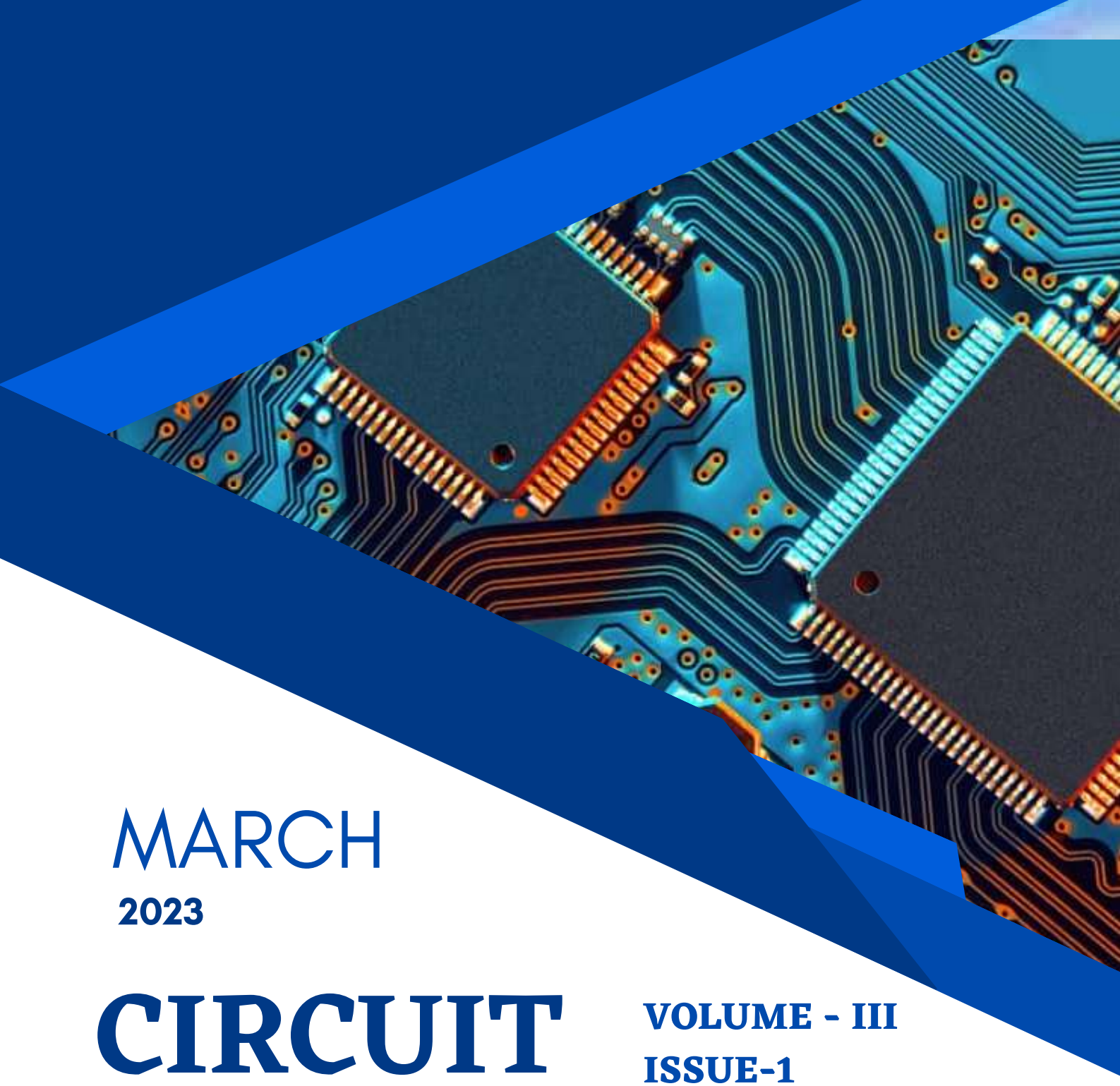


MARCH

2023

CIRCUIT TIMES

VOLUME - III
ISSUE-1

SVCE | SRI VENKATESWARA COLLEGE OF ENGINEERING

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

IN THIS ISSUE :

ARTICLE

- IOT SECURITY IMPEDIMENTS – CHALLENGES AND DEFENSE MECHANISMS
- DATA ANALYTICS IN NETWORK

EVENTS CONDUCTED

ACHIEVEMENTS

- BY FACULTY
- BY UG STUDENTS
- FACULTY PARTICIPATION
- FACULTY PUBLICATION

VISION OF THE DEPARTMENT

To excel in offering value based quality education in the field of Electronics and Communication Engineering, keeping in pace with the latest developments in technology through exemplary research, to raise the intellectual competence to match global standards and to make significant contributions to the society.

MISSION OF THE DEPARTMENT

- To provide the best pedagogical atmosphere of highest quality through modern infrastructure, latest knowledge and cutting edge skills.
- To fulfill the research interests of faculty and students by promoting and sustaining in house research facilities so as to obtain the reputed publications and patents.
- To educate our students, the ethical and moral values, integrity, leadership and other quality aspects to cater to the growing need for values in the society.

Program Educational Objectives (PEOs)

PEO1: Create value to organizations as an EMPLOYEE at various levels, by improving the systems and processes using appropriate methods and tools learnt from the programme.

PEO2:Run an organization successfully with good social responsibility as an ENTREPRENEUR, making use of the knowledge and skills acquired from the programme.

PEO3:Contribute to the future by fostering research in the chosen area as an ERUDITE SCHOLAR, based on the motivation derived from the programme.

Program Specific Outcomes (PSOs)

PSO-1: An ability to apply the concepts of Electronics, Communications, Signal processing, VLSI, Control systems etc., in the design and implementation of application oriented engineering systems.

PSO-2: An ability to solve complex Electronics and communication Engineering problems, using latest hardware and software tools, along with analytical and managerial skills to arrive appropriate solutions, either independently or in team.

ARTICLE

IoT Security Impediments – Challenges and Defense Mechanisms

Dr.T.J.Jeyaprabha, Associate Professor, ECE, SVCE.

Abstract:

Devices that are connected to the Internet of Things (IoT) have assimilated into daily life. As more and more devices are connected to a worldwide network, the IoT is expanding swiftly. The data and applications on many IoT devices are extremely sensitive and should only be accessible by authorized users. In order to prevent failure, these apps rely on real-time or almost real-time conditions. They also use consumption data to analyze and forecast the future using artificial intelligence algorithms. More than simply the IoT device itself should be protected by IoT security. IoT devices are poorly secured and have numerous faults. Many believe that IoT manufacturers do not give security and privacy enough consideration. But despite these security issues, IoT adoption is continuing. Therefore, in order to increase security, users and security practitioners alike must learn about it.

Introduction

IoT refers to a group of connected devices that use controllers and nodes to collect and exchange data. IoT is a network of individually recognizable physical objects or "things" that have the ability to perceive and communicate with one another, with their surroundings, or with both. These devices might be able to think and behave autonomously as well as gather information for a variety of purposes thanks to controllers and cloud computing.

SPECIAL FEATURES OF IoT

The following traits apply to numerous "things":

- Totally integrated, either with or without an operating system (OS).
- Largely real-time data collection.
- Utilize all networks, including cellular LPWAN (narrowband IoT and LTE-M) and local area networks (LAN, LPWAN, and cellular).
- Have ongoing or sporadic cloud connectivity, necessitating the requirement to store data with a time stamp.

- Physical parameters measurement.
- Ability to make decisions based on the information gathered by these devices, which is required to accomplish centrally automated decision-making.

The purpose of IoT is to raise living standards and benefit both consumers and businesses. IoT facilitates the following goals:

- The usage of energy is reduced.
- Improvements in security and safety.
- Advancements in the automation of routine chores.
- Improvements to the standard of living.

IoT DEPLOYMENT

IoT implementation can be divided into five categories:

- Industrial IoT—Enables better customization of goods and services for clients in less time, resulting in an improvement in customer service. IoT has improved connectivity and communication between manufacturing and the assembly line, allowing manufacturers to tailor their products to the needs of their clients and create in response to market demand (e.g., smart factories).
- Smart business buildings are included in commercial IoT.
- IoT in healthcare enhances patient care. For continuous monitoring of medical data, IoT devices connect patients to healthcare systems. Doctors, nurses, and family members can access patient data, as well as machines and algorithms that generate automatic feedback based on the processed data.
- IoT for transportation – Tracks the progress of cargo transportation and takes necessary preventive action while in route. IoT devices, for instance, may track parcels from beginning to finish to check on temperature, location, and potential tampering.
- Devices that connect to consumers' accounts, such as smart TVs, smart speakers, toys, wearables, and smart appliances

CONSTITUENTS OF IoT

IoT systems' building blocks are hardware and software, which connect with one another utilizing a wide range of protocols. IoT devices need these five basic building pieces to function:

- Depending on the purpose and usage, different IoT devices have different hardware components. Smart device components include things like sensors, actuators, accelerometers, gyroscopes, and radio-frequency identification (RFID) chips.

- The software consists of platforms and programs that decide what information should be gathered, which data sources should be connected to, which decision-making algorithms should be used, and how to use application programming interfaces (APIs) to link with other software parts. This also contains firmware, which facilitates communication between APIs and programs, and hardware.

- All elements that analyze, process, store, and visualize data are referred to as data.

- The hardware, software, and information components are all connected. The phrase "Internet of Things" may imply that everything is interconnected, but multiple forms of connectivity and communication protocols are needed based on the device type and proximity, among other variables.

All the other components, including connectivity, must have security. The security of devices, networks, APIs, and data must all be ensured because a security flaw in any one of these areas could jeopardize the security of the entire system.

TOP THREATS IN IoT SECURITY

The IoT implementation faces numerous difficulties. IoT security goes beyond simply protecting the devices themselves because it also involves protecting the cloud, mobile applications, network interfaces, software, use of encryption and authentication, and physical security. IoT application services are offered on a broad scale, in many different sectors, and through numerous ownership entities. Users of the system must be able to trust that information and services are being shared in a secure setting, which requires a trust foundation. According to the Open Web Application Security Project (OWASP), the following factors are the most frequently occurring flaws in the data security of IoT applications:

- Unreliable web interfaces.
- Inadequate permission or authentication
- Services on unsecured networks
- Insufficient transport encryption
- Privacy issues
- Vulnerable cloud interface
- Unreliable mobile interface
- Inadequate security configuration abilities
- Unreliable software or firmware
- Inadequate physical safety

The main issues are end-point security and IoT application security. IoT becomes a potential target for cyberattacks when its devices and apps are not properly secured. Security-wise, application developers or IoT gadget makers are still in their infancy. Security, however, is an essential component of every IoT architecture. Hardware and software design are both impacted from the outset by integrating security in IoT. Rapid change is occurring in connectivity and device security technologies. It is difficult since security is an essential component of all current systems, not just an add-on. To support the device from the start, the security scope should be end-to-end.

Most current security techniques, including authentication, encryption, access control, and auditing, are too complex to be implemented on IoT devices since many of them are small and have limited processor, memory, and power capabilities.

Because of the complexity of the infrastructure and the density of buildings in urban areas, where IoT devices are commonly utilized, it is simple for attackers to gain direct physical access to the IoT devices. Denial-of-service (DoS) assaults can also turn IoT devices into weapons and enlist them in a vast zombie army. Another important issue to think about is insecure IoT databases or data repositories.

IoT devices have a lengthy shelf life, may no longer receive support, and may be employed in situations that make it difficult or impossible to upgrade or reconfigure them, leaving them open to cybersecurity threats. Furthermore, incorrect data disposal methods without sufficient wiping raise major issues.

The eyes and ears of an IoT device are its built-in features, which include microphones, cameras, and night vision. These gadgets unintentionally capture petabytes of data that may end up in the wrong hands and compromise user privacy. Lack of clear, full disclosures regarding data collection, use, and sharing, especially where such practices may be unanticipated, puts the collector in danger of legal action.

IoT devices frequently come with weak default credentials. This might include passwords that are hard-coded into the system and shared among a group of devices, making it simple for hackers to compromise these systems. There are numerous built-in default usernames and passwords for IoT devices. Malware searches for IoT devices and typically tries to attack them using the username and password that are set by default. Once it has been accepted, the malware can take control of the computer and engage in coordinated botnet attacks.

SECURITY PATTERNS

To safeguard organizational assets against risk, several tiers of administrative, technical, and physical controls are typically utilized. As a result, a well-planned defense that is intense and powerful is created. For an information security structure to be successfully established and maintained, top management's commitment and support are crucial. Management must pay attention to IoT's huge potential. Security must be considered during the design phase by manufacturers and suppliers. To secure IoT, the best approach is to concentrate on the foundations. To do this, IoT platform developers, IoT platform architects, IoT application developers, IoT service developers, and IoT experience designers should collaborate. It is crucial for everyone involved in the development of IoT to include security measures while creating their IoT solution designs.

Designing for security, incorporating firewall features to add an additional layer of defense, offering encryption capabilities, and including tamper detection tools are some of the best ways to prevent attacks. Consumer safety and confidence may be in jeopardy if manufacturers fail to thoroughly test their products.

Every component of the ecosystem powering a certain IoT product, service, or device must be specifically designed with security in mind. Vendors should always follow best practices and strive for confidentiality, integrity, and availability (the CIA trinity) when developing products for the Internet of Things. The number of devices, the intended use for each device, and the physical state of each device are the primary differences between IoT security and conventional IT security. By creating market-accepted test criteria, testing helps ensure that the device and its protocols can function inside the IoT ecosystem. This facilitates acceptance of devices that may interact with other IoT objects and introduces the testing period required for the product or protocol. Testing IoT web interface management, monitoring IoT network traffic, evaluating the necessity for physical ports, evaluating authentication, and examining how devices interact with the cloud and mobile applications are all necessary for improving security configurability.

IoT device segmentation improves network security. The same goes for creating IoT protocols that not only cooperate but also guarantee privacy and security. Unused networking services and ports need to be terminated and closed because they expose the system to additional attack vectors. Deactivating superfluous services is crucial because they could go undetected, allowing an attacker to exploit them covertly as an attack vector or target. In order to ensure that only reliable devices may share data, it is also essential to provide authentication between devices. To manage several IoT credentials, a reliable password management system must be in place. Training in user awareness aims to make users and consumers more conscious of the device's potential risks. Customers should demand that the vendors have protected the device against typical attacks when choosing an appropriate IoT device. To keep user data secure, processing and encryption are required. From the sensors to the service providers, the entire communication path must be secure. The provision of encrypted communication streams, encrypted data storage, and the use of hash integrity checkers are some strategies for closing the enormous security gap. Other strategies include the provision of authentication procedures so that the devices communicate with recognised and reputable entities, and the provision of security updates in the form of patches and bug fixes.

BEST PRACTICES FOR IoT SECURITY

- Enable security and control from scratch.
- Include security in the process of developing IoT applications.
- Enable access control, log management, patch management, and IoT hardening.
- Make data collection, privacy, storage, sharing, handling, and disposal audit controls available.
- Access management, session management, and remote access network protocols have to be enabled.
- By developing and testing use cases and abuse scenarios, controls are tested and vulnerabilities are looked for.
- Demonstrate the monitoring controls on the IoT program's effectiveness.
- Create a watchdog protocol to track connectivity over time, identify connection failure, and manage resource usage. The watchdog will keep tabs on the IoT items' activity, making it simple to respond to incidents right away.
- Place a strong emphasis on the importance of both usefulness and security.
- Place a strong emphasis on the importance of both usefulness and security.

- Build and improve the IT security and assurance team's expertise to cover IoT risks and benefits as well as cybersecurity.
- Align the use of business IoT with IT functions.
- Plan the creation, purchase, and maintenance of IoT systems.
- IoT device trust should be regulated.
- IoT device disposal, asset management, and inventory maintenance.
- Implement governance over IoT projects.
- Consider security when designing gadgets.
- Malware defense must be included in IoT apps.
- Review the code and do a security audit of the IoT environment.
- Define the IoT environment's data flow.
- Create a program to manage vulnerabilities.
- Penetration testing and vulnerability assessments.
- Create a threat model for IoT.
- Establish accountability and governance.

CONCLUSION

IoT technology applications have both potential and security risks, hence IoT device security presents enormous hurdles. Before implementing IoT, a thorough assessment of security risk is required to identify all pertinent, underlying issues.

IoT won't be effective in the long term if data security and protection are not sufficiently strong. Therefore, it is a challenge for any IoT producer to add adequate security measures to every stage of the development process and equipment operation. To maintain confidentiality, integrity, and availability, it is crucial to provide a framework for realizing and analyzing security risks within IoT.

REFERENCES

1. Marc Langheinrich, "The Internet of Thugs?", IEEE Pervasive Computing, vol.20, no.3, pp.4-6, 2021.

2. Hasna Uddin, Marcia Gibson, Ghazanfar Ali Safdar, Tahera Kalsoom, Naeem Ramzan, Masood Ur-Rehman, Muhammad Ali Imran, "IoT for 5G/B5G Applications in Smart Homes, Smart Cities, Wearables and Connected Cars", 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), pp.1-5, 2019.

3. Rodrigo Román-Castro, Javier López, Stefanos Gritzalis, "Evolution and Trends in IoT Security", Computer, vol.51, no.7, pp.16-25, 2018.

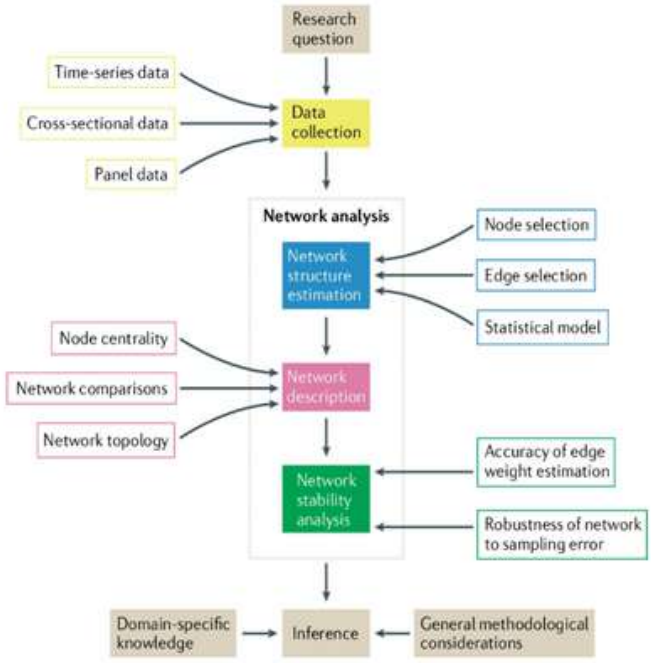
STUDENT ARTICLE

DATA ANALYTICS IN NETWORK

Ms.M.SAKTHI MAHESWARI, 3rd Year ECE

Communication networks allow the exchange of information between interconnected devices. Data analytic allows us to examine and analyze data sets to get meaningful information from them. Combining these two domains, the information which is shared can be analyzed and results can be obtained.

Advanced computational techniques and tools are used to analyze the data generated by the communication systems. An organization's use of the network and the network's performance can be better understood with the help of network analytic. The combination of data analytic and computer networks provide various applications such as mitigation of security threats like network intrusions and data breaches, providing better user experience (by designing more effective services which will meet their need as per the data obtained), analyzing network traffic, and analyzing user behavior.



Network Data Analysts are those who work combined in both fields. Their role is to examine the data from communication networks to find the best solutions to boost the network performance, address network problems and enhance overall network efficacy. Overall, data analytic in communication networks has revolutionized the way we communicate, and do business. As the volume and complexity of data continue to grow, professionals who can effectively analyze and optimize communication networks will remain in high demand across a range of industries.

EVENTS CONDUCTED

- The Department of Electronics and Communication Engineering in collaboration with the ECE Alumni Association had successfully organized “HACKELITE” a 24-hour inter-department hackathon on 06/03/2023 and 07/03/2023. The Hackelite had problem statements on themes such as Smart Education, Smart Transportation, Disaster Management, and Automation.

Hackelite Inauguration

- ECEA, IETE-SF & RAIC organized a Guest Lecture on VLSI by Dr.K.Saravanan, Design Engineer, Cerium Systems, Bangalore on 7th March 2023 for III Year ECE students.

Dr. K. Saravanan

- ECEA, IETE-SF & RAIC organized a Guest Lecture on Medical Electronics by Mr.Srinivasa Raja, Lead Engineer (Test and QA), R & D, Phoenix Medical Systems P(Ltd), Chennai on 7th March 2023 for II Year ECE students.

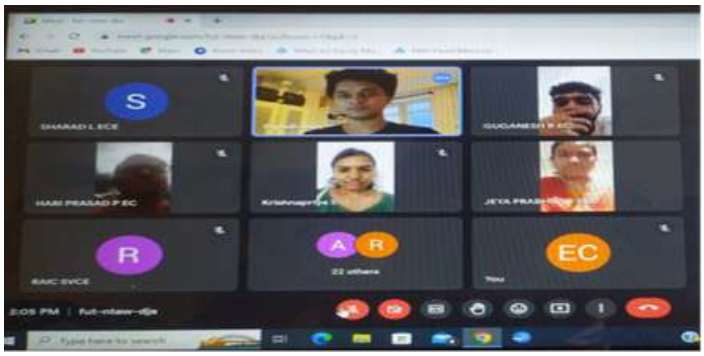
Mr.Srinivasa Raja

- ECE Department in association with SVCE Science Club organized a “ONE DAY WORKSHOP ON HAM RADIO-INTRODUCTION CUM DEMONSTRATION” on 17.03.2023 for 200 SVCE students and 15 SVCE faculties.

CHIEF GUESTS AND CONVENORS OF THE WORKSHOP

DEMONSTRATION OF HAM-RADIO

- RAIC organized a Guest Lecture on Artificial Intelligence by Mr. M. Piyush, Machine Learning Engineer, 6sense Innovations Ltd., Helsinki, Southern Finland, Finland on 19.03.2023 for 40 RAIC students.



Screenshot of Guest lecture

- The Department of ECE inaugurated the FODSE club for the year 2023 on 20th March 2023 with an invited talk on ML by Shri. Srinivasan Thanukrishnan, CTO & Director, Glosys Technology Solutions Pvt. Ltd to 250 students of ECE, IT, EEE, and CSE. Dr.S.Muthukumar, HOD-ECE Dr.V.Vidhya, HOD-INT, Dr.T.J.Jeyaprabha, and Shri. Srinivasan Thanukrishnan, CTO & Director, Glosys Technology Solutions Pvt. Ltd were the dignitaries on the dais.

- The MAKE-A-THON 4.0 intercollegiate Technical was organized by the Electronics and Communication Engineers Association (ECEA) in association with the Institution of Electronics and Telecommunication Engineers- Chennai Centre (IETE) and Robotics and Artificial Intelligence Club (RAIC) from 31.03.2023 to 01.04.2023. The chief guest for the inaugural function was Dr. D.Vijendra Babu, Honorary Secretary, IETE Chennai Centre; Dr.Venmathi A R, Professor & Head Department, Biomedical Engineering, Kings Engineering College; Mr.Vishnusai, MS in Software Systems Development, Tufts University. Dr.S.Muthukumar, Head of the Department, ECE addressed the crowd and appreciated all the participants and organizers for their fervent efforts for the event. Dr.D.Vijendra Babu addressed the crowd, spoke about the importance of having a vision, and prompted them to think and build products that would benefit society. The Make-a-thon 4.0 began at 10.00 AM shortly after the inauguration. Food and refreshments were provided for the participants. The event had 3 rounds of judging done by experts, faculties, and alumni from various industries. The chief guest for the valedictory function was Dr.Ashwin, MothersonTechnology, and Dr.Arun, Assistant Professor in ECE, Panimalar Institute of Technology. The winners were awarded cash prizes and internship opportunities were provided for the best performers.

Inauguration of Make - a - thon 4.0

ACHIEVEMENTS

BY FACULTY

- Mr.K.Ragupathi acted as a jury member in the “Paper Presentation Contest” in AGNIESZKA 2K23 National Level Technical Symposium organized by the Department of Electronics and Communication Engineering, Velammal Institute of Technology, Panchetti, Chennai on 04.03.2023.

- Dr.D.Menaka acted as a mentor for 2 batches of students in “HACKELITE” a 24-hour inter-department hackathon organized by the ECE department, SVCE on 06.03.2023 to 07.03.2023

- Mrs.L.Anju acted as a mentor for 4 batches of students in “HACKELITE” a 24-hour inter-department hackathon organized by the ECE department, SVCE on 06.03.2023 to 07.03.2023 and 2 batches got first prize in the event.

- Mr.P.Arul and Dr.A.Prasanth acted as Judges in “HACKELITE” 24 hours inter-department hackathon organized by the ECE department, SVCE on 06.03.2023 to 07.03.2023

- Mr.L.K.Balaji Vignesh received a digital credential for the course “Introduction to IoT” verified by Cisco Networking Academy on 14.03.2023

- Dr.T.J.Jeyaprabha acted as a mentor for a batch of students and won II Prize in “HACKELITE” a 24 hours inter-department Hackathon organized by the ECE Department, SVCE from 06.03.2023 to 07.03.2023

- Dr.T.J.Jeyaprabha acted as a Judge and Valedictory Guest for Compete to Compute Club Activity “Challenge N Build” organized by the Department of CSE on 21.03.2023

- Mr.L.K.Balaji Vignesh acted as a mentor for three batches of students in “SVCE Innovates 2023-Students Research Day” organized by Sri Venkateswara College of Engineering, Sriperumbudur on 30.03.2023

- Mrs. L. Anju acted as a mentor for 2 batches of students in Make-a-thon 4.0 organized by the ECE department, SVCE from 31.03.2023 to 01.04.2023 and 1 batch was awarded a special mention prize with internships.

- Dr.P.Jothilakshmi, Dr.R.Gayathri, Dr.S.R.Malathi, Dr.M.Bindhu, Dr. D.Menaka, Ms.K.S.Subhashini, Mr.S.Senthilrajan, Ms.R.Kousalya, Mrs.L.Anju, Ms.B.Sarala, Mr.P.Muthukumaran, Ms.C.GomatheeswariPreethika, Mr.P.Arul, Dr.A.Prasanth, Mr.L.K.Balaji Vignesh acted as Juries in the 24 hours inter-collegiate Make-a-thon 4.0 organized by the Department of ECE, SVCE in association with IETE Chennai Center from 31.03.2023 to 01.04.2023

- Mr. L.K. Balaji Vignesh reviewed three papers at IEEE International Conference on Data Science and Network Security (ICDSNS) in association with the IEEE Bangalore Section organized by Kalpataru Institute of Technology, Tiptur.

- Mr.L.K.Balaji Vignesh reviewed four papers at the International Conference on Applied Intelligence and Sustainable Computing (ICAISC-2023) in association with IEEE Bangalore Section organized by Shri Dharmasthala Manjunatheshwara College of Engineering and Technology, Dharwad.

BY UG STUDENTS

- Final Year Students Ms.Keerthana, Ms.Krishnapriya, and Mr.Maheeraj have won first place in the 24-hour Hackathon (with a cash award of Rs.30,000) conducted by PVP Siddhartha Institute of Technology, Vijayawada held during March 2023. They developed a web application under healthcare for virtual interaction with a medical robot.

THE HANS INDIA

CHENNAI TEAM BAGS FIRST PRIZE IN HACKATHON

HANS NEWS SERVICE
VIJAYAWADA (NTR DISTRICT)

THE Institute Innovation Council of PVP Siddhartha Institute of Technology, Vijayawada, organised 24 hour national-level Hackathon, CODEASTHRA-2023 at its campus in Kanuru, Vijayawada, for the first time. The total prize money worth more than Rs 2 lakh was given to the winning teams and other teams participated from across the country.

In all, 38 teams were scrutinised in the initial rounds held during March 2023. Out of which, a total of 14 teams were selected for the grand finale held on April 1 and 2. The participating teams gave solutions to various themes such as cyber security, medical and health, waste management, education and agricultural sectors. The students showcased skill in the area of applications such as IOT, AI&ML, Block Chain and Open Innovation.

While addressing the students during the event, Dr K Sivaji Babu, Principal of PVPSIT, said that the college has given special emphasis on innovation and held this hackathon to create an integrated platform among young minds from various parts of the country to solve societal problems.

Dr Jagadish Vengala, Convenor, IIC, informed the winning teams and Team 'Technocrats' from SVCE, Chennai, bagged first prize for the healthcare application and Teamstack from CBIT, Hyderabad, bagged second prize for the theme on online technology for education.

He said Team 'PCAS Hackers' from Patrician College of Arts and Science, Chennai, Tamil Nadu, bagged third prize for the theme of hand gesture recognition for differently abled people. The teams from Delhi, Bangalore, Chennai, Hyderabad and Visakhapatnam participated in the event.

The winners of national level Hackathon at Institute Innovation Council of PVP Siddhartha Institute of Technology, Vijayawada

- Third year students Keerthana D, Pooja V, and Nivetha won 3rd prize in the SVCE Innovates 2023.

- SARVESHWAR V bagged the “Regional Winner -State level” Title at the event sustainability hackathon challenge (round1) conducted by the Entrepreneurship development institute of India, Ahmedabad on 29/03/2023.

- Second year student Umesh Anandh won 3rd prize in the SVCE Innovates 2023.

- Our pre-final year students Mr.HARIHARAN G, Mr. HARSHAVARDHAN R (Team ID-1553) and Ms.SAHANA BALASUBRAMANIAM, Mr. RASWANTH U, Ms. AISWARYA SRINIVASAN, Mr. RAJA PANDI (Team ID-1681) won the prelims of Innovation Challenge 2023 event organized by IEEE in Panimalar Institute of Technology. Subsequently, they are shortlisted for finals in Egypt mentored by Dr.T.J.Jeyaprabha.

- Third year student V.S.Prithiviraj received a special mention in the Hardware category in Hackelite conducted by the ECE department in collaboration with ECE Alumni Association.

- Make a thon 4.0 Prize winners

First Prize
Team name: Smart Blink
Project: Hardware-based innovative method to improve delivery and learning outcomes for specially-abled children.
Team Members
1. Magesh S
2. Nithish Kumar B
3. Kiran Sekar
4. Robin Kumar
5. Priyadharshini S

- Special Mention- Internships

Team name: Team GT
Project: An IoT-based technological solution based on live CCTV feeds, that can automatically detect incidents related to street crime, violence, burglary, theft, infiltration, unauthorized access, etc., and generate alerts to the nearest police station
Team Members
1. Parvesh R
2. Ram Solaiappan A
3. Oviya Srinivasan
4. Pragatheeshwar S
5. Nawras Ahamed

The list of prize winners of "Hackelite" in the hardware and software category is as follows:

HACKELITE - HARDWARE CATEGORY - Winners		
Team Name	**Name of Students**	**Prize**
Team GT	R.Parvesh - II Year ECE	First
	A.Ram Solaippan - II year ECE	
	P.C.Dhanshrepriya - II Year ECE	
	N.Nawraz Ahamed - II Year EEE	
	S.Pragatheeswar - II Year IT	
	S.Stany Romero - II Year CS	
The Sixth Sense	Aiswarya Srinivasan - III Year ECE	Second
	Sahana .B - III Year ECE	
	Srivani .M - III Year ECE	
	Sivadharini .S - III Year ECE	
	Rajapandi.K - III Year ECE	
	Sanjay Lokesh .A.M - III Year ECE	
Rebooters	R.M.Manikandan - II Year ECE	Third
	Rahul .K - II Year ECE	
	Logeshwar.A - II Year ECE	
	Praveen.A.S - II Year ECE	

	Harini.G.V- II Year BioTech	
	Sai Sriraman.B- II Year CSE	

HACKELITE - SOFTWARE CATEGORY - Winners		
Team Name	Name of Students	Prize
Hextrabyte	Rajeshvar M Swamy - III Year ECE	First
	Revanth T R - III Year ECE	
	Sanmugam J - III Year ECE	
	Sudarshan C - III Year ECE	
	Supraja.R - III Year ECE	
	Vishnupriya .V.T - III Year ECE	
Cypher Assassins	Madhav B - II Year ECE	Second
	Mukesh.S - II Year ECE	
	Subash .V - II Year IT	
	Kiran Yadav .V - II Year ECE	
	Madhuvanthi.M.K - II Year ECE	
	Ram Sureth Kumar .S - II Year ECE	
	Nithish P - III Year ECE	
	Kaviarasu.C - III Year ECE	
Code Red	Mervin Jarel .D - III Year ECE	Third
	Maanasa.R - III Year ECE	
	Deepak Victor.A -III Year AI&DS	
	Kesavaran .V - III Year AI&DS	

FACULTY PARTICIPATION

- Dr. G. A. Sathish Kumar, Dr. D.Menaka, Mrs.L.Anju, and Mr.P.Arul attended a five-day international short-term training program on “Advanced Approaches and Insights on Artificial Intelligence and Deep Learning in Health Care” Organized by Department of ECE, Sri Venkateswara College of Engineering, Sriperumbudur from 27.03.2023 to 31.03.2023.

- Mr.R.Ramesh Kumar attended 6 days offline FDP on Tamils and Technology at CEG, Anna University from 20.03.2023 to 25.03.2023

- Mr.L.K.Balaji Vignesh attended five days online FDP on “Research Challenges and Issues on Antennas”, organized by Sathyabama Institute of Science and Technology, Chennai (IEEE Antennas and Propagation Society-Madras Section) from 27.02.2023 to 04.03.2023

- Mr.P.Arul, Mr.L.K.Balaji Vignesh attended one day FDP on “PALS VLAB Domain Specific Training”, organized by IITM PALS, Chennai on 02.03.2023

- Mr.P.Arul attended 2 days FDP On Fintech conducted by Imarticus Learning from 17.03.2023 to 18.03.2023

- Mr.L.K.Balaji Vignesh, Mr.D.Silambarasan attended five day online national level seminar on “Emerging Trends in Intelligent Computing”, organized by VIT-AP University, Amaravatifrom 14.03.2023 to 18.03.2023

- Mrs.S.M.Mehzabeen, Dr.M.Kavitha, Mr.K.Ragupathi, and Mr.P.Arul attended five-day online training program on “Research Data Management”, organized by VIT University, Vellore from 13.03 .2023 to 17.03.2023

- Mr. L.K. Balaji Vignesh completed Eight Week online course on Module 2-Professional Ethics & Sustainability conducted by NITTT, Chennai, and secured 70% on 25.03.2023.

- L.K.Balaji Vignesh completed Eight Week online course on Module 6-Student Assessment and Evaluation conducted by NITTT, Chennai, and secured 69% on 25.03.2023

- Kanagaluru Venkatesh has participated in a six-day national-level workshop on “Effective filling of NAAC AQAR - Streamlining Institutional Performance” held on 13th to 18th March 2023 conducted by Vardhaman College of Engineering, Hyderabad.

- Dr.S.Vijayanand has participated in six days national level workshop on “Effective filling of NAAC AQAR -Streamlining Institutional Performance” held on 13th to 18th march, 2023 conducted by Vardhaman College of Engineering, Hyderabad.

FACULTY PUBLICATION

- Dr.A.Prasanth has published an SCI paper titled “A hybrid ANFIS reptile optimization algorithm for energy-efficient inter-cluster routing in Internet of things-enabled wireless sensor networks” at Peer-to-Peer Networking and Applications (Springer), March 2023.

- Mr.L.K.Balaji Vignesh, Mr.D.Silambarasan presented a paper titled “Design of Field Programmable Gate Array based DSS Clock Generator” at the 2nd International Conference on Next Generation Computing Systems (ICNGCS-2023) at PSG Institute of Technology and Applied Research, Coimbatore from 17.03.2023 to 18.02.2023 (Online Mode)

- Mr.D.Silambarasan, Mr.L.K.Balaji Vignesh presented a paper titled “Real Time Monitoring Of Oxygen Saturation (Spo2) At Arteries Using Non Invasive Optical Sensor” in the 2nd International Conference on Next Generation Computing Systems (ICNGCS-2023) at PSG Institute of Technology and Applied Research, Coimbatore from 17.03.2023 to 18.02.2023 (Online Mode)

- Mr.L.K.Balaji Vignesh, R.Chandralekha, Dr.S.Vaira Prakash, K.Neerathilingam, V.Paranitharan, “Rectangular Microstrip Patch Array Antenna for Short Wave Radio Band Applications”, International Conference on Artificial Intelligence and Smart Energy (ICAIS 2023) and published in IEEE xplore (Scopus Indexed), DOI: 10.1109/ICAIS56108.2023.10073819

- Priyadharshini R, Geetha G, “Performance analysis of a heterogeneous network employing DAPSK based OFDMA-PON,” China Communications, vol. 20, no. 3, pp. 128-145, 2023. DOI: 10.23919/JCC.2023.03.010

EDITORIAL BOARD

CHIEF EDITOR

Dr.S.MUTHUKUMAR

HOD/ECE

CO-EDITORS

Dr. A. PRASANTH

ASSISTANT PROFESSOR, ECE

Mr. L.K. BALAJI VIGNESH

ASSISTANT PROFESSOR, ECE

STUDENT EDITORS

Mr. V.S.PRITHIVIRAJ - III Year ECE

Programme Offered By Department of Electronics and Communication Engineering

- B.E – Electronics and Communication Engineering
- M.E – Communication Systems
- Ph.D / MS (by Research)

Approved as a research center by Anna University, Chennai. (More than 48 Scholars doing their doctoral studies through our research center)

TOP RECRUITERS