

# Sakshin

Monthly Newsletter of Dept. of CSE

2026

SEPTEMBER

## VISION

Nurturing globally competent Computer science and Engineering graduates capable of taking challenges in the industry and Research & Development activities.

## MISSION

M1. Imparting quality education to meet the needs of industry, and to achieve excellence in teaching and learning.

M2. Inculcating value-based, socially committed professionalism for the development of society.

M3. Providing support to promote quality research.



## ABOUT ASIET

Adi Shankara Institute of Engineering & Technology in Kalady, established by the Adi Sankara Trust, aims to provide value-driven technical education that promotes professional excellence and ethical values. Under the blessings of the Jagadgurus of Sringeri Sharada Peetham, the trust has over 50 years of experience in managing educational institutions. The institute focuses on the holistic development of its students.

## S5 CSE Class Committee Meeting



The S5 CSE Class Committee meeting was held on 11 September 2026 at 1:30 PM in the NP Lab of Adi Shankara Institute of Engineering and Technology. The meeting was attended by the Head of the CSE Department, faculty members, and students. It provided an opportunity to discuss academic progress, students' feedback, and academic concerns.

# Certificate of Excellence in Peer-Reviewing



Dr. Suji Pramila R, of the Department of Computer Science and Engineering, Adi Shankara Institute of Engineering and Technology, Kalady, received the Certificate of Excellence in Peer-Reviewing from BP International in September 2026, in recognition of her outstanding contribution to maintaining the quality of academic books through peer-reviewing.



## ASIET Faculty Member Qualified UGC-NET



Ms. Ambily Mohan, Assistant Professor in the Department of Computer Science and Engineering at Adi Shankara Institute of Engineering and Technology (ASIET), successfully qualified the University Grants Commission National Eligibility Test (UGC-NET). This achievement reflected her dedication to academic excellence and professional development. ASIET congratulated her on this milestone and wished her continued success in her academic and professional journey.

## Certificate of Appreciation – ComNet 2026

Dr. Suji Pramila R of Adi Shankara Institute of Engineering and Technology, Kalady, received a Certificate of Appreciation for her valuable contributions as a reviewer at the International Conference on Communication Systems and Networks (ComNet 2026), organized by Mar Baselios College of Engineering and Technology (Autonomous), Thiruvananthapuram, in association with Universiti Teknologi Malaysia and technically co-sponsored by IEEE Kerala Section, from 16 to 18 September 2026.



## ASIET Faculty Member Serves as Reviewer at IEEE INDISCON 2026



Ms. Sharika T R, Assistant Professor of CSE department was presented with a Certificate of Appreciation for serving as a Reviewer for INDISCON 2026, the 7th IEEE India Council International Subsections Conference. The conference was organized by the IEEE Rajasthan Subsection and the IEEE India Council, and was held at Malaviya National Institute of Technology Jaipur from 11 to 13 September 2026.

The Organizing Committee acknowledged the valuable time, expertise, and diligent effort she contributed to the peer-review process, which helped maintain the quality of the research presented at the conference. The certificate was signed by Prof. Lava Bhargava, Chair, and Prof. Ranjan Kumar Mallik, TPC Chair, of INDISCON 2026.

The recognition reflected her academic contribution and commitment to the research community, and was celebrated as a proud moment for the department and the institution.

## Certificate of Excellence in Reviewing



Dr. Suji Pramila R, Professor in the Department of Computer Science and Engineering at Adi Shankara Institute of Engineering and Technology, Kalady, received the Certificate of Excellence in Reviewing from the Asian Journal of Advances in Agricultural Research in September 2026, in recognition of her outstanding contribution to maintaining the quality of the journal through peer-reviewing.



## Poster Design Challenge Winners



The ASIET ACM Student Chapter organized a Poster Design Challenge as part of the Independence Day celebrations under the theme “From Freedom to Innovation: India’s Tech Journey.” Vyshnavi P Vinod of S1 CSE-C secured first prize, while Madhav Surendran of S3 CSE-B won second prize. The participants showcased their creativity and innovative use of artificial intelligence to represent India’s technological journey. The event encouraged creative expression and highlighted the role of technology in shaping the nation’s future.

## CHATURA: Battle of the Grid – Sudoku Challenge Winners

The Mathematics Club of Adi Shankara Institute of Engineering and Technology (ASIET) organized CHATURA: Battle of the Grid, a five-round team Sudoku challenge that tested participants’ logical reasoning, problem-solving skills, and teamwork. Abhinav and Aman Sharaf of S1 CS DS secured first place, while Vismaya P V and Ziya Fathima K T of S3 CSE-C won second place. Arjun R and Salmanul Fariz C S of S1 ME secured third place. The competition encouraged analytical thinking, strategic planning, and collaboration among students while providing an engaging platform to showcase their mathematical abilities.



## ASIET Team Secures Second Prize and ₹1,00,000 at ILEAD 2026

A team from Adi Shankara Institute of Engineering and Technology secured the Second Prize and a cash reward of ₹1,00,000 at ILEAD 2026, hosted by LEAD College Autonomous. The team's performance reflected their dedication, innovative vision, and strong teamwork throughout the competition.

The team comprised Rohin Francis (S7 RA), Bashim Hadi (S7 CSE-B), Adinath C B (S7 EEE), Mohammed Rizwan Rafeek (S7 EBE), and Nandukrishna M (S7 CSE-DS). Their combined effort earned the institution a place among the top performers at the event.

The achievement was celebrated as a proud moment for the institution, with the team encouraged to continue aiming higher and achieving greater success.



## ASIET Chess Team Secures 2nd Runner-Up Position at D-Zone Inter-College Championship

The ASIET Chess Team secured the 2nd Runner-Up position at the D-Zone Inter-College Chess Championship 2026-27, held at RSET, Kochi. The team's performance reflected strong strategic play and dedicated preparation throughout the tournament.

A notable highlight of the championship was the achievement of Sarangi C., S5 CSE, who was crowned the Women's Individual Champion for the second consecutive

time. Her consistent performance added a special distinction to the institution's success at the event.

The achievement was celebrated as a proud moment for the institution, and the team was wished continued success in upcoming competitions.



## ASIET Students Secure Second Prize in "Echoes of Reason" Scientific Debate



Students of Adi Shankara Institute of Engineering and Technology secured the Second Prize in "Echoes of Reason: The Scientific Debate." The team comprised Neeraja Ragesh, Ram Madhav R Kammath, and Devikripa Udayakumar, who were recognised for their impressive performance in the competition.

Their well-reasoned arguments, confident delivery, and thoughtful engagement with the topic reflected the importance of scientific temper and critical thinking. The achievement was celebrated by the Science Club ASIET and the Internal Quality Assurance Cell (IQAC) as another proud moment for the institution.

## IEEE CS SBC ASIET Organizes "Cyber-Connect" Online Session on Cybersecurity



IEEE CS SBC ASIET organized "Cyber-Connect," an online session designed to connect academic learning with real-world opportunities in cybersecurity. The session was held on 30 September 2026 at 8:30 PM through Google Meet, with the theme "Shape Your Cybersecurity Journey with IEEE."

The resource person was Mr. Ruben Shibu, Offensive Services Consultant at Ultraviolet Cyber and Treasurer of IEEE ComSoc KC. The session introduced students to industry practices, emerging threats, and career pathways in cybersecurity, along with an overview of the opportunities available through the IEEE journey.

The programme encouraged students to explore the field of cybersecurity and take informed steps toward building careers in this rapidly growing domain.

## Sarangi Sajith Selected as IEEE Xtreme 20.0 Ambassador



Sarangi Sajith, Chairperson of the IEEE IAS Student Branch Chapter at Adi Shankara Institute of Engineering and Technology, was selected as an IEEE Xtreme 20.0 Ambassador. The announcement was made by IEEE SB ASIET, which extended its congratulations on this achievement.

As an ambassador, she will play an important role in promoting IEEE Xtreme and encouraging students to take part in the global competition, empowering the next generation of technologists. The selection reflects her leadership, commitment, and active involvement in IEEE activities at the institution.

The IEEE Student Branch wished her an impactful and rewarding tenure and expressed confidence in the contribution she will make in this esteemed role.

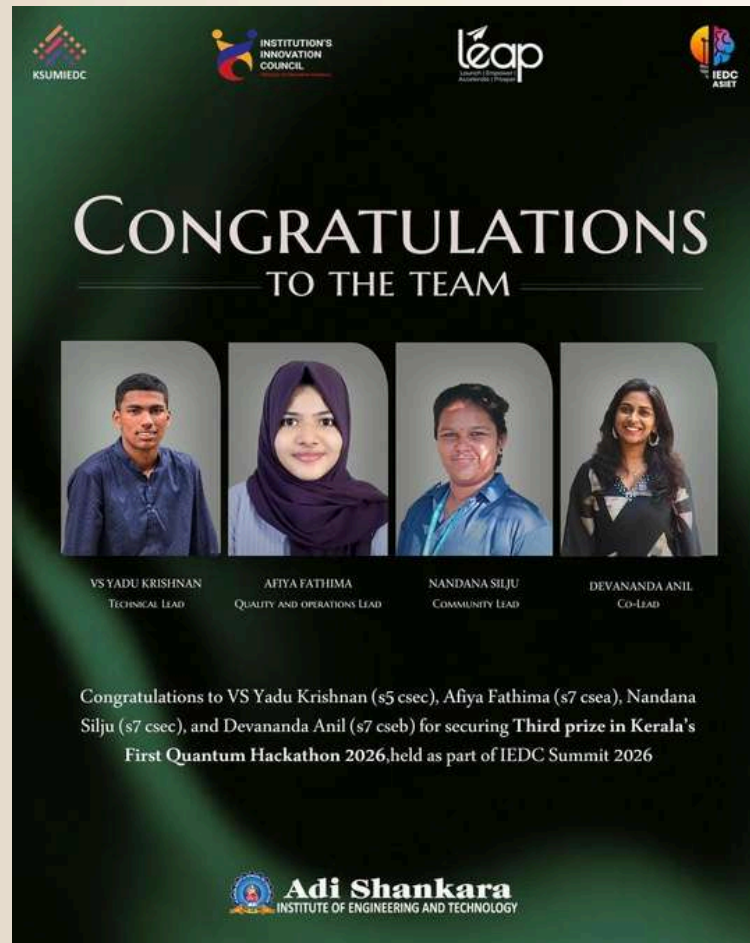
## IEDC ASIET Organizes 5 KM Run with Kerala Startup Mission



A 5 KM run was organized by IEDC ASIET in association with the Kerala Startup Mission, bringing together students and faculty in a show of fitness and community spirit. The run was flagged off by the Chief Operating Officer of the institution in the presence of the Sub Inspector of Police, Kalady.

The event aimed to promote health, teamwork, and active participation among the campus community, while reflecting the efforts of IEDC ASIET and the Kerala Startup Mission in encouraging an innovative and entrepreneurial culture among students. Participants took part with enthusiasm, and the event concluded successfully.

## ASIET Team Secures Third Prize in Kerala's First Quantum Hackathon 2026

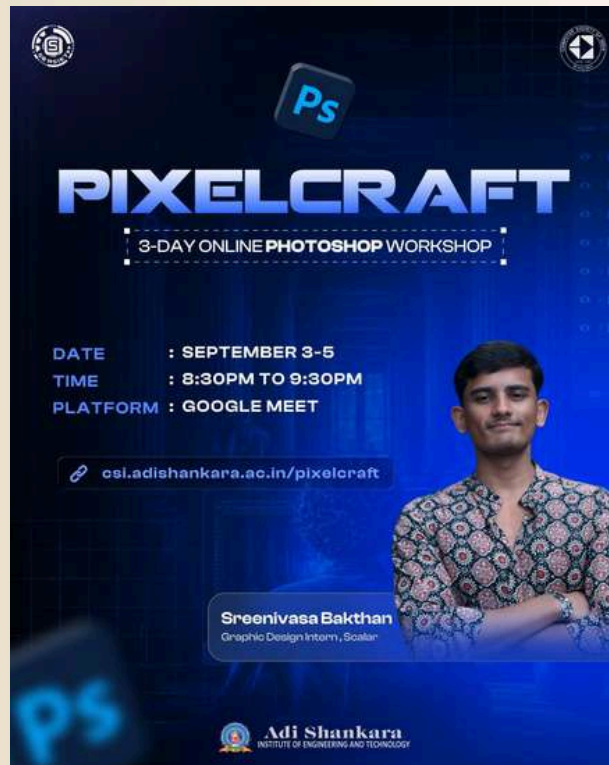


A team from Adi Shankara Institute of Engineering and Technology secured the Third Prize in Kerala's First Quantum Hackathon 2026, held as part of the IEDC Summit 2026. The achievement reflected the team's dedication, teamwork, and innovative thinking in tackling the challenges of this pioneering event.

The team comprised VS Yadu Krishnan (S5 CSE-C) as Technical Lead, Afiya Fathima (S7 CSE-A) as Quality and Operations Lead, Nandana Silju (S7 CSE-C) as Community Lead, and Devananda Anil (S7 CSE-B) as Co-Lead. Together, they demonstrated strong technical ability and collaboration in one of the state's first hackathons focused on quantum technologies.

The accomplishment was celebrated as another proud moment for the ASIET community, with the team wished continued success in their future endeavours.

## CSI SB ASIET Organizes "PixelCraft" Three-Day Online Photoshop Workshop

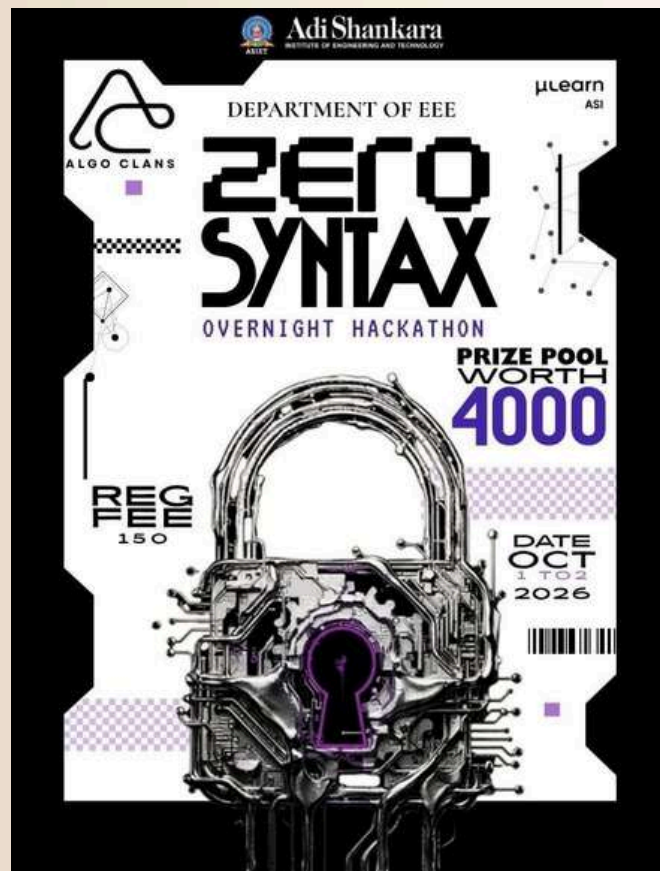


CSI SB ASIET organized "PixelCraft," a three-day online Photoshop workshop held from 3 to 5 September 2026 from 8:30 PM to 9:30 PM through Google Meet. The workshop aimed to introduce students to essential graphic design skills and help them turn creative ideas into professional visual designs.

The sessions were led by Sreenivasa Bakthan, Graphic Design Intern at Scaler and Chairperson of CSI SB ASIET. Participants received hands-on training in Photoshop fundamentals, layer management, masking, retouching, typography, and visual compositing, and took part actively in practical exercises and interactive Q&A sessions.

The workshop helped students strengthen their digital design skills and gain practical experience in creating professional layouts and compositions. It was coordinated by Hanna Nasrin and Andriya Mariya, with the support of the CSI SB ASIET core team.

## AlgoClans Organizes "ZeroSyntax" Overnight Hackathon



AlgoClans, the coding club of the Department of EEE at Adi Shankara Institute of Engineering and Technology, organized "ZeroSyntax," a 12-hour overnight VibeCoding Hackathon in association with MuLearn ASIET. The event was held from 5 PM on 1 October to 8 AM on 2 October 2026, bringing together student teams for a fast-paced coding challenge.

Participating in teams of two, students tackled real-world problems and turned their ideas into working prototypes using code and AI tools. The hackathon carried a prize pool of ₹4,000, with a registration fee of ₹150 per team, and encouraged participants to think smart, collaborate, and code fast.

The event offered students a platform to apply their technical skills, creativity, and teamwork in a competitive setting, reflecting the club's commitment to nurturing a strong coding culture on campus.

# Mastering GitHub: A Hands-on Workshop



MuLearn ASIET and the Department of Computer Applications jointly organized a hands-on workshop titled Mastering GitHub for MCA S1 students on 24 September 2026 at the ADP Lab, ASIET. The session was handled by Mr. R B Ravish, Tech Lead, MuLearn, and Mr. Krishnanunni H Pillai of the Cyber Security IG Team, MuLearn ASIET. The workshop covered essential Git and GitHub operations, including repository management, commits, pushing and pulling changes, branching, merging, stashing, and forking. Students worked in two-member teams and participated in a point-based challenge that encouraged practical learning, teamwork, and problem-solving. The session helped participants develop a foundational understanding of version control and collaborative software development.

# Cyber Safety: Securing Your Daily Digital Life



The ASIET ACM Student Chapter conducted a Cyber Security Awareness Session titled “Cyber Safety: Securing Your Daily Digital Life” for S1 CSE students on 8 September 2026, from 2:15 PM to 4:00 PM at the Main Seminar Hall. The session was led by five Kerala Police Academy-certified interns: Muhammed Nihal P A (ACM Web Team), Thobiyas M Babu (ACM Treasurer), Sana Fathima Salim (ACM Events Team), Nandana S Nair (ACM Membership Chair), and Sanjana Elizabeth K V (ACM Web Team). It covered cyber threats, phishing, online scams, privacy, account security, and safe digital practices, helping students strengthen their cybersecurity awareness and understand how to stay safe in the digital world.

## ASIET ACM Student Chapter Holds Annual General Meeting 2026



The ASIET ACM Student Chapter held its Annual General Meeting 2026 on 25 September at the Main Seminar Hall of Adi Shankara Institute of Engineering and Technology, under the theme "Reflect, Reconnect, Reimagine." The meeting marked the transition from the outgoing Executive Committee to the incoming team.

The programme included reflections on the previous term, the introduction of the new Executive Committee, distribution of certificates, and feedback from faculty members. The outgoing team also shared valuable insights from their experience, and a cake cutting was held to celebrate the occasion and express gratitude for their dedication.

The event concluded with appreciation for the outgoing and new Executive Committees, members, and all who contributed to its success. The AGM set the tone for a new chapter of learning, leadership, and growth for the chapter.

## Inauguration of the ASIET ACM-W Student Chapter Empowers Women in Computing



The ASIET ACM-W Student Chapter was inaugurated at Adi Shankara Institute of Engineering and Technology, marking the beginning of a community dedicated to empowering women to explore, learn, connect, and grow in the field of computing and technology. The inaugural ceremony was held with traditional lamp lighting and brought together students, faculty members, and distinguished guests to celebrate the start of this new journey.

The programme included an introduction to ACM-W, followed by an insightful session titled "AI in Action: Industry Tools and Practical Applications," delivered by Ms. Seethu PB, Databricks Architect at TCS Kochi. The session offered participants a practical understanding of how artificial intelligence is applied in industry and the tools used in real-world settings. The event concluded with a vote of thanks, acknowledging the collective efforts and support of everyone who contributed to its success.

With the chapter now established, the team aims to create opportunities that inspire learning, collaboration, leadership, and innovation, while encouraging more women to actively shape the future of technology. The inauguration reflected a shared vision of a future where women innovate, lead, and make a lasting impact in computing.

## ASIET ACM-W Expresses Gratitude to Guest Speaker Ms. Seethu P B



The ASIET ACM-W Chapter extended its sincere gratitude to Ms. Seethu P B, Databricks Architect at TCS Kochi, for being a part of the chapter's inauguration at Adi Shankara Institute of Engineering and Technology. She lit the traditional lamp along with the dignitaries and was felicitated with a memento in appreciation of her presence.

Her session, "AI in Action: Industry Tools and Practical Applications," gave students a deeper understanding of how artificial intelligence is shaping the industry and the practical tools and technologies in use today. Drawing on real-world perspectives and professional experience, she inspired students to explore, learn, and grow in the field of technology.

The chapter thanked her for sharing her time, expertise, and experience, and acknowledged her contribution to the successful beginning of the ASIET ACM-W journey.

## TinkerHub ASIET Hosts "Useless Projects 3.0" Overnight Event



TinkerHub ASIET organized "Useless Projects 3.0," an overnight creative event held in the AI Lab of Adi Shankara Institute of Engineering and Technology on 11 September 2026, under the theme "Because 'Why Not?' Is a Valid Reason." The event brought together a large gathering of curious students to build weird, pointless, and wonderfully unnecessary projects.

With no real problems to solve and no pressure to be practical, participants were free to tinker, experiment, learn, and create. The event encouraged a playful approach to technology, allowing students to explore ideas purely out of curiosity and strengthen their creativity, problem-solving, and collaboration skills along the way.

The programme concluded with a group gathering of participants and organizers, reflecting the enthusiastic spirit of the maker community on campus.

## Design2Hack 24-Hour Hackathon Winners Announced



The 24-hour hackathon held as part of Design2Hack, organized by the ASIET Design and Animation Club at Adi Shankara Institute of Engineering and Technology, concluded with the announcement of its winners. Participating teams worked through the day to develop creative design solutions, demonstrating teamwork, innovation, and the ability to perform under time pressure.

The First Prize was awarded to Team Nexus, comprising Shahana S and Rosemol Joshy of S5 CSE. The Second Prize was secured by Team Dsign, comprising Chethan Krishna K M and Arjun Krishna K M of S1 CSE.

The winners were recognised for their creativity and technical skill, and the achievement was celebrated as a proud moment for the club and the institution.

## Design2Hack Brings Together Creativity and Innovation Through UI/UX Workshop

The ASIET Design and Animation Club successfully conducted Design2Hack, a UI/UX design workshop followed by an engaging design challenge, at Adi Shankara Institute of Engineering and Technology. The event brought together students in a collaborative setting to learn, design, and build creative solutions.

Participants showcased impressive talent, innovative ideas, and strong teamwork throughout the programme. The workshop introduced them to the fundamentals of user interface and user experience design, while the challenge gave them the opportunity to apply their learning to real design problems. The event was concluded with appreciation for the participants, resource persons, coordinators, volunteers, and faculty members whose contributions made it a memorable and successful experience.



## Design and Animation Club Conducts "Pixel Bloom" Digital Pookalam Competition

The Design and Animation Club of Adi Shankara Institute of Engineering and Technology conducted "Pixel Bloom," a digital Pookalam designing competition that brought together students to showcase their creativity through digital art. The event offered participants a platform to blend the traditional floral carpet art of Onam with modern design tools.

Behanan Abin Varghese of S1 DS was awarded the First Prize, while Mathew Joseph T A of S7 CSE secured the Second Prize. The winners were presented with trophies in recognition of their creativity and artistic excellence, and the event was concluded successfully.



## Old Age Home Visit

NSS Units 303 and 228 conducted an old age home visit on 21 September 2026 as part of their community service activities. The volunteers interacted with the residents and spent meaningful time with them, promoting empathy, care, and respect for the elderly. A total of five students participated in the programme, including Niranjana N (CSC), Nijiya PJ (CSE C), and Nandhana Sabu (CSE C) from S3, and Neeraj N Kumar (CSE C) and Athulya Santhosh (CSE B) from S5. The visit provided an opportunity for students to engage with the elderly and reinforced the importance of compassion and social responsibility.



## NSS Volunteer Orientation Programme



A one-day orientation programme was organized for newly joined National Service Scheme (NSS) volunteers to introduce them to the values, objectives, and activities of NSS. The programme included sessions on the history, philosophy, and objectives of NSS, anti-drug awareness, and the university's flagship programmes. An HIV/AIDS awareness session was also conducted to educate volunteers on related issues and promote responsible attitudes.

The programme further featured a leadership training session led by Shri Brahma Nayakam Mahadevan, which aimed to develop leadership qualities, teamwork, and a sense of social responsibility among the volunteers.

## NSS ASIET Conducts Blood Donation Camp with 74 Donations



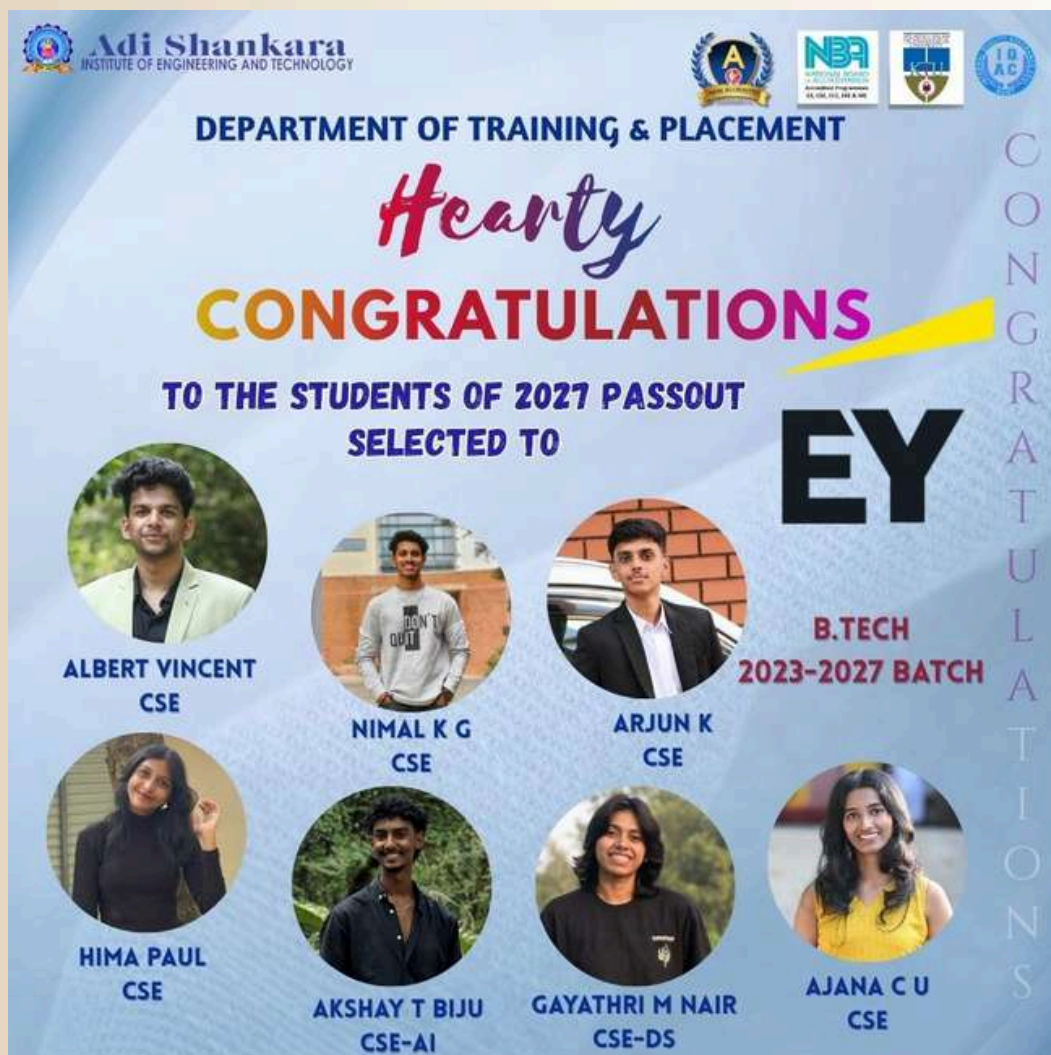
The National Service Scheme (NSS) unit of Adi Shankara Institute of Engineering and Technology conducted a blood donation camp in association with Amrita Hospital, with the Blood Mobile unit stationed on campus for the event. The camp was held alongside a free medical camp and brought together students, faculty members, and staff in support of a noble cause.

A total of 74 donations were recorded during the camp, with girls accounting for 45 percent of the donors. The enthusiastic participation of students reflected their sense of social responsibility and commitment to community service.

The NSS unit expressed its gratitude to all donors, volunteers, organizers, and the medical team for their support in making the camp a success.

## Placements: B.Tech Students Placed at EY

The Department of Training & Placement at Adi Shankara Institute of Engineering and Technology achieved a significant milestone as seven students from the 2023-2027 B.Tech batch secured placements at EY. The selected students from the Computer Science and Engineering streams included Albert Vincent (CSE), Nimal K G (CSE), Arjun K (CSE), Hima Paul (CSE), Akshay T Biju (CSE-AI), Gayathri M Nair (CSE-DS), and Ajana C U (CSE). This achievement reflected the students' technical dedication and the institution's commitment to delivering quality career opportunities, marking a proud moment for the entire campus community as these future graduates stepped forward into their professional careers.



# When Seeing Is No Longer Believing: Fighting Deepfakes with Explainable Artificial Intelligence

## Introduction

Imagine receiving a video call from your organization's director requesting an urgent financial transaction. The face looks familiar, the voice sounds genuine, and the conversation appears completely natural. However, the person on the screen is not your director but an AI-generated impersonation.

This scenario highlights one of the growing challenges of the digital era: **deepfake technology**. Deepfakes are artificially generated or manipulated images, audio recordings, and videos created using advanced Artificial Intelligence techniques. While these technologies have useful applications in entertainment, education, and digital media, their misuse can lead to financial fraud, identity theft, misinformation, and reputational damage.

As AI-generated content becomes increasingly realistic, distinguishing authentic media from manipulated content is becoming more difficult. This raises an important question: **Can Artificial Intelligence itself provide a solution to the problems created by Artificial Intelligence?**

One promising approach is the integration of **Deep Learning and Explainable Artificial Intelligence (XAI)** to develop intelligent systems capable of detecting suspicious media and explaining the reasons behind their predictions.

## The Problem: Can We Still Trust What We See?

Traditional methods of verifying digital content often depend on human observation, metadata analysis, and identifying visible inconsistencies. However, modern generative technologies, including Generative Adversarial Networks (GANs) and diffusion models, can produce highly realistic synthetic content.

Consider a manipulated video circulating on social media that appears to show a university official making a statement they never made. Such content can spread rapidly, potentially damaging reputations before its authenticity is verified.

Deepfake technology also creates serious concerns in cybersecurity, digital forensics, and financial transactions. A convincing synthetic voice may be used to impersonate an authorized person, while manipulated video evidence may complicate investigations.

The major challenge is that **human perception alone is no longer sufficient to establish the authenticity of digital media**. Therefore, automated systems are needed to identify possible manipulation and support reliable verification.

**The Proposed Solution: Deepfake Detection Using Explainable AI**

An innovative solution involves combining deep learning models with Explainable AI techniques to detect potentially manipulated content and provide interpretable evidence.

Deep learning models, such as Convolutional Neural Networks (CNNs) and Vision Transformers, can analyze digital images and videos to identify unusual patterns in facial textures, lighting, boundaries, and temporal consistency. However, these models often operate as black boxes, producing predictions without clearly explaining how the decisions were made.

Explainable AI addresses this limitation by helping users investigate the factors influencing a model's prediction. Techniques such as **Grad-CAM (Gradient-weighted Class Activation Mapping)** and **SHAP (SHapley Additive exPlanations)** can provide visual or feature-based explanations.

For example, when analyzing a suspicious video, the system may highlight facial regions that strongly influenced its prediction. These visual explanations help investigators examine model behavior, although they do not independently prove that manipulation occurred.

**Working of the Proposed System**

The proposed framework operates through the following stages:

1. **Media Input:** An image, audio recording, or video is submitted for verification.
2. **Preprocessing:** Video frames are extracted, facial regions are identified, and relevant features are prepared for analysis.
3. **Deepfake Detection:** A trained deep learning model analyzes the content and estimates the likelihood of manipulation.
4. **Explainability:** Grad-CAM or SHAP helps identify features that influenced the model's prediction.
5. **Authenticity Assessment:** The system combines detection results with available metadata and content provenance information.
6. **Report Generation:** An interpretable report presents the findings, uncertainty, and areas requiring further verification.

The proposed workflow can be summarized as:

**Digital Media → Preprocessing → Deep Learning Detection → Explainable AI → Authenticity Assessment → Verification Report**

This approach aims to move beyond simple *Real or Fake* classification toward a more transparent and evidence-supported verification process.

**Real-World Applications**

The integration of deepfake detection and Explainable AI can benefit several domains.

**Cybersecurity:** Detecting suspicious synthetic audio and video used in impersonation attacks and financial fraud.

**Digital Forensics:** Assisting investigators in examining potentially manipulated multimedia evidence.

**Journalism and Social Media:** Supporting fact-checking and verification of digital content before publication or redistribution.

**Education:** Helping institutions identify misleading announcements, fabricated recordings, and manipulated academic communications.

**Healthcare and Public Services:** Supporting the verification of digital communications where identity and information integrity are important.

These applications demonstrate how intelligent verification technologies can contribute to digital safety and public trust.

### **Challenges and Future Research Opportunities**

Despite its potential, deepfake detection faces several limitations. Rapid improvements in generative AI can make manipulated content increasingly difficult to identify. Detection models may also produce incorrect predictions or perform poorly on unfamiliar datasets.

Furthermore, explainability techniques do not guarantee that a model's decision is correct. Privacy concerns, dataset bias, and computational requirements must also be addressed.

For engineering researchers, this creates opportunities to develop lightweight detection models for mobile devices, multimodal systems combining audio and video analysis, and privacy-preserving approaches using Federated Learning.

Another promising direction is integrating detection models with digital content provenance technologies such as **C2PA (Coalition for Content Provenance and Authenticity)**, which supports verification of information about media origin and modification history.

Future systems could combine AI-based detection, provenance verification, and human expertise to establish more reliable digital trust mechanisms.

### **Conclusion**

Artificial Intelligence has transformed the creation and consumption of digital media. While generative technologies offer remarkable opportunities, their misuse through deepfakes presents significant challenges to authenticity, privacy, and security.

Combining Deep Learning with Explainable Artificial Intelligence offers a promising approach to identifying suspicious digital content while improving the transparency of automated decisions.

However, trustworthy verification requires more than a single AI prediction. It demands reliable models, interpretable evidence, content provenance, and responsible human oversight.

**In a world where seeing is no longer believing, the real technological challenge is not merely detecting what is fake, but developing intelligent systems that help society establish what can be trusted.**

Naznin M Ali  
Assistant Professor  
CSE Department



## HACKING THE HUMAN BODY

The next frontier of cybersecurity might be beneath your skin.

Your heart beats. A small electronic device beneath your skin helps keep its rhythm steady. You go about your day without thinking about it, trusting that the technology will do what it was designed to do.

But every piece of technology has a weakness worth asking about.

What if the device keeping your heart in rhythm had a software vulnerability? What if a flaw in a medical system put the treatment you depend on at risk?

It sounds like science fiction. It isn't.

Pacemakers help regulate heart rhythms. Insulin pumps deliver medication. Brain-computer interfaces are allowing researchers to translate brain activity into speech for people who have lost the ability to speak. Technology is no longer just something we carry. In some cases, it has become part of how our bodies function.

And that changes the stakes.

When the body becomes a target

In 2011, security researchers demonstrated vulnerabilities in insulin pumps, drawing attention to the cybersecurity risks of wireless medical devices. Their research highlighted a problem the medical world could no longer ignore: even a device designed to help a patient could have weaknesses in its digital systems.

This does not mean every medical implant can be remotely hijacked. The risks depend on the device, its design, and its security measures. But the lesson is clear: technology that interacts with the human body must be protected as carefully as it is engineered.

Medical-device cybersecurity is now an established field. Regulators such as the US Food and Drug Administration issue guidance on designing secure devices, managing software vulnerabilities, and protecting patients throughout a device's life cycle.

Because when a security failure involves a medical device, the consequences may extend beyond stolen information. They could affect the device's operation, the availability of treatment, or even a patient's safety.

From silicon chips to the human brain

The story doesn't end with pacemakers and insulin pumps.

Tiny chips implanted beneath the skin can already be used for tasks such as identification and access control. These are relatively simple devices, but they hint at a world in which technology becomes a more direct part of everyday life. Meanwhile, brain-computer interfaces are pushing the boundary much further. In 2026, researchers reported a brain-computer interface being used in a participant's home to translate brain activity into speech, offering a glimpse of how these systems might support communication beyond the laboratory.

These technologies are not interchangeable. A chip that unlocks a door is not a medical implant, and a brain-computer interface is not a machine that can freely read someone's mind. Each has different capabilities, limitations, and risks.

Yet they point toward the same question: as technology becomes more closely connected to our bodies, how do we protect that connection?

Who controls the software inside an implant? How should vulnerabilities be fixed when a patient depends on the device? And how do we protect sensitive biological data without compromising the technology that makes treatment possible?

The future is not something to fear

The answer isn't to reject these advances. Medical technology can restore movement, support essential bodily functions, and give people new ways to communicate. These are extraordinary achievements.

The challenge is to make these devices secure by design, maintain them responsibly, and ensure that patients remain protected as the technology evolves.

It might be beneath your skin.

## Sources

1. US Food and Drug Administration: Cybersecurity in Medical Devices
2. US Food and Drug Administration: Medical Device Cybersecurity: What You Need to Know
3. Black Hat: 2011 Security Conference Briefings
4. National Institutes of Health: Brain-computer device helps a man speak



-Tejas KM  
S3,CSE-C

## Post-Quantum Cryptography: Preparing for the Quantum Era

Technology is advancing at an unprecedented pace, and one of the most exciting developments in computing is the emergence of Quantum Computing. While traditional computers have transformed the digital world, quantum computers have the potential to solve certain complex problems in fundamentally different ways.

This advancement could bring major breakthroughs in fields such as medicine, artificial intelligence, scientific research, and optimization. However, it also creates a significant challenge for cybersecurity. Many of the cryptographic systems protecting our digital world today could become vulnerable to sufficiently powerful quantum computers.

As a Computer Science graduate exploring Post-Quantum Cryptography, I have become interested in how we can prepare today's digital systems for the security challenges of tomorrow.

### Understanding Quantum Computing

Traditional computers process information using bits represented as 0 or 1. Quantum computers use quantum bits, or qubits, which can make use of properties such as superposition and entanglement.

This allows quantum computers to approach certain computational problems differently from classical computers.

Quantum Computing has potential applications in:

Scientific Research

Drug Discovery

Artificial Intelligence

Optimization

Financial Modelling

Cryptography

Although large-scale quantum computers are still under development, their potential impact on cybersecurity is already an important area of research.

## The Quantum Threat

Modern digital security depends heavily on cryptography. Online banking, digital payments, secure websites, messaging applications, and government systems all rely on cryptographic algorithms to protect sensitive information.

Some widely used public-key cryptographic systems depend on mathematical problems that are extremely difficult for classical computers to solve.

However, quantum algorithms such as Shor's algorithm could potentially solve some of these problems much more efficiently with a sufficiently powerful quantum computer.

This could create risks for:

Secure Communication

Online Banking

Digital Payments

Government Systems

Digital Signatures

Cloud Infrastructure

Sensitive Data

There is also a concern known as "Harvest Now, Decrypt Later", where attackers collect encrypted information today with the possibility of decrypting it in the future when powerful quantum computers become available.

## What is Post-Quantum Cryptography?

Post-Quantum Cryptography, or PQC, focuses on developing cryptographic algorithms that are designed to remain secure against attacks from both classical and quantum computers.

Unlike Quantum Cryptography, which uses principles of quantum physics for secure communication, Post-Quantum Cryptography uses mathematical algorithms that can operate on existing computers and networks.

The goal is to develop security systems that can protect digital information even after practical quantum computers become available.

## Modern Post-Quantum Cryptography

Researchers around the world are developing and evaluating new cryptographic techniques to address the quantum threat.

Important areas of PQC include:

Key Encapsulation

Digital Signatures

Secure Key Exchange

Authentication

Encryption

Algorithms such as ML-KEM and ML-DSA are examples of modern post-quantum cryptographic standards designed to provide protection against future quantum attacks.

## Applications of Post-Quantum Cryptography

### Secure Communication

Messaging platforms and communication systems can use quantum-resistant cryptography to protect sensitive information over long periods.

### Financial Systems

Banks and financial institutions can adopt PQC to help protect transactions, customer information, and long-term financial data.

### Government Systems

Government organizations handle information that may need to remain confidential for decades. Quantum-resistant security can help protect such data from future threats.

### Cloud Computing

Cloud platforms store large amounts of sensitive information. PQC can help secure communication and data exchange between users and cloud services.

## Digital Identity

Digital signatures are widely used for authentication and digital identity. Post-quantum signature algorithms can help protect these systems against future quantum attacks.

### A Practical Project in Post-Quantum Security

As part of my academic work, I explored these concepts through a project focused on secure real-time communication using Post-Quantum Cryptography.

The system combines technologies such as ML-KEM-768, ECDH P-256, ML-DSA, AES-256-GCM, SHAKE-256, WebSockets, Node.js, and React.

The project follows a hybrid approach, combining established cryptographic techniques with post-quantum algorithms to explore how secure communication systems can prepare for the quantum era.

## Challenges and Concerns

Although Post-Quantum Cryptography provides an important path toward quantum-resistant security, its adoption also introduces challenges.

### Performance

Some post-quantum algorithms require larger keys, ciphertexts, or signatures, which can affect storage, bandwidth, and performance.

### Migration

Replacing existing cryptographic systems across large organizations is a complex process, particularly when legacy systems are involved.

### Compatibility

New cryptographic algorithms must work with existing applications, networks, and infrastructure without causing major disruptions.

## Continuous Research

Cryptography must continuously evolve as researchers discover new vulnerabilities and develop improved attack techniques.

### Skills Students Should Focus On

For current Computer Science students, Quantum Computing and cybersecurity offer exciting areas for learning and research. Valuable skills include:

- Cryptography
- Cybersecurity
- Programming
- Data Structures and Algorithms

- Computer Networks
- Mathematics
- Quantum Computing Fundamentals
- Web Technologies
- Information Security

## Research and Problem Solving

Hands-on projects, internships, research activities, cybersecurity competitions, and experimentation with modern technologies can help students develop practical knowledge in these emerging fields.

## Conclusion

Quantum Computing represents a major technological shift that could transform many areas of computing while also challenging the foundations of modern cybersecurity.

Post-Quantum Cryptography provides a way to prepare for this future by developing security systems designed to withstand both classical and quantum attacks.

The transition to quantum-resistant security may take years, making it important to understand and prepare for these technologies today. For Computer Science students, this represents not only a challenge but also an opportunity to explore one of the most important areas shaping the future of technology.

As technology continues to evolve, the security systems we build today must be prepared for the computers of tomorrow.

Paul Eldhose  
2022-26 Batch  
CSE



## FOLLOW US ON OUR SOCIALS:

### CONTACT US:

newslettercse@adishankara.ac.in



---

## EDITORIAL BOARD

### CHIEF EDITOR



DR. RAMANI BAI V (Professor & Head - CSE)

---

### EDITORS



MS. SHANY JOPHIN



MS. NAZNIN M ALI

---

### CREATIVE DESIGN



NANDANA SUDHIR VARMA  
(S5 CSE-C)



NIRANJANA KP  
(S5 CSE-C)

---

### CONTENT TEAM



SANA  
FATHIMA  
(S7 CSE-C)



SANJANA  
ELIZABETH  
(S7 CSE-C)



SREENANDA  
K SHAHJAHAN  
(S3 CSE-C)



ASWATHY  
PRASAD  
(S3 CSE-A)

---