RAMAPURAM SRM INSTITUTE OF SCIENCE & TECHNOLOGY

ELE3T

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

RAMAPURAM CAMPUS,CHENNAI-600089,TAMIL NADU,INDIA

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

WITH SPECIALIZATION IN CYBERSECURITY

CYBER CHRONICLE

CYBER CARNIVAL '23

srmist.rmp | srmist.rmp | srmrmp.edu.in

CHIEF PATRONS

Dr. R. Shivakumar
Chairman, SRM Group of Institutions,
Ramapuram & Trichy campus

Mr. S. Niranjan
Co-Chairman, SRM Group of Institutions,
Ramapuram & Trichy campus

PATRONS

Dr.N.Sethuraman
Chief Director, SRM Group of Institutions
(Ramapuram & Trichy campus)

Dr. V. Subbiah Bharathi
Director, SRM Group of Institutions,
Ramapuram campus

Dr. M. Murali Krishna
Dean (E&T), SRMIST, Ramapuram campus

Dr. Balika J Chelliah
Vice Principal (Admin), SRMIST,
Ramapuram campus

Dr. G. Prabhakaran
Vice Principal (Academic), SRMIST, Ramapuram campus

CONVENOR

Dr. K. Raja
Professor & HoD
Department of Computer Science and Engineering

CO-CONVENOR

Dr. Shiny Duela J
Associate Professor & Deputy HoD-CS
Department of Computer Science and Engineering

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.

About Cyber Carnival '23

A cyber carnival is a event that brings together people with an interest in cybersecurity to participate in various activities and learn about the latest trends and technologies in the field. Here is a brief overview of some of the events that may be part of a cyber carnival:

Cyber Conclave: A gathering of cybersecurity experts to discuss trends and share knowledge on online privacy, data protection, hacking, and cybercrime.

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.

Paper presentation: An opportunity for participants to present their research and findings on various topics related to cybersecurity.

Shipwreck: A simulation exercise where participants work in teams to respond to a cyberattack on a fictional organization and defend against the attack.

Cyber Safe Cinema: A film festival that showcases short movies related to cybersecurity and privacy issues.

Cybershot: A photography competition focused on cybersecurity-related themes.

Behind the Crime: A talk show-style event where cybersecurity experts discuss real-life cybercrime cases and share their insights on how to prevent them.

Capture the Flag: A team-based competition where participants compete to solve various cybersecurity challenges and capture virtual "flags."

Seminar on Cyber Opportunities in India: An event that explores the current state and future prospects of the cybersecurity industry in India, including job opportunities, training programs, and research initiatives.

Overall, a cyber carnival is a great way to bring together cybersecurity professionals, researchers, students, and enthusiasts to learn, share ideas, and network with each other.

Dean's Desk

Dr.M.Murali Krishna

Dear Students,

I am delighted to wish you all a very happy Cyber Carnival! This event is a testament to the hard work and creativity of our students and faculty who have come together to create a fun-filled and exciting program for everyone to enjoy.

As technology continues to play an ever-increasing role in our lives, it is essential that we understand its potential and use it responsibly. The Cyber Carnival provides an excellent opportunity for us to learn more about the digital world in a safe and enjoyable environment.

I encourage all of you to participate fully in the festivities and take advantage of the numerous activities and workshops available. Have fun, make new friends, and most importantly, learn something new!

Dr. Murali Krishna
Dean

HOD's Desk

Dr.K.Raja

As the Head of the Department, it is my pleasure to welcome everyone to the Cyber Carnival. This event is an incredible opportunity for all of us to come together and celebrate the advancements and innovations in the field of cybersecurity.

With the rapid evolution of technology and the ever-increasing threat of cyber attacks, it is essential for us to stay ahead of the curve and keep up with the latest trends and best practices in cybersecurity. The Cyber Carnival provides an excellent platform for all of us to share our knowledge, expertise, and experiences in this vital field.

I would like to express my gratitude to the organizers for putting together such an incredible event, and I wish all the participants the best of luck in their endeavors. Let's make the most of this event, learn from each other, and collaborate to make the world a safer place for everyone.

Thank you, and enjoy the Cyber Carnival!

Dr.K.Raja
HOD

Deputy HoD's Desk

Dr.Shiny Duela J

Hello and welcome to the Cyber Carnival!

As the co-convener of this exciting event, I would like to extend a warm welcome to all participants and guests. This carnival is a celebration of the incredible advancements and innovations in the field of cybersecurity, and we are thrilled to have so many brilliant minds and industry leaders in attendance.

Throughout the carnival, we will have a wide variety of events, including keynote speeches, panel discussions, interactive workshops, and fun activities. Our goal is to promote learning, collaboration, and networking within the cybersecurity community.

I hope you all have a fantastic time at the Cyber Carnival and take away valuable insights and connections that will help you in your future endeavors. Thank you for joining us and making this event a huge success!

Dr.Shiny Duela J
Deputy HOD

Student Coordinator's Desk

Shyam Sunder M

Dear participants, faculty members, and esteemed guests,

I am thrilled to welcome you all to the Cyber Carnival event hosted by SRM Institute of Science and Technology, Ramapuram Campus. As the event coordinator, I am honored to organize an event that aims to foster awareness and appreciation of the importance of cybersecurity in our daily lives. Our event features a wide range of cyber-based events such as capture the flag, behind the crime, and paper presentations, as well as non-technical events such as shipwreck, cyber safe cinema, and cybershot. Our objective is to not only promote technical expertise but also encourage creativity, innovation, and teamwork among our participants.

I believe that this event will provide a platform for students to showcase their skills, learn from their peers, and network with industry professionals. I hope that this Cyber Carnival event will be a grand success and serve as a catalyst for future initiatives in the field of cybersecurity. I wish all the participants the very best of luck and hope that you have a great time at the event.

Let us all work together to make this event a grand success!

Student Coordinator's Desk

Sandheep R

Hello everyone,

Welcome to the Cyber Carnival event at SRM Institute of Science and Technology, Ramapuram Campus. I'm thrilled to be the event coordinator and organize an event that focuses on cybersecurity. We have planned a Cyberthon event along with activities such as capture the flag, behind the crime, and paper presentations. Our objective is to not only promote technical expertise but also encourage creativity, innovation, and teamwork among our participants.

The Cyberthon event provides an opportunity for participants to showcase their cybersecurity skills and compete with each other. We believe that this event will be an excellent platform for students to learn from each other and connect with industry professionals.

I'm confident that the Cyber Carnival event will be a grand success and inspire future initiatives in the field of cybersecurity.

Teacher's Corner

CYBER FRAUDS AND SIDE EFFECTS OF DIGITALISATION

Cyber Security is an important concern emerging in our society. Many fraud companies conceal the data of customers by using tactics of misleading Advertisements. Digitization has a proven impact on reducing unemployment, improving quality of life, and boosting citizens' access to public services but its side effects are data theft of customers, Breaching of Copyright of Companies, Plagiarism in social media websites, Social dis-connectivity.

According to data from the National, Crime Records Bureau states that 50,030 cybercrime cases were reported in the year 2020-21 in India. Cyber Fraud is the key motive and intent in 30,218 cases recorded in frauds. In India, more than 2200 cyber-attacks are committed per day, whereas cyber security is the biggest concern that emerges in society.

Increases in the number of cyber-attacks result in government increased budget and attention on cyber security. The First Cyber Attack occurred in the late 1970s but over time nature of cyber-attack changed. Phishing, data breach, cyber extortion, Identity Theft, Harassment are types of Cyber Crimes. Increasing digitalization leads to excessive use of Technology which may effect on Mental Health of People. The development of the Mind is depending on the growth of Mental Health which might be diminished due to excessive use of technology, social media by Youngsters and Adults.

Dr.Shiny Duela J
Associate Professor/CSE

THE ROLE OF BLOCKCHAIN TECHNOLOGY IN ENHANCING CYBER SECURITY

Blockchain technology has been gaining attention in recent years as a potential solution to some of the security challenges faced by organizations across different sectors. Blockchain, which is the underlying technology behind cryptocurrencies such as Bitcoin, is a distributed ledger technology that enables secure, transparent, and tamper-proof transactions between parties without the need for a central authority.

One of the key benefits of blockchain technology in enhancing cyber security is its ability to provide a decentralized and transparent approach to data storage and sharing. Blockchain technology works by creating a digital ledger of transactions that are stored in a distributed network of computers. Each computer, or node, in the network has a copy of the ledger, and any changes made to the ledger must be approved by all nodes in the network, making it difficult for hackers to manipulate or compromise the data.

Dr.Shamili Varsha
AP/CSE

Teacher's Corner

CYBER WAR - THE MODERN WARFARE

The rise of technology has brought about a new form of warfare: cyber war. Cyber war involves the use of technology to launch attacks on critical infrastructure, disrupt communications, and steal sensitive information. In this article, we will explore the concept of cyber war and its implications for modern warfare.The use of cyber war has become increasingly common as technology has advanced. Nation-states and non-state actors alike have recognized the value of cyber war as a tool for achieving political and military objectives.

What is Cyber War?Cyber war involves the use of technology to launch attacks on an adversary's computer systems and networks. These attacks can take many forms, including:

1. Denial-of-service (DoS) attacks that disrupt communications and services.
2. Malware attacks that infect computers with viruses or other malicious code.
3. Advanced persistent threats (APTs) that infiltrate computer systems to steal sensitive information.
4. Cyber espionage that involves stealing sensitive information or trade secrets.
5. Ransomware attacks that encrypt an organization's data and demand payment for its release.

The implications of cyber war are significant. Unlike traditional warfare, cyber war can be launched from anywhere in the world, making it difficult to identify the source of an attack. This makes it easier for nation-states and non-state actors to launch attacks without fear of retaliation.Cyber war can also have a significant impact on critical infrastructure, such as power grids, water systems, and transportation networks. A successful cyber attack on these systems could cause widespread disruption and chaos.

The use of cyber war also raises ethical questions. For example, should cyber war be considered a legitimate form of warfare? What are the rules of engagement for cyber war? These are questions that policymakers and military leaders must grapple with as technology continues to evolve.Cyber war is a growing threat in the modern world. The use of technology to launch attacks on critical infrastructure and steal sensitive information has become an increasingly common tactic among nation-states and non-state actors. The implications of cyber war are significant, and the ethical questions it raises are complex. As technology continues to evolve, it is essential for organizations and governments to invest in cyber security measures to protect against cyber attacks.

-Dr.M.S.Minu
AP/CSE

Teacher's Corner

CYBER CRIME: A GROWING THREAT TO YOUNG ADULTS IN INDIA

The impact of cybercrime on young adults in India can be severe, both financially and emotionally. Many young adults in India use the internet for online shopping, banking, and social networking, putting them at risk of having their personal information and financial data stolen by cybercriminals.

In addition to financial loss, cybercrime can also have a significant emotional impact on young adults. Cyberbullying, for example, can cause depression, anxiety, and other mental health issues. Cyberstalking can be particularly frightening for young adults, as it involves the use of technology to harass, intimidate, or threaten someone.

To address the problem of cybercrime in India, several steps can be taken to protect young adults from these attacks:

Increase Awareness: One of the most important steps is to increase awareness among young adults about the risks of cybercrime. This can be done through education campaigns, workshops, and seminars.

Strengthening Laws: India has laws that address cybercrime, but they need to be strengthened to provide more protection to victims. The government should work towards making the legal framework more robust.Enhancing Cybersecurity: Cybersecurity measures need to be enhanced, including the use of advanced encryption technologies, antivirus software, and firewalls.

Promoting Responsible Use of Technology: Young adults need to be educated on the responsible use of technology, including the safe handling of personal information, strong password creation, and avoiding suspicious emails or links.

Reporting Cybercrime: Victims of cybercrime should report the incident to the authorities immediately. This will help in bringing the criminals to justice and preventing further attacks.Cybercrime is a serious threat to young adults in India. The impact of cybercrime can be severe, both financially and emotionally. However, with increased awareness, enhanced cybersecurity measures, and responsible use of technology, young adults can protect themselves from these attacks. It is essential for the government, educational institutions, and parents to work together to prevent cybercrime and create a safe digital environment for young adults.

-Dr..S.S.Subhaksha Ramesh
AP/CSE

Teacher's Corner

EXPLORING POTENTIAL CYBER SECURITY THREATS IN THE FUTURE

As technology continues to evolve, cyber security threats are becoming more advanced and sophisticated. The future of cyber security threats is unpredictable, but there are several potential threats that could arise in the near future. In this article, we will explore some of the potential cyber security threats that we may face in the coming years.

Artificial Intelligence (AI) Attacks:

AI is already being used in many industries, including cybersecurity, to identify and respond to potential threats. However, AI can also be used by cybercriminals to launch attacks. AI-powered attacks can be more sophisticated, targeted, and difficult to detect. For example, an AI-powered attack can bypass security measures by identifying vulnerabilities and exploiting them to gain access to sensitive information.

5G Network Attacks:

5G networks offer faster download and upload speeds, lower latency, and increased bandwidth. However, with this increased connectivity comes increased vulnerability. 5G networks have more entry points for cyberattacks, and the higher speed can make it easier for cybercriminals to steal sensitive information. Additionally, 5G networks are more complex than previous networks, making it more difficult to detect and prevent cyberattacks.

Quantum Computing Attacks:

Quantum computing is still in its early stages, but it has the potential to revolutionize computing power. With its ability to perform complex calculations at a speed that is exponentially faster than traditional computing, quantum computing can also pose a threat to cybersecurity. Quantum computers can be used to crack encryption methods that are currently considered secure, making it easier for cybercriminals to steal sensitive information.

Ransomware Attacks:

Ransomware attacks involve encrypting an organization's data and demanding a ransom in exchange for the decryption key. Ransomware attacks have become more common in recent years, and they are expected to become even more prevalent in the future. With the rise of cryptocurrency, cybercriminals can demand payment anonymously, making it more difficult to track and prosecute them.

As technology continues to evolve, so do cyber security threats. The potential threats mentioned in this article are just a few examples of what we may face in the future. To stay ahead of cybercriminals, it is important to be proactive and invest in cybersecurity measures that can detect and prevent attacks. This includes implementing strong security measures, such as encryption and two-factor authentication, training employees to identify and report suspicious activity, and staying up-to-date with the latest security threats and best practices. By being vigilant and proactive, we can help mitigate the potential cyber security threats that we may face in the future.

-Dr.C.G.Balaji
AP/CSE

Teacher's Corner

Cybersafe in Internet of Vehicles using Blockchain Technology

Internet of Vehicles(IoV) allow drivers and passengers to connect to the outside world while on the road. Cybersafe is the primary challenge for automakers and other stakeholders, because connected vehicles rely on wireless and cellular communication interfaces. Connected cars transfer information such as weather conditions, emergency attention, location information etc. IoV cannot store huge amount of information in its inbuilt devices. So it is transferred to cloud. But security in the cloud is an issue and focuses security challenges like DDos attacks, Data breaches, Data loss, insecure access point, Data piracy. So there should be a replacement for cloud. Block chain technology effectively replaces the cloud, since it is a distributed ledger technology. It facilitates not only data storage but also offers commutability, or protection against data being changed since it is stored in a block.

Researches under collision avoidance and resource scheduling are under process in vehicular block chain specially privacy preservation. For example, if there is an illegal activity monitored and sent to the block chain with identity of vehicle, it may reveal significant privacy information of the informer. It leads to threaten for the informer.But due to high mobility, limited storage space and computational resources of connected cars still remains a challenging problem. Connected cars are affected by issues such as identity validity and message reliability when vehicle nodes share data with other nodes. In cyberspace, trust and privacy are still open issues due to the unique characteristics of vehicles. It is crucial for Internet of Vehicles to prevent internal vehicles from broadcasting forged messages while simultaneously protecting the privacy of each vehicle against tracking attacks. Hence the there is an extensive researchwhich focuses on finding an efficient solution for preserving the privacy in connected cars using Block chain technology. While preserving the privacy, anonymous messages should also be avoided.

To build a reliable communication system, a new decentralized trust management model for Vehicle to Vehicle (V2V) using Block chain Technology is proposed. In this model Connected Vehicles can validate the messages received from other Connected Vehicles and it will validate the incoming messages from other Connected Vehicles. Based on the obtained result, it will generate a threshold value and send to Roadside Units (RSUs).RSUs collect the data from the involved vehicles and generate a block. By using Proof of Work and Proof of Consensus mechanisms, the block is added to a trusted Block chain which is generated by coordinating with other RSUs

An attacker may broadcast fake information in cyberspace which may mislead other vehicles. Hence, ensuring the authentication, non repudiation and authenticity of messages in Internet of Vehicle is crucial.

Finding a single trusted entity to store and distribute announcement messages can be challenging, and vehicles may not be inclined to participate

M.S.Bennet Praba,
AP/CSE

Teacher's Corner

CYBER SAFETY TIPS

- Internet-enabled crimes and cyber intrusions are becoming increasingly sophisticated and preventing them requires each user of a connected device to be aware and on guard.
- Keep systems and software up to date and install a strong, reputable anti-virus program.
- Be careful when connecting to a public Wi-Fi network and do not conduct any sensitive transactions, including purchases, when on a public network.
- Create a strong and unique passphrase for each online account and change those passphrases regularly.Set up multi-factor authentication on all accounts that allow it.
- Examine the email address in all correspondence and scrutinize website URLs before responding to a message or visiting a site.
- Don’t click on anything in unsolicited emails or text messages.
- Be cautious about the information you share in online profiles and social media accounts. Sharing things like pet names, schools, and family members can give scammers the hints they need to guess your passwords or the answers to your account security questions.
- Don't send payments to unknown people or organizations that are seeking monetary support and urge immediate action.

Dr. Preethi
AP/CSE

Student's Corner

CYBERCRIMES AND CYBERSECURITY

In the modern digital age, cybercrime has become an increasingly pressing issue. Cybercriminals can cause significant harm to individuals, businesses, and even governments, making cybersecurity an essential consideration for anyone who uses a computer or the internet.Cybercrime refers to any illegal activity that involves a computer, network, or digital device. This includes a wide range of activities, such as hacking, identity theft, phishing, malware, ransomware, and denial of service (DoS) attacks. The motives behind cybercrime can vary from financial gain to political espionage, and the targets can range from individuals to multinational corporations.One of the most significant challenges of combating cybercrime is that it is constantly evolving. Cybercriminals are continually developing new techniques and tools to circumvent security measures, making it challenging for law enforcement and cybersecurity experts to keep up. For example, the rise of the internet of things (IoT) has created a new frontier for cybercriminals to exploit, with devices such as smart home appliances and medical devices being vulnerable to hacking.To combat cybercrime, it is essential to have robust cybersecurity measures in place. This includes having strong passwords, using two-factor authentication, regularly updating software and antivirus programs, and being cautious about opening emails or clicking on links from unknown sources. Additionally, individuals and organizations must be vigilant about monitoring their digital footprint and identifying any suspicious activity, such as unauthorized access to accounts or unusual network traffic.

K. Sowndarya Laxmi
CSE-CS-C

Student's Corner

POTENTIAL OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

AI refers to the simulation of human intelligence in machines that are programmed to think and learn like humans. In the context of cybersecurity, AI can be used to identify and respond to cyber threats in real-time. AI algorithms can analyze vast amounts of data to identify patterns and anomalies that could indicate a potential security breach. By doing so, AI can help security teams to quickly detect and respond to threats, reducing the risk of a successful cyber attack.

There are several benefits of using AI in cybersecurity, including:

Real-time threat detection: AI can help security teams to quickly detect and respond to threats, reducing the risk of a successful cyber attack.

Automated response: AI can automate the response to known threats, freeing up security personnel to focus on more complex threats.

Improved accuracy: AI algorithms can analyze vast amounts of data with greater accuracy than humans, reducing the risk of false positives and negatives.

Predictive analysis: AI can analyze data to identify patterns and trends that could indicate a potential threat, allowing security teams to take proactive measures to prevent on attack

While there are many benefits of using AI in cybersecurity, there are also several challenges that must be addressed. Some of these include:

1. Data quality: AI algorithms rely on large amounts of high-quality data to function effectively. If the data is incomplete or inaccurate, the algorithms may produce inaccurate results.
2. Complexity: AI algorithms can be complex and difficult to understand, making it challenging for security teams to identify and respond to false positives or false negatives.
3. Adversarial attacks: Cybercriminals can use AI-powered tools to launch sophisticated attacks that can bypass traditional security defenses.

AI has the potential to revolutionize the way we approach cybersecurity. By leveraging the power of AI, security teams can quickly detect and respond to threats, reducing the risk of a successful cyber attack. However, there are also several challenges that must be addressed, such as data quality and complexity. As the threat landscape continues to evolve, it is essential for organizations to embrace AI-powered cybersecurity tools to stay one step ahead of cybercriminals.

-Shyam Sunder M
III year CS-A

Student's Corner

In today's digital age, we're more connected than ever before. We can communicate with people from all corners of the globe, shop online, and even work remotely. But with all this convenience comes a great risk: the danger of cybercrime. It was a typical morning, and I was sitting at my desk, scrolling through my social media feed, when a notification popped up. It was an email from an unfamiliar sender, and the subject line read, "Urgent: Your Account Has Been Compromised." My heart raced as I quickly clicked on the email and began to read. The message was well-written and professional, and it claimed that my bank account had been hacked. It asked me to click on a link and enter my login information to verify my account details. I hesitated for a moment, but then I remembered hearing about this kind of scam before. I knew that if I clicked on that link, I would be giving the hackers access to my account. I immediately deleted the email and changed my account password. But it got me thinking about how vulnerable we all are to cybercrime. It's easy to forget that behind every computer screen is a potential hacker, waiting to steal our personal information or infect our devices with malware. As I sat there, I decided to do some research on cyber awareness. I learned about the importance of strong passwords, the dangers of clicking on unfamiliar links, and the need to keep my computer and antivirus software up to date. I also discovered the value of two-factor authentication and how it can help protect my accounts from unauthorized access. Armed with this knowledge, I felt more confident navigating the digital world. I knew that I could take steps to protect myself and my information. And I also realized that I could use my voice to spread awareness about cybercrime and the importance of cyber awareness. So, I decided to write a blog post about my experience and share it with my friends and family. I wanted to encourage them to be vigilant and take the necessary steps to protect themselves from cybercrime.

In the end, my experience with the phishing email turned out to be a wake-up call. It made me realize how vulnerable we all are to cybercrime and how important it is to be aware and take action. And as I continue to learn and educate others, I know that we can all work together to create a safer digital world.

K.Kaarthik Roshan
III year CS-A

Student's Corner

"Digital Dreams and Cybersecurity Schemes"

In a world of digital dreams,
Where data flows in endless streams,
We surf the web with ease and speed,
But danger lurks, we must take heed.

Cyber criminals prowl and scheme,
To steal our data, it's their dream,
They hack and phish, with stealth and guile,
And leave us feeling lost and vile.

But fear not, for there's a way,
To keep our data safe each day,
With passwords strong and firewalls high,
We'll keep those hackers far and nigh.

Encrypt our data, lock it tight,
And keep our systems up-to-date,
With backups stored in a safe place,
We'll be protected from disgrace.

So let's be wise and take control,
Of our data, our digital soul,
With cyber-smarts and vigilance,
We'll stay secure in every sense.

- Srinivasan V
I year CS- B

As they say, there are only 2 personalities,
One is those that have been hacked and
Other is those do not know they have been hacked.

- Samprithi V
II year CS - A

Student's Corner

With passwords complex and firewalls strong,
We can keep the hackers from doing us wrong.
But it's not just technology, it's a state of mind,
Being aware and careful, so we don't fall behind.

With unique passwords, and security at the core,
We can keep our data, safe forever more.
With encryption and firewalls, we can build a wall,
And keep the hackers, at bay one and all.

Try not to give up hope,
There's a way to cope.
Secure your systems, update your code,
And you'll be safe on the cyber road.

- Sravya Yamali
III year CS- A

Internet Security Awareness or Cyber Security Awareness measures how much end users know about the [Cyber Security] threats their networks face, the risks they pose, and the mitigation of security best practices to manage their behaviour. The cyber threat landscape continues to evolve at an alarming rate, with nearly 8 billion records exposed in data breaches in the first nine months of2019 alone. Despite heavy investments in advanced defence systems, many businesses still fall victim to cyberattacks. Human error has played a key role in the majority of data breaches. Studies show that more than 80% of security breaches involve errors such as clicking malicious links in phishing emails, using weakpasswords, or exploiting stolen credentials. Hackers are actively exploiting these vulnerabilities to infiltrate networks and systems, highlighting the critical need or ongoing cybersecurity awareness and education.

- Harsh Jain
III year CS - A

Department Archives

Industrial Visit

The department of CSE organized a one-day industrial visit to Monolith Research and Training Labs Pvt. Ltd., Chennai on 13th and 14th October for II Year Cyber Security - A, B & C and III Year Cyber Security - A & B students. Dr. M. Murali Krishna, Dean E & T addressed the students prior to the industrial visit and advised the students to utilize the opportunities. Dr. K. Raja, HOD - CSE also motivated the students to learn the industrial practices and standards. Around 130 students benefited through the industrial visit. They experienced VR Technologies at their labs which were truly scintillating. It was a modern and well equipped lab that constituted games ranging from car racing to gun shooting that utilizes VR Technology.

Department Archives

Cyber Security and Ethical Hacking Workshop

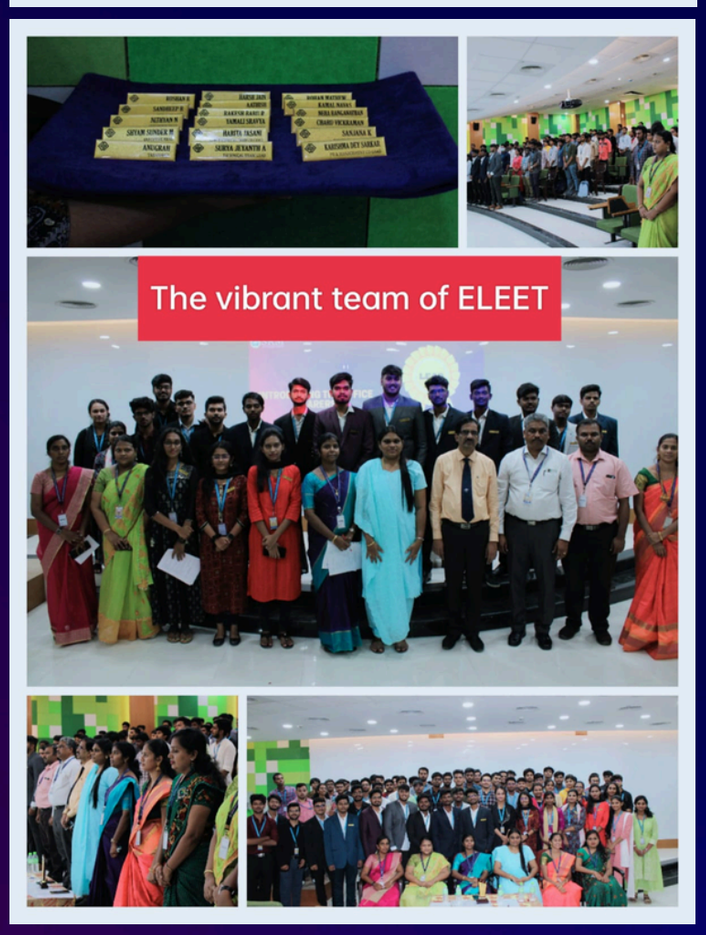
The department of CSE organized a one-day industrial visit to Monolith Research and Training Labs Pvt. Ltd., Chennai on 13th and 14th October for II Year Cyber Security - A, B & C and III Year Cyber Security - A & B students. Dr. M. Murali Krishna, Dean E & T addressed the students prior to the industrial visit and advised the students to utilize the opportunities. Dr. K. Raja, HOD - CSE also motivated the students to learn the industrial practices and standards. Around 130 students benefited through the industrial visit. They experienced VR Technologies at their labs which were truly scintillating. It was a modern and well equipped lab that constituted games ranging from car racing to gun shooting that utilizes VR Technology.

Department Archives

Cyber Safety Guest Lecture

Cyber Security is a critical area of concern for individuals, businesses, and governments alike. The increasing number of cyber-attacks and data breaches has raised awareness of the need for better cyber security practices and education. Guest lectures in cyber security provide a valuable opportunity to raise awareness and educate students, employees, and other stakeholders about cyber security threats, best practices, and trends. In this article, we will explore the importance of guest lectures in cyber security and provide tips for success.

Department Archives



Eleet Club - Inauguration

The Department of Computer Science and Engineering with specialization in Cyber Security inaugurated the club "ELEET" on 30th September 2022 at 10.30 am in the Gallery Hall, Block 5,SRMIST, Ramapuram Campus. The inaugural ceremony started with the invocation through the devotional expressive Tamil Thai Vaazhthu. The dignitaries lighted the lamp as the symbol of auspiciousness. Mrs.Gowthamy, Assistant Professor presented an exclusive welcome. ELEET is an exclusive cyber security club that is set with a goal to teach individuals about cybersecurity and help them gain their knowledge necessary to arm themselves against modern-day computer exploits.

Department Archives

31337 V1.0

Eleet, the newly inaugurated club at SRMIST Ramapuram, Chennai, conducted their first official event on October 1, 2022, which was a resounding success. The event focused on raising awareness about the importance of cybersecurity in today's rapidly changing digital world. The students were briefed on the basics of cybersecurity, wireless technologies, and ways to protect wireless devices from cyberattacks. The event also included a non-technical debate competition and an interactive cybersecurity-focused mobile game called WebME. The technical session covered various topics such as password protection, cyber-hygiene etiquettes, CIA Triads, and Web API. The event concluded with feedback from the participants and a speech by Saranya ma'am. Overall, Eleet's first event was a remarkable success, and the club is looking forward to showcasing more innovative ideas in their next event.

Department Archives

Hackers Hardware

The Eleet Club recently hosted an event called "Hacker's Hardware" to raise awareness about the importance of cybersecurity in our increasingly digital lives. The event featured a lineup of knowledgeable speakers including Harsh Jain, Aathish M, and Shyam Sunder, who covered a range of topics from Raspberry PI Pico to Kali Linux. Attendees had the opportunity to learn about the latest hacking devices and techniques, and participate in fun activities like logo quizzes and debates. The event was a resounding success and left participants with a better understanding of cybersecurity threats and how to stay safe in the digital age and gadgets that were showcased at the event, includes Raspberry PI Pico, ESP8266 V2, Digispark Attiny 85, HAK5 site, Wireless Adapters, Flipper Zero, HackRF One, Ubertooth, OMG Elite cable, Proxmark 3, and Mouse Jack. The speakers delved into the intricacies of MAC and IP addresses, de-authentication attacks, and vulnerabilities in Wi-Fi networks. With its informative sessions and engaging activities, Hacker's Hardware was a great platform for both technical and non-technical individuals to learn about cybersecurity and its significance in today's world."

ABSTRACTS- PAPER PRESENTATION

CYBERSECURITY THREATS AND DIFFICULTIES IN THE EDUCATIONAL FIELD

P. Davesh Prabu ,Dinesh kumar
Kongu Engineering College, Perundurai

ABSTRACT:
Higher education will continue to see an increase in the demand for computer security. Catastrophic data breaches have already occurred as a consequence of poor risk management and more are likely. Attacks against academics, students, and universities have been ongoing all over the globe. The review of various educational surveys is the foundation of this research. New research avenues in higher education security will be made possible as a consequence of this study. This study analyses a number of sources to give a broad overview of cyber security issues. Our classification of the review is primarily based on the research issues we address. It will benefit both businesses and scholars to establish a foothold in the educational community. The Covid-19 pandemic had a major effect on the organisation of studies in higher education institutions. Since March 2020, the only option for continuing education was via distance learning. In the wake of the Covid-19 pandemic, technologies like cloud computing, online learning platforms, and video conferencing software whose use was previously quite restricted in HEIs have emerged as the key tools for conducting online research. As a result, there is now a significantly higher risk of DoS and DDoS attacks.

INTERNET OF THINGS (IOT) SECURITY AND PRIVACY ISSUES

Sedhumadhavan V, Sanjay R D ,Yogeshwaran P
Kongu Engineering College, Perundurai.

ABSTRACT:
Everyday life is significantly impacted by the Internet of Things. It is a tool that allows people to object to one another, to objects, and to other objects. IoT is employed in various industries, including home automation, transportation, healthcare, and medicine. Connectivity between various devices is made possible by the Internet of Things (IoT). In this system, items that have detector technology integrated in them connect with one another through a wireless communications channel to exchange and convey information without the need for human contact. Because to the openness and simplicity of their networks, these devices are vulnerable to attacks. Consequently, the two main issues with this technology are privacy and security. It is essential to draw attention to the privacy and security risks posed by IoT in order to advance its development. The purpose of the article is to outline the many security and privacy issues that an IoT is experiencing as well as the current defences in place. The article primarily focuses on the privacy and security aspects of IoT, such as the Civil services security needs, privacy and security concerns, and the remedies that must be managed to avoid these privacy and security threats. Therefore, we need mechanisms to protect personal data and monitor their flow from things to the cloud. In this talk, we describe threats and concerns for security and privacy arising from IoT services, and introduce approaches to solve these security and privacy issues in the industrial field.

ARTIFICIAL INTELLIGENCE (AI) FOR CYBERSECURITY: OPPORTUNITIES AND CHALLENGES

Rohith G,Suryah Prakash M R,Sujith R
Kongu Engineering college

ABSTRACT:

Artificial Intelligence (AI) in Cyber security Market lets enterprises monitor, discover, report, and combat cyber threats to maintain information confidentiality. Artificial Intelligence (AI) has the potential to significantly improve cyber security by providing advanced threat detection, faster incident response times, and enhanced predictive analytics. However, it also presents unique challenges such as the risk of AI being manipulated by cybercriminals and the potential for AI to cause unintended harm if it is not designed and implemented properly. One of the key benefits of AI in cyber security is its ability to analyse vast amounts of data and detect anomalies that might go unnoticed by human analysts. This can help organizations detect and respond to threats more quickly, reducing the impact of cyber-attacks. AI can also be used to automate routine security tasks, such as patching vulnerabilities, freeing up human analysts to focus on more complex threats. However, there are also challenges associated with AI in cyber security. AI models can be vulnerable to manipulation by cybercriminals, who could use adversarial attacks to trick AI systems into misclassifying data. This could lead to false positives or false negatives in threat detection, potentially leaving organizations vulnerable to attack. Another challenge is the potential for AI to cause unintended harm. For example, if an AI system is not designed properly, it could inadvertently cause disruptions or damage to critical systems. There is also the risk of AI being biased, which could lead to unfair or discriminatory decisions. Overall, while AI presents significant opportunities for improving cyber security, it is important to approach its implementation with caution and ensure that appropriate safeguards are in place to mitigate the risks.

MACHINE LEARNING TO DETECT AND PREVENT CYBER ATTACKS

Harshia K.D,Catherine Amala.A,Krishnapriya.S
Mookambigai College of Engineering, Pudukkottai

ABSTRACT:

The development of effective techniques to overcome cybercrime is been challenging to combat the vulnerability in computing. Ethical hackers have been increasing day to day in committing various breaches of data in recent days. A few of the cyber attacks are Ransomware attacks, DDOS attacks, Phishing, Malware, etc. Machine learning can be used as one of the counterfeiting measures to detect and prevent cyber attacks such as malware detection, intrusion detection, spam detection, and phishing detection. The algorithms in Machine learning can train and detect the above-mentioned cyber attacks. An alert or notification by e-mail would be sent to the users once an attack is detected. The various learning techniques are Supervised Learning, Unsupervised learning. Reinforcement learning etc. implements various Machine Learning algorithms. Supervised learning algorithms like classification can be used to detect cyber attacks. A recent cyber attack occurred in New York, USA, a few days ago. A more frequent attack is ransomware attack where people steal one's data and ask for money.

CYBERSECURITY THREATS AND CHALLENGES FOR AUTONOMOUS VEHICLES AND CONNECTED CARS

Prithi G,
Raaghavi K R,
Shrivarshini K
Amrita School of Engineering, Chennai

ABSTRACT:

The increasing use of automated vehicles has had significant positive impacts on the automotive industry. However, their reliance on software and data also exposes them to cyber security threats. The purpose of the paper is to examine cyber threats and challenges faced by automated cars, such as hacking, data breeches and malicious attacks, as well as the implications and mitigation measures to be taken. In this regard, it is in the need of the hour to develop advanced technologies and proper regulations to be implemented to ensure the safety and secure operation of automated vehicles. In conclusion, the paper stresses the importance of collaboration between industry stakeholders and cyber security experts for developing and deploying automated vehicles.

BIOMETRIC AUTHENTICATION AND ITS VULNERABILITIES

Puvisha Shanmugam
Sri Sai Ram Engineering College

ABSTRACT :

As the world evolves, the technology grows rapidly at the same time with much higher complexity. Technologies are becoming increasingly complicated and interconnected. One such technology which is currently in use is the biometrics. Biometrics is the measurement of the body and calculation of human characteristics. Generally, biometrics are used for authentication purposes. Previously authentication system works by comparing the provided data with the validated user details stored in the database like passwords. In biometrics authentication, we use physical or behavioural traits such as fingerprint scanning, DNA matching, Retina scanning etc. The main characteristics for the increasing use of biometrics in leading industries are due to its uniqueness in differentiating between the users. We mainly use the Multimodal biometric system. This system is used to overcome the limitations of unimodal biometric systems. This system consists of sets of information related to the same user. The use of biometrics has become very common and has grown rapidly in the last few years especially due to the pandemic. We use this concept in almost all industries and also in day-to-day life like smart phones which contain fingerprint sensors and even facial recognition for locking and unlocking the device. Even though biometrics are secure they are subjected to the risk of hacking or can be misused by people for their own personal benefit. There are a lot of scopes for malicious attacks which can be performed on such a system using various techniques like downloading a user's photo, using a fake silicon fingerprint or a 3D mask. This paper describes the various helpful as well as threatening issues faced using biometric technology in our day-to-day life. It also explains about the various attacks faced in biometrics and the existing solutions proposed.

CYBERSECURITY RISKS AND CHALLENGES IN GAMING INDUSTRY

Dhinesh D, Shrenath A R, Preethi S
Manakulavinayagar Institute of Technology, Pondicherry

ABSTRACT:
The gaming industry has become a popular target for cybercriminals, who use various methods to steal user data, disrupt gaming services, and damage the reputation of gaming companies. Our paper explores the cyber security risks and challenges faced by the gaming industry, and discuss the different types of cyber threats that target gaming platforms. To mitigate these risks, gaming companies can implement strong security protocols, use encryption to protect user data, and educate users about cyber security best practices. Collaboration between gaming companies, law enforcement agencies, and cyber security experts is also important to enhance the security of the gaming industry. Overall, our paper emphasizes the importance of cyber security in the gaming industry and urges gaming companies to take proactive measures to protect their platforms, engines (eg. Unity, Unreal) and users from cyber threats.

CYBER SECURITY AND PRIVACY ISSUES IN SOCIAL MEDIA

Siva surya.V,Naveen Chinnadurai,Dharanidharan.P
Sengunthar Engineering College

ABSTRACT:
Internet and social media becomes essential factor for the human life and the internet is upgrading rapidly. In this modern era, everything has been made virtual. Especially, during pandemic situation human life becomes virtual and we realized the importance of Internet. Government and Banking services become virtual so that every citizen can utilize them through online. More the internet used, more the crimes registered. The citizens were thought only "how to use the internet or social media" but there is no awareness for the crimes in the internet and social media. The crimes that happen on internet or social media are considered as cyber crime. Cyber security is the practice of protecting systems, networks and programs from digital attacks. These Cyber attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. The social media connects internet with people and it allows us to have conversations, share information and enables us to Communicate with others. When users create a social media account and use the platform, they leave a digital footprint on the internet and they agree to the terms and conditions, which enable Companies to collect personal information. Other than the companies, the hackers who illegally access user's data and misuse the personal and sensitive details. The companies use our data for marketing, but the hackers misuse our data in multiple ways. Once a hacker has access to your account, they can do a lot of damage, like stealing your personal information, posting offensive content or contacting your friends and family.

MACHINE LEARNING FOR DETECTING AND PREVENTING CYBER ATTACKS

N.Kannan,D.Sanjay,R.Vignesh
Guru Shree Shantivijai Jain Arts and Science College,Nallur Branch

ABSTRACT:

Cyber-attacks are becoming increasingly frequent and sophisticated, posing a growing threat to individuals, businesses, and governments worldwide. Cyber security refers to the practice of protecting digital systems, networks, devices, and data from unauthorized access, theft, damage, or other malicious activities. It aims to ensure the confidentiality, integrity, and availability of digital assets and prevent cyber-attacks that could compromise sensitive information or disrupt operations. Conventional security systems lack efficiency in detecting previously unseen and polymorphic security attacks like increased frequency, Ransomware attacks, Supply chain attacks and Cloud security risks. To overcome these challenges of cyber-attacks, we are using an advanced tool “Machine Learning”. It has become a crucial tool in the fight against cyber -attacks. With the increasing frequency and sophistication of cyber threats, ML-based approaches are being used to detect and prevent attacks in real-time. It learn from historical data to identify new types of attacks and also can be continuously updated and improved to stay ahead of evolving threats that have not been seen before. Machine learning (ML) techniques are playing a vital role in numerous applications of cyber security. Here are some ways machine learning can be used for cyber security are Intrusion detection, Malware detection, User-behaviour analytics and Fraud detection.

ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

O.S.Abishek,J.R.Thiyanesh Kumar,S.Divyesh
Mepco Schlenk Engineering College, Sivakasi

ABSTRACT:

The objective of this paper is to provide knowledge on artificial intelligence (AI) applied in the field of cyber security and cyber defence of critical infrastructures such as banking systems, military industries and others big infrastructures that affect large number of persons and security of nations. The implementation of artificial intelligence assures us a future with high level of security and professionals with abilities to protect endpoints, data, and networks which include SCADA, PLC, HMI and DSC systems. By using advanced or updated technical abilities, we can predict problems by using predictive analysis based on the solutions and ability to use natural language processing (NLP) in the machine learning and deep learning with different algorithms to of security operations center (SOC), with integration of the right SOAR (Security Orchestration and Automation Response), and AISIEM (Artificial Intelligence Security Information and Events Management) technologies to quickly and cost effectively stop intrusions or even prevent them before they happen. In addition, different algorithms of artificial intelligence are implemented in the next generation of firewalls. It also the only way to protect a network and end point against malicious attackers and zero day and unknowing malware also using artificial intelligence. The implementation of zero trust and micro segmentation strategy is recommended to avoid an eventual risks and errors caused in the past.

DIGITAL FORENSICS INVESTIGATION

T.Hariharan,V.Durekshveer,C.Madhumitha
Manakula vinayagar Institute of Technology

ABSTRACT:

Digital forensics investigation is a rapidly evolving field of computer science that deals with the recovery, collection, analysis, and presentation of digital evidence for legal proceedings. In this paper, we present an overview of current practices and trends in digital forensics investigation. We discuss the importance of digital forensics in criminal justice and identify techniques to maximize its effectiveness. We review the various types of digital evidence, such as metadata, emails, documents, and images, and explain how they can be used to support investigations. We also analyze the challenges and legal implications of digital forensics, including privacy and data integrity. Finally, we discuss emerging technologies and practices that could further enhance digital forensics capabilities. Our presentation provides an overview of digital forensics and its implications for criminal justice, giving the audience an understanding of the fundamental principles of digital forensics and its applications in criminal investigation

CYBER SECURITY: BIOMETRIC TO INCREASE DATA PRIVACY

Arun . E,Lingeswaran. B
S A Engineering College

ABSTRACT:

Biometrics is any physical or biological feature that can be measured and used for the purpose of identification and authentication. Its features can be either physiological like: fingerprint, hand geometry, the face, the iris, the retina or behavioural. This Project is about to create a Biometric Security System for IOT ,Cloud, Network, Application Security .We face many unauthorized security breach for our personal and confidential data , to avoid these kind of data breach some firewalls and protections can be used .The Biometrics has seen an increase in the invasion of individual privacy due to security concerns. Many experts today argue that because biometrics identifiers are unique to everyone, biometric identification is ultimately more secure than traditional passwords, two-factor authentication, and knowledge-based answers. Biometric authentication methods such as facial recognition and fingerprint recognition are becoming increasingly popular tools to secure digital transactions while providing customers with a frictionless user experience. One of the key benefits of biometric security devices is that they can help to increase your protection. It's much harder, for example, to clone or steal a fingerprint than an access card. In situations where you need to increase security, biometrics can also be used for multifactor verification. In this paper, we discuss the privacy concerns in biometrics and also provide some remedies to these concerns. The Biometric system may find application in attendance system, identification purpose, data security and more applications. The prevalent system would be worked upon and modified for error free secure system

CYBER SECURITY RISKS IN CLOUD COMPUTING AND MITIGATING MEASURES

Raghavi M,Boobash Ayyanar M,Manojkavin K S
SRM Institute of Science and Technology, Ramapuram

ABSTRACT:

Cloud computing has revolutionized the way; businesses and individuals store, access, and manage data. Cloud computing is said to be the way forward, offering great facilitations for start-up organizations with cost reduction and flexible and handy scalability. However, with the convenience of cloud storage comes the risk of cyber security threats. Cyber criminals are constantly looking for ways to exploit cloud computing systems, making it essential to understand the potential risks and how to mitigate them. The risks of this technology are not only the ones related to the cloud but also those that are inherited from the Internet itself. This presentation will explore the various cyber security risks associated with cloud computing and the measures that can be taken to protect against them. It will also provide an overview of the latest technologies and best practices for mitigating cyber security risks in the cloud.

BLOCKCHAIN TECHNOLOGY FOR SECURING ONLINE TRANSACTIONS AND DATA

Mithun Ganapathy V,Ragul N,Akash A
Mepco Schlenk Engineering College, Sivakasi

ABSTRACT:

This paper provides a basic understanding and knowledge on “Block chain Technology” which is used for securing online transactions and protecting data from cyber-attacks and other misuses. Hopefully, this will demonstrate the working of block chain technology in the security of transaction and data. This technology works mainly on the concepts of immutability, decentralization, and transparency. Block chain is a distributed database or Ledger that is shared among the nodes of a network. This technology is also known as “Distributed Ledger Technology.” It is programmable, secure, anonymous, unanimous, time-stamped, immutable, and distributed. Block chain is a new form of database which is nothing but an organized collection of data, so that it can be easily accessed and aged. Thus, each of our interactions with the internet is generating data. The main objective of this technology is to produce a tamper-proof ledger. The worldwide block chain technology industry is anticipated to reach $1,432 billion by 2030, with a Compounded Annual Growth Rate (CAGR) of 85.9% between 2022 and 2030 according to Grand View Research. Security in the block chain environment is very critical. It provides protection against unauthorized access ensures data integrity, prevents cyber attacks and double spending of money and fraud mitigation. This security is sometimes disputed due to the absence of a central authority to monitor and control the network. Major hacking incidents in a blockchain are THORChain Hack which cost over $7 million crypto currencies and Binance Hack which costed over $40 million crypto currencies.

FACULTY COMMITTEE

Dr.SHINY DUELA J	DEPUTY HOD/CS
Dr.SUBASHKA RAMESH.S.S.	AP/CSE
Dr.BALAJI.C.G	AP/CSE
Dr.G.V.SHAAMILI VARSA	AP/CSE
Dr.MINU.M.S	AP/CSE
Dr. J.JOSPIN JEYA	AP/CSE
Dr.S.RAJA RATHNA	AP/CSE
Dr.SUGANTHI N	AP/CSE
Dr.D.PREETHI	AP/CSE
Dr.URMELA	AP/CSE
Dr.VINOTH	AP/CSE
Dr.M.AYYADURAI	AP/CSE
Ms.J.ARTHY	AP/CSE
Ms.R.SATHYA	AP/CSE
Ms.SARANYA G	AP/CSE
Ms.GOWTHAMY .J	AP/CSE
Ms.J.JUSLIN SEGA	AP/CSE
Ms. W.ANCY BREEN	AP/CSE
Mr.A.VADIVELU	AP/CSE
Ms.S.SRIDEVI	AP/CSE
Mr.KINGSLY STEPHEN R	AP/CSE
Ms.PREETHY JEMIMA P	AP/CSE
Ms.MARY JOSEPH	AP/CSE
Ms.SIVASANKARI K	AP/CSE
Ms.L.SASIKALA	AP/CSE
Mr.G.RAGU	AP/CSE
Mr.EZRA VETHAMANI	AP/CSE
Mr.M.SADHASIVAM	AP/CSE
Mr.SENTHIL P	AP/CSE

STUDENT COMMITTEE

SHYAM SUNDER M	III CSE CS-A
SANDHEEP R	III CSE CS-B
KAARTHIK ROSHAN K	III CSE CS-A
KIREN DHARSHINI	III CSE CS-B
MOKAN KUMAR B V	II CSE CS-A
SANJANA DURGA K	II CSE CS-A

SPONSORS

LANCOR
CREATING ENDURING VALUE

Lancor Holdings Limited a Public Limited company listed on the Bombay Stock Exchange, has been creating landmarks through execution of commercial and residential development projects in Chennai for over 37 years. Among its more well-known projects include The Atrium, Westminster, Menon Eternity, and large-scale development in Sholinganallur under the title "The Central Park".Lancor was given "the Highest transparency" award at The CNBC CREDAI AWAAZ REAL ESTATE AWARDS 2009 is testimony to the fact.

ICTACADEMY®

ICT Academy is an initiative of the Government of India in collaboration with the state Governments and Industries. ICT Academy is a not-for-profit society, the first of its kind pioneer venture under the Public-Private-Partnership (PPP) model that endeavours to train the higher education teachers and students thereby exercises on developing the next generation teachers and industry ready students.

GES
General Engineering & Services

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

SRM-IST RAMAPURAM

"CYBERSECURITY IS A SHARED RESPONSIBILITY. STOP. THINK. CONNECT." - NATIONAL CYBERSECURITY ALLIANCE

CYBER CARNIVAL '23

ELE3T

LANCOR
CREATING ENDURING VALUE

ICTACADEMY®

GES
General Engineering & Services