications at a beginning phase and subsequently holds various significant licenses here.

3. EYETRACKING APPLICATION REGIONS

There are a few purchaser applications for which eye tracking can be utilized. Game applications and traveller vehicles are two territories that are near a more extensive business discovery.

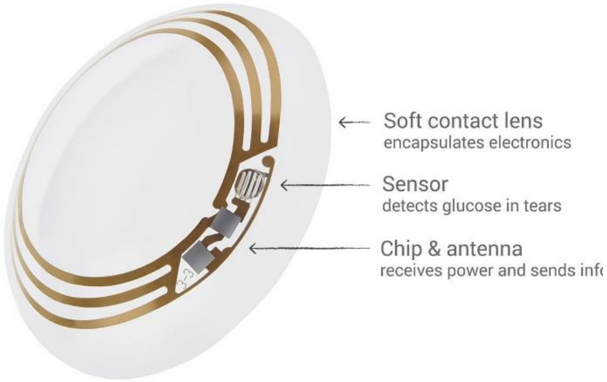


Fig 2: Smart Contact Lenses

- **Automobile Industry**:- Eye tracking is utilized in the improvement of driver conditions, but at the same time is incorporated in vehicles, to expand wellbeing and take into account self-sufficient vehicles.
- **Researches**:- For a long while eye tracking has been utilized to examine human conduct inside such regions as brain research, social science, neuroscience, ophthalmology and learning.
- **Market Reviews**:- Eye tracking is a compelling method of concentrating how an individual sees a commercial, item or store climate.
- **Communication Help** :- For the debilitated, eye tracking is a method for cooperating with the rest of the world, utilizing a PC or imparting as a rule.
- **Modern Applications** :- There are an enormous number of modern applications where eye tracking is utilized, for example, clinical innovation, test systems, reconnaissance, security and military applications.
- **PC Games**:- Utilizing eye tracking in PC games makes new coordination techniques, improving the client experience.
- **Computers**:- Eye tracking can supplant the PC mouse, however can likewise be utilized as an enhancement, to build adequacy and improve the client experience.

4. PROPOSED SYSTEM

- **Route Navigation**
  GPS captures current location the client then checks whether it is objective great or not. If the opportunity, the goal is legal, then method reaching that goal is given in kind of voice orders. GPS consistently monitor the size and width of the figures while managing the client. The voice commands they are the basic and effective foundations. The earphones used to provide all commands, such as the correct course of the route as well will notify the client if there will be any obstruction way.

- **Face detection and recognition**
  Face & notification module uses camera photography of objects in front of a client and save those photos to SD card, volume card within small control. Camera is focused on client's shirt. Webcam it has three different types of lamps that light up naturally in secret. In addition, it has 16 embellishments and 10 foundations outlines. For technical reasons, the camera catches 20 faces and photos are included away from the name of the individual. This physically done before the gadget became placed in pragmatic use. If possible that the same person comes before client again, at which point the camera will do take a picture and compare it and compare it with something else and when a match is found, the person's name is shown. No voice output is introduced for self-defence if no similarity is available. Image capture and management complete OpenCV program help.

- **Eye blink detection**
  The indicator of eye squint is this used to renew the enter console. To distinguish the light of the

eyes, the size of the black pixel in the student area is approximate. Change from low to low-dim pixel number given eye-flicker identification for example the access key. Webcam is associated with Raspberry Pi computer microchip photo preparation and internal integration another module including apparatuses controlled, wheelchair and SMS mange module. Utilities are controlled module, another Arduino used for discovery order from Raspberry Pi with remote control books, Arduino will turn into a handoff Turn on or off as indicated by the command of Raspberry Pi, this device is used for unlocking Active or closed items.

5. SYSTEM ARCHITECTURE

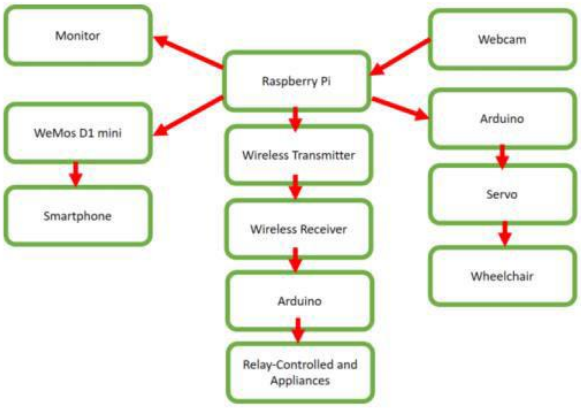


Fig 3: System Architecture

6. WORKING OF SMART EYE

The entire system can be divided into two simple subsystems namely route navigation and the other one is the face detection and recognition. The navigation module also includes the obstacle detection system. The device is used to guide the person to the pre-stored destination whose path is stored in the device. The user can choose his/her destination with the help of these buttons. The system is provided with 4 types buttons, which the user uses to select his/her desired location and then the navigation route for these locations are given as voice command using headphones.

7. REFERENCES

[1] http://www.corp.smarteye.se/en/technology/about-eyetracking/

[2] https://en.wikipedia.org/wiki/Smart_Eye

[3] https://smarteye.se/technology/

[4] http://www.ijcsejournal.org/volume5/issue2/ijcse-v5i2p5.pdf

[5] https://www.prnewswire.com/news-releases/smart-eye-integrates-the-future-in-todays-cars-through-eye-tracking-and-ai-at-ces-2020-300980781.html

SMART CAMERA FOR TRAFFIC SURVEILLANCE

Faculty Mentor:
Dr. Disha Grover

Student Author:
Rishabh Jain(MCA-2nd Year)

1. INTRODUCTION

“What a Smart Camera is, what is it made up of and how is it different from some normal camera?”.

A Smart camera is not just a regular camera that is presented on our mobile phones or something that is used as CCTV but it’s much more than that. It is a combination of different types of sensors and devices packed inside a single module.

A Smart Camera contains advanced CMOS Image Sensors with high-performance processors that are used to combine video sensing, video processing, and communication within a single device.

These cameras not only capture images or videos, but they also perform advanced image processing functions like “Face Detection” or “Motion Analysis”. It compresses the image or video and sends the video as well as the desired data over the network.

Fig 1: Smart Camera

2. COMPONENTS

A smart camera is usually made up of these components:

- Image Sensors
- Image Memory
- Image Digitization Circuitry
- Processor
- Communication Interface
- Ram
- I/O Lines
- Built-In Lens
- Illumination Device
- Real-time OS
- Video Output

3. REQUIREMENTS OF A SMART CAMERA

In general, smart cameras consist of a sensor, communication unit, and the processing unit. We have to understand the requirements of each of these units.

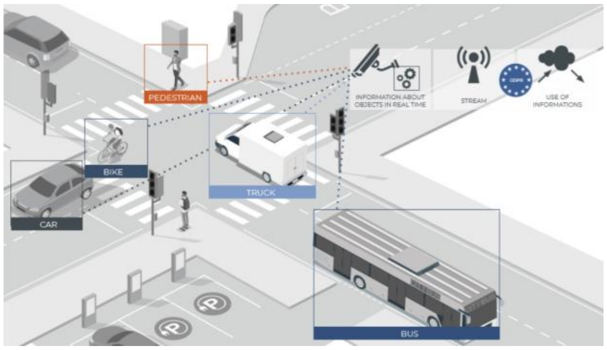


Fig 2: Detection of objects on the road

- **Sensor Requirements**
  - **Resolution and Frame Rate: -** CIF and QCIF image formats cannot be used with digital cameras because, in order to do image processing, digital cameras require images with higher resolution and more fps therefore PAL resolution is used to deliver images in most of the surveillance systems.
  - **Digital Interface: -** To minimize the effect of aging and temperature drift and to keep away from glue logic the sensors need to send digital video output, therefore the image sensor needs to incorporate an analog amplifier.
  - **Dynamic Range: -** Sometimes when high-intensity areas like a high beam of a vehicle appear synchronously with low-intensity areas, the image sensors that have high dynamic range and limited blur are preferred.
- **Processing Requirements**
  - **Video Analysis: -** Video analysis is used to extract useful data from raw video data. Video analysis is used to detect an extraordinary situation like detecting a wrong-way driver or some lost object. And after detection, an alarm gets activated and sends a notification to the main control station.
  - **Video Compression: -** In order to reduce the bandwidth, whenever sending video or any media, we need to compress that video or any media within the digital camera setup. Compression uses some video compression algorithms in order to reduce the size of the media.
  - **Camera Control and Firmware: -** Aperture and flash control, these tasks come under camera control. Firmware is used to manage all the software related tasks and to configure the software using some network and to control all peripherals.
  - **Computation of Traffic Statistics: -** This is the task of surveillance cameras to do all the computations related to Traffic statistics like calculating the number of vehicles per second or per minute, lane occupancy, or average speed of the moving vehicles on the road and sending that data over some wireless network.

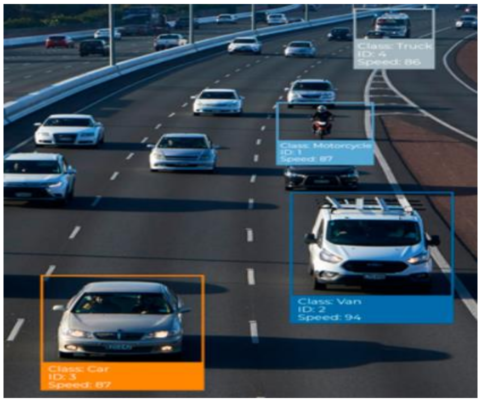


Fig 3: Smart camera calculating the speed of vehicles

- **Communication Requirements**
  - After doing the tasks like video compression and video analysis, the compressed video needs to get transferred to the central hub or the station via some network.

  - Different types of networks like Ethernet or Wireless-LAN are used together in order to transmit the media to the central station.

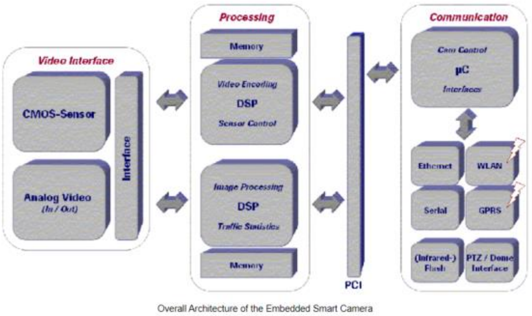
  - The smart camera should be able to download the data so that the camera's firmware can be updated later on via some network.
- **System Requirements**
  - **Real-Time: -** Real-time smart cameras have certain time constraints

which are concerned with camera control and peripherals like flash triggers. There are certain image and video analysis algo's, which act as timing constraints in a real-time system.

- **Low-Power: -** In low powered smart cameras, the release of heat should be less so that we can get rid of an active cooling system which consists of cooling fans.

4. ARCHITECTURE OF SMART CAMERA

For doing traffic monitoring the camera with all of its components are packed inside a case which can then be placed on highways or tunnels and they can be used as either solar power or can be plugged in some socket as well.



Overall Architecture of the Embedded Smart Camera

Fig 4: Architecture of Smart Camera

Broadly it is divided into 3 parts:

1) **Video Sensor**
It shows the first stage when data flow starts in a smart camera. The video sensor takes the incoming light and converts it into electrical signals that can then be sent to the processing unit. CMOS sensors are used to implement all of them.

2) **Processing Unit**
Now the next step of the entire data flow is the processing unit. Now requirements on all over processing are very high because of high-performance video and picture processing and these requirements are fulfilled with DSP (Digital Signal Processors). The smart camera contains two loosely coupled DSP's and each and every processor is attached to its local memory.

3) **Communication Unit**
This is the last step of data flow in smart cameras. A generic interface is used to transmit data to the processing unit. With the help of the interface, it becomes easy to implement different network connections like wireless LAN, Ethernet, and GPRS. In the case of ethernet as media access layer is previously there in DSP therefore just the physical layer needs to be included here.

5. OTHER USAGES OF SMART CAMERAS

Smart cameras are not just used in traffic surveillance, they can be used in many other places as well for different tasks. I have mentioned a few of them below:

- ➢ **In shopping centers**
  - ○ Measure queue and waiting time
  - ○ Measure average time spent in different areas
  - ○ Measure the flow of people
  - ○ Customer counting

- ➢ **In public transport and stations**
  - ○ Head-count at stations
  - ○ Counting passengers
  - ○ Detecting empty seats
  - ○ Checking capacity of the vehicle

- **For parking**
    - Checking free and occupied parking areas
    - Identifying the type of vehicles
    - Recording parking time
    - Identifying free and occupied parking time

6. CONCLUSION

A smart camera is a simple but very useful device which is a combination of different sensors and devices and it is fitted inside a single unit. Broadly a smart camera consists of 3 components which are video sensor, processing unit, and communication unit and it performs tasks like video sensing, video processing, and communication. A smart camera can be used in many other places as well as in shopping centers for measuring queues and waiting time or in public transports for measuring head-counts at stations. The only limitation of using the smart camera is its cost and maintenance as smart cameras are mainly installed in the open area and they are exposed to harsh climatic conditions like sun, rain, or hail storm.

7. REFERENCES

[1] https://www.ifsecglobal.com/video-surveillance/role-cctv-cameras-public-privacy-protection/

[2] https://www.swarco.com/products/detection-sensors/smart-camera/intelligent-camera-solutions

[3] https://www.swarco.com/products/detection-sensors/smart-camera/intelligent-camera-solutions

[4] https://pervasive.aau.at/BR/smartcam/smartcam.html

[5] https://bit.ly/3jCOJCM

[6] https://en.wikipedia.org/wiki/Smart_camera

VIRTUAL SURGERY

Faculty Mentor:
Ms. Geeta Sharma

Student Authors:
Ankita (MCA-2nd Year)
Tanya Tyagi (MCA-2nd Year)

1. ANALOGY

Everyone drives car , or travel , or take walk anything. We know where we're going most of the time . Same thing is done by a GPS that we use in our car . But don't you like when you have a map that's updated in real time and you can see the position of your car in relation to that map while you're driving it . What's the benefit then? It can make the drive a little more efficient and safer by integrating the navigation.

Considering this analogy, you can operate with far greater confidence and visual spatial awareness if you bring that simulation into your operating room and you can see that computer rendered three-dimensional scenarios right in front of you , brought into your operating environment to augment the reality that you have during surgery.

2. VIRTUAL REVOLUTION

Output tools for vision, tactile, hearing and power transmitter as well as input devices such as mouse, gloves, chaser, etc. , a virtual environment's graphical manufacturing system as well as an information software constitutes this Virtual Revolution. A stunning 360° CGI reconstruction , 4K 360° video from multiple angles , pain and physical therapy scan help students as well as Residents to get trained before attempting their surgeries on patients. In a virtual environment, all the features of activity such as severity, duration and type of response are adopted.

Human body has many crucial nerves , sensitive organs and minute parts that are like wet tissue paper , which makes it difficult to deal with having to remove fibroids or perform surgeries across those soft and delicate structures. Application of virtual reality, robotics , augmented and image guided surgeries into the field of surgery enables the medical practitioner to use high accuracy , precision in his practices.

3. WHY REVOLUTION? AUGMENTING THE SURGICAL EXPERIENCE...

- Google Cardboard Headset - Life Saver: - There was a case where baby Teegan Lexcen was born with only one lung and half her heart. Then Dr. Redmond Burke (Chief, Cardiovascular surgery) used a low-cost Google Cardboard headset to plan a surgery on the baby that enabled him see the 3D images of the baby's heart. Just four weeks after surgery, Teegan was taken off the ventilator.

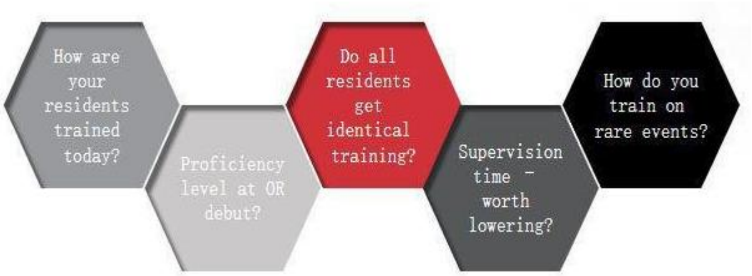

How are your residents trained today?
Proficiency level at OR debut?
Do all residents get identical training?
Supervision time – worth lowering?
How do you train on rare events?

Fig 1: Need for Change

- Your Virtual Operating Room:- In general, medical students watch actual surgeries on the cadavers with experienced doctors. But with the advances in virtual reality , they can actually feel as if they are physically present in operating room if the surgeries are filmed using virtual reality or 360-degree cameras.

- Cognitive-Behavioural Therapy:- Nowadays this concept is used worldwide in overcoming behavioural fears in patients. They give exposure to therapy that will force patients to confront their fears and cure phobias , all of this in safe and controlled environment. Fear of spiders, heights, storms, flying can be cured using this.
- VS For Practices in Post-Traumatic Stress Disorder:- Patients can see almost a 40% improvement in their symptom in a two-year trial. It is Similar to exposure therapy that cure phobias, VR is being used to ease Post Traumatic Stress Disorder , especially military veterans.

4. SURGICAL THEATRE

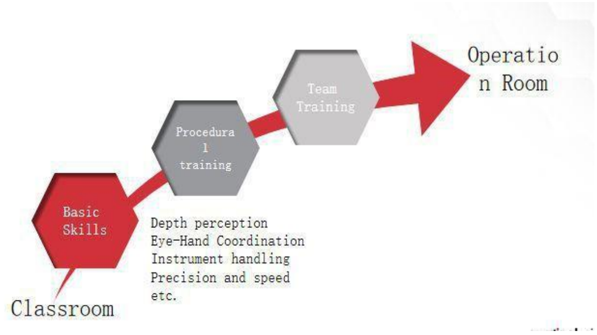


Fig 2: Process to improve Surgical Theatre turnaround time

5. PEAKPOINTSTHATCONTRIBUTEINVIRTUALSURGERY

- Safety
- Time
- Money
- Ability to re-use on a regular basis/skills refresh
- Can be used remotely
- Efficiency
- Realistic

6. FUTURE OF VIRTUAL SURGERY

With the increased challenges and complexity, medical experts observe that improper training and longer learning curves are the primary reasons for adverse impacts related to new technology's is essential that we take a move to improve things ,assessment and coordination of surgical teams. If these problems will not be sorted out, then delay or even shutting down promising emerging medical technologies may emerge. By improving these factors, we can ensure safe surgery and allow innovations to reach full potential in health care system.

7. REFERENCES

[1] www.surgicaltheater.net
[2] www.ncbi.nlm.nih.gov
[3] www.medicaldevicenework.com

NOTES: -

Sector-5,Rohini,Delhi

JAGAN INSTITUTE OF MANAGEMENT STUDIES
3, INSTITUTIONAL AREA, SECTOR 5, ROHINI, DELHI 110085
Email: techbyte@jimsindia.org
www.jimsindia.org/techbyte2k20