FR. CONCEICAO RODRIGUES INSTITUTE OF TECHNLOGY

Zephyr|

DEPARTMENT OF COMPUTER ENGINEERING

FROM THE HEAD OF THE DEPARTMENT

Dr. Lata Ragha
Head of the Department,
Computer Engineering

Nurturing creativity and inspiring innovation are the two key elements of a successful education, and a department magazine is the perfect amalgamation of both. Magazine is an excellent platform for the budding engineers to bring out their hidden talents.

It gives me immense pleasure to know that Department of Computer Engineering is bringing out the department magazine "ZEPHYR", in time. This helps to showcase the activities that are happening in the department. In addition to the numerous achievements of the department this is yet another milestone in the co-curricular activities.

I hope this magazine will be a guiding factor for today's youth and keep pace with the changing scenario and provide the platform to our students for exhibiting their true talent and creativity through various genres of writings. It also helps in building up teamwork which is very much needed today in the world of competition. It provides a platform for exposing the merits and academic achievements of the students.

I congratulate and thank all the students and staff coordinators who have made untiring efforts to bring out this magazine. I wish them all success.

DEPARTMENT DETAILS

The four year Computer Engineering Degree Course was started in the year 1994 and it was accredited for three years from 2006 and reaccredited for two years w.e.f 2012. B.E Computer engineering course offered introduces the student to the world of programming starting with the basics and slowly leading towards the high end programming technologies.

The Computer Engineering Department has domain specific, well equipped labs with Desktops having latest specifications and software.

Besides this, Computer Department Association – ACESS (Agnel Computer Engineering Students Symposium) plays a major role in conducting various workshops and Short term Training courses on Machine Learning, Storage Area Network (SAN), Big Data Analytics-Hadoop, Web Designing, Open Source Technologies, Python, Robotics, Advanced Mobile Technology etc. to keep the students at par with the requirements of the industry and to make them successful professionals. Also the department has set-up Cyber Security Cell in collaboration with EC-Council which imparts training and awareness on Cyber Security. Apart from this, students are also encouraged to become members of professional societies like CSI, IEEE etc., to enroll for various internship programs and to develop their programming skills thru Programmer's Club.

Department has well qualified faculty members who are specialized in various areas. Students implement real time projects which are mostly research oriented guided by faculty in the final year as part of their curriculum which trains them to be highly competent computer software professionals needed by industry. As part of final year projects, various groups have undertaken projects from reputed industries and research centres like Persistent, Reliance, BARC and TIFR. During the curriculum, the department provides a platform for students to present/publish technical papers in National and International Conferences and International Journals.

Contact Details:

Ms. M. Kiruthika,
Associate Professor,
Department of Computer Engineering,
Fr. C. Rodrigues Institute of Technology,
Sector 9A, Vashi, Navi Mumbai:400703
Tel: 022-41611000
Visit us@ www.fcrit.ac.in

DEPARTMENT VISION & MISSION

Vision:

To contribute significantly towards industry and research oriented technical education leading to self-sustainable professionals and responsible citizens.

Mission:

1. To provide quality and application oriented education to meet the industry requirements.
2. To prepare technically competent, ethically and socially committed professionals with good leadership qualities.
3. To facilitate an opportunity to interact with prominent institutes, alumni and industries to understand the emerging trends in computer technology.

The Program Educational Objectives (PEO's) for undergraduate program in Computer Engineering are listed below:

Graduates will be able to:

1. Excel in professional career and higher education in the thrust area of Computer Engineering.
2. Develop software products by adapting the trends in technology to solve real life problems.
3. Exhibit ethical practices, professional conduct and leadership qualities.

Program Specific Outcomes (PSOs)

At the end of Bachelor of Computer Engineering program, graduates will be able:

PSO1 - To comprehend, analyze and develop solutions in the areas of Web Technologies, Data Science, Networking and System Security.

PSO2 - To inculcate self-learning and research attitude for excelling in Software Development.

Program Outcomes (POs)

Engineering Graduates will be able to:

1. **Engineering knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
2. **Problem analysis:** Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
3. **Design/development of solutions:** Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
4. **Conduct investigations of complex problems:** Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
5. **Modern tool usage:** Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.
6. **The engineer and society:** Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
7. **Environment and sustainability:** Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
8. **Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
9. **Individual and team work:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
10. **Communication:** Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
11. **Project management and finance:** Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
12. **Life-long learning:** Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

FACULTY OF COMPUTER ENGINEERING DEPARTMENT

Sr.No.	Name of the Faculty	Designation
1.	Dr. Lata Ragha	Professor, Head of the Department
2.	Mrs. M.Kiruthika	Associate Professor
3.	Mr. Amroz Siddiqui	Assistant Professor
4.	Mrs. Smita Dange	Assistant Professor
5.	Mrs. Shweta Tripathi	Assistant Professor
6.	Mrs. Rakhi Kalantri	Assistant Professor
7.	Mrs. Sandhya Pati	Assistant Professor
8.	Mrs. Shagufta Rajguru	Assistant Professor
9.	Mrs. Dakshayani G	Assistant Professor
10.	Mrs. Kavita Shelke	Assistant Professor
11.	Mr. Mritunjay Ojha	Assistant Professor
12.	Mr. Rahul Jadhav	Assistant Professor
13.	Mrs. Nidhi R	Assistant Professor
14.	Ms. Arpita Raut	Assistant Professor

R & D PROJECTS

Sr. No	Fields of Research and Development
1.	Parallel Computing
2.	Data Science
3.	Data Mining
4.	Image Processing
5.	Advanced Networks
6.	Wireless Sensor Networks
7.	Mobile Applications
8.	Cyber Security and Digital Forensics

EVENTS ORGANIZED FOR STUDENTS BY COMPUTER ENGINEERING DEPARTMENT

Sr. No.	Name of the Seminar / Conference / Competition / Short Term Training Programme	Speaker	Convener
1.	**Project Poster Presentation** Competition for Final Year Projects		Mrs. Smita Dange
2.	**ACESS'2017** Seminar on "**Role of Technology in Environmental Issues**" Seminar on "**Solar storm and its effects on Earth**" Seminar on "**Approach towards higher studies and competitive exams**"	Dr. Bakul Rao Dr. P K Mohanty Mr. Ajay Pawar	Mrs. Shweta T
3.	**CRYPTEX'17** Workshops on : **a) Arduino** **b) Machine Learning** **c) Android** Competitions : **a) Decrypto** **b) Technical Treasure Hunt**	Conducted by Students of V Semester	Mrs. Shagufta R
4.	**ACESS'2018** Seminar on **"Cyber Security Awareness"**	Mr. Suresh Menon	Mrs. Shweta T
5.	Seminar on **"Project Management and Finance"**	Mr. Linto Kolanchery	

STTP / WORKSHOPS / CONFERENCES ORGANIZED BY COMPUTER ENGINEERING DEPARTMENT

Sr. No.	Name of the Seminar / Conference / Competition / Short Term Training Programme	Convener
1.	One week ISTE approved STTP on **"Machine Learning"** at Fr.C.R.I.T, Vashi from 2nd Jan to 6th Jan- 2018	**Convener :** Mr. Amroz S **Co-Convener :** Mr. Rahul J

FACULTYPUBLICATIONS*

Sr.No.	Name of the Faculty	National Conference	International Conference	International Journal
1.	Dr. Lata Ragha	13	48	40
2.	Mrs. M.Kiruthika	10	11	18
3.	Mr. Amroz S	02	-------	07
4.	Mrs. Smita Dange	09	07	08
5.	Mrs. Shweta Tripathi	06	03	08
6.	Mrs. Rakhi Kalantri	06	04	09
7.	Mrs. Sandhya P	04	02	13
8.	Mrs. Shagufta R	02	02	08
9.	Mrs. Dakshayani G	01	03	09
10.	Mrs. Kavita S	-------	02	09
11.	Mr. Mritunjay Ojha	01	04	09
12.	Mr. Rahul Jadhav	02	03	07

*- Till date

COMPETITIVE EXAM DETAILS

Year	Nature of examination	No. of Students	
		Appeared	Qualified
2017 – 2018	GATE	9	1
	GRE	7	7
	TOEFL	4	4
	MBA-CET	4	2

CAMPUS PLACEMENT 2017-2018

Sr.No.	Company	No. of Students Placed	Pay Package
1	TCS	36	3.36 Lacs
2	TCS (Differential)	1	6.3 Lacs
3	L & T INFOTECH	3	3.18 Lacs
4	INGRAM	4	3.8 Lacs
5	ATOS	4	3.1 Lacs
6	XORIANT	9	4.5 Lacs
7	HSBC	1	7 Lacs
8	TIAA	3	7 Lacs
9	ENVESTNET YODLEE	1	5.7 Lacs
10	ACS	1	2.10 Lacs
	Total	**63**	**3.82 Lacs(Average)**

PAPER PRESENTATIONS IN NATIONAL , INTERNATIONAL CONFERENCES AND INTERNATIONAL JOURNALS

Student Publications Record 2017-18			
Sr. No.	**Student Name**	**Paper Title**	**Details**
1.	Sanjana P K.V Maitreyi Merrill Gonsalves Kane Gonsalves	Implementation of a Navigation Application for the Visually Challenged	**International Journal** International Journal of Engineering Technology and Advanced Engineering. ISSN :2250-2459 ,Volume -7 Issue -10 ,October 2017 . Page No -137-140
2.	KanerePranali T.Sai Milind Shweta Patil KorolDhanda Waqar Ahmad	Gesture Glove	**International Journal** International conference on innovation and research in technology and Engineering organized by Padmabhushan Vasantdada Patil College of Engineering, Mumbai. Date -26th& 27th Oct 2017.
3.	Shruti Mahajan DevikaAntarkar Ryan Roy Manish Nagare	Deriving Insights and Analysis for Campaign Management	5th National Conference & Exhibition February 19th - 20th ,2018 Jointly Organized by Indian Institute of Technology, Kharagpur Govt. College of Engg. & Technology, Jammu Published in International Journal of Scientific and Technical Advancements ISSN: 2454-1532
4.	Aditya Vadhavkar Abhishek S Rishabh Patil Vaishnavi Patil	Unmute: an Android app for Deaf and Hard Hearing Students	**International Journal** International Journal of Computer Science and Engineering ,ISSSN-2347-2697 ,Volume5 –Issue 10 ,Page no 288-291. Oct 2017
5.	Danish Chaus Aayush Pathak Akshay Boramani	A Virtual Environment Forensic Tool	**International Journal** International Journal of Cyber Security and Digital Forensics , ISSN-2305-0012 , Page no-63-71
6.	Nixon Abraham Joshua Joseph Grace Marylyn Alveena Joseph	An Android Based Shopping Queue Reduction App Using NFC Technology	**International Journal** International Journal of Emerging Technology and Advanced Engineering ,ISSN : 2250-2459 ,Volume 7 ,Issue-11 ,November 2017 ,Pg No- 286 -289
7.	Sreya Fernandes Nisha Thomas Manisha Sharma Kevin Thomas	Vehicle Towing Automation System	**International Journal** International Journal of Research and Scientific Innovation . ISSN :2321-2705 ,Volume -4 ,Issue -1 ,January 2018,Page No -140-144
8.	Sanika Sawant Able Varghese Arun Koshy Yashashree Barhate	Enhanced Web Application Firewall using Machine Learning	**International Journal** International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, Volume-5 | Issue-1 , February 2018

9.	Kaustubh Yadav Blaze Rodrigues Thomas Chacko Amey Dixit	Blockchain Technology in Financial and Banking Sector	**International Journal** International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, Volume-5 | Issue-2 ,April 2018
10.	Elizabeth James Sachin George Vanessa Almond ShivomVishwakarm	Analysis of Electrical Power Consumption using Smart Meter Data"	**International Journal** International Research Journal of Engineering and Technology (IRJET) Volume 5, Issue 1 , January 2018
11.	Aditya Jadhav Swapnil Shinde Tanvi Rajadhyaksha Nirmal Menon	Analysis of Melanoma Skin Cancer	**International Journal** International Journal of Trend in Research and Development, (IJTRD), ISSN: 2394-9333, Volume-5, Issue-3, June 2018
12.	Sinimol Babu Darshana Chaudhari Nithin Jacob Alvina Malpan	eConf- A Generic Conference Management Tool	**International Conference** International Conference on Advanced Trends in Engineering" held in Datta Meghe Engg. College ,Airoli ,April 2018.ISBN:978-93-5267-422-0
13.	Shweta Patil Korol Dhanda T.Sai Milind Pranali Kanere Waqar Ahmad	Gesture Recognition Using Neural Network	3rd Biennial International Conference on Nascent Technologies in Engineering International Conference, Fr.C.R.I.T, Vashi
14.	Jude D'Silva Advaith Kamath Noble Kolarikkal Sanket Patil	Alexa Skill Development For Shop Floor	**International Journal** International Journal of Trend in Research and Development (IJTRD), Volume 5, Issue-2,Mar-April-2018, ISSN: 2394-9333, Pg.No.: 645-648
15.	Karishma Thakare Sherlyn Stanley Sharvari Mhatre Meghana Mathew	Sentiment Analysis of Tweets for Mapping of Stock Price Movement	**International Conference** International Conference on Advanced Trends in Engineering" held in Datta Meghe Engg. College ,Airoli ,April 2018.
16.	Madhavi M Radhika Kulkarni Harsh Singh Mahesh Reddy V	Automatic Classification of an Imbalanced Diabetic Retinopathy Dataset using Convolution Neural Networks	**International Conference** International Conference on Frontier in Engineering, Applied Science and Technology (FEAST2018),NIT Triruchirappalli
17.	Amey Gangal Stanely Nadar Aaron Mathew Fevin George	Live Data Forensics & Metadata	National Conference Recent trends in Cyber Frauds Investigations and Forensics held on 27th& 28th April 2018 organized by SIEM, Nashik, Maharashtra

STUDENT ACHIEVEMENTS

2017 – 2018			
Sr. No.	**Student Name**	**Title**	**Details with Positions held**
1	Felix Biju Deepti Paul Jithin Jose Leah Abraham	**Paper Title:** Free Space Optics System in Wireless Communication Technology	**First Prize: Cash prize of ₹3000** **Event:** National level Technical Paper Presentation held at RAIT, Nerul on 3rd October 2017
2	Fevin George Amey Gangal Aaron Mathews Stanley Nadar	Maharashtra State Level, Project Idea Presentation in Cyber Security	**First Prize: Cash prize of ₹2000** **Event:** Spectra'2017, held on Oct 03, 2017 at Zeal College, Pune.
3	Dheeraj Kallakuri Vinayak Kurup Madhura Dumbre Sharon Laurance Abhishek Roy	Project Presentation Competition. **Project title: PIBOT**	**Top 10 in the Competition** **Event:** Makers Square, Project Presentation Competition (Technovanza), held during 26-28 Dec, 2017 at VJTI, Matunga
4	Dheeraj Kallakuri Mohit Patil Madhura Dumbre	**Project title: PIBOT**	**I Prize: Cash prize of ₹2000/-** **Event:** Colloquim-2k18, Technical Fest, SFIT, Mumbai held on 19-20 Jan, 2018
5	Dheeraj Kallakuri Vinayak Kurup Madhura Dumbre Sharon Laurance	Project Presentation Competition. **Project title: PIBOT**	**First Prize: Cash Prize of ₹2500/-** **Event:** Project Mania (Spectra-2018), Project Presentation Competition, SPCE, Andheri held on 27th Jan, 2018
6	Dheeraj Kallakuri Vinayak Kurup Madhura Dumbre Sharon Laurance	Technical Paper Presentation **Paper Title: PIBOT: A Server controlled BOT**	**First Prize: Cash Prize of ₹2000/-** **Event:** National level Technical Paper Presentation, Alegria, held in Pillai's College of Engineering, Panvel on 6th Feb 2018.
7	Dheeraj Kallakuri Vinayak Kurup Madhura Dumbre Sharon Laurance	Project Competition **Project title: PIBOT**	**Best Student Project** **Event:** Computer Society of India-Mumbai (CSI) in association with FOSSEE & Spoken Tutorial, IIT Bombay hosted a 2-day Annual Industry and Academia Conference and Awards "TechNext India 2018" during 10th - 11th, Feb 2018, at Victor Menezes Convention Centre, IIT Bombay.
8	Felix Biju Akhil M. Ashley Antony	Technical Paper Presentation **Paper Title:** Human Area Networking: Red Tacton and its Applications	**First Prize** **Event:** CSI-Mumbai in association with FOSSEE & Spoken Tutorial, IIT Bombay hosted a 2-day Annual Industry and Academia Conference and Awards "TechNext India 2018" during 10th - 11th, Feb 2018, at IIT Bombay. **Pre-Event** of TechNext India 2018: National level Technical Paper Presentation, held at FCRIT, Vashi.

9	Manish Manepalli Kartik Jain Noble Kolarikkal Jude D'silva	Project Competition **Project Title**: Recognition of occluded faces. 65 teams from Mumbai University colleges had participated.	**2nd Runner up:** **Cash Prize of ₹25,000** **Event:** Deep Blue Project Competition held by Mastek Majesco.
10	Manish Manepalli Kartik Jain Noble Kolarikkal Jude D'silva	Inter College Festival **Project Title:** Recognition of occluded faces.	**1st Prize: Cash Prize of ₹5000.** **Event:** Inter College Festival Etamax-18 organized by FCRIT, Vashi on 23rd Feb, 2018
11	Robin Jaison Akshay Bhosale Gloria Benny Adil Khot	Inter College Festival **Project Title:** Golden Hour Response	**2nd Prize: Cash Prize of ₹2500/-** **Event:** Inter College Festival Etamax-18 organized by FCRIT, Vashi on 23rd Feb, 2018
12	Manish Manepalli Kartik Jain Noble Kolarikkal Jude D'silva	National Level Project Competition **Project Title:** Recognition of occluded faces.	**1st Prize: Cash Prize of ₹10000.** **Event:** Avlon2K18, National Level Project Competition held by Terna Engg College, Nerul on 14th March, 2018
13	Nisha Mariam Manisha Sharma Sreya Fernandes Fevin Thomas	National Level Project Competition **Project Title:** Vehicle towing automation system.	**2nd Runner up:** **Cash Prize of ₹1000.** **Event:** Avlon2K18, National Level Project Competition held by Terna Engg College, Nerul on 14th March, 2018.
14	Sachin George Vanessa Almond Tanvi Rajadhyaksha Aditya Jadhav Advaith Kamath Swapnil Shinde	Smart India Hakathon-2018 **Topic:** Detecting anomalies in ship trajectory for Ministry of Defence	**1st Runner up:** **Cash Prize of ₹75000.** **Event:** Smart India Hakathon-2018 during 30th and 31st March 2018 at Bangalore.
15	Pranali Kanere	**TCS Best Outgoing Student for the Year 2017-18**	
16	Ashish Dsa, Pearl Alex Sajeet F Jenson Mandy	**TCS Best Project for the Year 2017-18 titled "Drones for assistance in emergency situations"**	
17	Fevin George Amey Gangal Aaron Mathews Stanley Nadar	National Conference **Title:** Live Data Forensics and Metadata Analysis.	**First Prize** **Event:** National conference on Cyber Frauds Investigations and Forensics held on 27-28, April 2018 at Sandip Institute of Engineering, Nashik.
18	Gyandeep Akash Maurya Shrinidhi K.V Gloria	Govt. of Maharashtra Hakathon-2018 **Topic:** Prediction of Disease Spreading	**Fourth Prize: Cash of Rs.25000/-** Trident Hotel on 2nd June 2018 (30 HRS)

SEMESTER- VIII (2017 – 2018)

PROJECT POSTER PRESENTATION WINNERS(P-CUBE)

PROJECT		
	PROJECT TITLE	**TEAM MEMBERS**
I PRIZE	Drones for Assistance in Emergency Situations	Jenson Mandy
		Ashish D'sa
		Pearl Alex
		Sajeet Francis
II PRIZE	Screening of Diabetic Retinopathy using Machine Learning	Mahesh Reddy V
		Harsh Singh
		Radhika Kulkarni
		Madhavi Madangopal
	Analysis of Melanoma Skin Cancer	Aditya Jadhav
		Swapnil Shinde
		Tanvi Rajadhyaksha
		Nirmal Menon
III PRIZE	Automation of the currently implemented towing system	Manisha Sharma
		Sreya Fernandes
		Nisha Mariam Thomas
		Kevin Thomas Joseph
	Enhanced Web Application Firewall using Machine Learning	Able Varghese
		Arun Koshy Shaji
		Yashashree Barhate
		Sanika Sawant

POSTER		
	PROJECT TITLE	**TEAM MEMBERS**
I PRIZE	Analysis of Melanoma Skin Cancer	Aditya Jadhav
		Swapnil Shinde
		Tanvi Rajadhyaksha
		Nirmal Menon
II PRIZE	Enhanced web Application firewall using Machine Learning	Able Varghese
		Arun Koshy Shaji
		Yashashree Barhate
		Sanika Sawant
	Sentiment Analysis of Twitter Data for Prediction of Stock Market Movement	Karishma Thakare
		Sherlyn Stanley
		Sharvari P Mhatre
		Meghana Sereen Mathew
III PRIZE	Screening of Diabetic Retinopathy using Machine Learning	Mahesh Reddy V
		Harsh Singh
		Radhika Kulkarni
		Madhavi Madangopal

MODEL		
	PROJECT TITLE	**TEAM MEMBERS**
I PRIZE	Analysis of use Consumption Patterns using smart-meter Data	Elizabeth James
		Sachin George
		Vanessa Almond
		Shivom Vishwakarma
II PRIZE	E-conf: A Conference Management Tool	Sinimol Babu
		Darshana Chaudhari
		Nithin Jacob
		Alvina Malpan
	Live data forensics and meta data extraction	Amey Gangal
		Fevin George
		Aaron Mathews
		Stanley Nadar
III PRIZE	Air Pollution Monitoring and Analysis in industrial commercial and Residential areas of Navi Mumbai	Anuja Patole
		Shruti Jagtap
		Janardan Subhedar
		Victor Hembrom

SEMESTER- V (2017-2018)

SUMMER PROJECT PRESENTATION WINNERS

	PROJECT TITLE	TEAM MEMBERS
I PRIZE	Vehicle Theft Detection (Car Spy)	Deepti Paul
		Felix Biju
		Frezy Roy
		Jithin Jose
II PRIZE	PIBOT	Vinayak Kurup
		Madhura Dumbre
		Dheeraj Kallakuri
		Sharon Laurance
	Smart Drive	Annapurna Pandita
		Sheldon Karkada
		Rohan Dominic
		Sarath Sasidharan
III PRIZE	Smart Pantry System	Leo Varghese
		Lijo P Varghese Jose
		Sujith Amin
		Pheba Babu
	Queue Reduction System(Canteen APP.)	Shanita Sojan
		Robin Jaison

ARTWORK OF THE STUDENTS

-Nikhil Londhe(T.E.-Comp)

-Sreya Fernandes(B.E.-Comp)

-Tanisha Mittal(T.E.-Comp)

Know Why Your Smart Phone is Suspicious

While smartphones are the epitome of modern convenience, the dirty little secret is that these omnipresent devices, which we have with us 24X7, and keep switched on for most of that time, are also a serious threat to our privacy. Here's why:

1. Geotracking

A key feature of a smartphone is its ability to locate itself, via multilateration (a surveillance technique) to cell towers, or the integrated GPS chip. Even if you disable the GPS on your phone, it can be tracked via other sensors. While disclosing location data may seem harmless, it can be used for a phishing attack.

2. Malicious apps

Smartphone apps often ask for more information than is required. And we willingly provide this when we agree to the app permissions. We should at least be a little more suspicious why that new game needs access to our contacts, GPS and camera, and download apps from reputable sources only.

3. Wi-Fi tracking

Free Wi-Fi connection, while convenient, is too often in reality an invasion of privacy. The features that make Wi-Fi hotspots desirable to you also make it desirable for hackers; since it requires no authentication to establish a network connection. This allows hackers to get access to unsecured devices on the network.

4. Lack of antivirus software

Everyone accepts that their PC needs additional security, and so they download and install antivirus software. But the necessity of antivirus software is not as clear to most smart phone users, despite the amount of personal info the phones contain.

5. Your camera could be watching you

Smartphone cameras are also a security risk, as they can be activated and used to spy on the owner. Notorious hacker and author Kevin Mitnick says that this can be done by either installing software on the phone via physical access, or via a remote exploitation.

6. Microphone eavesdropping

Every smartphone has a microphone, and it's another security risk. While the main concern for many of us may be someone eavesdropping on private conversations, microphones also can be used for data collection.

7. Lack of security patches

Weekly security patches are a fact of life for Windows users, but when it comes to phones, while things are better for iOS and the Apple camp in general, there's a lack of updates for Android, and not everyone will be running the latest version of Android at a given time.

8. Beware of the backdoor

The Chinese have allegedly engineered a backdoor into smartphones from some manufacturers. This has recently led the US intelligence agencies to recommend that Americans do not purchase smartphones from those manufacturers. The concern is that users' data could be shared with a foreign government via a backdoor.

Source:*https://economictimes.indiatimes.com/tech/internet/beware-the-spy-is-right-in-your-pocket/articleshow/63449956.cms?utm_source=WAPusers&from=mdr*

-Shweta Tripathi,
Assistant Professor
Computer Engineering Department

A thing or two about Docker

Deployment: A pain in itself

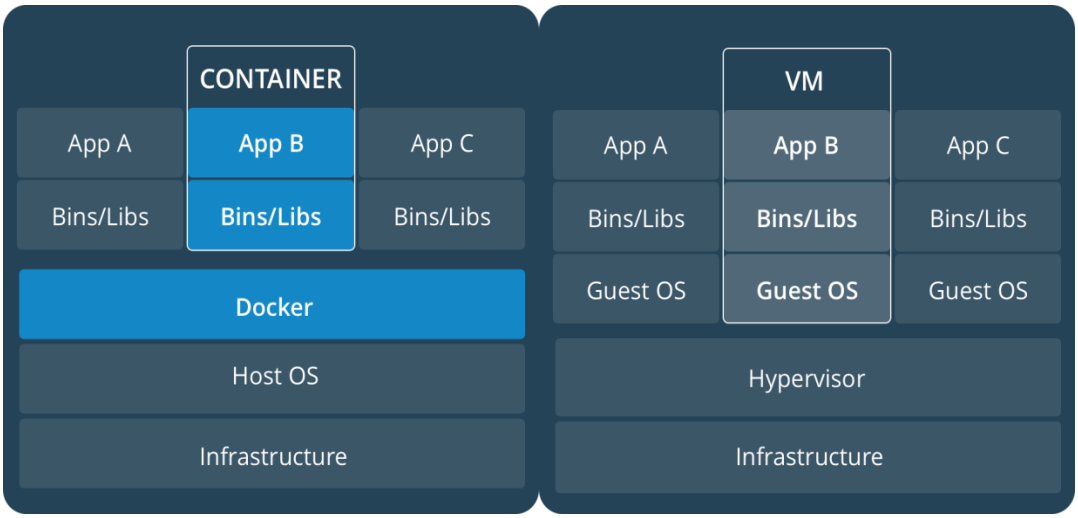
One of the biggest issues in software development is not creating it, but getting it to work everywhere. We've all heard of the phrase 'It works on my computer'. Keeping track of what settings were used in the dev environment is really challenging. Think about it, trying to remember what password you used for this database is a real pain, especially when you set up the database a while ago.

The solution

One of the earlier solutions to this problem was taking a VM, installing your environment and then shipping it. Sounds good and even worked for a while. The problem here was that VMs are just too big. It took up a lot of space on hosting even if the storage was dynamically growing. Simply too big for a small application. Also getting multiple VMs to work together was a little difficult to the point that people lose interest in it. What the devs needed was a fast way to spin up a VM and get to work as fast as possible. Enter Docker. Docker is a containerization platform, i.e. it helps to build containers, which are lightweight VMs

Containers vs VMs

A container is an abstraction that packages code and dependencies together, multiple containers can run on a single machine. Up until this point containers sound similar to VMs. This is true except that, the fundamental difference is that a container shares the kernel of the host OS, whereas a VM does not. As a result, containers take up much less space as compared to VMs A VM on the other hand is an abstraction of physical hardware. This creates a completely new hardware platform for each VM. Since the abstraction provided is of the hardware, a complete OS must be installed. This takes up a lot of space. This is where containers triumph over VMs.



Docker Compose Docker compose is a tool from docker for defining and running multi-container Docker applications. For example, I have a website for showing me curated fine dining. Let's think about what all we need to create the website. First off a web server, then a database, maybe also an external session storage. For each of these entities I can create a container and then tie them together. Docker compose allows me to define and tie containers together in a docker compose file which is of YAML format. Using Compose takes 3 steps:

1. Create a Dockerfile to create the environment of your choice (Usually this step is rarely done as a lot of pre-made images already exist)
2. docker-compose.yml file for defining all the services which your application requires
3. docker-compose up command to create it. That's how simple it is.

Here's an example of a Dockerfile

1.
```
#
# Simple example of a Dockerfile
#
FROM ubuntu:latest
MAINTAINER Dylan Dsouza "dsouzadyn@gmail.com"
RUN apt-get update
RUN apt-get install -y python python-pip wget
RUN pip install Flask
ADD hello.py /home/hello.py
WORKDIR /home
```

2. And here is an example of a docker-compose.yml file.

```
version: '2'

services:
  web:
    build: .
    ports:
     - "5000:5000"
    volumes:
     - .:/code
  redis:
    image: redis
```

The situation today

Containers are the future. A lot of companies have adopted this method of deployment as it is much easier and gives the developer full control over his/her application. One major factor is the reduction of hosting costs. Containers make the whole dev-ops business a whole lot transparent and the developer community likes that. Containers are here to stay, until another groundbreaking technology comes along. It's safe to say that won't happen for quite some time.

-Dylan Dsouza
(T.E-Comp)

Smart India Hackathon-2018

Smart India Hackathon (SIH) is an initiative by the HRD ministry of India to invest in the best minds of this country. It is a competition that empowers the students to tap into their potential and use their technological skills to develop products that can be adopted and implemented by various central ministries. It is world's largest Nation-Building Digital Initiative.

340 problem statements from 27 ministries and 17 state governments had been chosen for the Hackathon this year and were displayed on MyGov platform. A whopping number of over 17400 teams had submitted their abstracts of the proposed solutions to the problems. In all around a lakh of students of Engineering, Management and MCA had participated. 1296 teams were selected to compete in the two-day Grand Finale of SIH 2018, beginning on March 30.

The Grand Finale was held across 28 nodal centers in the country. First was the inaugural ceremony, which was graced by a number of dignitaries. Video-speeches by the AICTE Co-Chairman, Dr. Anand Deshpande and the AICTE Chairman, Prof. Anil Sahasarabuddhe exhorted the finalists to expand their horizon and innovate. The honorable minister of HRD, Shri Prakash Javadekar imparted a few words of wisdom and boosted their morale. Finally, he announced the commencement of SIH 2018. At 8:30 am, the Grand Finale went live.

It was a 36 hour Hackathon. All the finalists got their acts together and started to code. They worked with full focus and concentration. Each team had one or two mentors to guide them in achieving the perfect solution. There was a round of training session, in which the ministry trainers monitored the progress of the teams. They then offered their suggestions and ideas on the new features that could be added to make the product better. There were a number of breaks in between, for the finalists to replenish their energy reserves. Tea and snacks were regularly served at the table. The first round of

evaluation was conducted almost after 12hours, since the beginning of Hackathon. A panel comprised 3 judges. Each team was given 4 minutes to present its work and 3 minutes for Q&A session.

At 8 pm, the honorable Prime Minister of India, Shri Narendra Modi addressed the finalists. He advocated IPPP as the driving force behind innovation. IPPP stood for 'Innovate, Patent, Produce and Prosper.' He also emphasized, "Nobody is blessed with all the knowledge in the world. This applies to governments too... the biggest mistake governments make is to think they alone can bring about change. What brings about change is participative governance". The Prime Minister was keen on involving the youth in India`s quest for change and progress. He asserted that what the young minds are doing today will benefit the nation in the coming years.

The finalists had prepared themselves physically and mentally to skip their sleep. In the overnight phase, a special Zumba activity was conducted, so that all could let go for a short while, enjoy and then return to coding with freer minds. Another round of training was conducted, which was similar to the first session. Early morning, a 15 minute Yoga session was conducted to calm the tense minds.

The clock was ticking. All the teams had begun to reach the completion of their development of products. Soon the second round of judging followed. And then the final session of training. With the last few hours left, everyone anxious and excited at the same time, slogged to make the final changes.

It is 3 'o' clock. "Stop coding!" , comes a call.

All got their hands off their laptops. Time for the final judging round. For this round, the team had fifteen minutes to talk about their development. After an hour, the results were announced. Based on the scores of evaluation rounds, 10 teams were shortlisted for power judging round. In this round, each team had 4 minutes to describe their product.

In the valedictory session, all the judges of Hackathon were honored. Each team was felicitated. The top 4 winning teams for each center were announced accordingly. Their projects would be implemented by the respective ministries by the end of April or mid- May 2018. SIH-2018 had been concluded with the National Anthem.

SIH-2018 is an excellent opportunity for the Indian youth to explore and sharpen their coding skills and technical knowledge. If these are used in a way, smart and creative, products can be made such that they change the businesses. And revolutionize the Indian Economy.

-Annapurna Pandita(T.E.-Comp)

Search Engine Optimization Using Data Mining

Piyush Kurkure[1], Leah Abraham[2], Adil Khot[3]
Department of Computer Engineering, Fr. C. Rodrigues Institute of Technology, Vashi, Navi Mumbai
[1]piyushk10@gmail.com
[2]abrahamleah3997@gmail.com
[3]adilkhot81@gmail.com

***Abstract*-- In this fast-moving world, the demands for faster results have increased greatly as well as the number of available Web pages are growing day by day, thus it is becoming more difficult for users to find documents relevant to their interests. Search Engine Optimization is the procedure used to improve the visibility of the results searched for by using a search engine like Google, Bing etcetera. The result displayed is based on a certain set of conditions the website ought to satisfy to be given a higher priority in the search result. This involves a lot of processing and thus consumes a lot of processor time. In this paper we propose the 'K mean' algorithm of data mining to create a distributed design approach which reduces both processor time and processor effort. The traditional search engine uses content-based matching for the process of searching. Using 'K means algorithm' we can make search engines user friendly and reliable as it is based on Clustering which means classification of a data set into subsets (clusters), so that the data in each subset share some common attributes – mostly according to some defined distance. the 'K number of distinct clusters are identified by a set of points that are called the cluster centres and these data points are mapped to the cluster whose centre is closest from its position.**
Thus, now when we perform any search, only the relevant clusters related to that search string's keywords are processed and results are displayed faster.
Keywords: k means algorithm, data mining, content-based matching, distributed design, clustering

I. INTRODUCTION

Search engine optimization (SEO) is the practice of increasing the quantity and quality of traffic to your website through organic search engine results. Initially searching for content on the web was based on keywords but now we use page ranks for searching purposes which reduces the time taken for searches and increases the chances of your website to be placed at a higher rank based on the page rank provided. PageRank (PR) is an algorithm used by Google Search to rank websites in their search engine results.

According to Google:

"PageRank works by counting the number and quality of links to a page to determine a rough estimate of how important the website is. The underlying assumption is that more important websites are likely to receive more links from other websites[1]".

How SEO works is analogous to how a website does. Here we can think of a search engine as a website we visit to type a question into a box and Google, Yahoo!, Bing, or whatever search engine you're using magically replies with a long list of links to webpages that could potentially answer your question. Here's how it actually works : Google (or any search engine you're using) has a crawler that goes out and gathers information about all the content they can find on the Internet. The crawlers bring all those 1s and 0s back to the search engine to build an index. That index is then fed through an algorithm that tries to match all that data with your query. Thus, fulfilling our request for the given data.
Data mining is the process of sorting through large data sets to identify patterns and establish relationships to solve problems through data analysis. Data mining tools allow enterprises to predict future trends.

Data mining that is inclusive of Information science connected to on-page enhancement is a noteworthy theme, as great Web optimization not just enhances your natural movement (because of better presentation to google) additionally builds change rates. Conventional Website optimization apparatuses accessible, have been in essence, information science items.

On the off chance that you are searching for an information science extend for Website design enhancement you can utilize Google items to gather the information, separate it through their APIs or rub them straightforwardly. On the other hand, you can slither your own particular site.

II.OVERVIEW

A. History of SEO

A difficult problem with writing a history of search engine optimization (SEO) is the obscure etiology of its birth. By default, the term search engine optimization implies a relevant history must be considered after the development of search engines. A troublesome aspect of this implication is the fact that search engines and the Internet did not always have their modern form. For example, the Internet arguably can trace its roots back to 1958 when AT&T introduced the first commercial modem, enabling remote computers to communicate over ordinary telephone lines. SEO symptomatically grew out of the development of search engines and the World Wide Web. As natural language search capabilities were designed in search engine tools, relevancy of ranked results was discovered to have significance on traffic coming to web pages. Rather than the web just being a collection of shared files, the World Wide Web opened up concepts of e-commerce and internet marketing. With new avenues of sales to be gained, companies found value in creating and promoting their websites.

B. Data mining

There is a huge amount of data available in the Information Industry. This data is of no use until it is converted into useful information. It is necessary to analyze this huge amount of data and extract useful information from it. Extraction of information is not the only process we need to perform; data mining also involves other processes such as Data Cleaning, Data Integration, Data Transformation, Data Mining, Pattern Evaluation and Data Presentation. Once all these processes are over, we would be able to use this information in many applications such as Fraud Detection, Market Analysis, Production Control, Science Exploration, etc. Data Mining is defined as extracting information from huge sets of data. In other words, we can say that data mining is the procedure of mining knowledge from data[2].

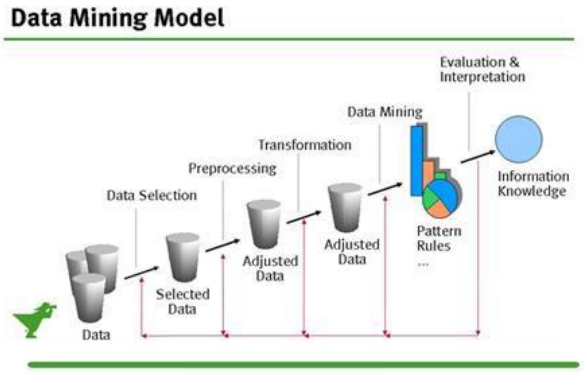


Fig. 1: Block diagram of Data Mining Model

C. How is SEO implemented using data mining?

Internet is an immense, huge and dynamic data collection that includes infinite hyperlinks and volumes of data usage information-hence requires effective data mining. But huge data is still a challenge in knowledge discovery. Web pages are more complex than text data: Web pages have dynamic data and do not follow any uniform structure. Web pages contains huge amount of raw data that is not indexed therefore searching in web data has become more complex; time consuming and difficult[3]. The Web constitutes high quantity of dynamic information: Web not only contains static data but also data that requires timely updating such as news, stock markets, live channels etc. Web users include different kinds of user communities: People from different communities have different backgrounds and use internet for different usage purposes. Many have different interests and lack knowledge of internet usage. Hence user gets lost within huge amount of data. Only a small portion of the Web's pages contain truly relevant information: A given user generally focuses on only a tiny portion of the Web, dismissing the rest as uninteresting data that serves only to swamp the desired search results.

Fig. 2: The SEO using Data Mining

D. Web crawlers and indexers

A web crawler (also known as a web spider or web robot) is a program or automated script which browses the World Wide Web in a methodical, automated manner[4]. Web crawlers can copy all the pages they visit for later processing by a search engine that indexes the downloaded pages so that users can search them faster. A web crawler starts with a list of URLs to visit, called the seeds. As the crawler visits these URLs, it identifies all the hyperlinks in the page and adds them to the list of URLs to 'visit' that list is called the crawl frontier. URLs from the frontier are recursively visited according to a set of policies. If the crawler is performing archiving of websites, it copies and saves the information as it goes. Those archives are usually stored in a way, so they can be viewed, read and navigated as if they were on the live web, but are preserved as "snapshots". The indexer processes the pages crawled by the crawler. First, it chooses which pages to index, for instance, it might discard duplicate documents, and then it creates different auxiliary data structures. Most search engines build some variant of an inverted index data structure for the word "text index" and links "structure index"". The inverted index contains for each word a sorted list of couples, such as doc ID and position in the document. It's particularly designed and optimized for indexing files. Using the index built by the indexer, the search engine can access almost directly to sections of the database which contains the information a user is looking for. Search engine ranking depends a lot upon the website indexing. The more the number of website's web pages included (indexed) by search engine, the better the ranking.

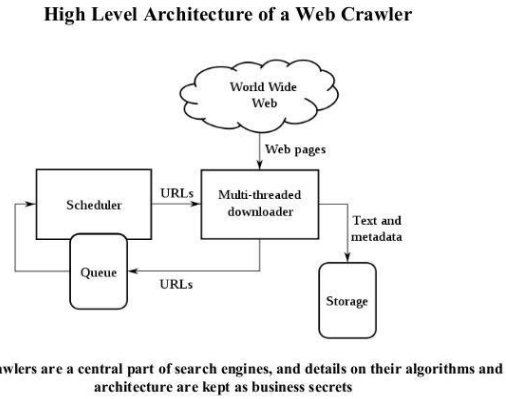


Fig. 3: Standard Architecture of a Web Crawler

E. Clustering

A loose definition of clustering could be "the process of organizing objects into groups whose members are similar in some way". A *cluster* is therefore a collection of objects which are "similar" between them and are "dissimilar" to the objects belonging to other clusters.
The goal of clustering is to determine the intrinsic grouping in a set of unlabelled data. But how to decide what constitutes a good clustering? It can be shown that there is no absolute "best" criterion which would be independent of the final aim of the clustering. Consequently, it is the user which must supply this criterion, in such a way that the result of the clustering will suit their needs. In some cases, we can easily identify clusters into which the data can be divided based on *distance*: two or more objects belong to the same cluster if they are "close" according to a given distance (in this case geometrical distance). This is called "distance-based clustering".

Another kind of clustering is "conceptual clustering": two or more objects belong to the same cluster if this one defines a concept common to all that objects. In other words, objects are grouped according to their fit to descriptive concepts, not according to simple similarity measures [5].

III.K-MEANS ALGORITHM

K-Means is an unsupervised learning algorithm that solves the well-known clustering problem. The procedure follows an easy way to classify a given data set through a certain number of clusters (assume k clusters) fixed with a priority. The main idea is to define k centroids, one for each cluster. These centroids should be placed in a smart way because their location causes different result [6]. So, the better choice is to place them as much as possible far

away from each other. The next step is to take each point belonging to a given data set and associate it to the nearest centroid. When no point is pending, the first step is completed, and an early groupage is done. At this point we need to re-calculate k new centroids as barycenter's of the clusters resulting from the previous step. After we have these k new centroids, a new binding has to be done between the same data set points and the nearest new centroid. A loop has been generated. As a result of this loop we may notice that the k centroids change their location step by step until no more changes are done. In other words, centroids do not move any more. Finally, this algorithm aims at minimizing an *objective function*, in this case a squared error function. The objective function

$$J = \sum_{j=1}^{k} \sum_{i=1}^{n} \left\| x_i^{(j)} - c_j \right\|^2 ,$$

Fig. 4: Standard Architecture of a Web Crawler

where $\|x_i^{(j)} - c_j\|^2$ a chosen distance measure between a data point $x_i^{(j)}$ and the cluster centre c_j, is an indicator of the distance of the *n* data points from their respective cluster centres[7].

The algorithm is composed of the following steps:

i. Place k points into the space represented by the objects that are being clustered. These points represent initial group centroids.

ii. Assign each object to the group that has the closest centroid.

iii. When all objects have been assigned, recalculate the positions of the k centroids.

iv. Repeat Steps ii and iii until the centroids no longer move. This produces a separation of the objects into groups from which the metric to be minimized can be calculated.

IV. CLUSTERING USING WEKA TOOL

As of now, we all are familiarized by various techniques of search engine optimization, a popular data mining technique (Cluster Analysis) is used to analyse and study crucial aspects of SEO that will be beneficial for webmasters. In this paper, a well-known tool Weka is used to create clusters in K-Means analysis[8]. It contains a collection of algorithms and visualization tools for predictive modelling and data analysis together with graphical user interfaces for easy access. Clustering is the task of grouping a set of objects in such a way that objects in same category (cluster) are more similar to each other than to those in other categories (clusters). In SEO, we use k-means algorithm where 6 clusters are created using Weka 3.6 by simply testing different parameter settings depending on the research data set and expected use of the results. All the missing values are adjusted by the algorithm automatically so as to get the expected results.

Different clusters are filled with data depending upon the attribute values as per observed during research. Now observing these results, it is easier to find some SEOT for improving rank of webpage in search engine result page.

Now as the user inserts any input that input is adjusted according to these attributes to any of these clusters and then accordingly the web results are shown in ranks. So, by inserting any input, the search engine frames itself into type of cluster it wants to insert and accordingly the result page is shown in ranks.

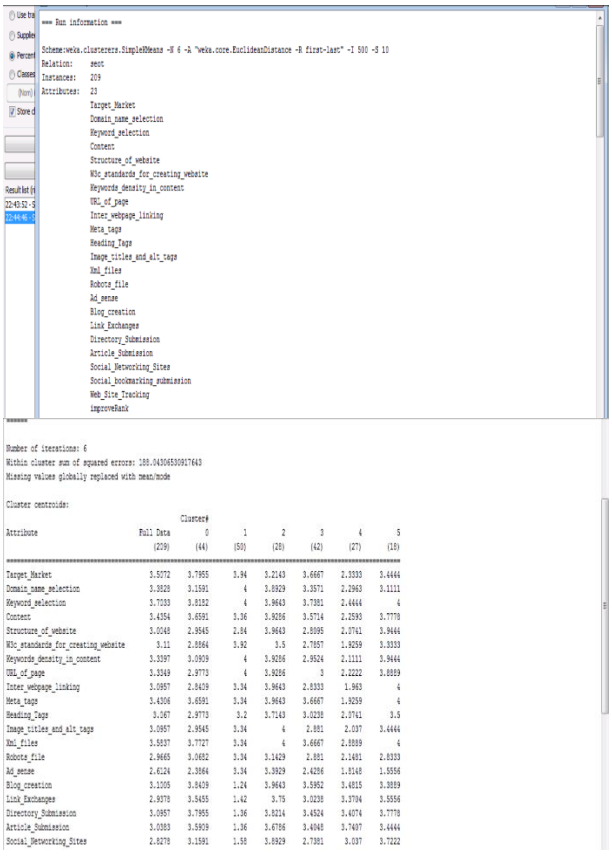


Fig. 5: Result of K means algorithm

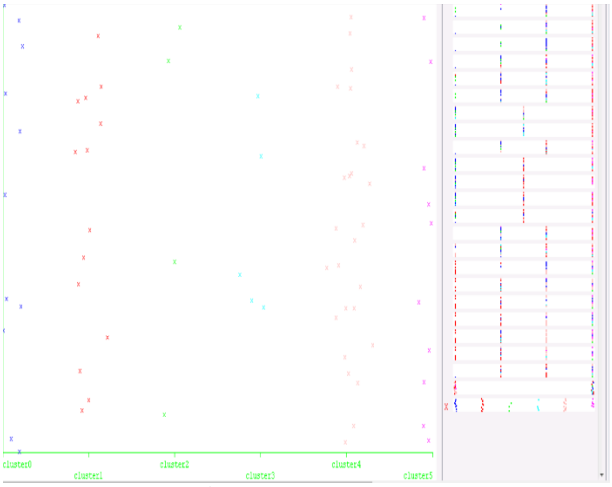


Fig. 6: Visualization of K means algorithm

V. CONCLUSION

Search engines are programs which find documents for specified keywords during the search for information on the World Wide Web and return with a list of the documents where the keywords were found. In this paper we included the study of the search engine Google, which includes an automated crawler, that can follow the links found on a site and an indexer, which builds an index of all the search terms found in the pages. The research aims to improve the search time of search engines to the greatest extent using the K-Means Algorithm, which does the clustering of the database. It is found that the algorithm produces better results without the clustering. As the size of data increases, the time used in searching is affected as search time increases to a great extent and the search process becomes slower. The MPAPI technique with the K-Means is used to solve the delay problem during search. Using this technique, search takes place in more one cluster in parallel. Each thread can connect to its own case; connection takes place through messages not by state transfer between threads. A system using K-Means with MPAPI to improve the search engine gives a good product and is not affected by increasing the number of keywords unlike the normal search engine. Such a system will reduce time taken in clustering of data.

REFERENCES

[1]https://en.wikipedia.org/wiki/PageRank#cite_note-2
[2]https://www.tutorialspoint.com/data_mining/dm_quick_guide.htm
[3] International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Web Site: www.ijettcs.org Email: editor@ijettcs.org
[4] https://www.sciencedaily.com/terms/web_crawler.htm
[5] https://home.deib.polimi.it/matteucc/Clustering/tutorial_html/
[6]https://www.ripublication.com/irph/ijict_spl/04_ijictv3n6spl.pdf
[7]https://home.deib.polimi.it/matteucc/Clustering/tutorial_html/kmeans.html
[8] http://www.ijcea.com/wp-content/uploads/2015/08/20-Khattab-O.-Khorsheed.pdf

Honeypot: Intrusion Detection

Sibi Biju[1], Aleena George[2]
Department of Computer Engineering, Fr. C. Rodrigues Institute of Technology, Vashi, Navi Mumbai
[1]sibibiju97@gmail.com
[2]aleenageorge117@gmail.com

***Abstract*-- The ever-rising attacks on the internet causes threat issues which makes it mandatory to keep the security system to detect them and block them. Traditionally information security has been defensive: firewall, intrusion detection/ prevention systems and encryption. Honeypots take an offensive security approach. It makes intrusion ineffective and strengthens defense tools. Honeypots can initiatively lure hackers to attack the internet, take a record of the ways and means of their invasion, and then analyze and study them. The concept basically is a trap to catch malicious network activity with a specifically prepared machine. The unwary intruder will have access to the system based on the type and purpose of the trap. Honeypot will proactively gather information about security threats by providing a real system with real applications and services to the attacker for interaction but with no production value. The actions of the intruder can be safely monitored without fear of compromising the system. The ability of Honeypots has been tested and its limitations and aspects to be improved have been identified. This trend for early prevention can be used in future so as to be able to take pre-emptive action before it does any unexpected harm to the system security.**

***Keywords*-- Honeypot, intrusion detection, system security.**

I. INTRODUCTION

The goal of an Intrusion Detection System (IDS) is to "identify, preferably in real time, unauthorized use, misuse, and abuse of computer systems by both system insiders and external penetrators"[1]. An IDS is used as an alternative (or a complement) to building a shield around the network. The shielding approach is deficient in several ways, including failure to prevent attacks from insiders. The exact definition of a honeypot is contentious, however most definitions are some form of the following: A honeypot is an "an information system resource whose value lies in unauthorized or illicit use of that resources"[2]. A more practical, but more limiting, definition is: "A server that is configured to detect an intruder by mirroring a real production system. It appears as an ordinary server doing work, but all the data and transactions are phony. Located either in or outside the firewall, the honeypot is used to learn about an intruder's techniques as well as determine vulnerabilities in the real system" [3]. In practice, honeypots are computers which masquerade as unprotected. The honeypot records all actions and interactions with users. Since honeypots don't provide any legitimate services, all activity is unauthorized (and possibly malicious). Honeypots as being analogous to the use of wet cement for detecting human intruder. The first publicly available honeypot was Fred Cohen's Deception Toolkit in 1998 which was "intended to make it appear to attackers as if the system running DTK [had] a large number of widely known vulnerabilities" [4]. More honeypots became both publicly and commercially available throughout the late nineties. As worms began to proliferate beginning in 2000, honeypots proved imperative in capturing and analysing worms. In 2004, virtual honeypots were introduced which allow multiple honeypots to run on a single server [5].

II. CLASSIFICATION

A. Based on deployment

Based on deployment, honeypots may be classified as:

1) Production honeypots: These are easy to use, capture only limited information, and are used primarily by companies or corporations. Production honeypots are placed inside the production network with other production servers by an organization to improve their overall state of security. Normally, production honeypots are low-interaction honeypots, which are easier to deploy. They give less information about the attacks or attackers than research honeypots do.

2) Research honeypots: They are run to gather information about the motives and tactics of the Blackhat community targeting different networks. These honeypots do not add direct value to a specific organization, instead, they are used to research the threats organizations face and to learn how to better protect against those threats. Research honeypots are complex to deploy and maintain, capture extensive information, and are used primarily by research, military, or government organizations.

B. Based on level of interaction

There are two broad categories of honeypots available today, high-interaction and low-interaction. These categories are defined based on the services, or interaction level, provided by the honeypot to potential hackers. Some authors classify a third category, medium-interaction honeypots, as providing expanded interaction

from low-interaction honeypots but less than high interaction systems.

1)High-interaction honeypots: It let the hacker interact with the system as they would any regular operating system, with the goal of capturing the maximum amount of information on the attacker's techniques. Any command or application an end-user would expect to be installed is available and generally, there is little to no restriction placed on what the hacker can do once he/she comprises the system.

2)Low-interaction honeypots: It present the hacker emulated services with a limited subset of the functionality they would expect from a server, with the intent of detecting sources of unauthorized activity [5]. For example, the HTTP service on a low-interaction honeypot would only support the commands needed to identify that a known exploit is being attempted.

3)Medium-interaction honeypot: It might more fully implement the HTTP protocol to emulate a well-known vendor's implementation, such as Apache. However, there are no implementations of a medium-interaction honeypots and for the purposes of this paper, the definition of low-interaction honeypots captures the functionality of medium-interaction honeypots in that they only provide partial implementation of services and do not allow typical, full interaction with the system as high-interaction honeypots.

Level of Interaction	Work to Install and Configure	Work to Deploy and Maintain	Information Gathering	Level of Risk
Low	Easy	Easy	Limited	Low
Medium	Involved	Involved	Variable	Medium
High	Difficult	Difficult	Extensive	High

Fig. 1: Trade-offs of Honeypot level of interaction

III. ADVANTAGES AND DISADVANTAGES

Unlike mechanisms such as firewalls and intrusion detection systems, a honeypot does not address a specific problem. Honeypot is used as a decoy or act as an add-on to the existing security systems. It cannot operate as a security system on its own, so it has its own advantages and disadvantages.

A. Advantages of Honeypots

1) Data value: One of the challenges the security community faces is gaining value from data. Organizations collect vast amounts of data every day, including firewall logs, system logs, and Intrusion Detection alerts. The sheer amount of information can make it extremely difficult to derive any value from the data. Honeypots on the other hand give precise information. All the data collected from honeypot are valuable information because any data is logged is mostly a probe, a scan or high-value attack information.

2) Resource exhaustion: Most of the security systems suffer from resource exhaustion. Resource exhaustion is when a security system cannot function because of its overwhelming resources. For example, a firewall may fail because its connections table is full, it has run out of resources, or it can no longer monitor connections. This forces the firewall to block all connections instead of just blocking unauthorized activity. An Intrusion Detection System may have too much network activity to monitor, perhaps hundreds of megabytes of data per second. When this happens, the IDS sensor's buffers become full, and it begins dropping packets. Its resources have been exhausted, and it can no longer effectively monitor network activity, potentially missing attacks. Since honeypots collect data from the attacks directed only at them they generate few megabits or no data every day.

3) Simplicity: Honeypots do not require complex algorithms, signature database or rule base to maintain. Hence it does not suffer from misconfigurations, failures or breakdowns. All we have to do is set up a system that emulates a host or a server, put it in the network and wait for an intruder/worm to attack the emulated system.

B. Disadvantages of Honeypots

Because of these disadvantages a honeypot couldn't replace a firewall or IDS, but can be used to add value to the existing security system.

1)Field of view: The greatest disadvantage of honeypot is field of view. They only manage or deal with traffic directed at them. Even if other systems or hosts in a network are compromised a honeypot in the same network may remain unaware about the intrusion. If the attacker has identified your honeypot for what it is, she can now avoid that system and infiltrate your organization, with the honeypot never knowing she got in.

2)Fingerprinting: Another disadvantage of honeypot is fingerprinting. Fingerprinting is when the attacker identifies the true identity of a honeypot. This is possible by monitoring certain behavior of a honeypot. For example, a honeypot may emulate a Web server. Whenever an attacker connects to this specific type of honeypot, the Web server responds by sending a common

error message using standard HTML. This is the exact response we would expect for any Web server. However, the honeypot has a mistake in it and misspells one of the HTML commands, such as spelling the word 'error' as 'error'. This misspelling now becomes a fingerprint for the honeypot, since any attacker can quickly identify it because of this error in the Web server emulation. An incorrectly implemented honeypot can also identify itself.

3)Risk: Honeypot can introduce risk to your environment. Once a honeypot is attacked it can be used to attack, infiltrate, or harm other systems or organizations. Simpler the honeypot or less the number of services are running, less is the risk of comprising other systems.

IV. INTRUSION DETECTION

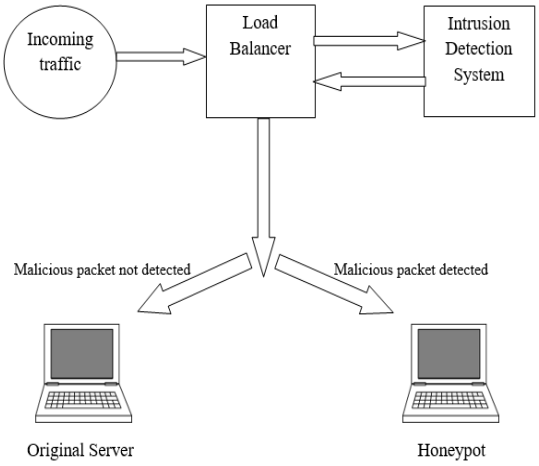
As the number and size of the Network and Internet traffic increase and the need for the intrusion detection grows in step to reduce the overhead required for the intrusion detection and diagnosis, it has made public servers increasingly vulnerable to unauthorized accesses and incursion of intrusions[7]. The approach used for intrusion detection is an integration between an IDS and a Honeypot where we can detect, deceive and even prevent an attacker from compromising the system. If in the process of forwarding requests, the balancer detects traffic as an attacker on the server, it is then redirected to an alternative server- a type of Honeypot. A Honeypot emulates as a host/server, deceiving the intruder and obtaining data from the intruders. Thus, the system will not only protect mission critical servers from unauthorized access in a manner transparent to the user, but allows for detailed data to be collected which can be later used to take appropriate legal actions against the incursion of intruders.

A. Background on IDS

An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system[6]. An IDS also collects and analyses the computer and device logs in a network. There are several ways to categorize an IDS, Misuse detection and Anomaly detection being two of them. In misuse detection, the IDS analyse the information it gathers and compares it to large databases of attack signatures. Essentially, the IDS looks for a specific attack that has already been documented. Like a virus detection system, misuse detection software is only as good as the database of attack signatures that it uses to compare packets against. In anomaly detection, the system administrator defines the baseline, or normal state of the network's traffic load, breakdown, protocol, and typical packet size. The anomaly detector monitors network segments to compare their state to the normal baseline and look for anomalies. IDS products have seen a drastic increase in its popularity in the past years because of its efficiency and highly accurate results. Existing products have substantial network monitoring capacity, and have been largely successful at providing accurate reports on unauthorized activity, but the problem is what actions are to be taken after detecting a malicious attack? Or even if the IDS were to predict the attack it sends the logs to the network administrator where the actions are to be determined by the administrator. In most of the cases the administrator fails to prevent an intrusion because of time constraints or delayed response. All too often all the IDS logs are consulted long after an attack has been done.

B. Source direct

Source direct is an attempt to address this problem by providing a fully automated response to specific network intrusions, it can eliminate the need for human decision making, and thus mitigate slow human response times.



Fig, 2: Architecture of IDS using Honeypot

The above architecture shows how by using a load balancer and an IDS, intruders/ attacker or even worms can be redirected to a honeypot. The activity at each process shown in figure 2 is as follows.

*1)*The load balancer receives the request to the virtual IP address. If the packet containing the request has been fragmented it is reassembled.

*2)*The Load balancer opens a TCP connection to the IDS Process and sends the content of the packet over to that connection.

*3)*The IDS process checks the content of the packet against its database of known attacks and returns a Boolean result to the load balancer over the same TCP connection.

*4)*On receiving the result, the load balancer closes the TCP connection. If the result from the IDS was "true"

meaning indicating the presence of an attack, the packet is forwarded to the Honeypot. Otherwise, a server is selected from the active server pool in a round-robin fashion and the packet is forwarded to the server. The design of this incurred many challenges.

C. Load balancer

Load balancing refers to efficiently distributing incoming network traffic across a group of backend servers, also known as a server farm or server pool.[10]. Modern high-traffic websites must serve hundreds of thousands, if not millions of concurrent requests from users or clients and return the correct text, images, video, or application data, all in a fast and reliable manner. To cost-effectively scale to meet these high volumes, modern computing best practice generally requires adding more servers. A load balancer acts as the "traffic cop" sitting in front of your servers and routing client requests across all servers capable of fulfilling those requests in a manner that maximizes speed and capacity utilization and ensures that no server is overworked, degrading the performance. If a single server goes down, the load balancer redirects traffic to the remaining online servers. When a new server is added to the server group, the load balancer automatically starts to send requests to it. In designing a load balancer for Secure Direct we have three main focuses namely, to provide High-Availability by handling hardware failure in the web-cluster, maintain high speed access to the cluster, and ensure the balancer itself does not become a security hole. High availability is achieved by simply pinging the servers at regular intervals, and removing them from the server pool if no response is received. The second challenge is to secure the load balancer. Our strategy is to protect it from any irrelevant traffic. Only traffic to a specific port on the virtual IP will be processed by the load balancer and any other malicious access is simply ignored. The load balancer uses a technique known as 'Proxy-ARP' to respond to ARP requests from the router to the virtual IP address[8]. The web servers have their loop back interface configured with the virtual IP address, but are set not to respond to ARP packets. This, at the network layer, there is no way to tell which servers are configured with the virtual IP. The load balancer process is implemented as a multithreaded process in Java. The main thread is responsible for reading packets off the wire and if they are destined to virtual IP and their destination port is our desired service port, it hands them to the control thread. The control thread then communicates with the IDS process and decides to pass the packet to the production servers or direct it to the Honeypot.The multithreaded design of the load balancer ensures that multiple requests from a client don't not get 'mixed up'; however, it is possible that an attack would occur from a single IP at the same time as a valid request. In this case, the initial, harmless packets may be safely forwarded to the real servers until the IDS process finds the attack packet and detects the signs of intrusion. At this point, it immediately informs the load balancer process to discontinue forwarding packets to the real server, and to send an RST packet to the corresponding server to end the connection. Thus, the server will never receive the attack. In the attacker side, observing silence from the server side causes it to assume the server has crashed and possibly causes it to try to reconnect. However, from this point, after detecting the intrusion, all the incoming traffic from the attacker's IP will be forwarded to the Honeypot.

D. Challenges faced by Secure direct

Secure Direct is designed like any good security product to be failed-closed system, which means if it crashes, it is no longer possible to access either web server through the virtual IP. Consequently, the attackers cannot crash Secure Direct and access the unprotected system. One of the major challenges for Secure Direct is to deal with attackers who try to fool the system by forcing it to analyze the packets inconsistent with what is received in the end-system. In the cases that the intrusion detection system runs at the different host-OS than the end-system, this can be a serious concern. The attacker can take advantage of differences between the IDS and the end system in dealing with the packets that do not fully comply with the standard protocols, and send some packets that are discarded by the end-host but accepted by the IDS, or vice versa. If Secure Direct uses TCP/IP, the inconsistency between the IDS and the end-host may appear in IP level or TCP level [9]. TCP protocol uses sequence numbers to preserve the order of the incoming packets. The end-system waits until it receives all the sequence numbers required for re-assembling the data. If there is a missing sequence number, the end-system will not accept the consequent packets and waits until it receives the packet with the sequence number it is waiting for. Therefore, one way to try to fool the system is to send two packets with the same sequence numbers, one containing false data to be accepted by the IDS and discarded by the end-host, and the other one containing the attackers' desired data to be accepted by the end host, and skipped by the IDS. Thus, whenever it detects two different packets with the same sequence number for one connection, it considers it as an attack and prevents the load balancer from sending that packet to the end-host. Furthermore, it marks the source IP of this packet, as an attacker IP, causing the load balancer to forward all the consequent packets originated from this IP to the Honeypot. An alternative way to break into the system is using IP fragmentation, hoping that IDS and the end-host follow two different methods for reassembling IP

fragments. Secure Direct however re-assembles the IP fragmented packets in the load balancer and forwards the assembled packet to the end-host. Therefore, what IDS analysis is completely consistent with what end-host sees. This type of implementation should drastically reduce the chances of an attacker breaking into the system.

V. CONCLUSION

Initially Honeypot wasn't a great success but after a few years of release it grew popular and eventually went down the line because of its static and idle nature. However, the future looks bleak for intruders as Honeypot is back with integrations along with IDS, firewalls and other security tools leading to the development of a complete security system. Secure direct, an integration of Honeypot with IDS and load balancer can detect, deceive and prevent intrusion and obtain data about the attacker and attack patterns. The future of honeypots is extremely exciting. Many exciting technologies and concepts await development. There will be a dramatic growth of research honeypots, used to study and learn the threats that exist in cyberspace. However, as the system develops, the attacking patterns changes finding new vulnerabilities, improvising hacking tools and methods to compromise the system. The war between intruders and security systems in cyberspace prevails forever.

REFERENCES

[1]. Mukherjee, B., L. Heberlein and K. Levitt. "Network Intrusion Detection." IEEE Network May/Jun 1994: 26-41.

[2]. www.securityfocus.com

[3]. http://www.pcmag.com/encyclopedia_term/0,2542,t=hOneypot &i=44335,00.asp

[4]. Cohen, Fred. "The Deception ToolKit." The Risks Digest 9 March 1998.

[5]. Provos, Niels. "A Virtual Honeypot Framework." In Proceedings of the 13th USENIX Security Symposium. 2004. 1-14.

[6]. Intrusion Detection System Using Advanced Honeypots-Ram Kumar Singh

[7]. Cliaord Stoll. Stalking the Wily Hacker. Communications of the ACM 1988.

[8]. Honeynet Research Alliance. Project Honeynet Website. Retrieved May 16th 2003 from the World Wide Web: http://project.honey.org

[9]. Computer Emergency Response Team. dtscpd Exploit Advisory. Advisory CA-2002-01 Exploitation of Vulnerability in CDE Subprocess

[10]. https://www.nginx.com/resources/glossary/load-balancing/

Balloon Powered Internet Access in Remote and Rural Regions

Ruchira Sapkal[1], Shanita Sojan[2]
Department of Computer Engineering, Fr. C. Rodrigues Institute of Technology, Vashi, Navi Mumbai
rsapka25@gmail.com shanita.sojan@gmail.com

Abstract: At present we seek the service of Internet Service Providers to connect us to the global network. The telephone companies or the telecommunication operators provides this kind of service for us. This is reachable to only one out of three in the world's population. The remaining people are not able to get internet access. It is not an easy task to lay the telecommunication lines all around the world to provide internet connection everywhere. Since the developing countries cannot afford such a huge sum of money to lay fibre cables, this will not be the optimal solution. To provide internet facility in remote places and rural areas, we need a high-altitude platform. Google came up with a innovative solution to use balloons to provide internet connection in remote regions. Balloons are used for numerous purposes but here it is used to provide internet connection in remote regions. This project is a network of balloons floating in the stratosphere. It acts as a wireless station and provides internet service to the rural areas and remote regions in a cost-effective manner.

Keywords: Envelope, user antenna, wind data, solar panel.

I. INTRODUCTION

Internet is a global system of interconnected network to serve billions of users. It is a network of networks. We are bouncing from 3G (Third Generation) to 4G (Fourth Generation) yet, there are still people who don't get internet access. It is found that, for every two in a group of three of word's population, internet is unreachable technology. The use of satellite internet communication is also very expensive and common people cannot afford it. In order to overcome this problem, we can use fibre cable connections, since the developing countries cannot afford such a huge sum of money to lay the cable all over the country it would not yield optimal solution. Google searched for the solution somewhere around like the skies, which popped up with an innovative concept of balloon powered internet access to all. The quest resulted in 'Project Loon'. Through this they are able to bring internet access to all the remote areas at an affordable price. The project Loon is an aerial balloon network. It flies at an altitude of 20 km (kilo meters) above the earth surface in the stratosphere, and they provide wireless mobile network station in sky with up to 3G speeds. Utilizing the help of wind data obtained from the NOAA (National Oceanic and Atmospheric Administration) they govern the balloon movements. The balloons are equipped with transceivers to send and receive the signals which travel in the balloon network before reaching the ground station. In turn it joins the global network by establishing connection with ISP (Internet Service Provider) or using LTE (Long Term Evolution) technology we can directly connect to network using mobile phones.

II. THE LOON'S TECHNOLOGY

The technology implemented in this project avoids use of expensive fiber cables. Most of the equipment used in loon can be reused and recycled hence this loon is safe and environment scientific research.

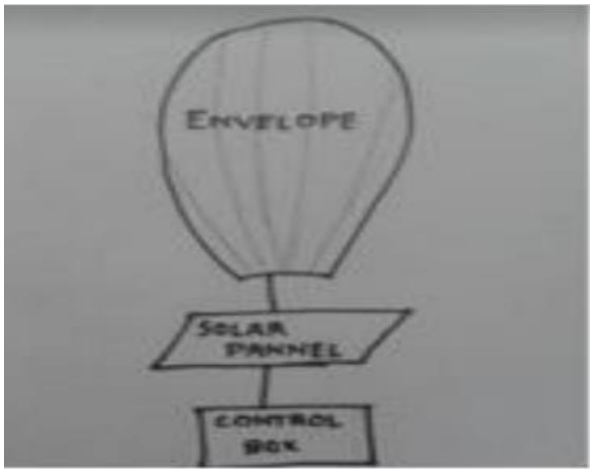


Fig. 1 Architecture of System

A. Envelope The inflatable part of balloon is made of sheets of polyethylene plastics, which is about 3 mil or 0.076 mm thickness. It forms the balloon envelope. When filled with Helium, it stands 15m (49 ft) wide and 12m (39 ft) tall, on full inflation. They are long-lasting than conventional weather balloons. These are super pressure balloons and have a maximum life time of 55 days. When a balloon is to be pulled out of service, first we have to release the gas in the balloon. This is achieved with the implementation of a custom air pump system, which is used to release air from or pump into the balloon in a periodic manner for controlled descendent. Unfortunately, if the balloons drops quickly or when the balloon is to be picked out of network safely, we use a parachute which is fixed at the top of the envelope.

B. Solar Panels The electronics of each unit are powered by solar panel array which is conveniently placed between the envelope and hardware part. These panels generate a power of 100 W (Watt) in full sun that is sufficient enough to run the entire unit during day time and for charging the battery, to use at night.

C. Control Box A small box weighing 10 kg hangs below the balloon's envelope which has all Wi-Fi circuits, batteries, a Linux-based computer, GPS (Geographical positioning System) devices and sensors to record the

temperature of air, altitude of balloon and its speed and circuit boards to control the unit.

III. NAVIGATION OF LOON

The balloons move by navigating the wind in the stratosphere. At stratosphere (twice the range of aircrafts travel altitude), 20km above the surface of earth, winds prefer to move in specific direction. There are different wind layers in stratosphere. Each layer varies in its direction and magnitude. We can determine the direction of wind from the wind data provided by NOAA and direct the balloons movement. The balloons are made to raise or fall to the desired altitude and move in desired direction at the specified speed by inflating or deflating the envelope using a air pump fixed in the setup. Actual life of balloons is estimated to be 100 days but, we can replace it constantly once in 55 days for checking which avoids unexpected failures. By doing so we could keep the balloon updated. Within this period it flies approximately 3 times around the globe. The extreme altitude presents many challenges to the loon like air pressure, extreme low temperature, less protection from UV(Ultra Violet) rays and the temperature swings. Yet it is able to overcome all these hurdles and withstand these conditions only by the perfect designing of balloon envelope. Hence, balloons are able to form a large communication network in the stratosphere.

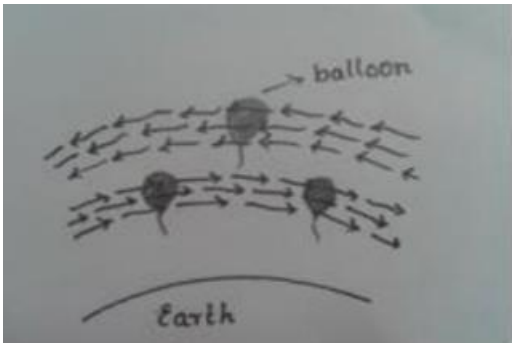


Fig. 2 Balloon movement in stratosphere

IV. ESTABLISHING THE NETWORK

The balloons form a network of airborne hot spots. It can deliver internet access over a broad area of about 1250 square kilometres at speeds comparable to 3G. For communication between balloon to balloon and to communicate to ground stations it uses a specialized radio frequency technology. Presently, the project loon uses ISM bands specifically 2.4-5.8 GHz bands. Each balloon unit has three transceivers for different purposes. First one is for the balloon to balloon communication and the second one is for balloon to ground communication and the other is the backup utility. The reflector plate placed between the antenna on top and radio in bottom is equipped together in the control box. It is used to establish the network connection. The head is composed of two parts which are called as "patch antenna" together. They serve to receive the signals reflected from the plate and direct signals. These signals when coupled together forms.

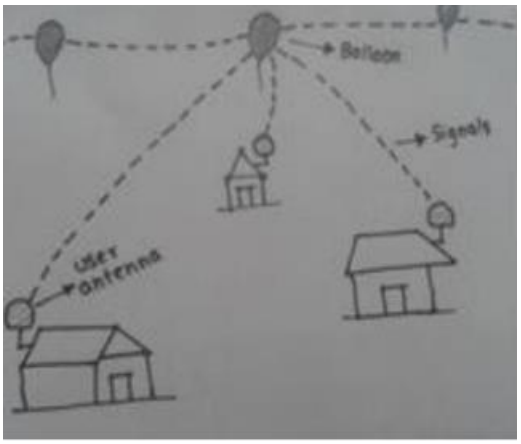


Fig. 3 Establishment of internet connection

V. CONNECTING PEOPLE

Once the entire setup is assembled then the balloon will be able to provide internet coverage for an area of 40 km in its diameter. Initially we can send and receive signals using the radios and antennas within the balloon network system alone. But now using a special technology called LTE, people can connect to network using their mobiles and other LTE enabled devices. The users send signals by the stationary antenna fixed on their building. The top of the balloon envelope consists of a reflector disc and a pair of patch antenna kept parallel. The signals from the user are reflected to the patch antenna and at the same time it also receives direct waves. These two waves interfere constructively only for the particular signal wavelength that are to be received by the balloon. The received signals bounces from balloon to balloon and finally reaches the ground station which are spaced about 100 km (62 mi) apart and there it joins the global network with pre-existing infrastructure for internet service like our local telecommunications partners. This is cost effective compared to the usage of satellite communication service, where the cost charged exceeds the monthly income of a common man. The developing countries that cannot afford to lay fibre cables is greatly benefited through this technology.

VI. PILOT TESTS CONDUCTED

This Project loon balloon network so called Google balloon is a research and development project by Google. Several pilot tests were conducted to improve its performance. One among them was conducted in New Zealand on June 2013 at Christchurch. Initially 40 balloons were launched. They offered 18 minutes of balloon based internet for 60 lucky volunteers on 40th

parallel south. The results of these tests are being used in the refinement of technology and the feedback is also used for the betterment of next phase of testing. National Space Research Institute of Brazil (Inpe) ran a test in São Paulo state. It yielded a positive response. The balloon was able to broad cast an Omni-directional internet signal from 31 miles away. Google is trying to test all manners of materials subjecting them to temperature resistance, durability..etc., Small private tests were conducted in California also. These tests are conducted with an urge to add more sophisticated technologies and to increase the balloons performance.

VII. CONCLUSION

Internet is emerged as the basic need in day to day life. While one part of the world is getting improved in a tremendous speed with the help of internet connection, about 2/3 of population is not even able to access it. Google tried to fill this void by the 'Project Loon' and fix the broad band problem. Project loon is one of the biggest idea of Google,. It acts as a wireless station for an area of about 25 miles in diameter. The technique to bring mobile internet connectivity to billions of people using balloons may sounds crazy but it might work. Google states that "It is highly experimental technology we have long way to go". This innovative attempt made by the Google to provide connection to rural areas and remote regions that deserve internet connection is an inspiring effort. The launch of 'Project Loon' made balloons too an option to provide internet access everywhere that too in a cost effective manner.

VIII REFERENCES

[1]. Yoshitaka Shibata, Yosuke Sato, Naoki Ogasawara, Go Chiba, Kazuo Takahata "A New Ballooned Wireless Mesh Network System for Disaster Use" in 2009 International Conference on Advanced Information Networking and Applications.

[2]. Morgenthaler, S., Braun, T., Zhongliang Zhao, Staub, T.,Anwander, M., "UAVNet: A mobile wireless mesh network using Unmanned Aerial Vehicles" in 2012 IEEE , vol., no., 3-7 Dec. 2012, pp.1603,1608, [online] http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnu mber=6477825&isnumber=6477486

[3]. Soujanya Katikala "GOOGLETM PROJECT LOON" in Rivier University, InSight: rivier academic journal, volume 10, number 2, fall 2014

[4]. Connectpeople [online] http://ipnsig.org/wpcontent/uploads/2014/02/Project-Loon.pdf

[5]. LoonFor All [Online] http://www.google.com/loon/

[6]. ProjectLoon[Online] http://en.wikipedia.org/wiki/Project_Loon

[7]. Introducing Project Loon: Balloon-powered Internet-access[online] http://googleblog.blogspot.in/2013 /06/ introducing-project-loon.html

[8]. Internet balloons to benefit small business, Google says [online] http://phys.org/news/2013-06-internetballoons- benefit-small-business.html

Free Space Optics System in Wireless Communication Technology

Deepti Paul[1], Felix Biju[2], Leah Abraham[3], Jithin Jose[4]
Department of Computer Engineering, Fr. C. Rodrigues Institute of Technology, Vashi, Navi Mumbai
[1]deeptipl4@gmail.com
[2]felixpalakan@gmail.com
[3]abrahamleah3997@gmail.com
[4]jithin06jose@gmail.com

***Abstract*-- Over the past few years, Free Space Optics (FSO) communication has been a preferred option over radio frequency communication. It is a technology that uses light propagating in free space to wirelessly transmit data for telecommunication or networking. It is the most practical choice where physical connections are impractical or high cost for development is involved, like in case of optical fibers. It is a line of sight communication technology that transmits a modulated beam of visible or infrared light through the atmosphere. They can be implemented using infrared laser lights or LEDs as point sources in short distance communication. In FSO, the energy beam is collimated and transmitted through space rather than guided wires. These beams of light operating in the terahertz portion of the spectrum are focused on a receiving lens connected to a highly sensitive receiver through an optical fiber. The high data rate and large information throughput available with FSO are many times greater than radio frequency system. This paper provides an overview of the effective role of FSO communication within next generation cellular networks. The main consideration is to increase the quality of communication and to pave a way for the growing reliance upon FSO communication with a view to support high bandwidth applications offered to mobile users.**

***Keywords*-- Free Space Optics; next generation network; line of sight communication; cellular networks.**

I. INTRODUCTION

FSO is an optical communication technology which uses lasers and photodetectors to provide optical connections without the fibre. FSO transmits data voice or video at speeds capable of reaching 2.5 Gbps. Products capable of speeds upto 10Gbps are expected to hit the market in the coming few years. This system use invisible infrared laser light wavelengths in the 750nm to 1550nm range. FSO communication offers potentially wide bandwidth and high data rate, which makes this type of communication system highly attractive in meeting the increasing demand for broadband traffic, which is mostly driven by internet access and high definition television broadcasting service. Working of FSO is quite similar to optical fibre networks with the only difference that optical beams are sent through free air instead of OFC cores that is glass fibre. FSO system is a line of sight communication system; thus no laying of fibre optic cables is needed, no expensive rooftop installations are required and no security upgrades are necessary. The system includes transreceivers at both ends to provide full duplex capability. It has drawn attention in telecommunications due to cost effectiveness, easy installation, quick establishment of communication and establishment of link of communication in disaster management scenarios with high bandwidth provisioning and various other wide ranges of communications.

II.OVERVIEW

A. History of FSO

FSO has been used for thousands of years in various forms. Around 800BC ancient Greeks and Romans used fire beacons for signalling. In 1880 Alexander Graham Bell created the photophone by modulating the sun radiation with voice signal. Later on invention of lasers in the 1960's led to the evolution of FSO communication. This led to transmission of television signals over 30 miles using LED by researchers, working in MIT Lincoln's Laboratory in 1962. The first laser to handle commercial traffic was built in Japan by Nippon Executive Company around 1970[4].

B. FSO transmission system

Today's systems pack more capacity in smaller volumes and lower price while measures to increase reliability are integrated into the solutions to increase the robustness of the link. A Free Space Optical transmission system is a wireless form of connection designed for the interconnection of two points which have a direct line of sight. The systems operate by taking a standard data or telecommunications signal, converting it into a digital format and transmitting it through free space. The carrier used for the transmission of this signal is Infrared and is generated by either high power LED or laser diode. The basic principles for the transmission of a signal along a fiber arethe same as for transmission through free space[9].

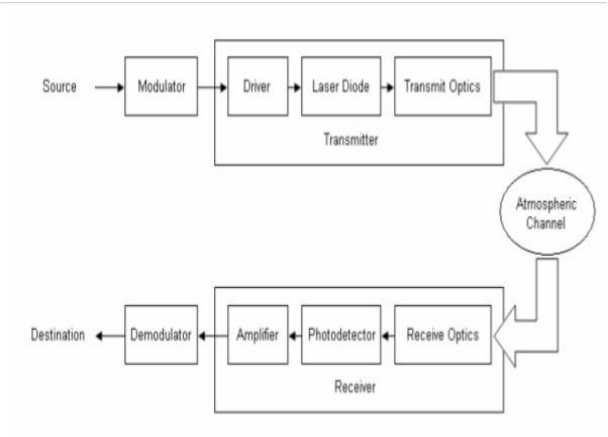


Fig. 1: Block diagram of FSO

C. Why FSO?

The increasing demand for high bandwidth in metro networks is relentless, and service providers' pursuit of a range of applications, including metro network extension, enterprise LAN-to-LAN connectivity, wireless backhaul and LMDS supplement has created an imbalance. This imbalance is often referred to as the "last mile bottleneck." Service providers are faced with the need to provide services quickly and cost-effectively at a time when capital expenditures are constrained. But the last mile bottleneck is only part of a larger problem. Similar issues exist in other parts of the metro networks. "Connectivity bottleneck" better addresses the core dilemma. The connectivity bottleneck is everywhere in metro networks. From a technology standpoint, there are several options to address this "connectivity bottleneck," but most don't make economic sense. Firstly, the most obvious choice is fibre-optic cable. Without a doubt, fibre is the most reliable means of providing optical communications. But the digging, delays and associated costs to lay fibre often make it economically prohibitive. Second option is the radio frequency (RF) technology. RF is a mature technology that offers longer ranges than FSO, but RF-based networks require immense capital investments to acquire spectrum license. RF technologies cannot scale and the bandwidth is limited to 622 megabits. The third alternative is wire- and copper-based technologies, (i.e. cable modem, DSL etc.). Although copper infrastructure is available almost everywhere and the percentage of buildings connected to copper is much higher than fibre, it is still not a viable alternative for solving the connectivity bottleneck. The biggest hurdle is bandwidth scalability. Copper technologies may ease some short-term pain, but the bandwidth limitations of 2 megabits to 3 megabits make them a marginal solution, even on a good day. Fourth and finally, the most viable-alternative is FSO. The technology facilitates an optimal solution, bandwidth scalability, speed of deployment (hours versus weeks or months), redeployment and portability, and cost-effectiveness(on average, one-fifth the cost of installing fibre-optic cable)[1].

D. Advantages of FSO over fibre optics

i. Cost is lesser compared to fibre optics.
ii. Fiber optic requires permit for digging but FSO requires no permit.
iii. Trenching is done in fibre optics but not in FSO.
iv. Installation is faster as compared to fiber optics.
v. FSO is mobile and reconfigurable.

E. Advantages of FSO over RFcommunication

i. Ultra high wireless bandwidth in FSO as compared to RF which has low bandwidth.
ii. No licensing is required for FSO.
iii. FSO provides high data rates upto several Gbps.
iv. FSO has highly secure system whereas RF is susceptible to eavesdropping.
v. FSO solves last mile problem.

F. Limitations of FSO

As the medium of the transmission is air for FSO and the light passes through it, some environmental challenges are unavoidable.
Geometric losses can be called optical beam attenuation that are induced due to the spreading of beam and reduced power level of signal as it travels from transmitted end to receiver end.

Atmospheric turbulence is the atmospheric disturbance that happens due to weather and environment structure. It is caused by wind and convection which mixes the air parcels at different temperatures. This causes fluctuations in the density of air and it leads to the change in the refractive index of air. The scale size of turbulence cell can create different type of effects given below and which would be dominant :(i) If size of turbulence cell is of larger diameter than optical beam then beam wander would be the dominant effect. Beam wander is explained as the displacement of the optical beam spot rapidly.(ii)If size of turbulence cell is of smaller diameter than optical beam then the intensity fluctuation or scintillation of the optical beam is a dominant one. Turbulence can lead to degradation of the optical beam of transmission. Change in the refractive index causes refraction of beam at different angle and spreading of optical beam takes place. Atmospheric attenuation is the resultant of fog and haze normally. It also depends upon dust and rain. It is supposed that atmospheric attenuation is wavelength dependent but this is not true. Haze is wavelength dependent. Attenuation at 1550nm is less than other wavelengths in haze weather condition. Attenuation in fog weather condition is wavelength independent[2].

III.FSO ARCHITECTURES

FSO systems can be designed and engineered to work in any network topology, including mesh, PMP (Point-to-Multipoint), PTP (Point-to-Point), and Ring. This gives metropolitan area service providers the freedom to rapidly build and extend networks that deliver fibre-optic speeds to today's customers[8].

A. Mesh Architecture

A mesh network shown in Figure -2 is composed of a series of interconnected nodes with some degree of redundancy. In such a network, every node is connected to every other node, either directly or by a series of hops. The level of redundancy in the network determines the level of connectedness in the network. Thus, higher the number of nodes, the better the system. Mesh networks offer high reliability with easy node addition but restrict distances more than the other options. It can support 622 Mbps at a distance of 200m to 450m. For scalability, most analysts would prefer mesh topology, which allows carriers to add nodes to the network more easily. The mesh also allows alternate routing, while other topologies suffer from a single point of failure.

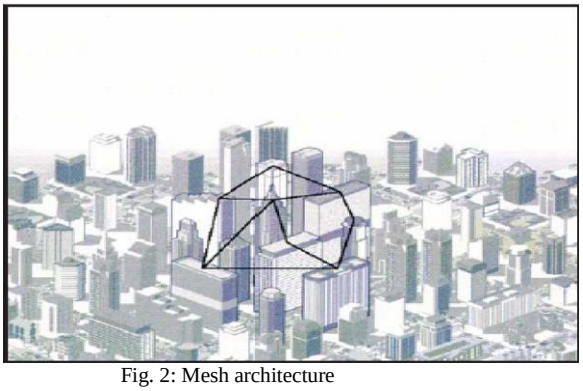


Fig. 2: Mesh architecture

B. Point-to-Multipoint Architecture

In Point-to-Multipoint Architecture or Star Configuration, a single node serves as an originator and multiple links emanate from it. The most effective method is to connect each FSO link into a layer 2 or 3 device located in a building closet. Then the links are fibre coupled to the switch or router and placed at arbitrary locations either on the building rooftop or in an interior room or office therein. Attempts have been made to sectorize the optical beam to serve more than one customer at a time from a single node, as done in LMDS systems, but this architecture is restricted by power limitations imposed by regulatory authorities. Point-to-Multipoint Architecture shown in Figure-3 offers cheaper connections and facilitates node addition but at the expense of lower bandwidth than the PTP.

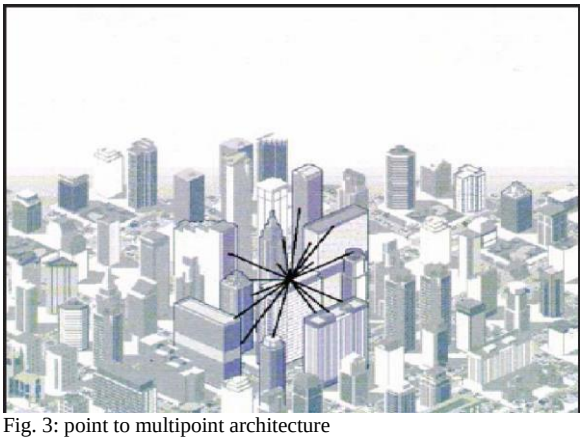


Fig. 3: point to multipoint architecture

C. Multiple PTP Architecture:

Multiple PTP architecture shown in figure-4 is suitable in cases where it is desirable to create an extensive link path that exceeds the product range limit or the recommended weather constrained distance for an optical link. It is a dedicated connection that offers higher bandwidth. In this architecture connection is established between two nodes or endpoints. This is in contrast to multipoint or broadcast connection in which many nodes can receive information transmitted by one node. Some examples of this type of communication are leased lines, microwave rely links and two way multi radio[1].

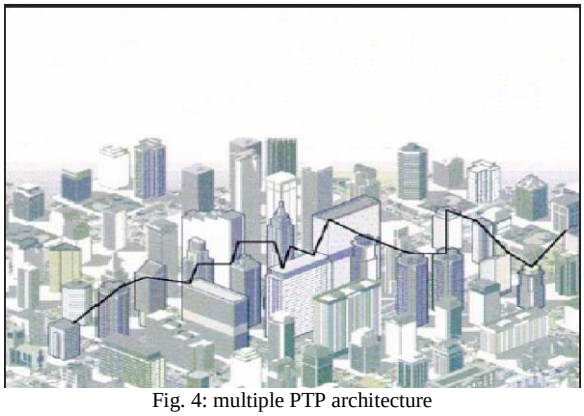


Fig. 4: multiple PTP architecture

IV. APPLICATIONS

Free-Space Optics has several applications in Telecom Networks where an optical gap exists between the network core and the network edge. FSO delivers cost-effective optical connectivity and faster returns on investment (ROI) for enterprises and service providers. Although the growth in the usage of the FSO technology is slow at the moment, but with high-bandwidth demands and the need for economically viable optical solutions, FSO is likely to outpace the deployment of fibre-optic cable. These applications have been discussed below:

1) Outdoor Wireless Access:

It can be used by wireless service providers for communication and it requires no license to use the FSO as it is required in case of microwave bands.

2) Storage Area network:

FSO links can be used to form a SAN. It is a network which provides access to consolidated, block level data storage.

3) Last-mile access:

To lay cables of users in the last mile is very costly for service providers as the cost of digging to lay fibre is so high and it would make sense to lay as much fibre as possible. FSO can be used to solve such problem by implementing it in the last mile along with other networks. It is a high speed link. It is also used to bypass local-loop systems of other kinds of networks.

4) Enterprise Connectivity:

They are easily installable. This feature makes it applicable for interconnecting LAN segments to connect two buildings or other structures.

5) It can be used as a backup link in case of failure of transmission through fibre link.

6) Backhaul:

It can be helpful in carrying the traffic of cellular telephone from antenna towers back to the PSTN (Public Switched Telephone Network) with high speed and high data rate.

7) It can be used to communicate between PTP links for example: two buildings, two ships or point to multipoint links e.g.: from aircraft to ground or satellite to ground.

8) As it is an undetectable and a secure system it can be used for military applications with minimal planning and deployment time.

9) In case of natural disasters like seismic activity, the receiver and the transmitter alignment is disturbed. FSO based optical wireless system use a divergent beam to maintain connectivity. When combined with tracking, FSO based systems provide greater performance and enhanced installation simplicity [2].

V. SIGNAL PROPAGATION IMPEDIMENTS

1) Fog:

The major challenge to FSO communication is fog. One way to counter fog when deploying FSO is through a network design that shortens FSO link distances and adds network redundancy. FSO installations in foggy cities such as San Francisco have successfully achieved carrier class stability.

2) Absorption:

Absorption occurs when suspended H_2O molecules in the atmosphere extinguish photons. This causes a decrease in the power density of the FSO beam and directly affects the availability of a system.

3) Scattering:

Scattering is caused when the wavelength collides with scatterer. The physical size of the scatterer determines the type of scattering. When the scatterer is smaller than the wavelength, this is known as Rayleigh scattering. When the scatterer is of comparable size to the wavelength, this is known as Mix scattering.

4) Scintillation:

Heated air rising from earth or man-made devices such as heating ducts creates temperature variations among different air pockets. This can cause fluctuation in signal amplitude which leads to image fluctuation at the FSO receiver end.

5) Physical Obstruction:

Flying birds can temporarily block a single beam, but this tends to cause only short interruptions, and transmissions are easily and automatically resumed.

6) Building sway/seismic activity:

The movement of buildings can upset the receiver and the transmitter alignment.

7) Safety:

To those unfamiliar with FSO, safety is often a concern because the system uses lasers for transmission[3].

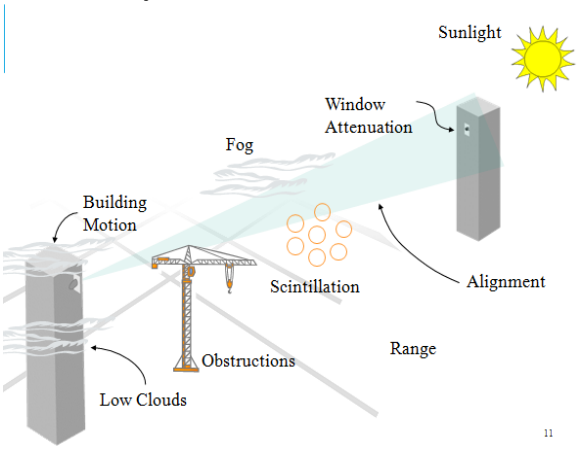


Fig. 5: Signal Propagation Impediments

VI. LAST MILE BOTTLENECKS

In about 5% of all buildings in the US we have a direct connection to a high speed fibre optic backbone, yet more than 75% of the businesses are with one mile of fibre backbone. Most of these businesses are running some high speed data network these buildings such as fast Ethernet (100 mbps). Yet their Ethernet access is provided by the significantly lower bandwidth technologies available through existing infrastructure such as copper wire, cable modem and digital subscriber line (DSL). The last mile problem is the connection of the high bandwidth from the fibre optic backbone to all of the businesses with high bandwidth networks. DSL and cable modems cannot provide true broadband services. Cable modems enjoy higher capacity, yet the channel is shared

and the amount of bandwidth at any given time is not guaranteed. Copper lines provide data rates to a fraction of 1 Mbps. T1 lines (Digital Transmission Service) can reach upto a few Mbps but are still far away from the Gbps speed which the fibre backbone can support. A high-bandwidth cost-effective solution to the last mile problem is to use free-space laser communication (also known as optical wireless) in mesh architecture to get the high bandwidth quickly to the customers[6]. Wavelength Division Multiplexing (WDM) technologies will work in free space further increasing the bandwidth potential of wireless optical lines. Along with significantly increased data rates, FSO has many advantages over other wireless technologies. They include license free operation, increased security due to laser's narrow beam which makes detection and interception nearly impossible.

VII. CONCLUSION

FSO offers many advantages over existing techniques which can be either optical or radio or microwave. Less cost and time to setup are the main attraction of FSO system. Optical equipment can be used in FSO system with some modification. Merits of FSO communication system and its application area make it a hot technology but there are some problems arising due to the attenuation caused by medium. FSO system poses some problem like attenuation in medium that can affect the performance of transmission as power loss would be there. But extra care and restudy of the medium can guide what type of parameters to be considered before setting up the system. Many studies are going in this perspective to minimize the effect of attenuation by introducing new system design like WDM based FSO system. Different models based on these studies are used to study the system performance before installing it at the location. This can lead to the improvement of the system.

REFERENCES

[1]. http://tec.gov.in/pdf/Studypaper/White%20Paper%20-%20FSO.pdf

[2]. https://www.hindawi.com/journals/ijo/2015/945483

[3]. https://drive.google.com/file/d/0ByaLSRMhRNd3dGpkSXNUTWlYRjA/view?usp=sharing-*Free Space Optical Communication*, Prof. Sandeep J. Rajput

[4]. https://www.slideshare.net/hmoood1995/free-space-optical-communication-fso-ieee-paper

[5]. https://www.quora.com/Why-hasnt-Free-Space-Optics-been-adopted-for-communications-on-earth

[6]. https://www.youtube.com/watch?v=poby6FDJHho

[7]. http://www.fiberwork.net/products/fso.html

[8]. http://www.eujournal.org/index.php/esj/article/viewFile/7182/6915

[9]. http://www.laserfocusworld.com/articles/print/volume-37/issue-6/features/optical-communications/free-space-links-address-the-last-mile-problem.html

[10]. J. Kaufmann, "Free space optical communications: an overview of applications and technologies," in Proceedings of the Boston IEEE Communications Society Meeting, 2011.

LIST OF TOPPERS (2017 -2018)

FINAL YEAR TOPPERS

Ms. Pranali Kanere
(9.75 CGPI)

Ms. Tanvi Rajadhyaksha
(9.33 CGPI)

Ms.Nisha Mariam
(9.33 CGPI)

Ms.Madhavi Madanagopal
(9.11 CGPI)

THIRD YEAR TOPPERS

Mr. Shivanand Gollagi
(9.50 CGPI)

Ms. Ruby Veppineth
(9.50 CGPI)

Ms. Tanisha Mittal
(9.33 CGPI)

Ms. Krupa Jariwala
(9.17 CGPI)

Mr. Tushar Masane
(9.17 CGPI)

Ms. Shanitamol Sojan
(9.17 CGPI)

Ms.Madhura Dumbre
(9.17 CGPI)

Ms. Ruchira Sapkal
(9.17 CGPI)

SECOND YEAR TOPPERS

Mr. Atharva Agwekar
(10 CGPI)

Mr.Gavin Lewis
(10 CGPI)

Mr.Rajshankar Khattar
(10 CGPI)

Mr. Makasare Gaurav
(10 CGPI)

Mr. Srujan Patel
(10 CGPI)

Mr. Reddy C Sai
(10 CGPI)

Ms. Ankita Shinde
(10 CGPI)

Mr. Naeem Patel
(9.93 CGPI)

Ms. Shruthi Nair
(9.89 CGPI)

2014-2018 BATCH

2015-2019 BATCH

2016-2020 BATCH

CSI – ACESS - 2017

PROJECT POSTER PRESENTATION

(2017-2018)