



SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)
RAMAPURAM



CYBER CARNIVAL

2024

PRESENTS

CYBER CHRONICLE

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

FACULTY OF ENGINEERING AND TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

WITH SPECIALIZATION IN CYBER SECURITY

RAMAPURAM , CHENNAI - 600 089



cybercarnival.in



[cyber_carnival_srmrmp/](https://www.instagram.com/cyber_carnival_srmrmp/)



hello@cybercarnival.in

Department of Computer Science and Engineering



The department of Computer Science and Engineering (CSE) at SRM Institute of Science and Technology was established in the year 2004 with the aim of imparting quality education to students and bring out the best in them. The key goal of the department is to provide best IT infrastructure, world class learning and research environment, adopt industry practices through industry collaborations and inculcate moral and ethical values, with students hailing from all states and union territories of India, the department was established to meet the demand for well-qualified computer professionals. The promptness of the students to learn makes it easier for the industry trained experienced faculty to produce top-notch engineers who are being recruited by reputed companies all over the world.

About Cyber Security Department

The specially designed B.Tech. Programme in Cyber Security exclusively offers the students a thorough knowledge and hands-on skills in the areas of secure system architecture, secure coding, analysing the cyber-attacks, ethical hacking, evaluating the strength of using penetration testing and cyber forensics. The curriculum is also aimed to provide adequate knowledge in the areas of digital and cyber forensics, ethical hacking, penetration testing, secure coding, steganography, watermarking techniques and malware analysis.



Patrons

CHIEF PATRONS

Dr. R. Shivakumar

Chairman, SRM Group of Institutions,
Ramapuram & Trichy

Mr. S. Niranjan

Co-Chairman, SRM Group of Institutions,
Ramapuram & Trichy

PATRONS

Dr. N. Sethuraman

Chief Director, SRM Group of Institutions

Dr. K. V. Narayanan

Associate Director, SRM Ramapuram

Dr. M. Murali Krishna

Dean(E&T), SRMIST Ramapuram

Dr. Balika J Chelliah

Vice Principal/Admin), SRMIST Ramapuram

CONVENOR

Dr. K. Raja

Professor & HoD, Dept. of CSE
SRMIST, Ramapuram

CO-CONVENER

Dr. Shiny Duela J

Deputy HoD - Cyber Security,
SRMIST, Ramapuram

Dr. Sathya Priya S

Associate Professor, Dept. of CSE
SRMIST, Ramapuram

FACULTY COORDINATOR

Dr. Subashka Ramesh S

Associate Professor , Dept. of CSE
SRMIST, Ramapuram

Chairman's Desk



SRM Group of Educational Institutions

Dr. R. Shivakumar, M.D.,

Chairman: SRM Group of Institutions
Chennai Ramapuram & Trichy



Dr. R. Shivakumar, M.D

CHAIRMAN'S MESSAGE

It is heartening to know that the Department of Computer Science and Engineering (Cyber Security), SRM Institute of Science & Technology, Ramapuram is conducting Cyber Carnival 2024 on 12th February 2024.

The world is currently witnessing vast digitization and use of cloud services in all fields. This is closely accompanied by very many challenges especially related to data, the chief of which is data security. Businesses are constantly jolted by data theft and damage which mainly impacts the reputation of the organization. In this context cyber security assumes huge significance.

The conduct of Cyber Carnival will lead to creating awareness among all stakeholders on various stealth methods employed during cyber attacks and helps them to stay alert on a personal as well as professional front. The collaborative efforts will help in promoting critical security controls and ensure a commitment to a secure digital future.

I am confident that this forum will be a source of inspiration, knowledge exchange and the birthplace of groundbreaking solutions. Together, let's navigate the challenges and create positive change in the cybersecurity landscape.

Best wishes!

R. Shivakumar

CHAIRMAN

SRM Ramapuram & Trichy Campus

Co-Chairman's Desk



SRM Group of Educational Institutions



Mr. S. Niranjan, M.S.,

CO-CHAIRMAN'S MESSAGE

I am delighted to learn that Cyber Carnival 2024 is being organized by the Department of Computer Science and Engineering (Cyber Security), SRM Institute of Science & Technology, Ramapuram, Chennai.

The uncontrolled and unprecedented growth of digital networking in all arenas have opened up innumerable possibilities in the digital tapestry. Of the many challenges being faced, securing data from malicious attacks is crucial. This involves critical factors like visibility, mitigation, prioritizing, and encryption. Cyber security measures are the need of the day for businesses to keep off cybercrimes and cyber-attacks.

Cyber Carnival 2024, I believe will unfold as a masterpiece of diverse activities, entwining the excitement of the Cyber Hackathon, the enlightening discussions of the Cyber Conclave, the resonance of the impactful Cyber Awareness Campaign and a captivating array of both technical and non-technical events. This can go a long way in sculpting a secure and harmonious digital future.

My best wishes!

A handwritten signature in black ink, appearing to read 'N. S.'

CO-CHAIRMAN

SRM Ramapuram and Trichy Campus

No. 50, Bharathi Salai, Ramapuram, Chennai - 600089, Phone: +91 4392 3256 / 3098

Chief Director's Desk



SRM Group of Educational Institutions



Dr. N. Sethuraman

CHIEF DIRECTOR'S MESSAGE

I am happy that the Department of Computer Science and Engineering (Cyber Security), Faculty of Engineering and Technology, SRM Institute of Science & Technology, Ramapuram is organizing Cyber Carnival 2024.

Digital transformation is being embraced by innumerable companies in the current internet age. The corollary of this is the impending risk of cybercrimes which is increasing at a rapid rate and hence the need for cybersecurity. Businesses are investing heavily against hackers to protect from unauthorized access or attacks to data. To mitigate this, the right tools and robust strategies are required.

It is heartening that the department has planned this carnival as it will serve as an eye opener to the gullible students and common man. The awareness created will lead them on to protect themselves against frauds and online assaults and prevent theft or loss of sensitive and confidential information. Also, the carnival will be a source of inspiration, fostering collaboration and yielding groundbreaking solutions. I am confident that the discussions, connections and insights gained during Cyber Carnival 2024 will leave an indelible mark on our collective journey toward a safer digital landscape.

Best wishes for a successful and enriching Cyber Carnival 2024!


Dr. N. SETHURAMAN
CHIEF DIRECTOR
SRM Group of Institutions
Chennai Ramapuram & Trichy

No. 50, Bharathi Salai, Ramapuram, Chennai - 600089, Phone: +91 4392 3256 / 3098

Associate Director's Desk



Dr. K. V. Narayanan

Dear Participants, Collaborators, and Honored Guests,
With immense delight, I extend warm wishes to all as we commence on the exhilarating journey of Cyber Carnival 2024. My sincere gratitude goes to our esteemed sponsors, partners, and dedicated participants for their invaluable contributions, as your unwavering support is the very heartbeat of this exceptional event.

This carnival transcends being a mere gathering; it is a jubilation of shared dedication to propelling cybersecurity forward. From the thrilling Cyber Hackathon to the enlightening Cyber Conclave, the impactful Cyber Awareness Campaign, and the diverse spectrum of technical and non-technical events, we witness a harmonious convergence of expertise and innovation.

May this occasion stand as a vibrant wellspring of inspiration, nurturing collaboration and sparking the emergence of groundbreaking solutions. I am confident that the dynamic interactions and profound insights gained during Cyber Carnival 2024 will play a pivotal role in steering our collective journey toward a more secure and resilient digital landscape.

My best wishes for a triumphant and enriching Cyber Carnival 2024!

Dr. K. V. Narayanan
Associate Director
SRM IST Ramapuram

Dean's Desk



SRM Institute of Science & Technology
Ramapuram Campus



Dr. Murali Krishna, B.E, M.Tech, Ph.D, MISTE, FIE, C.Engg,
Dean's Desk



Dr. Murali Krishna

Dear Participants, Esteemed Colleagues, and Cyber Enthusiasts,

It is with great pleasure that I extend a warm welcome to all as we embark on the enthralling journey of Cyber Carnival 2024. In expressing my sincere gratitude to our esteemed sponsors, partners, and dedicated participants, I acknowledge the invaluable contributions that shape the essence of this extraordinary event.

This carnival stands as more than a mere celebration; it is a testament to our shared commitment to advancing cybersecurity. From the electrifying Cyber Hackathon to the enlightening Cyber Conclave, the impactful Cyber Awareness Campaign, and the diverse array of technical and non-technical events, we find ourselves immersed in a fusion of expertise and innovation.

I encourage you to embrace this occasion as a unique opportunity to deepen your understanding of the cyber landscape. In a world where every sector is increasingly intertwined with technology, the Cyber Carnival serves as a vital platform to explore the intricate web of cybersecurity challenges and solutions.

May this event serve as a catalyst for inspiration, fostering collaborative discussions and paving the way for groundbreaking perspectives within the cyber domain. I am confident that the insights gained during Cyber Carnival 2024 will not only enrich your experience but also contribute significantly to our collective journey towards a more secure and resilient digital future.

Best wishes for a successful and enlightening Cyber Carnival 2024!

A handwritten signature in blue ink, appearing to read "M. M. Krishna".

Dean

Dr. Murali Krishna

SRM Institute of Science & Technology
Ramapuram Campus

SRM Institute of Science & Technology

Ramapuram Campus, Bharathi Salai, Ramapuram, Chennai - 600089, Tamilnadu, India
Phone: +91 44 4392 3133 | E-Mail: office.admin@ist.srmrmp.edu.in | Website: <https://srmrmp.edu.in>

Vice Principal (Admin)'s Desk



Dr. Balika J Chelliah

Dear Participants, Collaborators, and Honored Guests,
With immense delight, I extend warm wishes to all, as we commence on the exhilarating journey of Cyber Carnival 2024. My sincere gratitude goes to our esteemed sponsors, partners, and dedicated participants for their invaluable contributions, as your unwavering support is the very heartbeat of this exceptional event.

From the thrilling Cyber Hackathon to the enlightening Cyber Conclave, the impactful Cyber Awareness Campaign, and the diverse spectrum of technical and non-technical events, we witness a harmonious convergence of expertise and innovation. May this occasion stand as a vibrant wellspring of inspiration, nurturing collaboration and sparking the emergence of groundbreaking solutions. I am confident that the dynamic interactions and profound insights gained during Cyber Carnival 2024 will play a pivotal role in steering our collective journey toward a more secure and resilient digital landscape. My best wishes for a triumphant and enriching Cyber Carnival 2024!

A handwritten signature in blue ink, appearing to read "Balika J Chelliah".

**Dr.Balika J Chelliah M.E., Ph.D.
Professor & VP Admin
SRM IST, Ramapuram**

HOD's Desk



Dr. K. Raja

Dear Participants, Collaborators, and Honored Guests, With immense delight, I extend warm wishes to all as, we commence on the exhilarating journey of Cyber Carnival 2024. My sincere gratitude goes to our esteemed sponsors, partners, and dedicated participants for their invaluable contributions, as your unwavering support is the very heartbeat of this exceptional event.

This carnival transcends being a mere gathering; it is a jubilation of shared dedication to propelling cybersecurity forward. From the thrilling Cyber Hackathon to the enlightening Cyber Conclave, the impactful Cyber Awareness Campaign, and the diverse spectrum of technical and non-technical events, we witness a harmonious convergence of expertise and innovation. May this occasion stand as a vibrant wellspring of inspiration, nurturing collaboration and sparking the emergence of groundbreaking solutions.

I am confident that the dynamic interactions and profound insights gained during Cyber Carnival 2024 will play a pivotal role in steering our collective journey toward a more secure and resilient digital landscape. My best wishes for a triumphant and enriching Cyber Carnival 2024!

A handwritten signature in blue ink, appearing to read "K. RAJA".

**Dr. K. Raja M.E., Ph.D.
Professor & HOD –CSE
SRM IST, Ramapuram**

Deputy HOD's Desk



Dr. Shiny Duela J

Dear Participants, Supporters, and Cyber Aficionados,
It brings me immense joy as the co-convener of Cyber Carnival 2024 to extend heartfelt wishes for an unequivocal success in this exciting odyssey we are poised to undertake.

A genuine note of appreciation goes out to all participants, sponsors, and contributors, whose dedication and fervor have been instrumental in shaping this event. Your commitment sets the stage for what promises to be an extraordinary convergence at the crossroads of innovation and cybersecurity. This Cyber Carnival transcends the conventional. From the riveting Cyber Hackathon to the enlightening Cyber Conclave, the impactful Cyber Awareness Campaign, and the diverse spectrum of technical and non-technical events, each facet has been meticulously curated to offer a distinctive and enriching journey. May this carnival serve as a nexus for establishing new connections, garnering profound insights, and igniting innovative solutions in the perpetually evolving realm of cybersecurity. Wishing you all an exceptionally successful, enlightening, and indelibly memorable Cyber Carnival 2024!

A handwritten signature in blue ink, appearing to read "Shiny Duela J".

Dr. Shiny Duela J
Deputy HoD - Cyber Security
SRM IST, Ramapuram

Co-Convenor's Desk



Esteemed Participants,

Dr.Sathya Priya S

In my capacity as the Coordinator of the eagerly anticipated Cyber Carnival '24, I am brimming with anticipation as we approach the realization of this exceptional event. It signifies a pivotal moment in our academic journey, embodying the dynamic convergence of technology, innovation, and the extraordinary talents of our student community.

Amidst the lively ambiance of the carnival, students will have an exceptional opportunity to showcase not only their technical acumen but also to engage in idea exchange, collaboration, and mutual inspiration. It serves as a vibrant stage where innovation takes the spotlight, providing a platform for participants to delve into cutting-edge concepts and push the boundaries of what is possible. Together, we can establish a benchmark of excellence and craft enduring memories that will resonate far beyond the event itself.

May the Cyber Carnival thrive with resounding success...

A handwritten signature in blue ink, appearing to read "S. Sathya Priya".

Dr. Sathya Priya S

Associate Professor, Dept. of CSE

SRM IST, Ramapuram

Faculty Coordinator's Desk



Dear Participants,

Dr. Subashka Ramesh S

As the Coordinator of our highly anticipated Cyber Carnival '24, I am filled with excitement as we approach the realization of this extraordinary event. It signifies a pivotal moment in our academic journey, embodying the dynamic intersection of technology, innovation, and the remarkable talents of our student community.

Within the bustling atmosphere of the carnival, students will have a remarkable opportunity to not only demonstrate their technical prowess but also to exchange ideas, collaborate, and inspire one another. It serves as a vibrant showcase where innovation takes center stage, providing a platform for participants to delve into cutting-edge concepts and push the boundaries of possibility. Your active involvement and collaboration are paramount to the success of this event. Let us unite our efforts to ensure that the Cyber Carnival exceeds expectations and leaves a lasting impact on all who attend. Together, we can set a standard of excellence and create enduring memories that will resonate far beyond the confines of the event itself.

May the Cyber Carnival thrive with resounding success..

A handwritten signature in blue ink, appearing to read "Subashka" followed by a surname.

Dr. Subashka Ramesh S
Associate Professor, Dept. of CSE
SRM IST, Ramapuram

President's Desk



I am deeply humbled as I reflect on the journey that has led to the success of Cyber Carnival 24. As the president of this esteemed event, I am profoundly grateful for the collective efforts that have made this achievement possible. Since its inception, my focus has been to exceed expectations and deliver an unforgettable experience for our participants, sponsors, and attendees. Through meticulous planning and tireless coordination, my team and I have crafted a program that reflects the dynamic landscape of cybersecurity. I am especially thankful for the invaluable partnerships and sponsorships we have secured, which have enriched the experience for our participants and provided them with unparalleled networking opportunities. Central to our success is the spirit of collaboration within our department. It is through the dedication and talent of our team members that our vision has come to fruition.

As Cyber Carnival 24 unfolds, I am filled with gratitude for the opportunity to lead this incredible endeavour. I look forward to witnessing its continued success and growth in the years to come.

**V.P. Yukesh
B.Tech CSE CS 'B'
3rd Year**

Vice President's Desk



As the Vice President of Cyber Carnival at SRMIST, Through effective communication and decision-making, I've steered the ship of Cyber Carnival, ensuring that our initiatives not only meet but exceed expectations, creating a lasting impact on the tech landscape of SRMIST. I have led various tech events aimed at creating a space where students can experiment and innovate together. Workshops, industry-driven talks and experiential activities have offered students the unique perspective that goes beyond what they learn in classrooms spawning a cross breed between academia and practice. The events of the tech department with my leadership have become an incubator for ideas and attract students from different fields. Stepping beyond the traditional borders of tech events, Cyber Carnival is a symbol that passion and purpose are indeed one. We don't just talk about what happened, but of growth through experiences and the tireless support that characterizes SRM tech enthusiasts.

**Ashwathaman. S
B.Tech CSE CS 'B'
3rd Year**

Carnival Coordinator's Desk



As the Carnival Coordinator, I am privileged to offer a unique perspective on this upcoming event. While the Cyberthon, a 24-hour Cyber Security Hackathon provided a thrilling prelude, the true spectacle unfolds on February 12th and 13th at SRMIST, Ramapuram. More than a competition, Cyber Carnival serves as a vibrant platform for learning, connection, and fostering a future where cybersecurity awareness and innovation flourish. The carnival caters to diverse interests. Technical workshops led by industry veterans delving into ethical hacking, digital forensics, and blockchain security will equip participants with cutting-edge skills, while technical events like "Capture The Flag" and "Behind The Crime" offer an engaging, collaborative approach to understanding cybersecurity concepts. Beyond technical prowess, Cyber Carnival fosters discussions on critical issues like cyber ethics and the future of information security. Cyber Conclave invites participants to voice their opinions and actively shape the evolving digital landscape. It's a collaborative ecosystem where students, professionals, and enthusiasts come together to learn, share knowledge, and contribute to a more secure digital future. It's the combined dedication of our team, the passion of participants, and the collaborative spirit that make this event truly remarkable. My role as Coordinator lies in orchestrating this symphony of learning, innovation, and connection. Witnessing the event come to life and seeing participants from diverse backgrounds unite under the banner of cybersecurity is immensely rewarding.

Sarvesh M Rao
B.Tech CSE CS 'A'
3rd Year

About Cyber Carnival '24

The **Cyber Carnival** at SRM IST Ramapuram is an electrifying event hosted by the cybersecurity department, promising an immersive journey into the world of digital defense and innovation. Fusing education with excitement, the carnival showcases cutting-edge technologies, interactive workshops, and engaging competitions designed to sharpen skills and raise awareness about cybersecurity threats and solutions. Participants can expect riveting demonstrations, insightful talks by industry experts, and hands-on experiences that illuminate the importance of safeguarding our digital landscape. Whether you're a novice or a cybersecurity expert, the **Cyber Carnival** offers something for everyone, fostering collaboration, knowledge exchange, and a shared commitment to building a safer online environment. Join us for an unforgettable celebration of cybersecurity excellence and empowerment at **SRM Ramapuram's Cyber Carnival !**

TECHNICAL EVENTS

Cyberthon:-

A hackathon-style competition where participants work on various cybersecurity challenges and compete to solve them in the fastest and most efficient way possible.

Capture The Flag:-

Capture The Flag competition requires Participants to use their cybersecurity skills to solve various tasks from Domains like Reverse Engineering, OSINT, and cryptography. These flags are usually either a secret string or a hidden code. CTFs stimulate real-life cybersecurity events and require problem-solving skills and teamwork.

About Cyber Carnival '24

Behind The Crime:-

The World Of Digital Forensics: Step into the realm of digital forensics, where omnipresent eyes leave no refuge in our digitized world. Navigate with meticulous precision and empathy as you probe recent crimes, delving into the digital sphere. Uncover information by penetrating the intricacies of digital lives, where each virtuous pursuit may reveal unexpected dead-ends, eluding our initial scrutiny.

Bug Bounty:-

Embark on an exciting cybersecurity adventure with our Bug Bounty Challenge! Ethical hackers and enthusiasts, your mission is to uncover vulnerabilities in the system! Join us in creating a safer online landscape. Register now to be part of this exciting Bug Bounty Challenge and contribute to a more secure digital future!

NON-TECHNICAL EVENTS

Surviva:-

Surviva immerses participants in life's tempests, a shipwreck experience revealing the raw power of nature. Navigating simulated challenges, individuals confront adversity, testing resilience. Every decision is critical as they face survival's harsh realities.

Lights Out:-

The short film competition invites filmmakers to tell captivating stories in a limited timeframe, typically ranging from a few minutes to 15 minutes. It's a platform for emerging talent to showcase creativity, exploring diverse themes and genres. Judged on originality and technical skill.

About Cyber Carnival '24

What's On TV?:-

Get ready to surf through the channels of creativity in this high-energy event! Teams will bring the TV to life as they imitate popular channels, from sports to news to cooking shows. But here's the twist the judge holds the remote, with the power to change channels and give commands like reverse, pause, and fast-forward. It's a whirlwind of entertainment, improvisation, and quick wits as teams perform on demand, making this event a rollercoaster of fun and surprises!

Ad Pro:-

Adpro is the perfect example of an interactive marketing project in which users create and present spontaneous commercials. This lively arena, which is frequently found in academic and professional contexts, calls for creativity, spontaneity, and skillful communication. To captivate audiences, participants must construct brief yet compelling narratives. This creates an engaging platform for brand exposure and showcasing.

Squad Up:-

Embark on an adrenaline-pumping gaming adventure with Valorant! , this thrilling first-person shooter is a captivating blend of strategy and skill. Join us for an exciting gaming session where you'll choose unique agents, each with their special abilities, and team up for heart-pounding 5v5 matches. Bring your friends, make new ones, and let the gaming excitement begin!

Last On Standing:-

It is a title event where only one participant can claim the title, and the judges determine the topics and rounds on the spot, with their decisions being final. This setup adds an element of unpredictability and challenge for the participants.

About Cyber Carnival '24

Cyber Conclave:-

Cyber Conclave offers a vital forum, where industry experts illuminate the significance of data protection, privacy, and cybersecurity. Through insightful panel discussions, attendees gain actionable strategies and understanding to fortify digital defenses and safeguard valuable information in an increasingly interconnected world.



Dr. Mahesh Kalyanaraman

Associate Vice President Risk and
Compliance
HCL Technologies



Mr. Abhishek Kokate

Clients Advisor
Digital Risk Management
Kanoo Elite



Mr. Bharani Ramasamy

Senior Director
Global Networks & Security
Virtusa Corporation



Mr. Ramu Para

Associate Director - Cybersecurity
HTC Global Services



Mr. Suresh Vedakumar

Associate Vice President
& Lead - ITSM
Mphasis



Mr. Balachandar Natarajan

Platform Engineering Manager
Ford Motor Company



Mrs. Panchi Samuthirakani

Founder and Managing Director –
YesPanchi Tech Services

About Cyber Carnival '24

SEMINAR AND SHARK TANK:-

TOPIC: CYBER SECURITY ENTREPRENEURSHIP

Elevate your knowledge at our seminars which give a platform for insights, discussions, and growth, where industry experts share insights on cutting-edge technology and entrepreneurship in an innovation-packed session. Then, witness the Shark Tank session where aspiring entrepreneurs can present their innovative business ideas to our panel of judges, who will provide valuable feedback and guidance to help refine their concepts. Seminars for Wisdom, Shark Tank for Ventures – Your Dual Ticket to Knowledge and Innovation!



Mr. Renganathan P
Founder of R Protocols
Ethical Hacker



Mr. Abhisek R
Security Researcher
Team Inflnity (team lead)



Mr. Gnana Aravind K
Roboticist and Hacktivist
Founder and Director of the
Threat Cops

About Cyber Carnival '24

WORKSHOP:-

TOPIC: MASTERING ETHICAL HACKING AND CYBERSECURITY WORKSHOP

Join our '**Mastering Ethical Hacking and Cybersecurity Workshop**' for a deep dive into ethical hacking methodologies, tools, and best practices. Gain hands-on experience in penetration testing, vulnerability assessment, and risk analysis. Learn legal and ethical considerations while exploring real-world case studies. Elevate your cybersecurity skills and protect digital assets effectively in today's dynamic threat landscape.



Mr. Upendra

Head of RedTeaming
Supraja Technologies



Mr. Krishna

Senior Security Analyst
Supraja Technologies



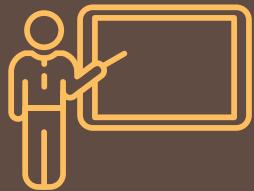
Mr. Kumar

Mentor
Supraja Technologies

Cyber Awareness Campaign



The Cyber Awareness Campaign, "Think Before You Click," unfolded with a dynamic lineup of interactive elements to engage participants. From immersive cyber games to captivating interactive campaign stalls, the event aimed to educate and empower individuals to make informed decisions in the digital realm. The inclusion of a human chain and a miming act added a creative touch, reinforcing the campaign's message in a memorable and impactful way. Through these diverse activities, the initiative not only raised awareness but also actively involved attendees, encouraging a collective commitment to online safety and responsible digital practices.

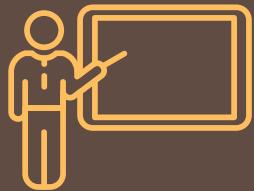


Faculty's Corner

The Opportunities and Threats of Implementing AI in Cybersecurity

The integration of Artificial Intelligence (AI) into cybersecurity heralds a transformative era, presenting a dual landscape of unprecedented opportunities and subtle yet potent threats. AI's capacity to rapidly analyze vast datasets and discern complex patterns enhances threat detection, allowing cyber security systems to evolve beyond traditional rule-based approaches. As AI algorithms become more sophisticated, cybercriminals may exploit these very technologies to orchestrate advanced, AI-driven attacks, posing a serious threat to digital security. Striking a delicate balance between leveraging AI's potential to fortify cyber defenses and navigating the evolving threat landscape requires a nuanced approach, involving continual innovation, adaptive strategies, and a vigilant cybersecurity community to harness the opportunities while mitigating the inherent risks. In conclusion, the synergy of AI and cybersecurity presents an era of unprecedented potential and peril. As organizations increasingly rely on cloud services, understanding and implementing robust security practices within the cloud environment is paramount. By adopting a proactive approach, regularly assessing security measures, and staying informed about the evolving threat landscape, businesses can harness the full potential of cloud computing while mitigating potential security risks. Cloud security is a shared responsibility, and collaboration between CSPs and their customers is crucial for building a secure and resilient cloud infrastructure.

**Dr. Pavithra Guru
Assistant Professor/CSE**

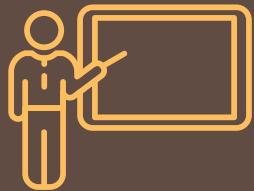


Faculty's Corner

The Dark Web: A Haven for Cybercriminals

The Dark Web, a cryptic enclave concealed beneath the surface of the internet, stands as an ominous haven for cybercriminals, operating beyond the scope of conventional oversight. This clandestine corner of cyberspace, accessible through specialized browsers like Tor, is characterized by anonymity, encryption, and decentralized architecture, creating an ideal environment for covert and illicit activities. The Dark Web operates as a hidden economy where cybercriminals engage in a myriad of nefarious enterprises, from the sale of stolen data and hacking tools to the distribution of illicit substances. This collaborative nature of the Dark Web poses a significant challenge for cybersecurity professionals, as cyber threats evolve rapidly in this dynamic environment. Ethical hackers play a crucial role in navigating the treacherous terrain of the Dark Web. Armed with the mission to uncover vulnerabilities and identify potential threats, these cybersecurity professionals tread cautiously in this digital underworld. Their work involves monitoring forums, analyzing trends, and collaborating with law enforcement to gather intelligence on emerging cyber threats. As the Dark Web evolves, the delicate balance between privacy and security intensifies. The global imperative to fortify digital defenses becomes increasingly paramount. Governments, businesses, and cybersecurity professionals must collaborate on an international scale to dismantle the infrastructure supporting cybercrime on the Dark Web.

**Mr. Hariharan B
Assistant Professor/CSE**



Faculty's Corner

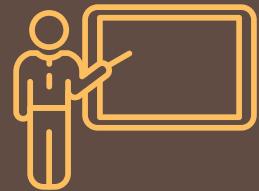
Escalating Cyber Threats: Urgent Steps for Enhanced Protection

Cyber threats are rapidly evolving, with advanced persistent threats (APTs) and supply chain attacks on the rise. The SolarWinds breach exposed vulnerabilities in widely used software, emphasizing the need for heightened cybersecurity. Ransomware attacks, exemplified by the Colonial Pipeline incident, pose a growing risk to corporations and critical infrastructure.

As technology advances, cybercriminals leverage artificial intelligence and exploit IoT vulnerabilities. A collaborative approach is crucial; governments, industries, and cybersecurity experts must unite to share intelligence and establish robust regulatory frameworks. Proactive measures, including regular security audits, employee training, and advanced threat detection, are essential to safeguard our digital landscape. Adapting to the evolving threat landscape requires a collective effort, to ensure the resilience of our interconnected systems.

In conclusion, as the article advocates for a collective effort to adapt to this evolving threat landscape, it underscores the necessity for a united front in safeguarding our digital infrastructure. The emphasis on collaboration among governments, industries, and cybersecurity experts, coupled with the implementation of proactive measures, serves as a rallying call. The narrative encourages a comprehensive approach involving routine security audits, continuous employee training, and the integration of advanced threat detection technologies.

**Mrs. Sridevi
Assistant Professor/CSE**



Faculty's Corner

Digital Predators: Unmasking the Menace of Cybercrime

Cybercrime is haunting young people,
all the time, all the time, never giving them a rest.

Cybercrime is a cancer. Cybercrime is a pest.

Poison on a computer screen.

The worst thing I've ever seen.

Young people like to share the most intimate bits of information.

Surfing the net is their passion and exchanging pictures is a fashion.

It happens in every country, in every nation,
in every sort of way, all day.

What they don't realize is that there's a danger
when pictures and personal stuff
can be seen on the screen by a stranger.

The kind of people I despise will make their lives a living hell.
They are so embarrassed, they are so ashamed
that they're afraid to tell and so it goes on and on.
When no one does anything to stop them
these Cyberspace villains have won.

Healthy young girls who were once so vibrant and cheerful
become a shadow of themselves, desperate, depressed, tearful.
They scream and shout but don't see a way out.

More than often it ends with death.

Cybercrime killers see it as a game.

They like to threaten, they like to toy
with a picture, a face, a name.

They don't care who they destroy.

I think it's time for worldwide wrath.

Even when a victim survives
it's one of so many ruined lives.

Cybercrimes left them with wounds and scars.

Each villain committing a cybercrime
should end up behind bars
and have a hard time!

MS. Juslin sega J
Assistant Professor/CSE

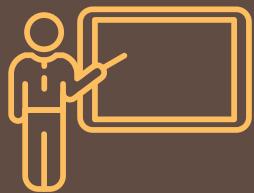


Faculty's Corner

Securing the Cloud: An Introduction to Cloud Service Provider (CSP) Security

The rapid adoption of cloud computing has transformed the way businesses operate, offering unprecedented scalability, flexibility, and cost-effectiveness. As organizations migrate their data and applications to the cloud, ensuring the security of these resources becomes paramount. Cloud Service Providers are companies that offer a range of cloud-based services, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Popular CSPs include Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). One fundamental concept in cloud security is the Shared Responsibility Model. This model outlines the division of security responsibilities between the CSP and the customer. Generally, the CSP is responsible for the security of the cloud infrastructure, while customers are responsible for securing their data, applications, and configurations within the cloud. Implementing robust IAM policies is crucial for controlling access to cloud resources. Organizations should regularly review and update user permissions, enforce strong authentication measures, and employ least privilege principles to limit access to necessary resources.

**Mrs. Ancy Breen
Assistant Professor/CSE**

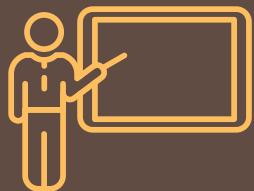


Faculty's Corner

Cybersecurity in Healthcare: Safeguarding Patient Data

The healthcare industry has witnessed a digital revolution, with electronic health records (EHRs), telemedicine, and interconnected medical devices enhancing patient care. However, this digital transformation has also exposed the industry to increased cybersecurity threats, making the protection of patient data more critical than ever. Healthcare organizations store vast amounts of sensitive patient information, including medical history, personal details, and payment information. Unauthorized access to this data can lead to privacy breaches, identity theft, and financial fraud. The healthcare sector is subject to stringent data protection regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States. Employ stringent access controls and multi-factor authentication to ensure that only authorized personnel have access to sensitive data safeguarding patient data in the healthcare industry is a complex task that requires a comprehensive and proactive approach to cybersecurity. As technology continues to advance, healthcare organizations must continually reassess and strengthen their security measures to protect sensitive information and maintain the trust of patients. By investing in cybersecurity infrastructure, fostering a culture of awareness, and staying compliant with industry regulations, healthcare providers can create a resilient defense against evolving cyber threats. The protection of patient data is not just a regulatory requirement; it is a fundamental responsibility that ensures the integrity of healthcare systems.

**Dr. Manju A
Assistant Professor/CSE**

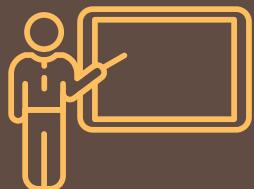


Faculty's Corner

Legal Implications of Developments in Cybersecurity Behavioral Biometrics

As advancements in technology continue to shape the landscape of cybersecurity, behavioral biometrics has emerged as a powerful tool for enhancing authentication and security measures. Behavioral biometrics involve the collection and analysis of unique patterns in individuals' behavior, such as keystroke dynamics, mouse movements, and voice recognition. Compliance with data protection laws, such as the General Data Protection Regulation (GDPR), is crucial to upholding individuals' privacy rights. Safeguarding behavioral biometric data is paramount to prevent unauthorized access and potential misuse. In the event of a data breach involving behavioral biometric data, organizations may be held legally liable. Establishing clear policies for reporting and addressing breaches, along with proactive measures to prevent them, is essential. While behavioral biometrics offers innovative solutions for strengthening cybersecurity, organizations must navigate the legal landscape carefully. Balancing the potential benefits of enhanced security with the protection of individual privacy rights and legal compliance is key. As technology evolves, policymakers, legal experts, and industry stakeholders must collaborate to establish a framework that fosters responsible and ethical use of behavioral biometrics, ensuring a harmonized approach to cybersecurity while upholding legal standards and individual rights.

**Ms. Gowthamy J
Assistant Professor/CSE**

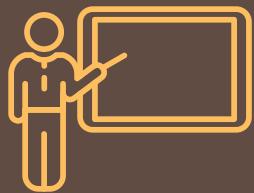


Faculty's Corner

Fortifying the Future: A Comprehensive Look at IoT Security in Recent Devices

The Internet of Things (IoT) has transformed the way we interact with technology, with interconnected devices enhancing efficiency and convenience. However, the proliferation of IoT devices also brings significant security challenges. Recent IoT devices prioritize strong authentication mechanisms, such as secure key exchange protocols and biometric authentication, to ensure that only authorized users and systems can access the device. Implementing role-based access control ensures that different users or devices have appropriate levels of access, reducing the risk of unauthorized manipulation or control. IoT devices are deployed on segmented networks, separating them from critical systems and data. This containment strategy limits the potential impact of a compromised device on the broader network. IoT devices adhere to industry and regional security standards, such as the IoT Security Foundation's guidelines or regulations like the European Union's Cybersecurity Act. Compliance helps ensure a baseline level of security and facilitates interoperability. As the IoT landscape evolves, ongoing collaboration between manufacturers, policymakers, and cybersecurity experts remains crucial to staying ahead of emerging threats and fortifying the future of connected devices.

Dr. Balaji C G
Assistant Professor/CSE

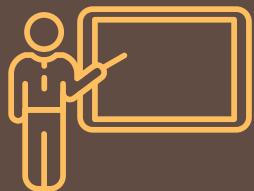


Faculty's Corner

Navigating the Future: Security Implications of 5G Networks

The deployment of 5G networks promises unparalleled connectivity and transformative possibilities for industries and consumers alike. However, this revolutionary leap forward comes with its own set of security implications. The accelerated speeds and minimal latency introduced by 5G networks present unparalleled advantages but also expose potential vulnerabilities. The ability of 5G to connect an extensive array of Internet of Things (IoT) devices introduces a new dimension to cybersecurity. The integration of edge computing with 5G networks marks a paradigm shift in network architecture. As 5G networks become an integral part of our digital landscape, understanding and addressing the associated security implications is paramount. By embracing innovative security measures, adhering to international standards, and fostering collaboration across industries, we can unlock the full potential of 5G networks while fortifying our digital future against evolving threats. The complex supply chain ecosystem underlying 5G infrastructure presents inherent security risks. Stakeholders can mitigate the inherent risks and build resilient 5G ecosystems that empower innovation while safeguarding privacy, integrity, and trust in the digital age.

**Mr. Kingsly Stephen R
Assistant Professor/CSE**

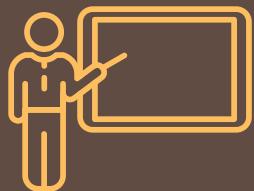


Faculty's Corner

Denial of Service (DoS) and Distributed Denial of Service (DDoS) Protection

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks pose significant threats to network availability and can disrupt the normal functioning of services. Implementing effective protection mechanisms is crucial to mitigate the impact of these attacks. A DoS attack aims to overwhelm a network, service, or system, rendering it inaccessible to legitimate users. Common techniques include flood attacks, exploiting vulnerabilities in protocols such as ICMP, SYN, and UDP. Distributed Denial of Service attacks involve multiple compromised systems working in concert to flood a target with traffic. Techniques include amplification attacks that exploit poorly configured servers to magnify the volume of attack traffic. To protect DOS attacks implement traffic filtering at the network perimeter and employ rate-limiting mechanisms to control incoming request rates. Distribute incoming traffic across multiple servers through load balancing. To protect DDos attacks utilize dedicated DDoS mitigation services for traffic scrubbing. Deploy anycast networks to distribute the load across multiple servers. As cyber threats continue to advance, so must the strategies for defending against them. Implementing a multi-layered approach to DoS and DDoS protection, combining traditional measures with advanced technologies and proactive planning, is essential for maintaining network integrity and ensuring uninterrupted services for users.

**Dr. Suganthi N
Assistant Professor/CSE**

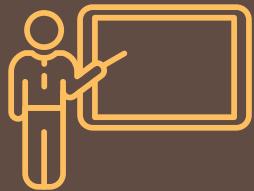


Faculty's Corner

The Role of Encryption in Network Security

In the intricate web of digital communication, encryption emerges as the linchpin of network security, playing a pivotal role in fortifying the confidentiality, integrity, and authenticity of sensitive information. As data traverses networks, encryption protocols such as SSL/TLS and Virtual Private Networks (VPNs) create secure tunnels, ensuring that communications remain shielded from prying eyes and cyber threats. This cryptographic layer is indispensable, particularly in an era marked by an escalating volume of online transactions, remote work dynamics, and interconnected systems. Encryption is not confined to safeguarding data in transit alone; its influence extends to protecting data at rest. Full-disk encryption acts as a formidable safeguard for stored information, rendering it indecipherable without the requisite decryption key. This becomes especially critical in scenarios where physical devices may be susceptible to loss or theft, emphasizing encryption's role as a last line of defense against unauthorized access. End-to-end encryption stands as a testament to the ever-growing importance of privacy in digital communications. By encrypting messages from sender to recipient, this approach ensures that intermediaries, including service providers, cannot access the content. This not only bolsters privacy but also fortifies the authenticity of digital communications, assuring users that their messages remain tamper-proof.

Dr. Azhagiri M
Associate Professor/CSE



Faculty's Corner

Unmasking the Threat: The Pervasive Danger of Malware

In the ever-evolving digital landscape, malware stands out as a potent and pervasive threat, capable of wreaking havoc on individual users, businesses, and entire networks. Malicious software, or malware, encompasses a spectrum of harmful programs designed to infiltrate, damage, or gain unauthorized access to computer systems. From viruses and worms to trojans and ransomware, the forms of malware are diverse and ever-adapting. The danger posed by malware lies in its ability to compromise the integrity, confidentiality, and availability of digital assets. Once unleashed, malware can exploit vulnerabilities, compromise sensitive information, and disrupt critical operations. Ransomware, in particular, encrypts valuable data and demands payment for its release, causing financial losses and operational downtime.

Malware is often disseminated through phishing emails, malicious websites, or infected software. Its stealthy nature and evolving techniques make detection challenging. Moreover, it continuously evolves to bypass security measures, making timely updates and robust cybersecurity practices imperative. To combat this pervasive threat, organizations and individuals must adopt proactive cybersecurity measures, including regular system updates, antivirus software, and user education. The battle against malware is ongoing, highlighting the need for constant vigilance and a collaborative effort to stay one step ahead of these digital adversaries.

Ms. Arthy J
Assistant Professor/CSE



Cyber Awareness

When little trinkets of thoughts submit to fruition, the extent to which an individual achieves it is powerful yet truly commendable. Humans have never failed to amaze us with innovations in this very field of technology. Beauty is in knowing, in realizing that ignorance kills. A deadly compulsion interwoven together by the intricacies of our mind. It could be as trivial as posting screenshots of a conversation online to incite drama and spice. It is a clear violation of privacy. Here, trust is built on a rather fragile constitution, a towering tower standing at the mercy of the wind. Sharing sensitive information such as your ID, password, banking details, social security number, etc. isn't a wise decision either. Deceptive leeches or people with rather shady intentions, obtain these by casting a façade of curiosity, mystery, and friendliness to varying decrees. They make you elicit answers as a product of pure circumstantial advancement that starts as a harmless question like "Hey, I am Dahlia and I was given this number by my boss from Xyz Company. Do you know Richard by any chance?". Cybercrimes could also involve breaching rules by leaking the secrets of a company. Certain software is also used during fresh recruitments to bewitch the interviewer. All in all, hand in hand will we combat chance occurrences and potential slip-ups upon which we act without prescience of our doom, for it's better to be safe than sorry, in a world where change and evolution are consistent. Where awareness is that weapon that could steer the ignoramus crowd away from harm's way.

**Suveeksha Viswanathan
B.Tech CSE AIML 'A'
1st year**



The Quantum Cat and Mouse Game: Cybersecurity in the Age of Supercomputing

Imagine a cat burglar who can slip through walls and teleport between safes. That's kind of what quantum computers could do to our current cybersecurity measures. These superpowered machines harness the mind-bending strangeness of quantum mechanics to solve problems that would take regular computers billions of years, including the complex math behind many encryption protocols. Think of your online security like a super-strong vault door. The lock is a mathematical puzzle so intricate that even the most skilled hacker would need centuries to crack it. But a quantum computer? It could waltz through that door like it's made of tissue paper. To grasp the significance of this quantum leap, it's crucial to understand how traditional computers and quantum computers differ. Classical computers, the workhorses of our digital age, process information using bits, which can exist in one of two states: 0 or 1. This quantum parallelism grants quantum computers a computational advantage, enabling them to solve complex problems faster than their classical counterparts. One of the pillars of cybersecurity is encryption, a process that scrambles information to make it unreadable without the appropriate decryption key. Currently, widely used encryption algorithms rely on the difficulty of certain mathematical problems, such as factoring large numbers, to secure data. However, quantum computers, armed with their ability to perform parallel calculations, could swiftly crack these cryptographic codes.

**Srivatsa S
B.Tech CSE 'E'
1st Year**



Student's Corner

Cyber Labyrinth

Amidst the cosmos of bits and bytes,
Where the galaxies of code ignite,
From "pixel" dust to dreams alight,
A universe takes birth, under the silicon starlight.
In silken strands, webs so grand,
Data slips away like shifting sand.

Beyond the screen, where shadows creep,
A world persists, where secrets sleep.
Luminous traps, beautifully laced,
Where freedom sings, with voice erased.

A crimson flicker in the firewall,
Infects the air in hues of blue,
Minds bewildered, look for a clue,
While Secrets kneel and data crawls,
"Ladies and Gentlemen, welcome to the sapphire thrall!"
Silver hooks, disguised as bait,
Cast in nets of email's wait.
Malware slithers, dark and sly,
A serpent coiled in circuit's tie.

Mortal denizens craving for fame,
Likes like embers feed the flame.
Clicks and likes, a hollow hymn,
Echoing through the digital din.
Perfect moments, staged and brief,
While shadows whisper, "Is this relief?"
Behind the lens, vulnerabilities bloom,
A poisoned chalice in a bejeweled room.



In mirrored screens, reflections lie,
Can we escape the digital eye?
Through coded bars, a yearning grows,
For sunlit paths, where no data flows.
In wary clicks, a cautious stride,
Dubious links, we cast aside.
For every "yes," a watchful glance,
To trace the thread, of phishing's trance.

In passwords forged, like fiery brands,
In knowledge, etched as silver script,
We build our haven, stone by sand,
Where phantoms fade, their webs unripped.
Educate the young, the old, the diverse,
Unwind the webs of deceit, break the silent curse.
Together we mend, we reshape, we rise,
Cyber spiders, with awareness as our eyes.
With caution as compass, awareness as key,
We'll reclaim the web, weave our own destiny.

Anushka Bhattacharji
B.Tech CSE AIML 'A'
2nd Year



Cyber Security and Cyber Awareness in the Modern Digital Landscape

Cybersecurity and cyber awareness are things that cannot be overlooked in the era of technological advancement where everything is interconnected. This is not just a problem for MNCs but it becomes critical to everybody surfing the huge digital space. The vulnerabilities in the cyber realm are increasing every passing year as we become more dependent on digital landscapes to communicate, transact, and even share information. First of all, the rapid increase in cybercrime has become a great threat both for individuals and organizations. Since cyber threats vary from identity theft to financial fraud, the threat spectrum is broad and constantly changes. Established cybersecurity systems significantly contribute to protecting both individuals and MNCs from malicious activities leading to potentially how serious financial damage may occur, and reputational losses. As for the conclusion, it is significant to say that in our interconnected life today cybersecurity and awareness complement each other. Cyber threats keep on evolving so organizations must be proactive in protecting their members and employees within MNCs. The cost of failure to undertake such matters is substantial, moreover, the costs associated with implementing these measures are on the sheer curve. By promoting a culture of cyber awareness, and focusing on cybersecurity we'll all contribute to reinforcing our digital defenses while at the same time reducing risks as fast as human-cyber interactions are increasing.

**KishoreRaj M
B.Tech CSE CS 'C'**

1st Year



Digital Ballet: Guardians of the Binary Realm

In the code's silent dance,
shadows twirl,
Cyber guardians,
defenders of the digital swirl,
firewalls stand tall,
Like ancient tree,
IN encrypted realms,
secrets find ease.
Zero and ones in binary ballet,
where hackers prowl seeking prey,
phishing lives, a deceptive
but vigilant minds withstand the crime

Rashmi Ganesh
B.Tech CSE GT 'A'
1st Year

Linux Symphony

In the realm of penguins, where Tux does soar,
Linux whispers, an open-source lore.
Commands in terminal, a dance of control,
Roots run deep in the kernel's soul.

Code echoes through the open expanse,
A symphony of freedom, a system's dance.
In the world of bits and lines divine,
Linux's melody, an open-source shrine.

Jasper Sofi
B.Tech CSE AIML 'D'
3rd Year



Phishing Attacks and Prevention: Safeguarding Against Cyber Threats

In an increasingly interconnected world, the threat of cybercrime looms large. One of the most prevalent and damaging forms of cyber attack is phishing. This article aims to shed light on phishing attacks, their potential consequences, and effective preventative measures that can be taken to safeguard against them. Phishing attacks are a devious tactic employed by cybercriminals to manipulate unsuspecting individuals into revealing sensitive information, such as usernames, passwords, credit card details, or personal identification numbers (PINs). This is typically done through well-crafted fraudulent emails, instant messages, or websites designed to mimic legitimate organizations or individuals. The impact of falling victim to a phishing attack can be devastating both for individuals and organizations. Financial Loss is done by tricking individuals into divulging their financial information, cybercriminals can gain unauthorized access to bank accounts or credit cards, leading to significant monetary losses. Organizations that fall prey to phishing attacks can suffer severe reputational damage, eroding customer trust and loyalty, and potentially leading to significant financial loss. Phishing attacks can also involve malware that infiltrates computer systems, granting hackers unauthorized access to sensitive corporate or personal data, potentially leading to data breaches or blackmail.

**Harini G
B.Tech CSE CS 'A'
1st Year**



Cybernetic Resilience

In the era of fast-paced hands
takes effort for safety to stand
unfazed and unhinged by threats afar
far away in a virtual land

how does one shield oneself
from cyber bullies and crime
when hackers and predators
wait for that right strike time

we can't just close our eyes
and pretend calamity won't spike
As for every person existing online
there is one ready to strike

managing passwords, authentication
and firewalls are your mates
to either hunt or be hunted
that's your fate

fight valiantly we must
till our last stand
keep hunters at bay and
protect our virtual land

never surrender to threats
even though none are eye-to-eye
keep safe as you must
and not trapped in this virtual lie.

granting hackers unauthorized access to sensitive
corporate or personal data, potentially leading to data
breaches or blackmail.

Abhinav Pallath
B.Tech CSE AIML 'B'
1st Year



Navigating the Cyber Frontier: A Chronicle of Our Digital Age

In the tapestry of human history, the emergence of the digital realm has woven an intricate thread, transforming the way we live, communicate, and conduct business. The Cyber Chronicle unfolds like a modern-day epic, where the protagonist is not an individual, but the collective consciousness of humanity navigating the vast landscapes of cyberspace. As we delve into this narrative, the first chapter introduces us to the inception of the internet—an unparalleled innovation that bridged geographical gaps, connecting minds across oceans. The World Wide Web became our portal to a realm where information flowed freely, breaking the shackles of traditional boundaries. Yet, with this newfound freedom, we discovered the dual nature of the digital frontier—a space where creativity flourished, but also where shadows lurked. The second chapter unfolds as technology advances, introducing us to the era of social media. Platforms like Facebook, Twitter, and Instagram become the modern-day agora, where ideas are exchanged, friendships kindled, and revolutions sparked. However, the intoxicating allure of virtual validation and the undercurrent of cyberbullying remind us that the digital agora is not immune to the complexities of human nature. As we progress through the Cyber Chronicle, the third chapter opens a gateway to the age of cybersecurity. With the proliferation of online transactions and sensitive data exchange, the need for digital guardians becomes paramount.

Karthik V
B.Tech CSE BDA 'B'
2nd Year



Guardians of the Digital Realm : A Cybersecurity Ode

In the realm where digital shadows dance,
A silent guardian takes its stance.
Cybersecurity, a vigilant shield,
In the vast digital battlefield.

Bits and bytes, a virtual land,
Where dangers lurk, unseen, unplanned.
Guarding data, secrets untold,
Cyber warriors brave and bold.

Firewalls rise like towering walls,
Defending networks, protecting calls.
Encryption weaves its intricate thread,
Shielding messages from prying dread.

Viruses swarm like unseen foes,
Seeking to disrupt, to impose.
Yet cybersecurity stands firm and true,
Defending against the malicious crew.

In this age of bytes and code,
Where information is the golden load,
Cybersecurity, our silent knight,
Protects our world, day and night.

With every click, with every byte,
It keeps us safe, it keeps us right.
In the digital realm, where dangers reside,
Cybersecurity is our steadfast guide.

**Pinak Mukherjee
B.Tech CSE CS 'A'**

1st Year



Cybersecurity Trends to Watch in 2024: Staying Ahead of Emerging Threats

In today's rapidly evolving digital landscape, staying ahead of emerging cybersecurity threats is crucial for individuals and organizations alike.

1. Artificial Intelligence and Machine Learning in Cybersecurity

Artificial intelligence (AI) and machine learning (ML) are revolutionizing the way cybersecurity professionals detect and respond to threats. By leveraging AI and ML algorithms, security systems can analyze vast amounts of data to identify anomalous patterns and potential security breaches in real time. According to a report by Statista, the global AI in cybersecurity market is projected to reach \$38.2 billion by 2026, reflecting the growing reliance on AI-driven security solutions.

2. Zero-Trust Security Model

The traditional perimeter-based security model is no longer sufficient to protect against "sophisticated cyber threats. As a result, the zero-trust security model has gained traction as a more effective approach to cybersecurity. This model operates under the assumption that no entity, whether inside or outside the network, should be trusted by default. Instead, it requires continuous verification of identities and strict access controls to mitigate the risk of insider threats and unauthorized access.



3. Cloud Security and DevSecOps

The widespread adoption of cloud computing has brought about a shift in the way organizations manage and secure their digital assets. As a result, integrating security practices into the development and operations (DevOps) lifecycle has become essential. This approach, known as DevSecOps, emphasizes the need for security to be built into the development process from the outset, rather than being treated as an afterthought.

4. Cybersecurity Automation and Orchestration

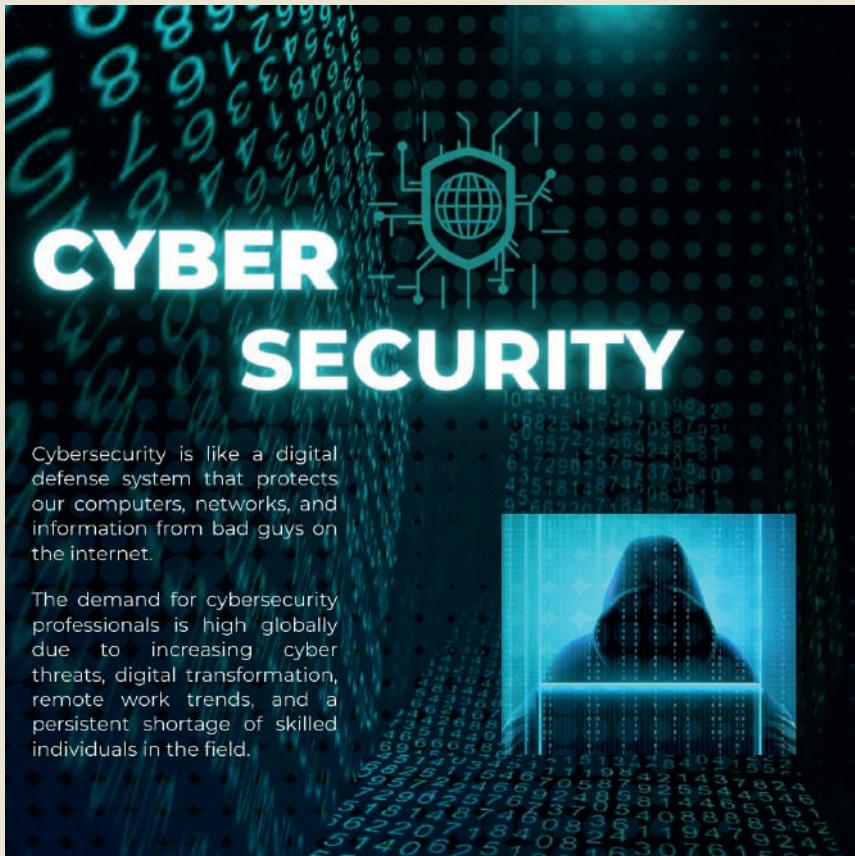
The increasing volume and complexity of cyber threats have made it challenging for security teams to respond effectively without automation. Cybersecurity automation and orchestration tools help streamline incident response processes, enabling faster detection, analysis, and remediation of security incidents.

5. Supply Chain Security

The supply chain has emerged as a prime target for cyber attacks, posing significant risks to organizations that rely on third-party vendors and suppliers. Strengthening the security of supply chains has become a top priority. In conclusion, the cybersecurity landscape in 2024 is characterized by rapid technological advancements and evolving threat landscape. Staying ahead of emerging threats requires a proactive approach, leveraging cutting-edge technologies and best practices to fortify digital defenses.

Harini G
B.Tech CSE CS 'A'
1st Year

Student's Corner

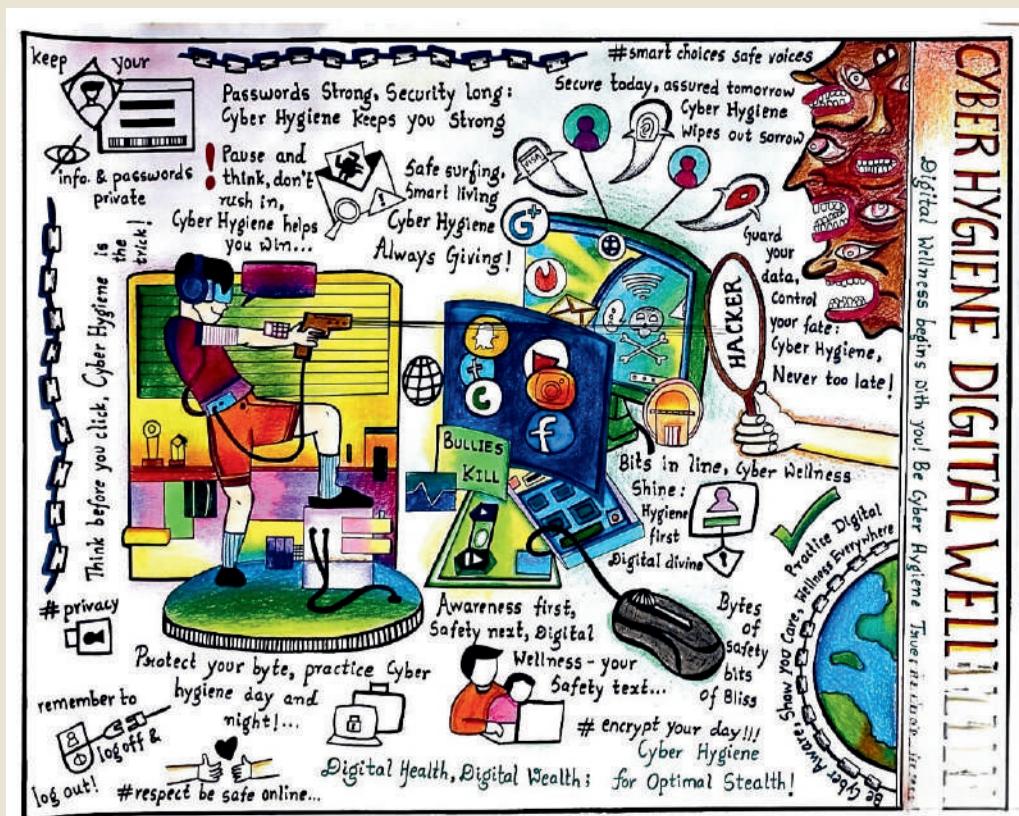


Cybersecurity is like a digital defense system that protects our computers, networks, and information from bad guys on the internet.

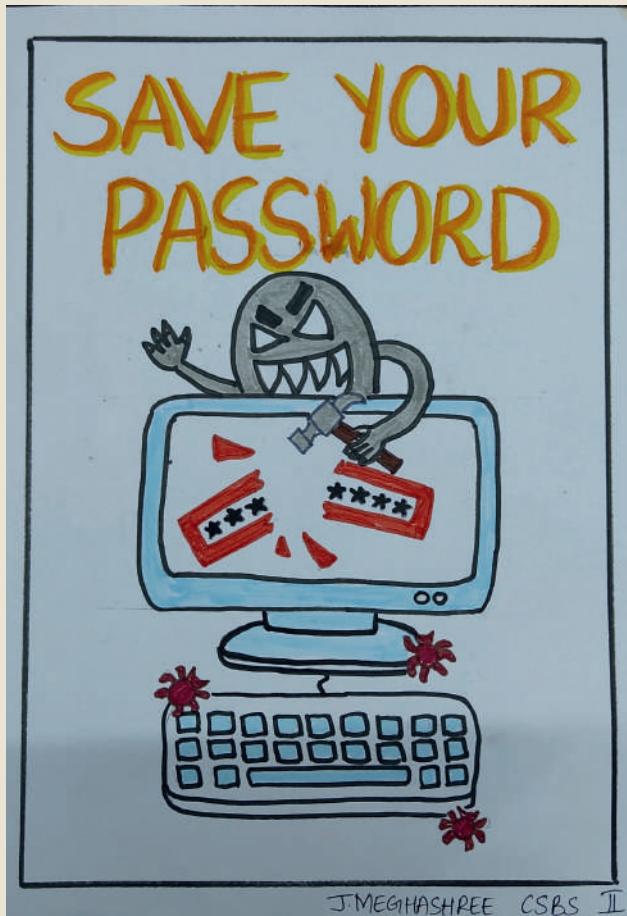
The demand for cybersecurity professionals is high globally due to increasing cyber threats, digital transformation, remote work trends, and a persistent shortage of skilled individuals in the field.

KishoreRaj M
B.Tech CSE CS 'C'
1st Year

Komal Bharati
B.Tech CSE CS 'B'
1st Year



Student's Corner



J.MEGHASHREE CSBS II

Meghashree J
B.Tech CSBS 'A'
1st Year

Soumya Singh
B.Tech CSE CS 'C'
1st Year



Student's Corner



**"Guardian of the Digital Realm:
Unleash Cyber Awareness!"**

Here are 5 tips to have a secure system

- 1.Lock It Tight: Strong Passwords**
 - .Use complex, unique passwords.
 - .Change passwords regularly.
- 2.Think Before You Click: Avoid Phishing**
 - .Verify sender legitimacy.
 - .Beware of suspicious links and emails.
- 3.Stay Updated: Secure Software**
 - .Enable automatic updates.
 - .Keep antivirus programs current.
- 4.Guard Personal Info: Be Mindful Online**
 - .Limit social media details.
 - .Control privacy settings.
- 5.Backup Your World: Protect Data**
 - .Regularly back up important files.
 - .Use secure storage options.

**Rakshana Baskar
B.Tech CSE CS 'C'
1st Year**

Student's Corner



Essack. R
B.Tech CSE AI/ML 'B'
1st Year



Ragunathan C
B.Tech CSE 'K'
3rd Year



Department Archives



Cyber Carnival 2023 Inauguration at SRMIST, Ramapuram on 13th March 2023.

Department Archives



Cyber Carnival 2023 Awareness Campaign at SRMIST,
Ramapuram on 13th March 2023.

Department Archives



MOU signing ceremony between SRMIST, Ramapuram & **Network Intelligence Pvt. Ltd., Bangalore** on 13th March 2023.

Department Archives



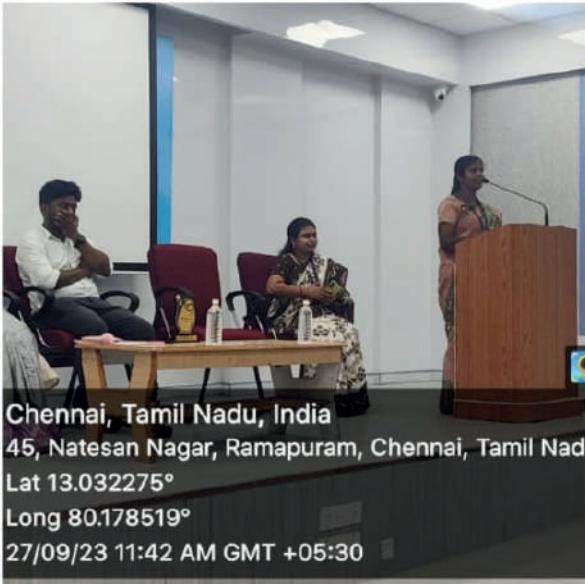
Lecture on ***Internals Of Cybersecurity and Real-time Cyber threats*** by ***Dr. Mahesh Kalyanaraman, Associate Vice President, Risk & Compliance, HCL Technologies Limited*** on 21st March 2023.

Department Archives



Guest Lecture on **Cybersecurity Career Plans** delivered by **Mr. Bharani Ramasamy, Senior Director of Global Networks and Security at Virtusa Corporation** on 5th September 2023.

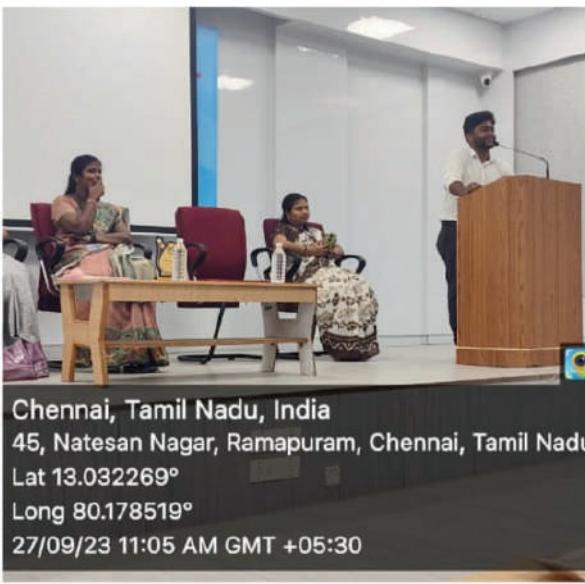
Department Archives



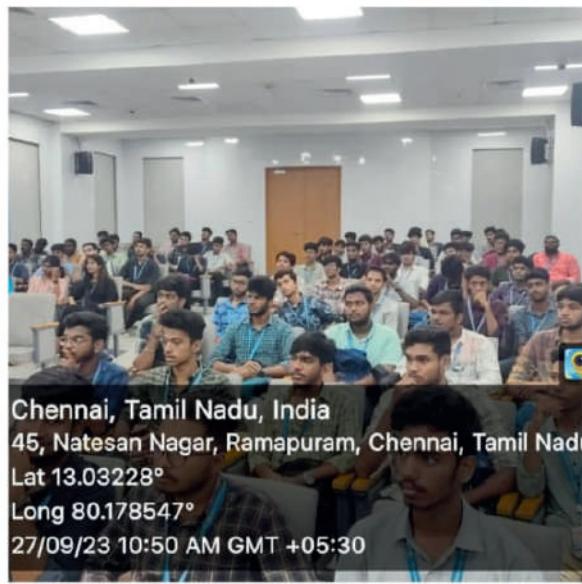
Chennai, Tamil Nadu, India
45, Natesan Nagar, Ramapuram, Chennai, Tamil Nadu
Lat 13.032275°
Long 80.178519°
27/09/23 11:42 AM GMT +05:30



Chennai, Tamil Nadu, India
45, Natesan Nagar, Ramapuram, Chennai, Tamil Nadu
Lat 13.03228°
Long 80.178547°
27/09/23 10:51 AM GMT +05:30



Chennai, Tamil Nadu, India
45, Natesan Nagar, Ramapuram, Chennai, Tamil Nadu
Lat 13.032269°
Long 80.178519°
27/09/23 11:05 AM GMT +05:30



Chennai, Tamil Nadu, India
45, Natesan Nagar, Ramapuram, Chennai, Tamil Nadu
Lat 13.03228°
Long 80.178547°
27/09/23 10:50 AM GMT +05:30

Guest Lecture on **Cyber Threat Management** delivered by **Mr. Balachandar R, Team Lead at Sophos Technology** on 27th September 2023.

Department Archives



The **BreachXamine** Event at SRMIST, Ramapuram, hosted by the Department of Computer Science and Engineering with a focus on Cybersecurity, was a dynamic session held in BMS 501. Student coordinators Prem Kumar S and Manoj A. introduced Cyber Crime Investigation and Cyber Warfare succinctly. Teams were then assigned unique crime study reports, which they diligently examined and presented during the event. Dr. S. Sathya Priya and Dr. J. Shiny Deula adjudicated the participants' presentations, culminating in the recognizing of deserving winners. The event showcased the student's analytical skills and provided valuable insights into the ever-evolving realm of cybersecurity.

Department Archives



Cyber Jagrookta Diwas, an initiative by the Ministry of Home Affairs and AICTE conducted on 4th October 2023 where **Dr. D. Ashok Kumar, Superintendent of Police, Cyber Crime Wing** navigated the audience through the labyrinth of current cybercrimes transpiring in Tamil Nadu.

Department Archives



Cyber Jagrookta Diwas- Second Edition with the topic Phishing 101 on 1st November 2023. The session, spearheaded by the Head of the CSE Department, offered valuable insights into cybersecurity. An address by the Deputy HoD of Cybersecurity shed light on the event's significance, emphasizing its role in enhancing awareness. Participants were warmly welcomed by an Associate Professor, setting the stage for an informative and engaging session. This collective effort aimed to provide a comprehensive understanding of cybersecurity, fostering a proactive approach among attendees.

Subsequent **Cyber Jagrookta diwas** will be conducted first week of every month

Department Archives

The screenshot shows a Google Meet interface. At the top left is the SRM Institute of Science and Technology logo and details about the event: "SRM INSTITUTE OF SCIENCE AND TECHNOLOGY Ramapuram Campus COLLEGE OF ENGINEERING AND TECHNOLOGY DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING WITH SPECIALIZATION IN CYBER SECURITY Organizes Online Guest Lecture On CYBER SECURITY THREAT LANDSCAPE CYBER DEFENSE AND COUNTERMEASURES Date 16-09-2023 (Saturday) | Time 9:00 AM - 10:00 AM RESOURCE PERSON Dr. NARESH KSHETRI Assistant Professor of CSE, School of Business & Technology, Emporia State University, Emporia, Kansas, USA". Below this is a photo of the resource person, Dr. Naresh Kshetri. To the right, there's a circular seal of Emporia State University. A participant grid shows several users with their names and profile pictures. The bottom of the screen displays the meeting controls and a toolbar.

The screenshot shows a presentation slide titled "2.1 Exploring Cybersecurity Threats – Threat Actors". The slide content includes a bulleted list of common types of threat actors and a diagram illustrating the hierarchy of threat actors based on tools used and motivation. The diagram shows a pyramid with levels: "ADVANCED TOOLS" (Nation states, Intelligence / espionage / economic, Terrorist organizations, Nation-state sponsored groups, Criminal groups, Espionage), "BESPOKE TOOLS" (Secret, Buy on the dark market, Motivated individuals (hacktivists), Ideology / disgruntled, Bedroom hackers or script kiddies, Fun / play fighting), and "FREE TOOLS" (Readily available). The bottom of the slide credits "Source: Threat Landscape, Cyber Defense, & Countermeasures © Dr. Naresh Kshetri, Emporia State University". The bottom of the screen shows the meeting controls and a toolbar.

Guest Lecture on **Cyber Security threat landscape cyber defense and counter measures** given by **Dr. Naresh Kshetri Assistant Professor Of CSE, School of Business and Technology, Emporia State University, Emporia, Kansas, USA** on 16th September 2023.

Department Archives



Mr. Sudhanshu Patel has completed the Data Mining and Business Intelligence for Cyber Security Applications **Summer Programme** in **Ben Gurion University, Israel.**

Student Achievements



The World Mental Health event at Bharathiyan Mandapam graced by the presence of **Thiru R.N. Ravi, the Hon'ble Governor of Tamilnadu** on 10th October 2023 organized a Short film contest. The winning entry, titled "Dear Diary," was created by the II-year students from the Department of Cybersecurity. The second prize, accompanied by a cash prize of **Rs.15,000** and certificates was awarded.

Student Achievements

66
IT spans five locations across the country, with the Chennai campus boasting over 20,000 students and 600 staff. It ranks among top eight institutions in India. The edition of eVIT, held October 5, celebrated innovation, creativity, risk, and innovative projects.

"Additionally, they've launched 424 satellites from their facilities worldwide, increasing their capacity. Out of 216 missions, 124 satellites are currently in orbit serving the nation," she informed.

Jeyenthal explained that ISRO fails under the Department of Space, which is part of the PMO. She added, "Since 2015 when 203 satellites were using ISRO data, Prime Minister Narendra Modi has emphasised maximising civilian use for government and developmental purposes. Currently, 60 ministries employ 170 applications, contributing to the widespread impact of Digital India."

Jeyenthal pointed out the immense potential for students to pursue careers in space exploration, with both government agencies and private enterprises seeking talent. She informed that over 150 industries have been involved in development, with a growing presence of space industries in India's private sector. She encouraged students to play a vital role in the burgeoning industry's growth.

During the valedictory ceremony of TechnoVIT'23, Dr Sekar Viswanathan, vice-president of VIT Chennai, thanked Karthik Rajaram, MD and co-founder of Xanadu Ltd and other guests. He lauded the participation of 15,000 students from 424 educational colleges in 264 events over the three days. He said that 56 foreign faculties from 41 different universities joined the event, showcasing remarkable international collaboration. Dr Sekar highlighted that the event not only enhanced technical skills but also fostered overall skill development, including leadership, management, and soft skills.

Karthik Rajaram, an alumnus of VIT and the MD of Xanadu Ltd., shared his entrepreneurial journey, reflecting on the challenges faced in climbing the corporate ladder. He drew parallels to the four industrial revolutions, highlighting how each revolution has propelled progress. Karthik underscored the transformative nature of the fourth industrial revolution and exuded confidence in technology to reshape the future.

He highlighted how there is a profound impact on humanity when we integrate technology. There are unanswered questions about how we will utilise technology and how it will affect individuals and society at large. Technology can potentially alter our fundamental values and strengths," Karthik noted.

All students who won various events from different colleges received awards. Dr Rajasekaran, director of Student Welfare at VIT Chennai, extended a vote of thanks. He commended the students and volunteers for their significant contributions to the TechnoVIT'23, making the event a success.

"How hackers can really hack?" an Event organized by a 1-day workshop followed by Capture the Flag competition, 3rd-year Cybersecurity Students have won 2nd place with 3000 points and were awarded a prize amount of **Rs. 2000/-** conducted by VIT, Chennai.

Source: Times of India

Student Achievements



3rd-year Students of the Cybersecurity department have won close to **\$2250 prize** money of track prizes from **Google, Ethereum and Replit** at Warpspeed 24-hour hackathon held on Saturday and Sunday at Bangalore.

OUR SPONSORS

Title Sponsor



VeritasTech Pilot Academy is fully devoted to delivering extraordinary pilot training, shaping students into proficient and accountable aviators. Backed by seasoned mentors and state-of-the-art resources, we are committed to providing an unparalleled learning journey, ensuring an optimal experience for every student. Let us be the bridge to realizing your aspirations of taking flight.



**No 5, 4th Scheme, ICF Colony, Ayanampakkam Road, Ambattur,
Chennai 600 058**

Industry Partner



GUVI

GUVI - Grab Ur Vernacular Imprint

GUVI is an IIT-M & IIM-A incubated Ed-tech company that focuses on providing personalized learning solutions for its learners right from online learning, upskilling & recruitment opportunities in world-class quality. And, bestow tech-skills with the comfort of your native language.



IITM Research park - phase 2, module #9, 3rd floor, D block, Kanagam Rd, Tharamani, Chennai, Tamil Nadu 600113

Industry Partner



બેંક ઓફ બરોડા
Bank of Baroda

Bank of Baroda is an Indian state-owned International banking and financial services company headquartered in Vadodara (earlier known as Baroda) in Gujarat, India.



Chennai, India

Event Sponsors



M G K Packaging is one of the leading manufacturer of corrugated boxes. We can provide solutions for all kinds of your corrugated box need, as per your specification.



**#.124/2A, Madhavaram Redhills Hight Road,
Vadaperumbakkam,
Chennai - 600 060.**

Event Sponsors



GES was found in the year of 2002 as a Small Scale Manufacturing unit to start the Manufacturing of HT Switchgears in the industry belt of North Chennai in India. The founder Mr. C. EDWIN THAYANANTHAM is specially Oracle'ed about his plan and was a seasoned Technocrat with several years work experiences of his hand in such renowned industrial houses such as Easun Limited, Crompton Greaves Limited & Siemens Limited



**Erneeswaran Koil, Ernavur, Chennai, Tamil Nadu
600057**

Event Sponsors



At Polaris, we have fun doing what we love by driving change and innovation. We empower employees to take on challenging assignments and roles with an elevated level of responsibility in our agile working environment. Our people make us who we are, and we create incredible products and experiences. At Polaris, we are an ambitious, resourceful, and driven workforce, which empowers us to THINK OUTSIDE.



Bangalore, India

Event Sponsors



S.K. Trading Co. is one of the largest wooden doors and windows manufacturers in Chennai. All our products are 100% solid hardwood or teakwood. They are imported from countries like Ghana, Ivory Coast, Burma, etc. The manufacturing technique embraces traditional heritage methods of production and construction with modern equipment, technologies, and ideology creating quality products with high durability. We have been providing solid hardwood and teakwood doors and windows for various residential projects in and around Tamilnadu and Kerala. We endeavor to provide our customers with the finest quality products at competitive prices and service for one hundred percent customer satisfaction.



**No.31-B, Natesan Nagar, Ayanambakkam,
Chennai - 600 058**

Event Sponsors



We are committed to providing the highest quality products possible. To do this, we have implemented a strict Quality Policy. This policy ensures that all of our products meet or exceed the expectations of our customers. We constantly monitor our manufacturing process and make sure that every step is performed to the highest standards. We also regularly test our products to ensure that they are of the highest quality. If at any time we find that a product does not meet our standards, we immediately take corrective action. This Quality Policy is an essential part of our business and ensures that we always provide the best products possible.



**No.3 MP, Thottam, Bharathi Nagar,
Tiruppur-641607,
Tamil Nadu, India**

Event Sponsors



Headquartered in Chennai, India, GoStudy is a pioneer in Overseas Education Consultation. With a legacy spanning over 15 years and a formidable team of 250+ Certified Educational Experts, we are dedicated to helping students achieve their dreams of studying abroad. Our unwavering commitment to quality and integrity is at the core of our values, fueling our passion for what we do. As partners of esteemed universities across 18+ countries, we provide students with a reliable pathway to their dreams. In an ever-evolving educational landscape, GoStudy remains at the forefront, adapting and expanding our services to meet the diverse needs of students. We strive to bridge the gap between ambition and achievement, turning students' study abroad aspirations into accomplishments.



**22/1A, Welcome Colony, Anna Nagar West Extension, Chennai,
Tamil Nadu 600101**

Editorial Board



V. MOHAN AADITYA

Department of CSE with
Specialization in Cyber Security
B.Tech CSE CS 'B'

MITHILA TAMILSELVAN

Department of CSE with Specialization
in Cyber Security
B.Tech CSE CS 'B'



JOHANA CATHERINE EZHIL

Department of CSE with Specialization
in Cyber Security
B.Tech CSE CS 'A'



SAMPRITHI V

Department of CSE with Specialization
in Cyber Security
B.Tech CSE CS 'A'



SRM IST RAMAPURAM



“ Cybersecurity is not just about protecting systems; it's about safeguarding the trust and confidence that individuals, businesses, and societies place in the digital world.”



cyber_carnival_srmrmp



Cyber Carnival SRM Ramapuram



cybercarnival.in



@srmrmp.ist



srmrmp.edu.in