



Cyber Security

Be aware... Connect with care



Message From Dean, FCAIT



The technique of protecting computers, servers, mobile devices, electronic systems, networks, and data from hostile intrusions is known as cyber security. These attacks could be motivated by a variety of factors, including financial gain, political motive, or sadistic enjoyment.

The worldwide cyber threat is evolving at a breakneck rate, with an increasing number of data breaches every year. Governments all over the world have issued recommendations to help businesses develop strong cyber-security policies in response to the growing cyber threat.

Malware (malicious software), which a cybercriminal or hacker has built to disrupt or damage a legitimate user's computer, is one of the most common tactics used to risk cyber-security. Other tactics include SQL injection, which steals data, phishing, which targets emails, man in the middle attacks, which intercept data, denial of service attacks, and so on.

As a result, teaching users various cyber security tips such as deleting suspicious email attachments, not plugging in unidentified USB drives, keeping software and operating systems up to date, using strong passwords, and various other important lessons is critical for the security of any individual or organization's data.

Our BCA and iMSc students have produced excellent pieces in this issue on Cyber Security, outlining in depth what cyber security is, why it is important, the various types of cyber risks that exist, as well as security tools and procedures.

I am confident that you will like the issue and acquire valuable insight into the subject of Cyber Security.

-- Dr. Savita Gandhi

From Editorial Desk

Dear Readers,

“It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it.” – Stephane Nappo

Cybercrime is the greatest threat to every company in the world. One needs to understand that in a digital era, privacy must be a priority.

During the pandemic rising above all the limitations, we are presenting the 19th issue of our half-yearly magazine “D-KOSMOS” with the theme “Cyber Security”. The present issue of DKOSMOS throws light on the need for cyber security, cyber terrorism, common cyber threats and how one can secure oneself from becoming the victim of cyberattacks.

This time, D-kosmos with its unique theme and design delineates the wonderful journey of FCAIT's achievements and success. To motivate students to build innovative career plans we inspire them to take part in many academic activities such as Alumni Talk, Tech Talk, Expert lectures, Seminars and Code Express. Students knowingly and unknowingly pick up various life skills by attending and participating in different activities carried out by FCAIT. The present issue gives an account of all these activities in brief.

We welcome your suggestions and remarks via email, so please get in touch for reviews at dkosmos@glsica.org.

-----Wishing you all a happy reading of D-kosmos!

Chief Editor

Dr. Tripti Dodiya

Members

Dr. Disha Shah, Dr. Poonam Dang
Prof. Bharti Shah, Prof. Monica Gupta
Prof. Garima Mishra, Dr. Kruti Vyas

Designer

Prof. Bharti Shah

Introduction

In many respects, the internet has made the world a smaller place, but it has also exposed us to never-before-seen influences that are both diverse and difficult. The hacking world grew at the same rate as security. [1] Today, an individual may receive and send any information, whether video, email, or just a click of a button, but has s/he ever considered how safe this information is delivered to another individual with no data spillage?

Cybersecurity is the appropriate answer. More than 61 % of whole industry transactions are now conducted via internet, necessitating a high level of security for direct and best exchanges in this field.[2]

Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks. Also known as Information Technology (IT) security, cybersecurity measures are designed to combat threats against networked systems and applications, whether they originate from inside or outside an organization.[2]

The average data breach costs in 2021 is \$4.24 million, a 10% rise from 2020 findings. This also sets a new data breach cost peak in the entire history of the IBM and Ponemon Institute report. [3] These costs include discovering and responding to the breach, the cost of downtime and lost revenue, and the long-term reputational damage to a business and its brand. Cybercriminals target customers' Personally Identifiable Information (PII) - Names, Addresses, National Identification Numbers (e.g., Social Security Numbers in the U.S., fiscal codes in Italy), credit card information - and then sell these records underground digital marketplaces. Compromised PII often leads to a loss of customer trust, regulatory fines, and even legal action.

The complexity of security systems created by different technologies and a lack of in-house expertise can amplify these costs. However, organizations with a comprehensive cybersecurity strategy, governed by best practices and automated using Advanced Analytics, Artificial Intelligence (AI), and Machine Learning, can fight cyber threats more effectively and reduce the lifecycle and impact of breaches when they occur.

History of Cyber-Security and Cyber- Crime

Cybercrime is latest in many heists like Pink Panther and Butch Cassidy. Robberies used to be fraught with drama, such as the theft of 13 items of art worth more than \$500 million from the Boston Museum. Digital goods, such as credit card information and film footage, have now attracted the interest of a new kind of crime. A gang of Russian hackers had electronically stolen over \$800 million from bank accounts in the last two years. One Russian hacker may potentially be blamed for obtaining crucial electoral data from the 2016 US election. [4]

The Computer Fraud and Abuse Act of 1986 was the first piece of legislation in the United States to address cybercrime. From Anonymous' advocacy-based vigilantes to mysterious lone wolves or government suspects reported in the press, cyber attackers have a widespread presence despite their recent origins. Computer crimes began in 1983, when the internet was first launched. So infecting networks, stealing personal data, assaulting foreign government activities, and holding crucial corporate information hostage are just some things they are renowned for Cyber-Crime.[4]



Figure: 1 History of Cyber-Crime [4]

In 1988, the Morris Worm, the first Denial-of-Service (DoS) assault, was unleashed: a few dozen lines of code that quickly duplicated and wrecked 10% of all computers connected to the internet. In mid-1990s, hackers exploited weaknesses in flash and browser add-ons to gain remote control of computers. Insecure, multi-access software has remained a problem in recent years. As people spend more time online, phishing had become increasingly prevalent. Mobilization has spawned a burgeoning spyware and tracking industry. Automotive and other machine software has also been hacked since 2014. As it stands at the core of the software, cloud, network, and physical access problems and IoT etc. has faced several security challenges.

Why Do We Need Cyber Security?

Protecting information and system against severe cyber threats is part of the scope of cyber security operations. These dangers come in variety of shapes and sizes. As a result, keeping up with cyber security strategy and operations may be difficult, especially in government and industry networks, where cyber-attacks frequently target a nation's personal, political, and military assets, as well as its people.

The following are some of the most frequent threats:

Cyber Terrorism:

Terrorist organizations' creatively use of digital technology to promote their political objectives. Attacks on networks, computer systems, and telecommunication infrastructures are common.

Cyberwarfare:

It entails nation-states utilizing Information Technology to infiltrate another nation's networks to wreak harm. Cyberwarfare has been recognized as the fifth domain of warfare in the United States and many other countries. Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.

Rather than shutting down a target's major networks, a cyber-warfare strike may be pushed to place networks in a state where vital data is compromised, communications are degraded, infrastructure functions such as transportation and medical services are harmed, or commerce is disrupted.

Cyber Spionage:

It is the activity of obtaining confidential information without the authorization of its owners or holders via the use of Information Technology. It is the most common way to obtain a strategic, economic, or military edge, and it is done using malware and cracking tools.

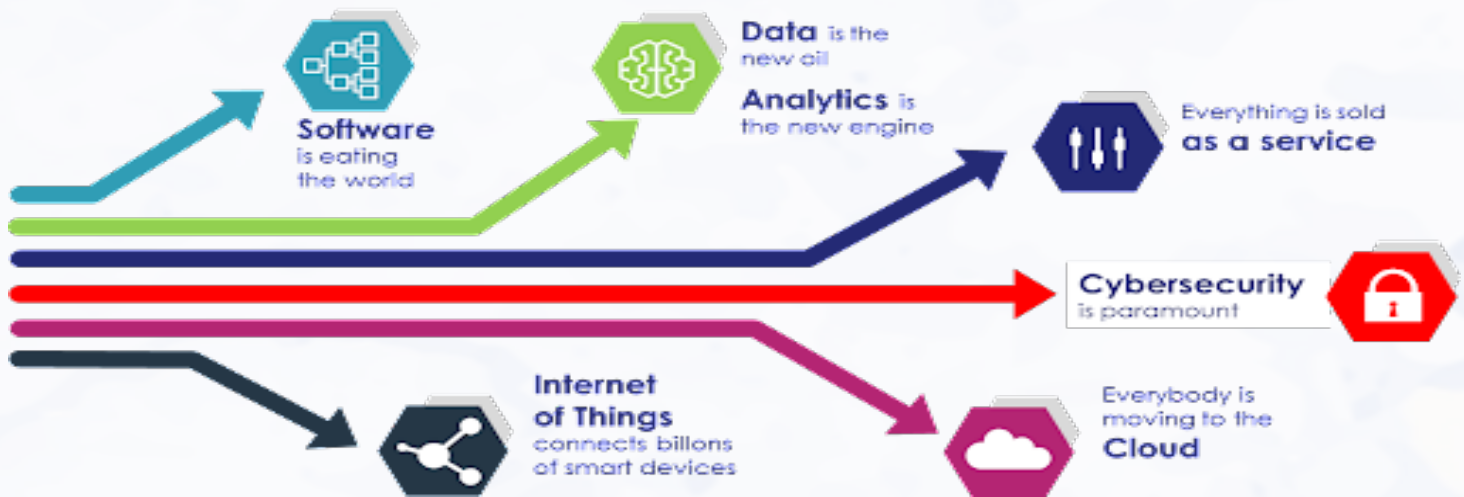


Figure:2 Need of Cyber Security [6]

Cyber Security Domains

A strong cybersecurity strategy has layers of protection to defend against cybercrime, including cyber attacks that attempt to access, change, or destroy data; extort money from users or the organization, or aim to disrupt normal business operations. There are the following domains listed below: [4]

Application Security:- Processes that help protect applications operating on-premises and in the cloud. Security should be built into applications at the design stage, considering how data is handled, user authentication, etc.

Cloud Security:- Specifically, true confidential computing that encrypts cloud data at rest (in storage), in motion (as it travels to, from and within the cloud) and in use (during processing) to support customer privacy, business requirements and regulatory compliance standards.

CYBER SECURITY

Information Security:- Data protection measures, such as the General Data Protection Regulation or GDPR, that secure your most sensitive data from unauthorized access, exposure, or theft.

End-User Education:- Building security awareness across the organization to strengthen endpoint security. For example, users can be trained to delete suspicious email attachments, avoid using unknown USB devices, etc.

Storage Security:- IBM FlashSystem® delivers rock-solid data resilience with numerous safeguards. This includes encryption and immutable and isolated data copies. These remain in the same pool to quickly be restored to support recovery, minimizing the impact of a cyber-attack.

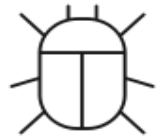
Disaster Recovery/Business Continuity Planning:- Tools and procedures for responding to unplanned events, such as natural disasters, power outages, or cybersecurity incidents, with minimal disruption to key operations.

Common Cyber Threats

Although cybersecurity professionals work hard to close security gaps, attackers are always looking for new ways to escape IT notice, evade defense measures, and exploit emerging weaknesses. The latest cybersecurity threats are putting a new spin on "known" threats, taking advantage of work-from-home environments, remote access tools, and new cloud services. These evolving threats include: [4]

Malware:-

The term "malware" refers to malicious software variants—such as worms, viruses, Trojans, and spyware—that provide unauthorized access or cause damage to a computer. Malware attacks are increasingly "fileless" and designed to get around standard detection methods, such as antivirus tools that scan for malicious file attachments.



Ransomware:-

The Ransomware is malware that locks down files, data, or systems. Unless a ransom is paid to the cybercriminals who launched the attack, it threatens to erase or destroy the data - or make private or sensitive data to the public. Recent ransomware attacks have targeted state and local governments, which are easier to breach than organizations and under pressure to pay ransoms to restore applications and websites citizens rely on.



Phishing / Social Engineering:-

Phishing is a form of social engineering that tricks users into providing their own PII or sensitive information. In phishing scams, emails or text messages appear from a legitimate company asking for sensitive information, such as credit card data or login information. The FBI has noted a surge in pandemic-related phishing, tied to the growth of remote work.



Insider Threats:-

Current or former employees, business partners, contractors, or anyone who has had access to systems or networks in the past can be considered an insider threat if they abuse their access permissions. Insider threats can be invisible to traditional security solutions like firewalls and intrusion detection systems, focusing on external threats.



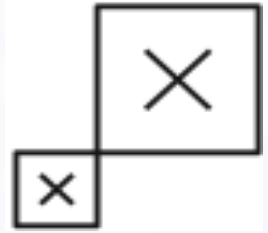
Distributed Denial-of-Service (DDoS) Attacks:-

A DDoS attack attempts to crash a server, website, or network by overloading traffic, usually from multiple coordinated systems. DDoS attacks overwhelm enterprise networks via the Simple Network Management Protocol (SNMP) used for modems, printers, switches, routers, and servers.



Advanced Persistent Threats (APTs):-

In an APT, an intruder or group of intruders infiltrate a system and remain undetected for an extended period. The intruder leaves networks and systems intact so that the intruder can spy on business activity and steal sensitive data while avoiding the activation of defensive countermeasures. The recent Solar Winds breach of United States government systems is an example of an APT.



Man-in-the-middle Attacks:-

This is an eavesdropping attack, where a cybercriminal intercepts and relays messages between two parties to steal data. For example, an attacker can intercept data being passed between a guest's device and the network on an unsecured Wi-Fi network.

----Mahmood Topiwala, SYBCA

----Vishwa Shah, SYBCA

Network Security Tools and Techniques

Access Control:- If threat actors cannot access your network, the amount of damage they will do will be minimal. However, in addition to preventing unauthorized access, be aware that even authorized users can also be potential threats. Access control allows you to increase your network security by limiting user access and resources to only the parts of the network that directly apply to individual users' responsibilities.

Anti-malware Software:- Malware, in the form of viruses, trojans, worms, keyloggers, spyware, etc. is designed to spread through computer systems and infect networks. Anti-malware tools are a kind of network security software designed to identify dangerous programs and prevent them from spreading. Anti-malware and antivirus software may also help resolve malware infections, minimizing the damage to the network.

Anomaly Detection:- It can be challenging to identify anomalies in your network without a baseline understanding of how it should operate. Network anomaly detection engines (ADE) allow you to analyze your network so that when breaches occur, you will be alerted to them quickly enough to be able to respond.

Application Security:- For many attackers, applications are a defensive vulnerability that can be exploited. Application security helps to establish security parameters for any applications relevant to your network security.

Data Loss Prevention (DLP):- Often, the weakest link in network security is the human element. DLP technologies and policies help protect staff and other users from misusing and possibly compromising sensitive data or allowing said data out of the network.

Email Security:- As with DLP, email security is focused on shoring up human-related security weaknesses. Via phishing strategies (which are often very complex and convincing), attackers persuade email recipients to share sensitive information via desktop or mobile device or inadvertently download malware into the targeted network. Email security helps identify dangerous emails and can also block attacks and prevent the sharing of vital data.

Endpoint Security:- The business world is increasingly Bringing Your Device (BYOD) to the point where the distinction between personal and business computing devices is almost nonexistent. Unfortunately, personal devices sometimes become targets when users rely on them to access business networks. Endpoint security adds a layer of defense between remote devices and business networks.

CYBER SECURITY

Firewalls:- Firewalls function much like gates that can be used to secure the borders between your network and the internet. Firewalls manage network traffic, allowing authorized traffic through while blocking access to non-authorized traffic.

Intrusion Prevention Systems:- Intrusion prevention systems (also called Intrusion Detection) constantly scan and analyze network traffic/packets to identify and respond to different types of attacks quickly. These systems often keep a database of known attack methods to recognize threats immediately.

Network Segmentation:- Many kinds of network traffic are associated with different security risks. Network segmentation allows you to grant the proper access to the correct traffic while restricting traffic from suspicious sources.

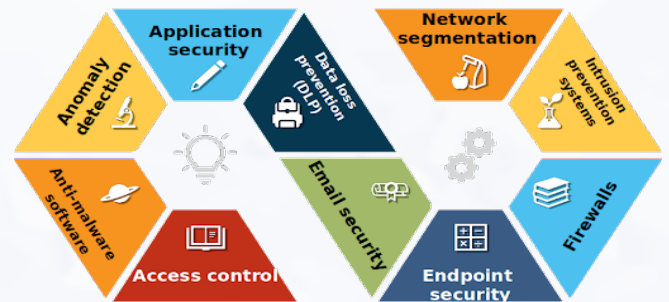






Figure-3 Tools and Techniques

Top 5 Cybersecurity Software and Tools in 2022

Software	Details	Feature
 SiteLock	<p>– Simply Powerful Website Security</p> <ul style="list-style-type: none"> SiteLock is a leading website security software that protects over 12 million websites from malicious cyber threats. It offers a 360-degree security including daily website scans, automated malware removal, and vulnerability/CMS patching, as well as a web application firewall to block harmful traffic before it ever reaches any site. 	Behavioral Analytics, Endpoint Management, Incident Management, Vulnerability Scanning, Whitelisting/Blacklisting.
 Heimdal CORP	<p>– Proactive Cyber Security Software</p> <ul style="list-style-type: none"> Heimdal CORP is an endpoint web security solution for malware monitoring, software management, internet traffic reporting, and web scanning and filtering. 	AI / Machine Learning, Behavioral Analytics, Vulnerability Scanning.
 WebTitan	<p>– DNS-based web content filtering & malware protection</p> <ul style="list-style-type: none"> Globally, WebTitan extends a protection from cybersecurity threats by blocking malware, ransomware, phishing and provides complete control over the web for businesses, educational institutions, and public WIFI providers. 	AI / Machine Learning, Behavioral Analytics, Endpoint Management, Incident Management, IOC Verification, Vulnerability Scanning.
 Teramind	<p>– Insider Threat Detection & Prevention using UBA</p> <ul style="list-style-type: none"> Teramind offers three types of security. Teramind starter provides employee monitoring solution for startups and small businesses. Teramind's UAM/User Behavior Analytics (UBA/UEBA) solution comes with everything essential one will need for employee monitoring, third-party monitoring, insider threat detection and workplace productivity optimization use cases. 	AI / Machine Learning, Behavioral Analytics, Endpoint Management, Incident Management, Whitelisting / Blacklisting.
 Pentest-Tools.com	<p>– Your pentesting arsenal, ready to go</p> <ul style="list-style-type: none"> Pentest-Tools.com is a robust penetration testing and vulnerability assessment platform. It's one of the most intuitive and user-friendly penetration testing tools commercially available. Today almost 2 million unique users rely on Pentest-Tools.com annually. 	Advanced reporting, Pentest robots, Attack surface mapping, Internal network scanning, Scan scheduling, API access, Bulk scanning, Shared items and workspaces.

References:

- https://www.researchgate.net/publication/329678338_Overview_of_Cyber_Security
- https://www.researchgate.net/publication/335322600_Cyber_Security
- <https://www.upguard.com/blog/cost-of-data-breach>
- <https://www.ibm.com/topics/cybersecurity>
- <https://cybersecurityventures.com/cybersecurity-ceo-the-history-of-cybercrime-from-1834-to-present/> (image)
- <https://diginetworks.co.in/why-do-we-need-cyber-security/> (image)
- <https://blog.gigamon.com/2019/06/13/what-is-network-security-14-tools-and-techniques-to-know/>
- [https://www.softwareworld.co/top-cybersecurity-software/\(software\)](https://www.softwareworld.co/top-cybersecurity-software/(software))

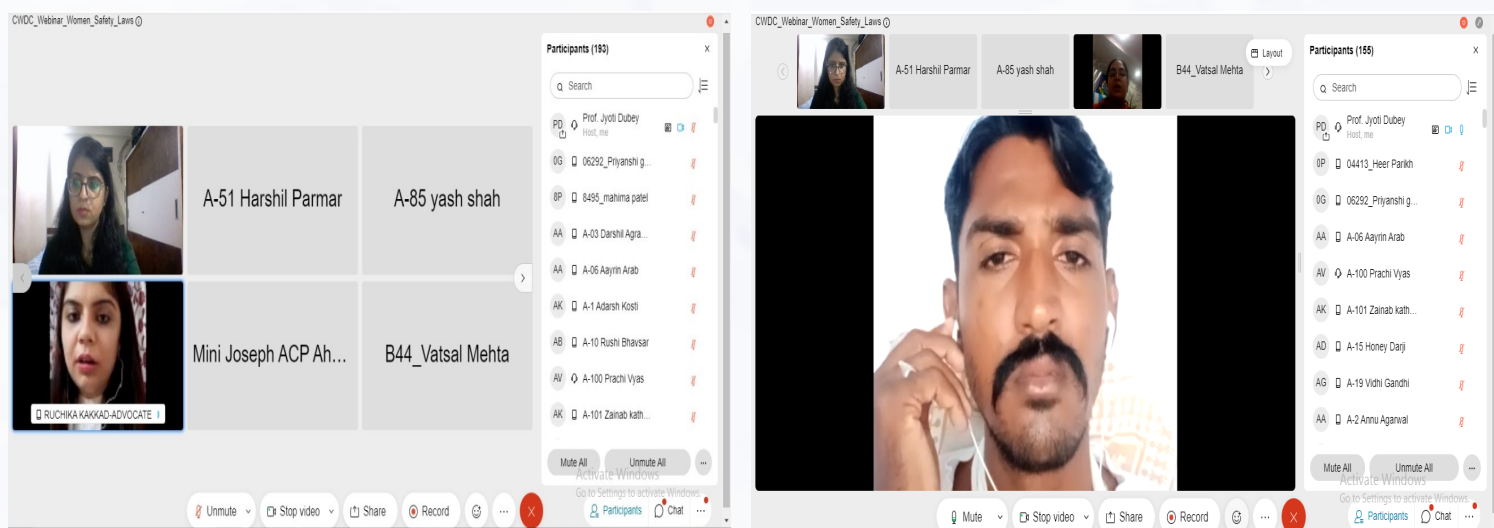
CO-CURRICULAR ACTIVITY

Collegiate Women Development Cell

Collegiate Women Development Cell organizes various awareness programmes for girls students. The following events were organized:

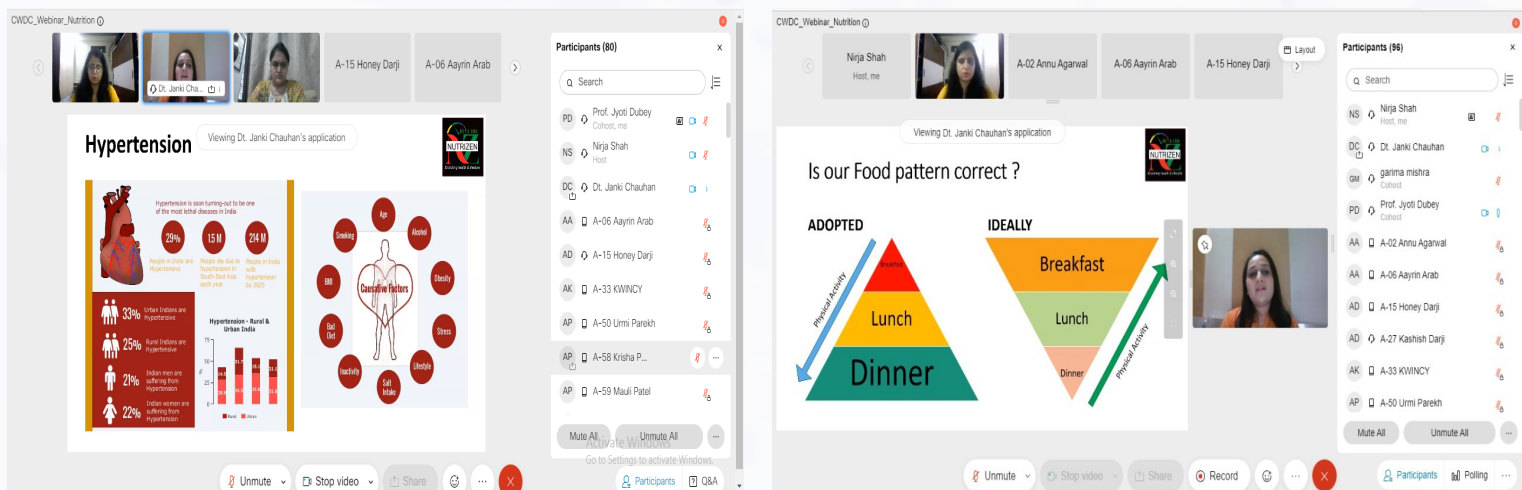
A virtual talk on Women Safety Laws: "Laws that protect women & their rights" was organized on 27th September, 2021. ACP Mini Joseph Sir, Ahmedabad Mahila Police station and Advocate Ruchika Kakad, Gujarat High Court, were the eminent speakers of the talk. Shri Jaldeepbhai from Ahmedabad Police Surakhsha Setu Cell was also one of the invitees of the programme.

The aim of this seminar was to build awareness about various laws that protect women and their rights. Students were made familiar with the availability of emergency helpline number -181 and mobile applications like 'Abhayam' and 'Grannus'. The talk concluded with an interactive session with students.



A webinar on 'Nutrition Demand for Youth' was held on 28th September 2021 with a motive to encourage youth for healthy eating. The expert, Dr Janki Chauhan, Clinical Dietitian from BAPS Yogiji Maharaj Hospital motivated students to embrace healthy food habits and discussed the diseases caused due to imbalanced diet and junk food.

She also discussed many health problems faced by women and how they need to take care of themselves to remain fit. She inspired them to lead a disease-free life by following a healthy lifestyle and good habits, such as exercise and a healthy diet that are likely to bring many benefits.



ACADEMIC ACTIVITIES

Alumni Talk

The institute is keen on being in touch with its alumni across the world. Sessions are arranged for Student-Alumni interaction. It provides students an exposure to alumni's work profile and culture. Moreover, students acquire knowledge about the recent trends and technologies of respective countries where alumni have settled.

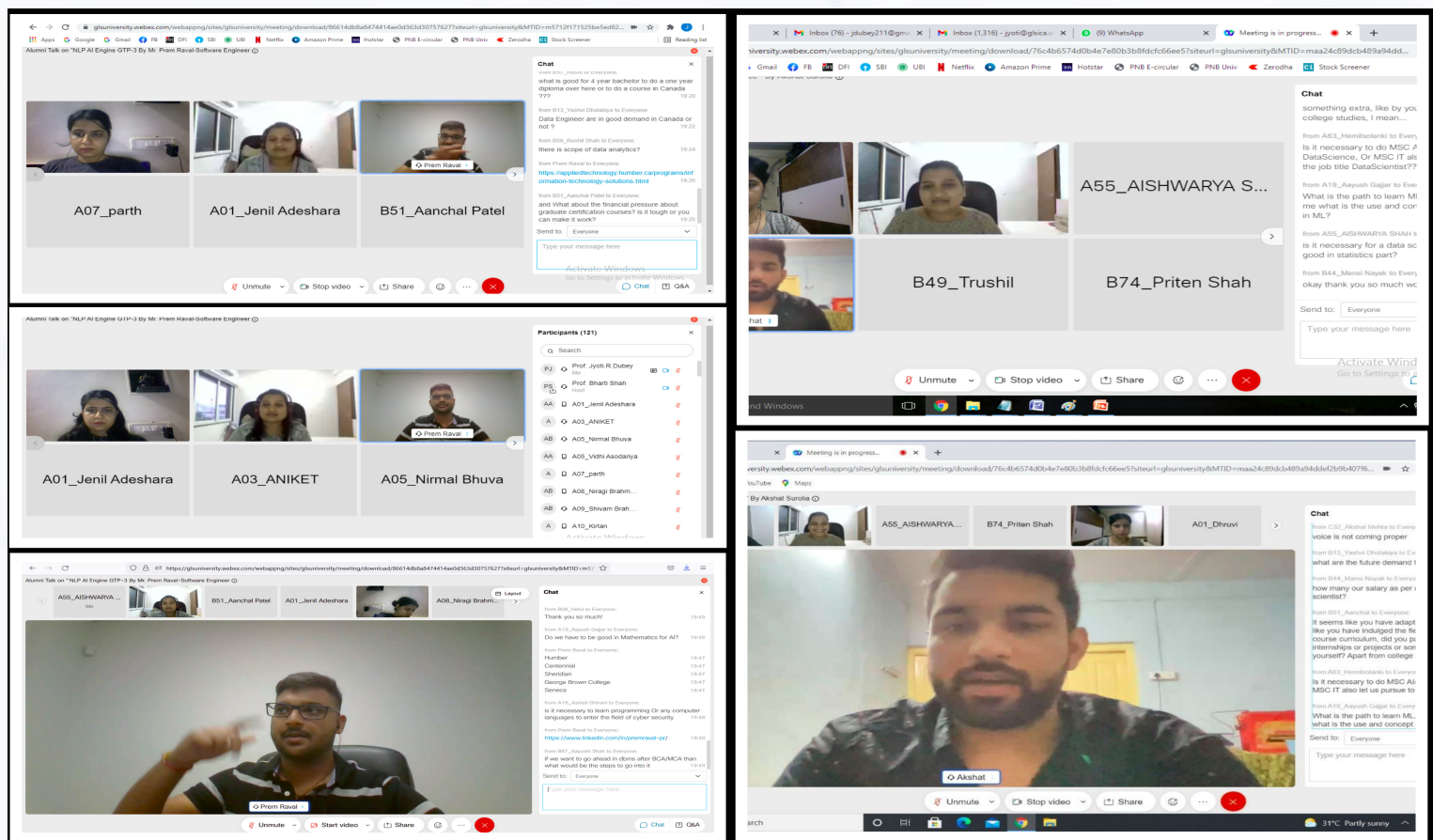
This semester we got connected to two of our alumni:

Mr. Prem Raval, software Engineer, STAN A.I., Toronto, Canada enlightened students with various emerging technologies such as NLP(Natural Language Processing) and Generative Pre-trained Transformer 3 (GPT-3) is an autoregressive language model that uses deep learning to produce human-like text. He shared information on Machine Learning and Artificial Intelligence correlation. Also he talked on various real time applications being developed at his current organisation based on Machine learning and AI. He also discussed the backend working of a virtual assistant technology Alexa. The talk was really interactive followed by question answer session.

He also talked on various trending technologies booming in IT sector in Canada and discussed the opportunities available for students aspiring to pursuing higher studies and job in Canada.

Mr. Akshat Surolia, Asso. Data Scientist, DSMATICS, Pune, Maharashtra shared his views on Data Science. He spoke on reflection of various applications of Data Science, its importance and advantages. He also explained the roles and responsibilities of the data scientist and how one can learn data science with python. Data scientists are experts who have business acumen and analytical skills as well as they can mine, clean and present data. Businesses use data scientists to source, manage, and analyze large amounts of unstructured data.

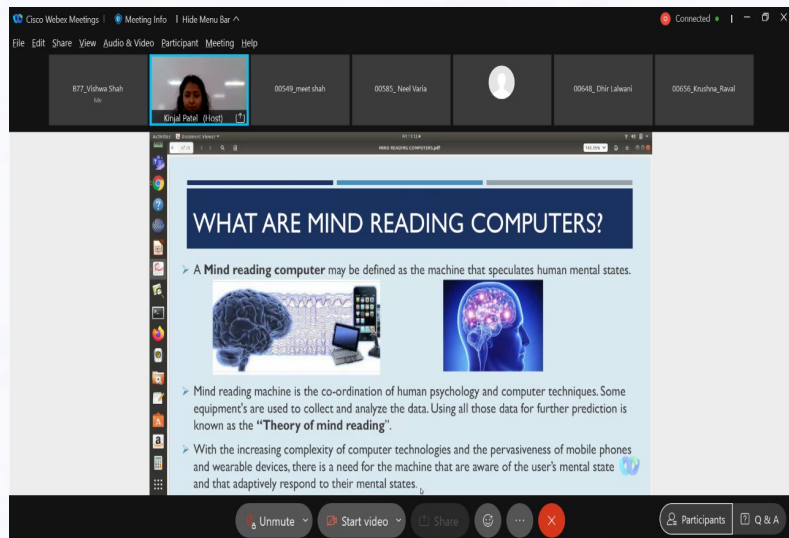
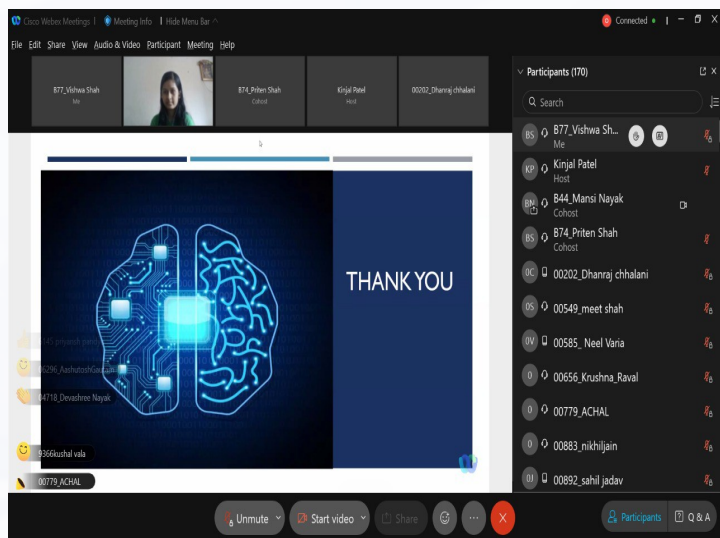
He defined the opportunities for Data Scientists at various IT companies in Pune. He too shared his personal inclinations to choose career as a data scientist. The talk ended with a question-answer session.



ACADEMIC ACTIVITIES

Tech Talk

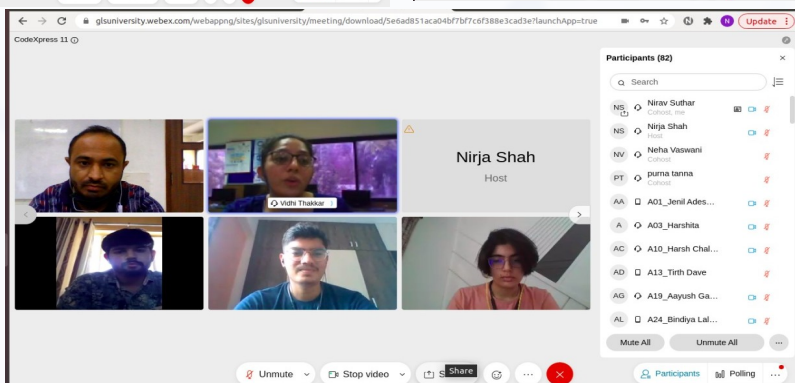
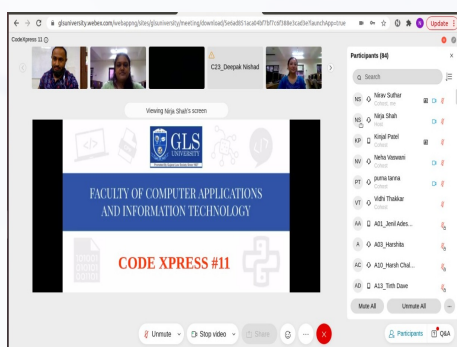
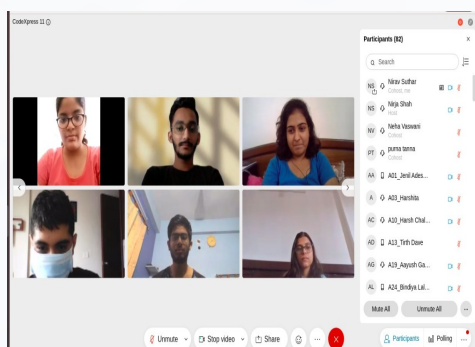
Tech Talks are futuristic technology-oriented talks wherein students explore various contemporary techniques and technologies and present the same to other students through talk shows. The Tech Talk ‘Mind Reading Computers’ was organized on 3rd September 2021. The theme was the concept of machines that speculate human mental conditions. The talk dealt with the applications of Mind Reading Computers specifically in the Military and Medical sectors and its future scope as advanced technology. Different mind-controlled devices as Neuralink and their functioning were also touched upon.



Code Express

The institute has started an initiative named Code Express where students can showcase their coding skills in a friendly yet spirited environment. Code Express#11 was held on 31st July 2021 on ‘Go language’. Around 85 students from BCA and iMSc (IT) participated in teams for the open-source programming competition.

A team of SY BCA - Aayush Gajjar and Jenil Adeshara as well as a team of FY iMSc (IT) - Yash Mehta and Krupesh Modi were the winners of this event. All the teams were well prepared and they used various programming skills to showcase their knowledge.



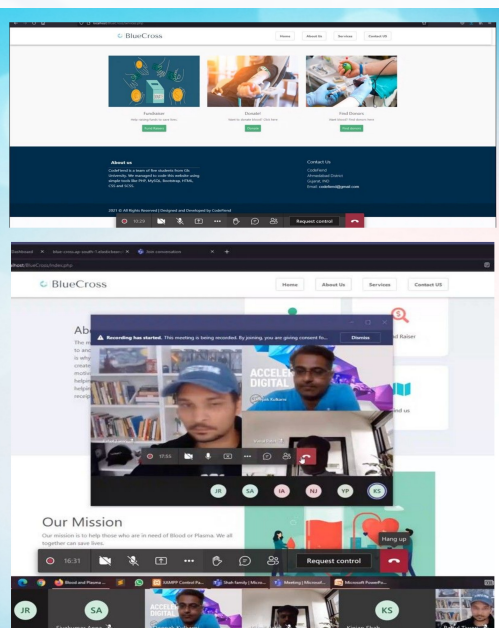
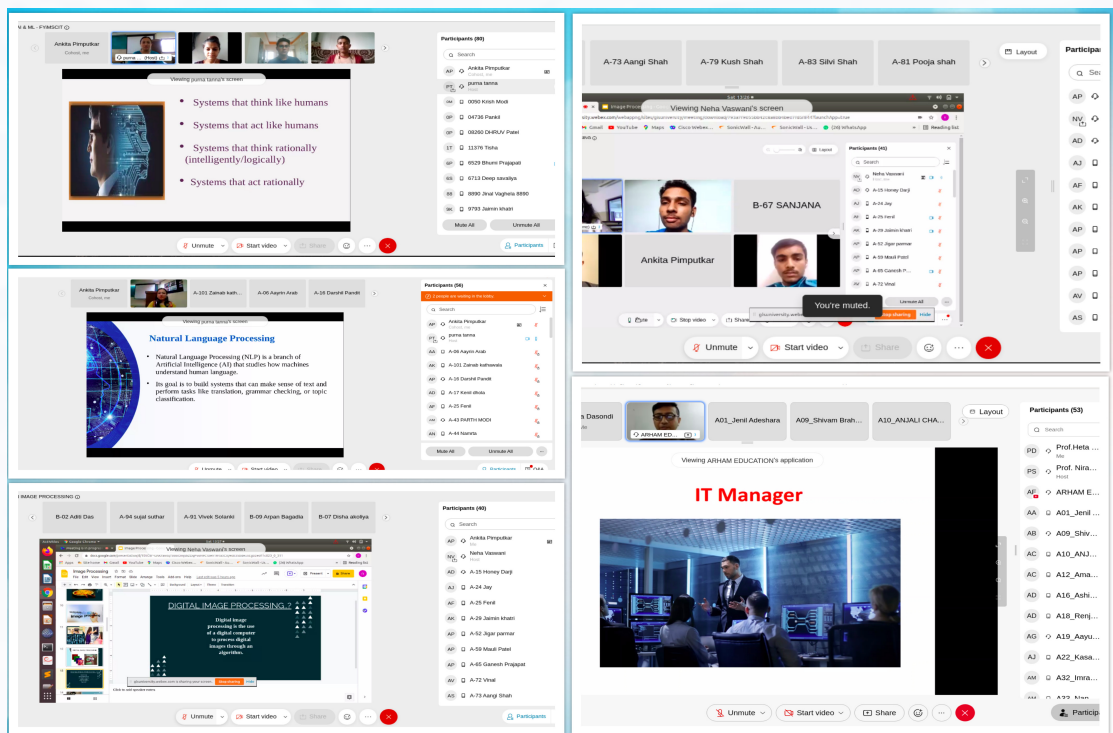
GLS UNIVERSITY
Faculty of Computer Applications & Information Technology
GLS FCAIT PRESENTS
CODE - XPRESS #11
THEME: GOOGLE GO
31 - 07 - 2021
2:00 to 4:00 PM
Webex Meet
For Registration visit:
<https://forms.gle/pPcMrdxtkxNuHTBR8>

ACADEMIC ACTIVITIES

Webinars & Expert Lectures

FCAIT organizes various workshops and seminars on upcoming technologies and current IT trends every year. Due to the pandemic this year various webinars were conducted online. Webinars on recent trends and technologies conducted are as below:

- * Big Data and Business Intelligence- Date: 3rd August 2021, Resource Person: Prof. Ankita Pimpotkar.
- * Emerging Trends in IT- Date: 11th September 2021, Resource Person: Prof. Ankita Kanojiya.
- * Artificial Intelligence & Machine Learning: Date: 18th September 2021, Resource Person: Dr Purna Tanna.
- * Swarm Intelligence: Date: 21st September 2021, Resource Person: Prof. Anjali Bobra.
- * Image Processing: Date: 25th September 2021, Resource Person: Prof. Neha Vaswani.
- * NLP: Date: 8th October 2021, Resource Person: Dr. Purna Tanna.
- * Cloud Computing: 16th October 2021, Resource Person: Prof. Nirav Suthar.
- * Career Options After BCA: 27th November, 2021, Resource Person: Mr. Umang Zaveri, Arham Education & I-inspire Education Pvt. Ltd.



Hackathon

Our team participated in State level "Smart Gujarat for New India Hackathon-Grand Finale" organised by SSIP, Gujarat Govt from 10th to 11th August, 2021. The theme of project was "Human Interacted Wireless Notice Board".

Our team "Code Fiend" participated in an International level HACK2VAX - GLOBAL HACKATHON 2021(PARTNER AWS), Organised by Infostrech from 09th to 11th July, 2021.

ACADEMIC ACTIVITIES

Faculty Achievements

- Ms. Tripti Dodiya, Faculty of Computer Applications & IT (FCAIT), GLS University was awarded the degree of Ph. D by Pacific University, Rajasthan under the guidance of Dr. Ali Yawar Reha. The topic of her Ph.D. research project was “Medical Question Answering System”.
- Ms. Poonam J. Dang, Faculty of Computer Applications & IT (FCAIT), GLS University was awarded the degree of Ph.D by GLS University, Ahmedabad under the guidance of Dr. Harshal Arolkar. The topic of her Ph.D. research project was “Automatic Online Evaluation of Electronic Circuits Designs”.
- Ms. Jyoti R. Dubey, Faculty of Computer Applications & IT (FCAIT), GLS University was awarded the degree of Ph.D by GLS University, Ahmedabad under the guidance of Dr. Ankit Bhavsar. The topic of her Ph.D research project was “Wireless Sensor Network Based Accidents Avoidance Architecture for the Fleet of Long Route Vehicles”.
- Dr. Ankit Bhavsar won best paper award for the paper entitled “Prototype Development using Arduino for WSN based Crowd Monitoring Architecture at KSCON2021 Conference organized by Gujarat University.
- Prof. Jyoti R. Dubey and Dr. Ankit Bhavsar presented a paper “Communication Protocols for WSN Based Accidents Avoidance Architecture for the Fleet of Long Route Vehicles”,ISSN: 1548-7741, JOICS, Volume 11, Issue 7th – July 2021.
- Prof. Kinjal Patel presented paper “An effective Approach to Classification of White Blood Cell using Deep Learning”, ISBN: 21945357, Springer Book Chapter International e-Conference on Intelligent Systems and Signal Processing -August 2021.
- Prof. Kinjal Patel presented paper “Automatic License Plate Detection & Recognition using Deep Learning”, ISSN: 00119342, Design Engineering (Toronto), November 2021.
- Dr. Disha Shah has invited as an Evaluator for “ProTech-2021 – A National Level Competition for Diploma students” scheduled on 7th and 8th May 2021[Online Mode] at Symbiosis Institute Of Technology.
- Dr. Ankit Bhavsar has published a book on “Object Oriented Concept & Programming (Core Java)”,ISBN NO: 978-93-91071-00-4, Publisher: Dr. BabaSaheb Ambedkar Open University, Ahmedabad, Publication Year: June 2021.

Cyber Security Crossword!!!!

Across

2. malware that employs encryption to hold a victim's information at ransom.
5. weaknesses in a system that gives threats the opportunity to compromise assets.
6. uses trial-and-error to guess login info, encryption keys, or find a hidden web page.
8. type of cybersecurity attack during which malicious actors send messages pretending to be a trusted person or entity

Down

1. the ability an organization or individual has to determine what data in a computer system can be shared with third parties.
3. intrusive software that is designed to damage and destroy computers and computer systems
4. threat that embeds itself within a computer or mobile device and then uses its resources to mine cryptocurrency.
7. type of malicious code or software that looks legitimate but can take control of your computer.

