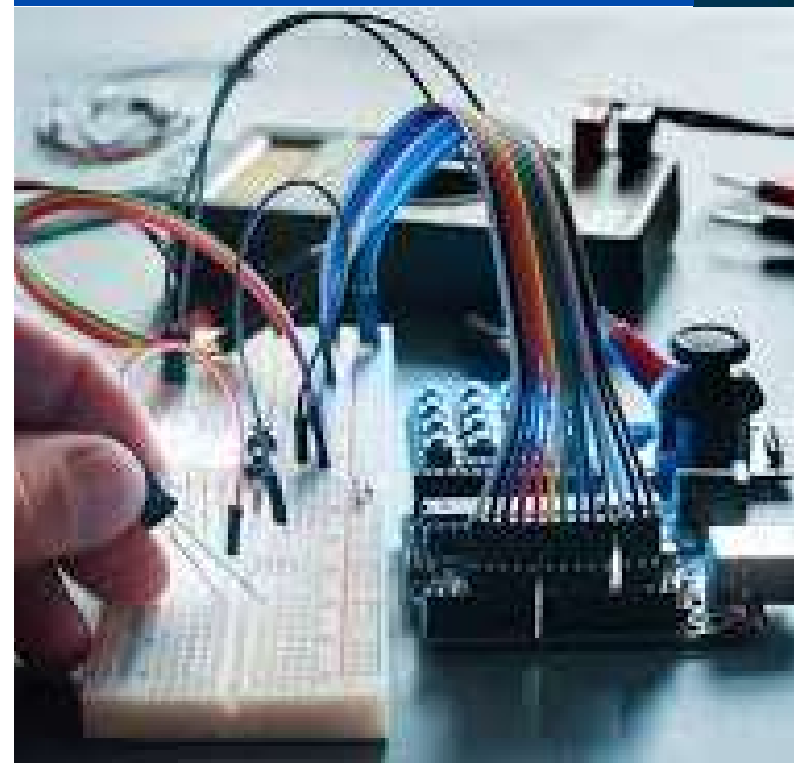
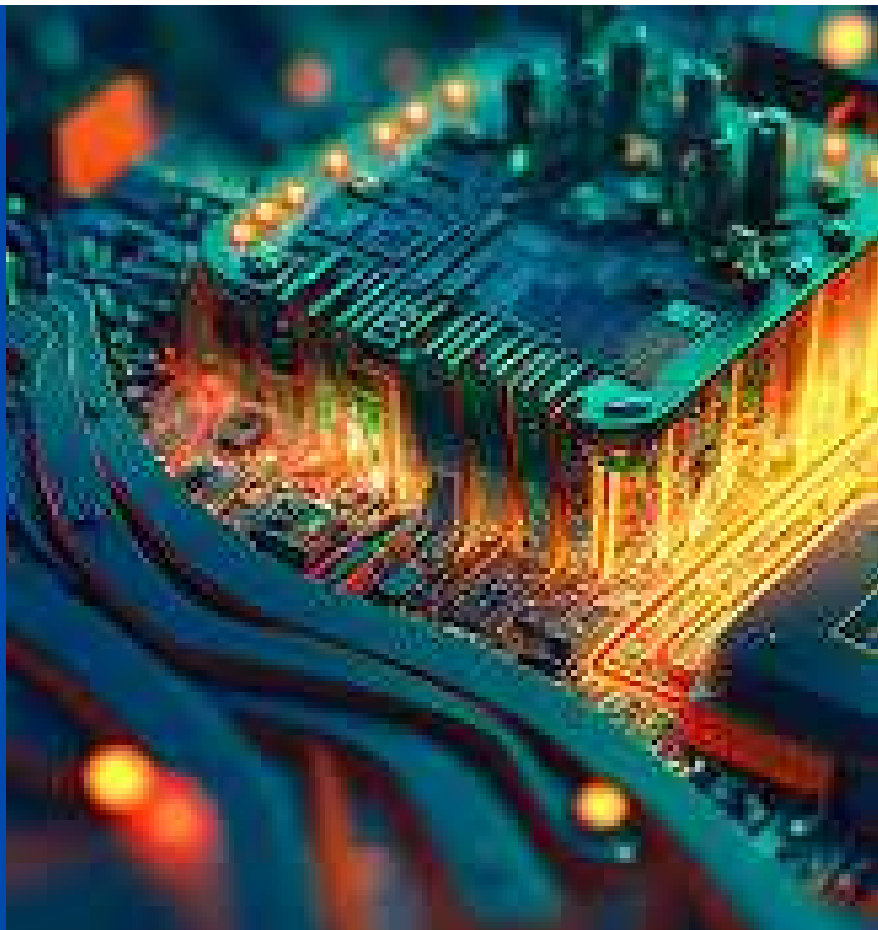


S V C E | Sri Venkateswara College of Engineering

CIRCUIT TIMES

INSIGHTS

- Faculty Article
- Faculty Participation
- Faculty Achievements
- Student Participation
- Student Achievements
- Academic Events
- PALS Activities
- Parents Teacher Meeting
- Alumni Activities
- Alumni Testimonial



VISION OF DEPARTMENT

To lead the future of Electronics and Communication Engineering, through developing accomplished people, transformative research, distinguished academics, developing break-through innovations and sustainable solutions to serve society at the national and global level.

MISSION OF DEPARTMENT

By fostering a culture of continuous learning and knowledge acquisition in electronics and communication engineering through rigorous academic programs, research opportunities, industry collaborations, with provision of necessary resources and support.

By nurturing an environment that empowers learners to progress and reach their full potential, contributing to the advancement of Electronics and Communication Engineering and prosper in their careers.

By contributing to society through innovative and sustainable engineering solutions to tackle national and global issues, thereby enhancing the quality of lives and communities.

FACULTY ARTICLE

CYBERSECURITY ADVANCES: NAVIGATING THE EVOLVING LANDSCAPE OF DIGITAL PROTECTION

Dr.S.Vijay Anand, M.E., Ph.D,

Associate Professor, Department of Electronics and Communication Engineering,
Sri Venkateswara College of Engineering (Autonomous), Sriperumbudur

ABSTRACT:

In the current cyber threat landscape, the level of complexity is increasing to the point that there is a need for ever more innovative digital security technologies. This extensive review delves into the latest developments in cybersecurity, featuring artificial intelligence-powered threat detection systems, zero-trust approaches in cybersecurity, quantum-resistant encryption techniques; new and exciting defensive methods emerging in the international cybersecurity landscape. With the growing dependence of organizations on digital infrastructures, it is imperative to grasp and apply these advancements to protect sensitive data and ensure operational integrity.

Keywords: Cybersecurity, Artificial Intelligence (AI), Zero-Trust Architecture, Threat Detection, Machine Learning, Quantum-Resistant Encryption, Homomorphic Encryption

1.INTRODUCTION

Cybersecurity, over the past several years, has also evolved from being a technical discipline, to one of global security importance, underscoring its importance to the very fabric and stability of national and economic security. With a growing dependence on digital infrastructure from cloud computing and Internet of Things (IoT) devices to critical infrastructure systems the need for strong cybersecurity has never been greater. This urgency is compounded by the increasingly vast and interconnected technological landscape, which while expanding efficiency and access also present systemic vulnerabilities and, in some cases, threats.

The digital landscape is a constantly evolving ecosystem that presents myriad opportunities, yet brings with it a multitude of sophisticated cyber threats. Attackers are constantly evolving and innovating, leveraging advanced persistent threats (APTs), ransomware attacks, phishing campaigns and insider threats.

2. ARTIFICIAL INTELLIGENCE IN THREAT DETECTION

2.1 Machine Learning-Powered Threat Intelligence

In the face of an ever-growing web of cyber threats that are becoming increasingly sophisticated and frequent, cutting-edge AI algorithms have proven to be vital weapons in bolstering cybersecurity defenses.

2.1.1 Advanced AI Algorithms for Threat Detection

These algorithms allow organizations to identify and react to threats in real time, enhancing their security fuselage overall. Here we explore three crucial spaces where AI fits and changes how we detect threats.

2.1.2 The Better Way of Identifying Anomalies

Real-time anomaly detection uses machine learning techniques to monitor network activity and user behavior on an ongoing basis. These algorithms can thus accurately detect any anomalies or variations from the norm, given a baseline of standard operations. For example, if a user does not download files after hours and starts downloading gigabytes of sensitive data late at night, the system can identify this action as unusual. With this feature, security teams can respond proactively to potential threats before they become major issues, such as by identifying and preventing data breaches or insider threats. In addition, as time progresses and machine learning models are trained on more datasets.

2.1.3 Predictive Threat Modelling

The reason is because predictive threat modelling is used to leverage historical data to identify potential patterns and trends that could imply potential vulnerabilities or attack vectors in the future. Using historical data of past breaches, organizations can model different attack scenarios where they can reflect on whether or not a particular threat can happen given vulnerabilities already present in their system.

By taking this proactive approach, organizations can shore up their defences prior to the occurrence of an attack. By leveraging such information, organizations can initiate department-specific phishing prevention programs if predictive models reveal a greater likelihood of attacks in a given department. Moreover, this modeling can guide resource allocation, so that cybersecurity economists can prioritize the most critical areas of vulnerability.

2.1.4 Self-Sufficient Counteraction Strategies

AI-Powered Systems in Autonomous Response systems automatically respond to detected threats, significantly reducing the time it takes to minimize potential damage. For instance, when a threat is detected—like an unauthorized access or a malware detection—the system can automatically quarantine compromised devices, block malicious IP addresses, or trigger predefined incident response protocols without human input.

Not only does this capability improve response times, but it also relieves the load from security teams to focus their attention on more strategic work that routine incident management. And, as they learn from past incidents, they can automate responses, adapting to new threats and ultimately making the entire organization more resilient. [1].

2.2 Intelligence Threat Predictive

Machine learning has garnered its relevance with the integration of it into cybersecurity. Here are some key capabilities that demonstrate the transformational impact of these nextgen technologies on predictive threat intelligence:

2.2.1 Detecting Potential Security Exploits

These machine learning models can analyze large volumes of code and system settings to detect security vulnerabilities that might otherwise be overlooked. Through static and dynamic analysis among others, these models are capable of identifying coding errors, misconfigurations, and outdated software components. Such a proactive approach to vulnerability management allows organizations to rectify vulnerabilities before they can be exploited by threat actors, thereby minimizing the effective attack surface.

2.2.2 Predicting Attack Vectors

Machine learning algorithms can analyse the historical data of cyber incidents to identify trends and patterns to comprehend where the next threats may come from. If an attack type is known to be effective against similar organizations, predictive models will indicate the probability of such an attack being attempted. By anticipating their targets, organizations can deploy resources accordingly, addressing likely points of attack and instigating more specific mitigations.

2.2.3 Building Proactive Defense Mechanisms

A predictive analysis helps you identify which areas you are most vulnerable to and how you can improve your strengths to redirect a future attack that may come. This can help organizations build security frameworks that include regular updates to security policies, employee education programs, and incident response plans. By using this proactive strategy, organizations can prevent risks from developing into threats while encouraging a culture of security awareness and resilience [2]

3. ZERO-TRUST ARCHITECTURE

3.1 Architectural Principles

Zero-trust security models are an epitome of the changing paradigm in how organizations are approaching Network Security and rigorous verification processes are unavoidable.

3.1.1 Removing Trusting by Default from the Network

This is because in a zero-trust model, trust is not granted based on the user's location, and thus requires authentication and verification regardless of their position on the network. All users and devices (unclear in/outside the network perimeter) must be verified before entering the resources. It reduces the threat of insider attacks and credential exposure.

3.1.2 Continuous Authentication Methods

Multi-factor authentication (MFA) and adaptive authentication can supplement the approach by ensuring users are verified throughout their sessions. Organizations can add an extra layer of security by implementing multi-factor authentication, which requires different forms of verification, including passwords, biometrics, or one-time codes, thereby improving their overall security posture and limiting the risk of credential theft.

3.1.3 Granular Access Control

The least privilege principle has become essential in a zero-trust architecture. This means, basically, users are granted only the access users need, based on their roles, to limit their capability to traverse the network as they desire. Organizations can mitigate the effects of compromised accounts by establishing role-based access controls (RBAC) and regularly reviewing access permissions.

3.1.4 Micro segmentation of network resources

It also improves security of internal segments by enabling to detect an anomalous activity within contained segments and makes it easy to respond to specific attack/benign activities.

3.1.5 Enforcement of dynamic access policy

Dynamic access policies are real-time-based access controls that adjust in response to the context of a user such as location, device health, and time of access. Monitoring of changes in user behavior provides information about when an activity is different and all of these elements help maintain operational compliance and risk management.

3.1.6 Techniques or Protocols for Continuous Verification

In a zero-trust world, user and device trust levels must be constantly reassessed. Organizations can adapt to evolving environments, new threats or behavior. Continuous verification protocols, ensuring that security is always proportionate to current risk [3].

4. ADVANCED ENCRYPTION TECHNOLOGIES

Quantum computing becomes more sophisticated, existing encryption techniques may become obsolete. New encryption techniques are being created to counter these threats.

4.1 Quantum Resistant Cryptographic Algorithms

Researchers are already developing post-quantum cryptographic algorithms that can withstand quantum computers. These algorithms use mathematical problems known to be hard for quantum algorithms to solve, ensuring that in the post-quantum world the data remains secure.

4.1.1 Lattice-Based Encryption Techniques

Rather, Lattice-based encryption is an advanced cryptographic approach that utilizes mathematical constructs called lattices to develop quantum-resistant cryptographic systems. This operation is becoming an increasing standard as a security against future quantum adversaries.

4.1.2 Quantum Key Distribution Technologies

Quantum key distribution (QKD) is a method based on the principles of quantum mechanics to securely distribute encryption keys. QKD guarantees that the interception of the key can be detected at the end of both parties [3], thus providing an additional layer of security.

4.2 Homomorphic Encryption

Homomorphic encryption is an exciting breakthrough in data security as it allows for computations on encrypted data to be carried out without needing to decrypt.

4.2.1 Privacy-Preserving Data Analysis

Regulations focusing on privacy and security are needed to govern how these two systems utilize sensitive data while ensuring no confidential information is leaking. Supervised learning could enable researchers to analyze patient-level data without compromising patient confidentiality, which also helps institutions comply with regulations like HIPAA.

4.2.2 Secure Cloud Computing

In cloud computing, homomorphic encryption is used to provide additional security for data by allowing cloud service providers to perform operations on the encrypted data without needing to decrypt it first. It ensures that sensitive data are protected even if they are processed in an insecure environment.

4.2.3 Confidential Machine Learning Applications

Homomorphic encryption enables the construction of machine learning models that can be trained on encrypted data. This technique maintains an individual's confidentiality throughout the machine learning process, enabling organizations to extract value from sensitive data without revealing it, and securing sensitive information from malicious outsiders [5].

5. EMERGING DEFENSE STRATEGIES

5.1 Threat Hunting and Proactive Security

Emerging techniques for the recognition of prospective security threats and their prevention are becoming more advanced.

5.1.1 Automated Threat Hunting Systems

Automated threat hunting systems are able to continuously monitor networks for potential threats using AI and machine learning. These systems sift through countless amounts of data and find anomalies, enabling security teams to attend to higher-level, more complicated concerns where human expertise is required.

5.1.2 Holistic Vulnerability Mapping

All possible vulnerabilities within an organization's infrastructure, to help prioritize remediation efforts. When visualizing vulnerabilities, it allows this to prioritize the most dangerous risks first.

5.1.3 Envisioned Security Intelligence

Data analytics helps in detecting trends and anticipating future threats, keeping organizations one step ahead of an attacker. Proactive measures like hardening infrastructures based on prediction from security intelligence can improve the overall security posture of the organization [6].

6. CONCLUSION

Artificial Intelligence, Architectural Approaches and newer encryption technologies are fundamentally changing the nature of Cyber Security. These developments are a definitive response to the evolving nature of fiercely challenging digital threat landscape. Taken together, AI, zero-trust principles, and advanced encryption technologies present a unique opportunity to build security and protection systems that are resilient, opportunistic and intelligent.

REFERENCES

- [1] M. Chen et al., "AI-Driven Cybersecurity: Adaptive Threat Detection Frameworks," *IEEE Transactions on Information Forensics and Security*, vol. 19, no. 2, pp. 345-362, Feb. 2024.
- [2] R. Kumar and S. Zhang, "Predictive Threat Intelligence Using Advanced Machine Learning Algorithms," *Journal of Cybersecurity Research*, vol. 47, no. 3, pp. 221-239, May 2024.
- [3] J. Rodriguez and L. Wang, "Zero-Trust Security Architectures: Comprehensive Design Principles," *IEEE Security & Privacy*, vol. 22, no. 4, pp. 56-73, Jul. 2024.
- [4] K. Nakamura et al., "Post-Quantum Cryptographic Frameworks," *Cryptography and Security Journal*, vol. 38, no. 1, pp. 102-119, Jan. 2024.
- [5] S. Patel and A. González, "Homomorphic Encryption: Advancements in Secure Computational Paradigms," *IEEE Transactions on Computers*, vol. 73, no. 5, pp. 678-695, May 2024.
- [6] L. Thompson et al., "Proactive Cybersecurity: Advanced Threat Hunting Methodologies," *International Journal of Information Security*, vol. 56, no. 2, pp. 201-220, Apr. 2024.

FACULTY PARTICIPATION

(SEMINAR/FDP/STTP/WORKSHOP/ONLINE COURSE/CONFERENCE)

- **Dr.D.Menaka and Mrs.L.Anju** attended three days short term training programme on the topic of “**Generative AI**” organized by Sri Venkateswara College of Engineering (Autonomous), Sriperumbudur from 11.11.2024 to 13.11.2024



- **Dr.D.Menaka and Mrs.L.Anju** attended one day seminar on the topic of “**Empowering Future Engineers for Space, Mobility, and Sustainability**” organized by **Mathworks** on 12.11.2024



- **C.Venkatesan, M.G.Sumithra, Mrs.B.Elakkiya & S.Saravanan** presented a paper titled “**CDR-CNN: Convolutional Neural Networks for Alzheimer’s Disease Severity Prediction with Clinical Dementia Rating**” during fifth IEEE International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI’24) organized by Kongunadu College of Engineering and Technology, Tamil Nadu (IEEE Xplore, doi: [10.1109/ICOSEC61587.2024.10722207](https://doi.org/10.1109/ICOSEC61587.2024.10722207))

FACULTY PARTICIPATION

(SEMINAR/FDP/STTP/WORKSHOP/ONLINE COURSE/CONFERENCE)

- **Dr.M.Bindhu** and **Mr.L.K.Balaji Vignesh** attended **Six Days AICTE Training and Learning (ATAL) Academy Faculty Development Program** on the topic of **“Next Generation Telecommunications-Advancements, Challenges and Future Prospects”** organized by Department of Electronics and Communication Engineering, **Madras Institute of Technology (Autonomous), Chennai** from 25.11.2024 to 30.11.2024



FACULTY ACHIEVEMENTS

- **Dr.P.Pattunnarajam** successfully completed the **NPTEL Online certification course** on “**Digital VLSI Testing**” and secured **Elite Certificate** during the academic year (July-November 2024)
- **Dr.G.Ayappan** successfully completed the **NPTEL Online certification course** on “**The joy of computing using Python**” and secured **Elite Certificate** during the academic year (July-October 2024)
- **Dr.S.Vidhayshree** successfully completed the **NPTEL Online certification course** on “**Electronic Systems Design: Hands-on Circuits and PCB Design with CAD Software**” and secured **Elite Certificate** in the NPTEL course during the academic year (July-November 2024)
- **Mrs.S.M.Mehzabeen** successfully completed the **NPTEL Online certification course** on “**Machine learning and deep learning fundamentals and applications**” during the academic year (July-October 2024)
- **Dr.T,J.Jeyaprabha** successfully completed the **NPTEL Online certification course** on “**Introduction to Industry 4.0 and Industrial Internet of Things**” during July-October 2024 (Awarded **Elite Silver** for being one among **Top 5% topper category**)
- **Mrs.L.Anju** successfully completed the **NPTEL Online certification course** on “**Electronic System Design: Hands-on Circuits and PCB Design with CAD Software**” during July-October 2024 (Awarded **Elite Silver** for being one among **Top 5% topper category**)

STUDENT PARTICIPATION

(Co-curricular Activities/Extra-curricular Activities)

- Around 169 Students (Second, Third and Final Year ECE) completed Online NPTEL Certification courses during July-November 2024. The courses (Introduction to Industry 4.0 and Industrial Internet of Things, Electronic Systems Design Hands-on Circuits and PCB Design with CAD Software, VLSI Design Flow: RTL to GDS, Introduction to Internet of Things and Optical Wireless Communications for Beyond 5G Networks and IoT) were completed by students.

Elite

NPTEL ONLINE CERTIFICATION
(Funded by the MoE, Govt. of India)

This certificate is awarded to
HARINI L
for successfully completing the course
VLSI Design Flow: RTL to GDS

with a consolidated score of **75** %

Online Assignments	22.81/25	Proctored Exam	51.75/75
--------------------	----------	----------------	----------

Total number of candidates certified in this course: 2041

Jul-Oct 2024
(12 week course)

Dr. Anand Srivastava
Coordinator
Continued Education Program, IITD

Prof. Andrew Thangaraj
NPTEL, Coordinator
IIT Madras

INDRAPRASTHA INSTITUTE OF INFORMATION TECHNOLOGY DELHI

swayam

Elite

NPTEL ONLINE CERTIFICATION
(Funded by the MoE, Govt. of India)

This certificate is awarded to
HARISH KANNAN D
for successfully completing the course
Introduction to Industry 4.0 and Industrial Internet of Things

with a consolidated score of **75** %

Online Assignments	25/25	Proctored Exam	49.5/75
--------------------	-------	----------------	---------

Total number of candidates certified in this course: 15725

Jul-Oct 2024
(12 week course)

Prof. Haimanti Banerji
Coordinator, NPTEL
IIT Kharagpur

Indian Institute of Technology Kharagpur

swayam

Elite

NPTEL ONLINE CERTIFICATION
(Funded by the MoE, Govt. of India)

This certificate is awarded to
AKASH VELAN R
for successfully completing the course
Electronic Systems Design: Hands-On Circuits and PCB Design with CAD Software

with a consolidated score of **83** %

Online Assignments	25/25	Proctored Exam	57.75/75
--------------------	-------	----------------	----------

Total number of candidates certified in this course: 1810

Jul-Oct 2024
(12 week course)

Prof. Andrew Thangaraj
Chair
Centre for Outreach and Digital Education, IITM

M. Vignesh
Prof. Vignesh Muthurajayan
NPTEL, Coordinator
IIT Madras

TOP
TOPPER
2%

Indian Institute of Technology Madras

swayam

STUDENT ACHIEVEMENTS

(Co-curricular Activities/Extra-curricular Activities)

- **Mr. S. Adarsh, Ms. V. Agnes Rose and Mr. F. Jakyim Jonan (III Year ECE)** participated in **Project Presentation (SYNSARA'24)** organized by Department of Computer Science and Engineering, Sri Sairam Engineering College (Autonomous), Chennai from 07.11.2024 to 08.11.2024



- **Mr.M.J.Sharva Jayan and Mr.M.Vikneshwaran (II Year ECE)** participated in the event of **Dream Design Compete win (DRESTEIN' 24)** and secured **second prize (Cash Award Rs.1500)** organized by Saveetha Engineering College (Autonomous), Chennai from 08.11.2024 to 09.11.2024



- **Mr.P.G.Sam Shashikiran, Mr.P.Sudharsan and Mr. S.Vishnoopriyen (II Year ECE)** participated in the event of **Dream Design Compete win (DRESTEIN' 24)** and secured **third prize (Cash Award Rs.1000)** organized by Saveetha Engineering College (Autonomous), Chennai from 08.11.2024 to 09.11.2024



STUDENT ACHIEVEMENTS

(Co-curricular Activities/Extra-curricular Activities)

- Mr.R.S.Aditya Vardan and Ms.B.Amruthaa (III Year ECE) participated in the event of “Hack Hustle Hackathon” and secured runner-up (Cash Award Rs.15000) organized by Saveetha Engineering College (Autonomous), Chennai from 08.11.2024 to 09.11.2024



- Mr.P.Chidhambaram (II Year ECE) participated in the event of “Brainy Bowl” and secured Cash Award-Rs.1500 organized by Saveetha Engineering College (Autonomous), Chennai from 08.11.2024 to 09.11.2024

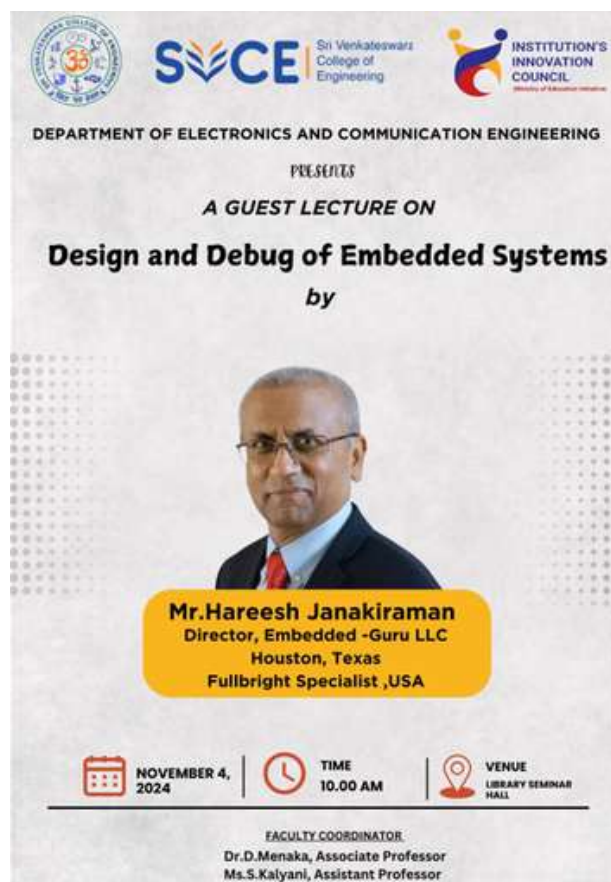


- Mr.M.Santhosh Karthick (I Year ECE) participated in the event of “Engima” and secured second prize (Cash Award Rs.300) organized by Sri Venkateswara College of Engineering (Autonomous), Sriperumbudur on 09.11.2024



EVENTS ORGANIZED

- The Department of Electronics and Communication Engineering organized a guest lecture program on the topic of “Design and Debug of Embedded Systems” on 04.11.2024. The session was handled by Mr.Hareesh Janakiraman, Director, Embedded Guru-LLC to pre-final year students. Dr.D.Menaka and Mrs.S.Kalyani coordinated the event. It aimed to provide students with an in-depth understanding of embedded systems, focusing on their design and debugging processes. The session emphasized the continued relevance of analog circuits, the practical applications of embedded systems, and the importance of critical thinking and innovation. Through interactive discussions, the speaker highlighted the growing significance of embedded systems in contemporary technology and their vast applications across industries. The session was highly engaging, providing students and faculty with a practical understanding of how these technologies shape industries today.



The poster features the logos of SVCE (Sri Venkateswara College of Engineering) and the Institution's Innovation Council. It is presented by the Department of Electronics and Communication Engineering. The main title is "A GUEST LECTURE ON Design and Debug of Embedded Systems" by Mr. Hareesh Janakiraman, Director of Embedded-Guru LLC in Houston, Texas, a Fullbright Specialist in the USA. The event is scheduled for November 4, 2024, at 10:00 AM in the Library Seminar Hall. Faculty coordinators are Dr. D. Menaka and Ms. S. Kalyani.



PALS ACTIVITIES

- Ms.B.Subhasri (III Year ECE) attended the “IIT Residential Student Workshop” organized by PALS from 28.11.2024 to 30.11.2024.

PARENTS-TEACHER MEETING

- The Department of Electronics and Communication Engineering organized parent-teacher meeting for first year students (2024 Batch) held on 23.11.2024. Parents were warmly received by the faculty. Detailed feedback regarding their ward's performance in the First Assessment Test (FAT) and attendance records was shared.
- Dr.G.A.Sathish Kumar, HoD/ECE delivered keynote session and emphasized the importance of skill enhancement programs such as the Study Abroad and Study-Industry initiatives. These programs aim to prepare students for global and industry-specific challenges. Additionally, the HoD highlighted the recent changes in the college's Vision and Mission.
- Parents acknowledged the department's initiatives to track and improve student's performance. Their appreciation and queries related to academic support, extracurricular development and career guidance were addressed by the faculty. Finally on a positive note, with parents expressing their gratitude for the department's dedication to their ward's success.



ALUMNI ACTIVITIES

- **Dr.D.Menaka, Head Alumni Relations, Executive member, SVCEAA** co-hosted the **ProConnect series** by the SVCE Alumni Association Sri Venkateswara College of Engineering (AASVCE) at College campus. **Mr.Sidharth Sivasailam, Head of Product Strategy & Management [Corporate Incubation], TCS** delivered a guest lecture as a part of the **“Pro-Connect”** series on **“Gearing up and navigating the complexities of an AI-driven future”** on 04.11.2024. This session was invaluable for transforming academic knowledge into practical skills and equipping students to succeed in today’s dynamic AI-driven environment.



ALUMNI TESTIMONIAL



**Mr.Srinivas Ramachandran,
Senior System Software Engineer,
Nvidia Corporation, USA**

“Mother, Mother tongue, Motherland and Alma Mater-I believe that these are the four pillars that shape one's life, the four pillars that one ought not forget about in their lifetime-and I am grateful to God for blessing me with the best in all of them. SVCE is one of the best among engineering colleges affiliated to Anna University, Chennai. I can recollect the joyful evening when I attended the Anna university counseling and I had no second thoughts in choosing SVCE for pursuing my B.E degree program. The vast infrastructure, excellent lab facilities, highly qualified faculty and equally talented, compassionate peers-are second to none”-**Mr.Srinivas Ramachandran, (Batch 2011-2015)**

PROGRAM OUTCOMES

PO1: Engineering Knowledge: Engineering Knowledge: Apply the knowledge of mathematics, science, engineering fundamentals and an engineering specialization to the solution of complex engineering problems.

PO2: Problem Analysis: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

PO3: Design / Development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

PO4: Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

PROGRAM OUTCOMES

PO5: Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

PO6: The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

PO7: Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

PO8: Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

PO9: Individual and team work: Function effectively as an individual and as a member or leader in diverse teams, and in multidisciplinary settings.

PROGRAM OUTCOMES

PO10: Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

PO11: Project management and finance: Demonstrate knowledge and understanding of the engineering management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

PO12: Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and lifelong learning in the broadest context of technological change

PROGRAM EDUCATIONAL OBJECTIVES

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

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.

PROGRAM OFFERED BY THE DEPARTMENT

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

EDITORIAL BOARD

CHIEF EDITOR

Dr.G.A.Sathish Kumar

Professor & Head

Department of ECE

CO-EDITORS

Mr.L.K.Balaji Vignesh

Assistant Professor/ECE

Dr.G.Ayappan

Assistant Professor/ECE



ELECTRONICS AND COMMUNICATION ENGINEERING

ABOUT THE DEPARTMENT

The Department of ECE was started in the year 1985 and is presently accredited by the NBA. The postgraduate program (M.E) in Communication Systems was started in 2002. There are about 38 faculty members in the department and 14 of them are doctorates. The department is well equipped with lab facilities and software tools like IE3D, ADS, CST Studio, Lab View, Tanner Tools, Cadence, MATLAB, and Prototype Machine.



SALIENT FEATURES OF ECE

- The Program has been accredited by the NBA since April 2002.
- Recognized by Anna University, Chennai as an approved research centre for Ph.D. and MS (by Research) with effect from May 2009.
- The major thrust areas of research are RF and Microwave Engineering, Wireless Networks, Network Security, VLSI, Cognitive Radio, Image & Signal Processing, Neural Networks & Soft Computing, Embedded Systems & IoT, Machine Learning, Nano Technology, Robotics, and Artificial Intelligence.
- The department is doing a good number of consultancy work in the field of PCB Prototyping and RF measurements using a Network Analyzer.
- On average over 75 companies visit our department for campus placements External Research grant of Rs 48.26 Lakhs received from ISRO and Cognizant Technology Solutions in the last five years for carrying out various projects.
- Students actively participate in research projects related to Wireless Communications, Networking, Embedded Systems & IoT, Virtual Reality, Robotics, Drones etc.
- Student Counselling Service at SVCE is committed one to promote the mental health and well-being of our students by providing accessible, quality mental health services.
- Student counsellors are available on campus for confidential counselling to all students.
- The department has signed over 12 MOUs with reputed companies to ensure the Industry Institute Interaction.
- Training programs are being conducted to enhance the employability skills of the students and also to achieve good placement in various Industries.

MESSAGE FROM HoD's DESK

The Department of ECE consistently does a commendable job in disseminating the latest knowledge and inviting specialists from diverse domains for discussions on the most recent advancement and trends besides conducting regular classes. We hope every student who visits our department has an engaging, motivating and positive experience. We consistently strive to ensure that instructors and other staff personnel possess the necessary abilities and knowledge to stimulate their students' intellectual curiosity, creativity and critical thinking. I hope you enjoy your time here and thoroughly use our amenities for promising career development



Dr. G.A. SATHISH KUMAR HoD/ECE

VISIT WWW.SVCE.AC.IN

SCAN & APPLY

Contact US

Sri Venkateswara College of Engineering
Post Bag No.1
Pennalur Village
Chennai - Bengaluru Highways
Sriperumbudur (off Chennai) Tk. - 602 117
Tamil Nadu, India



+91-44-27152000



admissionenquiry@svce.ac.in



CHOOSING SVCE: A PATHWAY TO SUCCESS AND GROWTH

- One of the prestigious and top ranked Autonomous engineering institution affiliated to Anna University, Chennai.
- Accredited by NAAC and NBA.
- Over 28 % of the alumni work abroad.
- Highest placement offers of Rs.25 LPA and 20 LPA in PayPal and Amazon.
- Highly qualified faculty and staff with an average experience of over 20 years.
- World class Laboratories to foster innovation and research.
- Alumni working in fortune 500 companies like Google, Microsoft, Facebook, Mercedes Benz, INTEL, etc.,
- State-of-the-art-campus with modern amenities in the industrial corridor of Chennai.

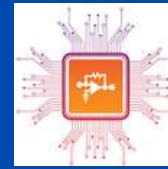


A Bachelor's Degree in Electronics and Communication Engineering with expertise in one of the following specialization

HONOURS SPECIALIZATION



Wireless Communication Systems



VLSI



Antenna and Microwave Technology



Signal Processing and Data Science



IoT Systems and Networking and Security its Applications



Our Recruiting Companies



MINORS



Artificial Intelligence and Machine Learning and Machine Learning



Data Science and Analytics



Robotics



Semiconductors



Advanced Communications



Bio-medical Signal Processing

Top Universities where our students are pursuing Higher Education



And Many More....



DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

ADMISSIONS OPEN FOR THE ACADEMIC YEAR 2024-25

SVCE started the Department of Electronics and Communication Engineering in the year 1985. The Department offers B.E. in Electronics and Communication Engineering and M.E. in Communication Systems. It is also approved as a Research Centre in Ph.D and MS (by Research) programmes by Anna University, Chennai.



ABOUT SVCE

Sri Venkateswara College of Engineering (Autonomous) is a premier self-financing institution started in the year 1985. The college offers 10 B.E/B.Tech Programmes and 10 M.E/M.Tech Programmes in Engineering and Technology. The Programs are approved by AICTE and the college is affiliated to Anna University, Chennai. The college is also accredited by National Assessment and Accreditation Council (NAAC). Many programs are accredited by National Board of Accreditation (NBA). The college is also certified by ISO 9001:2015. The institution received the autonomous status in the year 2016. Our Vision is to be a leader in Higher Technical Education and Research by providing state-of-the-art facilities to transform the learners into global contributors and achievers.

ADMISSION INFORMATION

A pass in a recognized Bachelor's degree or equivalent in the relevant field and should have obtained atleast 50% in the qualifying degree examination. Admissions are through Tamil Nadu Common Entrance Test (TANCET) conducted by Anna University or GATE

RESEARCH GRANTS

Our faculty members have received major external research grants from prestigious organizations such as ISRO, AICTE, DRDO, and TNSCST, etc., to the tune of ₹56.26 Lakhs in the last three years for doing various funded projects.

SCHOLARSHIPS FOR PG STUDENTS

- Tution fee (Rs. 50,000/year) waiver for 30% of the students of sanctioned class strength on merit basis, as applicable.
- Management Scholarship for tution fees and assistance for books and instruments.
- GATE Scholarship of Rs. 12,400 per month for students having valid GATE Score. Sponsorships for students to attend conferences.
- Intramural M.E/M.Tech Student Research Grant to carry out innovative projects.

RESEARCH AREAS

Join the Revolution: Transform Communication Systems with SVCE

- Biomedical Instrumentation
- Computer Networks & Network Security
- Digital Signal Processing & Image Processing
- Embedded Systems
- Fiber Optic Communication
- IoT (Internet of Things)
- Nano Electronics
- RF & Microwave Engineering
- Robotics & Artificial Intelligence
- VLSI & Microelectronics
- Wireless Communication Networks

MAJOR RECRUITERS

