69th ANNUAL
IETE Convention (AIC)

Other highlights

58th Bhabha Memorial Lecture

&

49th Ram Lal Wadhwa Award Lecture

Organized by

IETE Hqs

&

IETE Kolkata Centre

Venue:

Dr Jaya DebRoy Auditorium

RCC Institute of Information Technology (RCCIIT)
Canal South Road, Beliaghata,
Kolkata 700015, West Bengal, India

Theme:
Network Security and Blockchain Technology

25-26 September 2026

The Institution of Electronics & Telecommunication Engineers

#2 Institutional Area, Lodi Road, New Delhi-110003

Supported By

Springer

सत्यमेव जयते
MeitY
Government of India

IEEE
Advancing Technology for Humanity

About AIC

The Annual IETE Conference (AIC) is the flagship event of The Institution of Electronics and Telecommunication Engineers (IETE). This Conference serves as a platform for promoting technological innovation, research and knowledge exchange among professionals, academicians, researchers, industry experts and students.

The inaugural programme of AIC–2026 will bring together eminent academicians from leading national institutions and universities, members of the IETE Governing Council, distinguished Fellows, Lifetime Achievement Award recipients and other eminent awardees. Senior representatives from organisations such as DRDO and ISRO, Vice-Chancellors of leading universities, and distinguished dignitaries from government and industry are also expected to participate.

A major highlight of the Conference is the Annual IETE Awards Ceremony, during which more than 45 awards will be presented in recognition of outstanding contributions in various fields of electronics, telecommunications and information technology. The awardees include eminent professionals and academicians from premier institutions such as IITs, NITs, universities and leading research and development organisations in India and abroad.

AIC–2026 will also feature the Fifth International Conference on **Network Security and Blockchain Technology (ICNSBT–2026)**. The conference is being organised by IETE in association with the Computer Society of India (CSI), Kolkata Chapter. Selected proceedings of ICNSBT–2026 are proposed to be published by Springer Nature in a Scopus-indexed series.

The inaugural programme of AIC–2026 will be held on 25 September 2026 at the Dr Jaya DebRoy Auditorium, RCC Institute of Information Technology (RCCIIT), Kolkata.

Technical Sessions

Track-I : Security and Privacy

Track-II : Network Security & its Applications

Track-III : Blockchain Technology & its Applications

Track-IV : AI & ML in Information Security

PROGRAMME

69TH ANNUAL IETE CONVENTION (AIC) ON "NETWORK SECURITY AND BLOCKCHAIN TECHNOLOGY (ICNSBT 2026)" AT KOLKATA

Thursday 24th Sep 2026 Workshop For Students

Venue: ***IEM Salt Lake, Sector V, Godrej Genesis Building, 15th Floor (Near IETE Kolkata Centre)***

Chief Guest: Prof (Dr) Tapas Chakraborty, VC, Moulana Abul Kalam Azad University of Technology, Kolkata

14:30 – 16:30	**Tutorial Series:** Workshop on Aerial Robotics and UAV Systems
16:31 onwards	**High Tea**

Friday, 25th Sep 2026 Inaugural Session – AIC on ICNSBT 2026

Venue: ***Dr Jaya Deb Roy Auditorium, RCC Institute of Information Technology, Kolkata***

08:31 - 09:00 hrs	Registration & Networking
09:01 - 09:15 hrs	Arrival of dignitaries
09:16 - 09:17 hrs	Requesting dignitaries to come on Dias
09:18 - 09:22 hrs	Presentation of bouquets
09:23 - 09:25 hrs	Lighting of ceremonial lamp & Invocation
09:26 - 09:28 hrs	Ganesh Vandana
09:29 - 09:32 hrs	Welcome address by Dr Partha P Sarkar, Chairman IETE Kolkata Centre
09:33 - 09:37 hrs	Address by Dr Shiv Kumar, Chairman TPOC
09:38 - 09:42 hrs	Address by Dr Jyoti Sekhar Banerjee, Program Chair, ICNSBT 2026
09:43 - 09:47 hrs	Address by Dr J K Mandal, Zonal Mentor (East)
09:48 - 09:58 hrs	Address by the Shri Sunil, President, IETE (2024-26)
09:59 - 10:10 hrs	Address by the Guest of Honour Prof (Dr) Tapas Chakraborty, VC, Moulana Abul Kalam Azad University of Technology, Kolkata
10:11 - 10:30 hrs	Address by the Chief Guest
10:31 - 10:33 hrs	Release of Souvenir
10:34 - 10:40 hrs	Conferment of Honorary Fellowship-2025-26 - Shri Shashi Sekhar Vampati, Padma Shri Awardee & Chairman CBFC
10:41 - 10:55 hrs	Conferment of Life Time Achievement Awards-2026 - Lt Gen(Dr) AKS Chandele, PVSM, AVSM (Retd) President Emeritus and DFIETE - Prof GSN Raju, Chancellor Centurion University, AP
10:56 - 11:10 hrs	Presentation of Distinguished Fellowship-2025-26 - Col (Prof) S L Kapoor - Dr J W Bakal
11:11 - 11:20 hrs	Best Centre/ Sub-Centre Awards 2025-26
11:21 - 11:25 hrs	Announcement of installation of elected President (2026-27)
11:26 - 11:36 hrs	Address by the Dr D C Pande (2026-27)
11:37 - 11:42 hrs	Felicitation of Outgoing GC Members

11:43 - 13:00 hrs	**IETE AWARDS CEREMONY**
	Best ISF Awards 2025-26
1301 - 13:03 hrs	Vote of Thanks by Sharmila Ghosh, Immdt Past Chairman, IETE Kolkata Centre
13:04 - 13:07 hrs	National Song & National Anthem
	High Tea
13:08 - 13:47 hrs	58th Bhabha Memorial Lecture by ***Prof Kalobaran Maiti***, Director, Indian Association for the Cultivation of Science, Kolkata
13:48 - 14:30 HRS	**LUNCH**
14:31 - 16:00 hrs	**Technical Session- I**
Session Chair:	***Lt Gen (Dr) AKS Chandele, PVSM, AVSM (Retd),*** President Emeritus and DFIETE
Invited Talks:	• Prof Ram Mohan Narayanan, The Pennsylvania State University, USA (IETE - IRSI (83) Main Awardee-2025) • Prof Chinmoy Saha, Professor, IIST, Trivandrum • Prof A Arockia Bazil Raj, DIAT, Pune • Dr Krishan Berwal, Dean, MCTE, Mhow
Addl. Session Chairs: *(Technical Session- I)*	***Dr Debashis De***, Professor CSE, MAKAUT, Kolkata ***Dr Hiranmoy Roy***, RCCIIT ***Dr Radha Krishna Bar***, Asst. Manager, Home Affairs, Govt. of WB. • **Paper Presentation (4 papers with Ids): 222, 299, 295 & 298**
16:01 - 17:10 hrs	**Technical Session-II**
Session Chair:	***Dr M H Kori***, Vice President and Chairman BoRIS, IETE
Invited Talks:	• Dr Faruk A S Kazi, VJTI, Mumbai • Dr Sriparna, IIT, Patna • Dr Manas Kamal Bhuyan, IIT Guwahati
Addl. Session Chairs: *(Technical Session- II)*	***Dr Ajay Kumar***, Vice President IETE ***Dr Jyotsna Kumar Mandal***, Zonal Mentor (E)IETE ***Dr Abhijit Das***, RCCIIT • **Paper Presentation (4 papers with Ids): 357, 294, 366 & 242**
17:11 - 17:30 hrs	**High Tea**
17:31 - 18:40 hrs	**Technical Session-III**
Session Chair:	***Shri Narendra Nath*****,** Governing Council Member
Invited Talks:	• Dr Simranjit Singh, PEC, Chandigarh • Dr Taimoor Khan, NIT, Silchar. • Dr. Shivani Malhotra, Chitkara University, Punjab.
Addl. Session Chairs: *(Technical Session- III)*	***Dr Neelam Shrivastava***, GC Member (Elect.) ***Dr Jyoti Sekhar Banerjee***, Program Chair, ICNSBT 2026 ***Dr Indrajit Pan***, Professor, CSE (AIML), RCCIIT ***Shri Sairamakrishna BuchiReddy*** • **Paper Presentation (4 papers with Ids): 158, 335, 360 & 297**

Saturday, 26Th Sep 2026

09:31 - 10:10 hrs	**49TH Ram Lal Wadhwa Award Lecture – 2026**
Speaker	***Dr Binoy Kumar Das***, Director General, Electronics and Communication Systems (ECS), DRDO, Bengaluru
10:11 - 10:30 hrs	Sponsorship Program
10:31 - 12:00 hrs	**Technical Sessions IV, V and VI will be held parallelly**
	Technical Session-IV
Session Chair:	***Dr Debashis De***, GC Member (Elect.), IETE
Addl. Session Chairs:	***Mrs Renu Dwivedi***, GC Member (Elect.), IETE
(Technical Session- IV)	***Dr Subhankar Bhattacharjee***, EC Member, IETE Kolkata
	Dr Priti Deb, EC Member, IETE Kolkata Centre
	Ms Sharmila Ghosh, Immdt Past Chairperson, IETE Kolkata
	• **Paper Presentation (Online Mode) (10 papers with Ids): 91, 170, 244, 147, 175, 187, 252, 367, 162 & 94**
	Technical Session-V
Session Chair:	***Dr Jyoti Sekhar Banerjee***, Program Chair, ICNSBT 2026
Addl. Session Chairs:	***Dr Arpan Deyasi***, Associate Professor, ECE, RCCIIT
(Technical Session- V)	***Dr Debarati Dey Roy***, EC Member, IETE Kolkata
	Shri Snehasish Banerjee, TCS, Kolkata
	Dr Surender Singh Saini, Chairman IETE Chandigarh Centre
	• **Paper Presentation (Online Mode) (10 papers with Ids): 258, 292, 305, 309, 186, 243, 343, 213, 354 & 205**
	Technical Session-VI
Session Chair:	***Dr Vijenderbabu***, Chairman IETE Chennai Centre
Addl. Session Chairs:	***Shri Sandeep Sengupta*****,** ISOEH, Kolkata
(Technical Session- VI)	***Dr Amartya Mukherjee***, Secretary, IETE Kolkata Centre
	Dr Tapasi Bhattacharjee, EC Member, IETE Kolkata Centre
	Dr Raktim Chakraborty, Surendranath College, Kolkata
	Dr Rajeev Chatterjee, EC Member, IETE Kolkata Centre
	• **Paper Presentation (Online Mode) (10 papers with Ids): 117, 293, 246, 197, 337, 318, 192, 85, 327 & 263**
12:01 - 12:45 hrs	**Valedictory Session**
	Chief Guest: **Hon'ble Dr Pradip Kumar Verma**, Member of Parliament (Rajya Sabha), Jharkhand and National Secretary, BJP
	Dr Debashis De, GC Member (Elect.), IETE

12:46 - 13:30 hrs **LUNCH**

Saturday, 26Th Sep 2026 (Afternoon)

IETE GOVERNING COUNCIL MEETINGS

4TH (2025-26) FPPC; 5TH (2025-26) & 1ST (2026-27) GOVERNING COUNCIL MEETING & 72ND AGM

13:31 - 14:30 hrs	4th (2025-26) Finance and Policy Planning Committee (FPPC)
14:31 - 16:30 hrs	5th (2025-26) Governing Council Meeting
16:31 - 17:00 hrs	Joint Special Governing Council Meeting
17:01 - 17:50 hrs	1st (2026-27) Governing Council Meeting
17:51 - 18:00 hrs	Group Photo of Governing Council 2026-27
18:01 - 19:30 hrs	**72nd Annual General Meeting (AGM)**
19:31 - 20:31 hrs	Cultural Program from IETE Kolkata Centre
20:32 hrs onwards	Governing Council Dinner

Sunday, 27Th Sep 2026

09:30 - 11:30 hrs	Governing Council Meeting.

MESSAGE

It gives me immense pleasure that the Institution of Electronics and Telecommunication Engineers (IETE) is organising its **Annual Convention** on a contemporary and strategically important theme "**Network Security and Blockchain Technology**".

Rapid advancement of Information and Communication Technology has transformed the modern-day security environment. Increasing sophistication of cyber threats especially those harnessing AI, have created new challenges to the security and integrity of networks. Resilient networks are therefore an imperative for our operational preparedness. This calls for sustained efforts in research and development of indigenous technologies, which are secure and reliable.

IETE has been spearheading advancement of Electronics, Telecommunications and Information Technology in the country, and thus, plays a pivotal role in this national endeavour. As we strive towards the vision of **Viksit Bharat@2047**, I encourage IETE to further promote indigenous production of defence-oriented technological security solutions through the **integrated efforts of Defence, Industry and Academia** together.

I congratulate IETE and the organisers for bringing together experts and practitioners to deliberate upon the challenges and opportunities in **Network Security and Blockchain Technology**. I am sanguine that the convention will contribute meaningfully towards the development of indigenous technologies for the Armed Forces and the Nation.

JAI HIND

(Dhiraj Seth)
General
Chief of the Army Staff

एस. कृष्णन, आई.ए.एस.
सचिव
S. Krishnan, I.A.S.
Secretary

सत्यमेव जयते

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय
भारत सरकार
Ministry of Electronics &
Information Technology (MeitY)
Government of India

31st August, 2026

MESSAGE

It gives me an immense pleasure that IETE has selected the theme **"NETWORK SECURITY AND BLOCKCHAIN TECHNOLOGY"** for its **69TH ANNUAL IETE CONVENTION (AIC-2026)** scheduled on 25-26 SEP 2026 at KOLKATA. Established in the year 1953, The Institution of Electronics and Telecommunication Engineers (IETE) has taken a lead in the National Development domain by introducing several landmarks in the field of Science & Technology of Electronics; Telecommunication, Computer Science and Information Technology.

Blockchain technology could potentially rework delivery mechanism of some Government's services. It can play a key role in improving the information transaction challenges within Government. The proper linking and sharing of knowledge with Blockchain enable better management of knowledge between multiple departments. It improves the transparency and provides a far better way to monitor and audit transactions. Blockchain technology makes a distributed and cooperative cloud storage environment over a peer-to-peer network possible which might offer more resiliency and higher-speeds at a lower cost. The Ministry of Electronics and Information Technology drives national strategy, standards, and secure frameworks to integrate blockchain technology into transparent and tamper-proof digital governance in India

With a plethora of job opportunities waiting, the fields of Network Security and Blockchain Technology promise well paying job opportunities and career progression. As the Blockchain Technology grows, so does the need for skilled and trained individuals.

I convey my best wishes for the success of the Convention and believe that the deliberations will highlight the future prospects of implementing Blockchain Technology. The proceedings of the conference and the consequent recommendations will be of interest and may be forwarded to the concerned government departments and Industry.

(S. Krishnan)

Digital India
Power To Empower

इलेक्ट्रॉनिक्स निकेतन, 6, सी.जी.ओ. कॉम्पलेक्स, नई दिल्ली–110003 / Electronics Niketan, 6, C.G.O. Complex, New Delhi-110003
Tel. : 011-24364041 • email : secretary@meity.gov.in

राजेश कुमार सिंह, भा.प्र.से.
Rajesh Kumar Singh, IAS

सत्यमेव जयते
भारत सरकार
Government of India

सचिव, रक्षा अनुसंधान तथा विकास विभाग
एवं
अध्यक्ष, डीआरडीओ
Secretary, Department of Defence R&D
&
Chairman, DRDO

MESSAGE

1. I am pleased to know that the Institution of Electronics and Telecommunication Engineers (IETE) is organising its **69th Annual IETE Convention (AIC - 2026)** on the theme **"NETWORK SECURITY AND BLOCKCHAIN TECHNOLOGY"** on 25-26 Sep 2026 at Kolkata. Being at the forefront of Technical Education, IETE has consistently endeavored to empower the Engineering Community with access to resources, mentorship and networking opportunities. The Institution, since its inception, has achieved notable milestones exploring new frontiers to meet the expectations of its members.

2. Network security and blockchain technology transform India's defense sector by removing single points of failure, securing tactical communications, and blocking supply chain tampering. India increasingly relies on sovereign digital frameworks, combining military AI and quantum-resilient cryptography to protect vital infrastructure from state-sponsored cyber warfare. Blockchain technology serves as a vital "trust engine" for India's defense and space sectors. It enhances satellite communication security, ensures reliable geospatial intelligence, transforms military supply chains, and facilitates secure intelligence sharing on the battlefield, forming a robust foundation for trustworthy defense infrastructure. However, there is a notable gap in the literature regarding the implementation of blockchain in Indian space-surveillance programs, particularly within organisations such as ISRO, DRDO, and IAF, which warrants further research.

3. I convey my best wishes for the successful conduct of the Convention and believe that it will provide an effective platform for academicians, researchers, policymakers, legal professionals, technologists and students to discuss emerging developments in blockchain and its impact on law and governance.

Date : 02 Sep 2026
Place: New Delhi

(Rajesh Kumar Singh, IAS)

रक्षा मंत्रालय, रक्षा अनुसंधान तथा विकास विभाग, डीआरडीओ भवन, नई दिल्ली-110011
Ministry of Defence, Department of Defence R&D, DRDO Bhawan, Rajaji Marg, New Delhi-110011
दूरभाष/Phone : 011-23011519, 23014350 फैक्स/Fax : 011-23018216 ई-मेल/E-mail : secydrdo@gov.in

प्रो. योगेश सिंह
अध्यक्ष
Prof. Yogesh Singh
Chairman

सत्यमेव जयते

अखिल भारतीय तकनीकी शिक्षा परिषद्
(भारत सरकार का एक सांविधिक निकाय)
(शिक्षा मंत्रालय, भारत सरकार)
नेल्सन मंडेला मार्ग, वसंत कुंज, नई दिल्ली–110070
दूरभाष : 011–26131498
ई–मेल : chairman@aicte-india.org

ALL INDIA COUNCIL FOR TECHNICAL EDUCATION
(A STATUTORY BODY OF THE GOVT. OF INDIA)
(Ministry of Education, Govt. of India)
Nelson Mandela Marg, Vasant Kunj, New Delhi-110070
Phone : 011-26131498
E-mail : chairman@aicte-india.org

Message

It gives me immense pleasure to extend my warm greetings to the Institution of Electronics and Telecommunication Engineers (IETE) on the occasion of its 69th Annual IETE Convention (AIC-2026) being held on 25–26 September 2026 in Kolkata on the theme "Network Security and Blockchain Technology."

In an era of rapid digital transformation, network security and blockchain technology have emerged as critical pillars for building secure, trustworthy and resilient digital ecosystems. Their growing applications across education, governance, industry, finance and research underscore the need for continuous innovation, interdisciplinary collaboration and responsible technological advancement.

IETE has made significant contributions over the decades towards nurturing technical talent, promoting professional excellence and fostering meaningful engagement among academia, industry and research communities. The Annual Convention provides an important platform for experts, academicians, researchers, professionals and students to exchange ideas, share emerging developments and explore solutions to contemporary technological challenges.

I am confident that **AIC-2026** will stimulate insightful discussions, encourage new research collaborations and inspire young engineers to contribute towards a secure, innovative and technology-driven India.

I extend my best wishes to IETE, the IETE Kolkata Centre, the organisers, distinguished speakers, researchers and all participants for a successful and fruitful Convention.

(Yogesh Singh)
21/8/26

सह वीर्यं करवावहै

The Institution of Electronics and Telecommunication Engineers (IETE)
(Since 1953 in the services of The Nation)
2, Institutional Area, Lodhi Road,
New Delhi - 110 003
(SIRO Recognized by DSIR, Govt. of India)
EPABX : +91 (11) 45142153, 24649429, 98 21801866
Whatsapp : +91 9315422728
E-Mail : sec.gen@iete.org
Website : http://www.iete.org

MESSAGE

Kolkata, popularly known as the **'City of Joy'**, a name made famous by the French author Dominique Lapierre through his celebrated 1985 novel *The City of Joy*, is all set to host the Institution's flagship event, the **Annual Technical Convention**, on **25–26 September 2026**, in association with the Computer Society of India. The Convention will focus on **Network Security and Blockchain Technology**, covering diverse and contemporary areas including privacy, authentication, cybersecurity, security in social networks and the role of Artificial Intelligence and Machine Learning in information security.

I express my heartfelt gratitude to the Team of IETE Kolkata Centre and its Organising Committee for their assiduous efforts in planning and meticulously executing every finer detail of the programme. The large number of technical papers received and the meticulous manner in which they were reviewed are a testament to the team's exemplary coordination, dedication and commitment to delivering the entire programme in a well-planned and time-bound manner. I am particularly pleased to record that all accepted and presented papers will be published in the **Springer Lecture Notes in Networks and Systems**, providing a valuable and enduring platform for disseminating the technical contributions presented at the Convention.

The mind-boggling pace and exponential growth of Artificial Intelligence are confronting humanity with possibilities whose long-term consequences remain difficult to predict. The fact that technological developments are advancing faster than the Regulatory Frameworks of many nations calls for serious introspection and a globally coordinated response. Concerns are increasingly being voiced by eminent technologists and thought leaders about the possibility of AI systems becoming difficult to control, particularly in the midst of intense competition among technology giants. At the same time, we must recognize the remarkable contributions of AI across diverse domains, ranging from agriculture and healthcare to scientific research and drug discovery. Thus, while AI holds immense promise for human progress, its potential risks and unintended consequences can no longer be ignored. The real challenge before humanity is to ensure that the power of AI remains aligned with human values, safety and the larger public good. I hope that the deliberations under **Track IV** of the Convention will provide valuable insights into this critical dimension and contribute towards shaping a responsible and human-centric future for Artificial Intelligence.

I extend my warm greetings and best wishes to the IETE Kolkata Centre, the Organising Committee, the Computer Society of India, all participating authors, researchers, professionals and delegates for a highly successful and intellectually enriching Convention. I am confident that the deliberations and exchange of ideas during these two days will further strengthen our collective endeavor towards advancing technology for the benefit of society.

SUNIL
President, IETE

The Institution of Electronics and Telecommunication Engineers (IETE)
(Since 1953 in the services of The Nation)
2, Institutional Area, Lodhi Road,
New Delhi - 110 003
(SIRO Recognized by DSIR, Govt. of India)
EPABX : +91 (11) 45142153, 24649429, 98 21801866
Whatsapp : +91 9315422728
E-Mail : sec.gen@iete.org
Website : http://www.iete.org

MESSAGE

I extend my warm greetings and best wishes to the IETE Kolkata Centre, the Organizing Committee, the Computer Society of India and all the participants of the Institution's **69th Annual IETE Convention (AIC)**, being organized on the vital theme of **"Network Security and Blockchain Technology" (ICNSBT 2026)**. I am very happy to note that 69th AIC is being organized in Kolkata – "City of Joy" and the "Cultural Capital of India", the city has deep rooted passion for art, literature, music and resilient human spirit.

The Convention brings together renowned experts and academicians who will share their insights and perspectives across four important tracks: **Security and Privacy, Network Security, Blockchain Technology, and Artificial Intelligence & Machine Learning**. Such cross-fertilisation of ideas across closely interconnected domains adds tremendous value to our collective understanding and strengthens our ability to address the myriad challenges emerging at the intersection of rapid technological advancement and evolving societal needs. This continuous exchange of knowledge and ideas is essential for nurturing a thriving technological ecosystem that ultimately benefits society at large.

The rapidly evolving geopolitical and technological landscape is placing unprecedented demands on the scientific and engineering community. While the timelines for achieving technological goals are becoming increasingly compressed, the aspirations of researchers and innovators continue to rise. In this challenging environment, technologies such as **Blockchain and Artificial Intelligence** have emerged as powerful enablers of innovation, offering solutions of immense practical value across diverse domains including **education, defence, healthcare, agriculture and finance**. Their convergence with other emerging technologies is likely to create new opportunities while simultaneously presenting new challenges that merit deeper study and responsible application.

IETE, through its nearly dozen technical and professional Committees, continually endeavours to address the emerging challenges arising from rapid technological developments and their wider implications. The enthusiastic organisation of seminars, workshops and other technical programmes by IETE Centres and Student Fora provides members and students with opportunities to remain abreast of the latest developments. At the same time, our **Journals and Newsletter** serve as important platforms for knowledge dissemination, enabling the IETE community to remain connected with advances in science, engineering and technology.

As IETE enters a new phase of its continuing journey, I am confident that such initiatives will further strengthen the Institution's role in promoting professional excellence, fostering innovation and encouraging meaningful collaboration among academia, industry, researchers and young professionals.

I wish the **69th Annual Technical Convention** every success and hope that it will serve as a meaningful platform for knowledge sharing, intellectual exchange and collaboration. May the deliberations at the Convention generate new ideas, inspire further research and contribute towards harnessing emerging technologies for the advancement and well-being of society. I advise all the delegates & participants to enjoy the marvelous of city of India, during your stay in Kolkata.

(DR D C PANDE)
President (Elect)

सह वीर्यं करवावहै

The Institution of Electronics and Telecommunication Engineers (IETE)
(Since 1953 in the services of The Nation)
2, Institutional Area, Lodhi Road,
New Delhi - 110 003
(SIRO Recognized by DSIR, Govt. of India)
EPABX : +91 (11) 45142153, 24649429, 98 21801866
Whatsapp : +91 9315422728
E-Mail : sec.gen@iete.org
Website : http://www.iete.org

MESSAGE

It is my pleasure to welcome you all to the **69th Annual IETE Convention on** "Network Security and Blockchain Technology." scheduled on 25-26 September 2026.

The IETE Annual Convention is the flagship event of our Institution, strategically hosted at different locations across the country on significant scientific and technological themes. Its objective is to initiate, nurture, and promote research and innovation in engineering and technology for the greater benefit of society. The steady growth and recognition of this convention reflect its quality, impact, and relevance in today's fast-changing world.

The theme "Network Security and Blockchain Technology" in the present era of rapid digital transformation, secure and resilient communication networks have become indispensable to the functioning of governments, industries, businesses, and society. With the increasing dependence on interconnected systems, cloud computing, Internet of Things (IoT), artificial intelligence, and digital platforms, the challenges relating to cybersecurity have grown significantly in both scale and complexity.

I am confident that the thought-provoking deliberations and high-level discussions during this convention will contribute to developing effective strategies for a smooth transition towards a technology-driven and sustainable society. The event promises unique networking opportunities, valuable knowledge sharing, and avenues for professional growth.

I convey my best wishes for the grand success of the event and hope that it will prove to be intellectually stimulating, professionally rewarding, and highly fruitful for all participants.

Dr Jyotsna Kumar Mandal
Zonal Mentor (East), IETE

The Institution of Electronics and Telecommunication Engineers (IETE)
(Since 1953 in the services of The Nation)

MESSAGE

It gives me immense pleasure to extend my warm greetings and a heartfelt welcome to all the distinguished delegates, academicians, researchers, industry professionals, students, and participants attending the **69th Annual IETE Convention**, being held on **25–26 September 2026** on the theme **"Network Security and Blockchain Technology."**

The Annual IETE Convention has established itself as a significant platform for the exchange of ideas, dissemination of knowledge, and advancement of research and innovation in engineering and technology. Hosted at different locations across the country, the Convention brings together the academic, research, and professional communities to deliberate upon emerging technologies and their role in shaping the future of society.

The theme of this year's Convention is both timely and highly relevant. The unprecedented pace of digital transformation has made secure and trustworthy communication systems an essential foundation of modern society. Governments, industries, businesses, and individuals are increasingly dependent on interconnected networks, cloud platforms, the Internet of Things, artificial intelligence, and digital services. This growing digital ecosystem has, in parallel, introduced increasingly sophisticated challenges in cybersecurity, privacy, data protection, and digital trust.

In this context, **network security and blockchain technology** offer significant opportunities to address some of the most pressing challenges of the digital age. While robust network security is fundamental to protecting critical systems and information, blockchain technology has opened new possibilities for decentralized trust, transparency, secure transactions, and tamper-resistant data management. The convergence of these technologies has the potential to contribute significantly to the development of secure, resilient, and trustworthy digital infrastructure.

I am confident that the technical sessions, keynote addresses, research presentations, and intellectual deliberations of this Convention will stimulate meaningful discussions and encourage new ideas, collaborations, and innovations

Beyond the academic and technical dimensions, I believe that this Convention will provide an excellent opportunity for participants to establish new professional connections, exchange experiences, and build lasting collaborations.

On this auspicious occasion, I extend my sincere best wishes to the organizers, participants, and all associated with the **69th Annual IETE Convention**. May the Convention achieve great success and inspire new directions in research, innovation, and technological development.

I warmly welcome you all and wish you an enriching, productive, and memorable Convention.

Partha Pratim Sarkar

Dr Partha Pratim Sarkar
Chairman, IETE Kolkata Centre

The Governing Council 2025-26

Shri Sunil
President

Prof (Dr) A K Saini
Immdt Past President

Prof (Dr) V Gunasekhar Reddy
DIG of Police (Retd)
Immdt Past President

Dr M H Kori
Vice President & Chairman (BoRIS)

Dr Ajay Kumar
Vice President, Chairman (MC) & Co-Chairman (BoA)

Dr R D Kharadkar
Vice President & Zonal Mentor (West)

Brig V K Panday (Retd)
Hony Treasurer & Zonal Mentor (North)

Dr Shiv Kumar
Zonal Mentor (North) & Chairman (TPOC)

Prof (Dr) Jyotsna Kumar Mandal
Zonal Mentor (East), Chairman (APPC) & Co-Chairman (TP&OC)

Dr K Gnaneshwar Rao
Zonal Mentor (South), Chairman (CAGC) & Co-Chairman (BoRIS)

Col Balraj Anand (Retd)
Chairman (RGSC)

Dr K Jaya Sankar
Chairman (BoA) & Co-Chairman (AIEC)

Dr D C Pande
Chairman (T&R Pubs) & Co-Chairman (CEAAC)

Prof Harjinder Singh Bhatia
Chairman (WEELC)

Dr A Sarveswara Rao
Chairman (CEAAC) & Co-Chairman (CDDC)

Dr C P Dwivedi
Co-Chairman (MC & CAGC)

Ms Meenakshi Vij

Dr Ajay Agarwal
Co-Chairman (APPC & SDTC)

Shri Ramesh Gorantala
Chairman (CDCC)

Dr Baswaraj Gadgay
Chairman (BEAC)

Shri C Satyanandan
Chairman (CTCC) & Co-Chairman (RGSC)

Dr S Arumuga Perumal
Chairma (SDTC) & Co-Chairman (CTCC)

Ms Anupma Sharma

Dr K Seetha Ram Babu
Chairman (AIEC & Ch-Chairman (BEAC)

Shri Hari kumar R
(Rep ORG Member)

Dr R K Sinha
Nominated Member

Dr Rajkumar Upadhyay
Nominated Member

Shri G Narendra Nath
Nominated Member

EX-OFFICIO MEMBERS
(Chairpersons of the Centres)

Ms Anupma Sharma
Chairperson, Bengaluru Centre

Shri Radha K Khetan
Chairman, Bhopal Centre

Dr Surender Singh Saini
Chairman, Chandigarh Centre

Dr D Vijendra Babu
Chairman, Chennai Centre

Prof (Dr) Tarun Kumar Rawat
Chairman, Delhi Centre

Dr N Srinivasa Rao
Chairman, Hyderabad Centre

Dr Partha Pratim Sarkar
Chairperson, Kolkata Centre

Dr Shivaji B Ghungrad
Chairman, Mumbai Centre

Prof Gajendra Pal Singh
Chairman, Noida Centre

Dr Sandip Patil
Chairman, Pune Centre

IETE Functionaries, Committees and Boards of the Governing Council – (2025-26)

President

Shri Sunil

President Emeritus

Prof (Dr) A K Saini
Prof (Dr) V Gunasekhar Reddy

Vice Presidents

Dr M H Kori
Dr Ajay Kumar
Dr R D Kharadkar

Hony Treasurer

Brig V K Panday (Retd)

Zonal Mentors

North Zone	-	Dr Shiv Kumar
South Zone	-	Dr K Gnaneshwar Rao
East Zone	-	Dr J K Mandal
West Zone	-	Dr R D Kharadkar

FINANCE & POLICY PLANNING COMMITTEE (FPPC)

Shri Sunil	Chairman
Prof (Dr) A K Saini	Member
Prof (Dr) V Gunasekhar Reddy	Member
Dr M H Kori	Member
Dr Ajay Kumar	Member
Dr R D Kharadkar	Member
Brig V K Panday (Retd)	Member
Dr Shiv Kumar	Member
Dr J K Mandal	Member
Dr K Gnaneshwar Rao	Member
Col Balraj Anand (Retd)	Member
Dr K Jaya Sankar	Member
Shri Ramesh Gorantala	Member
Dr D C Pande	Member
Prof Baswaraj Gadgay	Member
Prof H S Bhatia	Member
Shri C Satyanandan	Member
Shri A Sarveswara Rao	Member
Dr S Arumuga Perumal	Member
Dr K Seetha Ram Babu	Member

A-1 BOARD OF AWARDS (BoA)

Dr K Jaya Sankar	Chairman
Dr Ajay Kumar	Co-Chairman
Dr M H Kori	Member
Dr J K Mandal	Member
Dr K Gnaneshwar Rao	Member
Dr D C Pande	Member
Dr C P Dwivedi	Member

A-2 BOARD OF RESEARCH, INNOVATION AND STANDARDS (BoRIS)

Dr M H Kori	Chairman
Dr K Gnaneshwar Rao	Co-Chairman
Dr R D Kharadkar	Member
Brig V K Panday (Retd)	Member
Dr J K Mandal	Member
Dr D C Pande	Member
Prof Baswaraj Gadgay	Member
Dr Ajay Agarwal	Member
Shri Hari Kumar R	Member
Shri N Sridharan	Member
Dr Shivaji B Ghungrad	Member

A-3 BOARD OF EXAMINATION & ASSESSMENT AND CERTIFICATION (BEAC)

Prof Baswaraj Gadgay	Chairman
Dr K Seetha Ram Babu	Co-Chairman
Shri Ramesh Gorantala	Member
Prof H S Bhatia	Member
Dr S Arumuga Perumal	Member
Ms Meenakshi Vij	Member
Dr C V Ravishankar	Member
Prof (Dr) Tarun Kumar Rawat	Member
Shri Ashwani K Sangamker	Member
Prof Gajendra Pal Singh	Member
Dr Sunil B Somani	Member

B-1 TECHNICAL PROGRAMMES AND OUTREACH COMMITTEE (TPOC)

Dr Shiv Kumar	Chairman
Dr J K Mandal	Co-Chairman
Dr M H Kori	Member
Dr R D Kharadkar	Member
Dr D C Pande	Member
Dr C P Dwivedi	Member
Dr Ajay Agarwal	Member
Shri G Narendra Nath	Member
Dr Umesh Kumar Tiwari	Member
Dr Sunil B Somani	Member
Dr Ajay Kumar	Co-opted
Dr K Seetha Ram Babu	Co-opted

B-2 REVENUE GENERATION & STRATEGY COMMITTEE (RGSC)

Col Balraj Anand (Retd)	Chairman
Shri C Satyanandan	Co-Chairman
Shri Ramesh Gorantala	Member
Prof Baswaraj Gadgay	Member
Prof (Dr) Tarun Kumar Rawat	Member
Shri Ashwani K Sangamker	Member
Dr Sunil B Somani	Member

B-3 MEMBERSHIP COMMITTEE (MC) (CORPORATE, ISF & ORG)

Dr Ajay Kumar	Chairman
Dr C P Dwivedi	Co-Chairman
Brig V K Panday (Retd)	Member
Dr Shiv Kumar	Member
Dr J K Mandal	Member
Dr K Gnaneshwar Rao	Member
Shri Hari Kumar R	Member
Dr Umesh Kumar Tiwari	Member
Prof Gajendra Pal Singh	Member

B-4 WOMEN EMPOWERMENT EXCELLENCE LEADERSHIP COMMITTEE (WEELC)

Prof H S Bhatia	Chairperson
Ms Sharmila Ghosh	Co-Chairperson
Col Balraj Anand (Retd)	Member
Dr K Jaya Sankar	Member
Shri Ramesh Gorantala	Member
Shri C Satyanandan	Member
Ms Anupma Sharma	Member
Ms Meenakshi Vij	Member

B-5 CENTRE EVALUATION ASSESSMENT AND AWARDS COMMITTEE (CEAAC)

Dr A Sarveswara Rao	Chairman
Dr D C Pande	Co-Chairman
Dr K Gnaneshwar Rao	Member
Prof H S Bhatia	Member
Dr S Arumuga Perumal	Member
Dr C P Dwivedi	Member
Ms Anupma Sharma	Member
Ms Meenakshi Vij	Member

C-1 ACADEMIC PROGRAMS AND POLICY COMMITTEE (APPC)

Dr J K Mandal	Chairman
Dr Ajay Agarwal	Co-Chairman
Dr M H Kori	Member
Dr K Gnaneshwar Rao	Member
Col Balraj Anand (Retd)	Member
Dr D C Pande	Member
Prof Baswaraj Gadgay	Member
Dr C V Ravishankar	Member
Prof (Dr) Tarun Kumar Rawat	Member
Dr Shivaji B Ghungrad	Member

C-2 TECHNICAL & RESEARCH PUBLICATION COMMITTEE (TRPuB)

Dr D C Pande	Chairman
Dr J K Mandal	Co-Chairman
Dr M H Kori	Member
Dr Ajay Kumar	Member
Brig V K Panday (Retd)	Member
Dr K Jaya Sankar	Member
Prof H S Bhatia	Member
Dr C P Dwivedi	Member
Dr R K Sinha	Member
Dr Umesh Kumar Tiwari	Member

C-3 COURSE DESIGN AND CONTENT COMMITTEE (CDCC)

Shri Ramesh Gorantala	Chairman
Dr A Sarveswara Rao	Co-Chairman
Dr R D Kharadkar	Member
Dr K Jaya Sankar	Member
Prof Baswaraj Gadgay	Member
Shri C Satyanandan	Member
Dr Ajay Agarwal	Member
Shri Ashwani K Sangamker	Member
Gp Capt Anupam Tiwari	Coopted
Dr G Prasad	Coopted

C-4 CENTRES ACTIVITIES GROWTH COMMITTEE (CAGC)

Dr K Gnaneshwar Rao	Chairman
Dr C P Dwivedi	Co-Chairman
Brig V K Panday (Retd)	Member
Shri C Satyanandan	Member
Dr C V Ravishankar	Member
Shri R K Khetan	Member
Dr Umesh Kumar Tiwari	Member
Shri N Sridharan	Member
Prof (Dr) Tarun Kumar Rawat	Member
Shri Ashwani K Sangamker	Member
Ms Sharmila Ghosh	Member
Dr Shivaji B Ghungrad	Member
Prof Gajendra Pal Singh	Member
Dr Sunil B Somani	Member

C-5 SKILL DEVELOPMENT & TRAINING COMMITTEE (SDTC)

Dr S Arumuga Perumal	Chairman
Dr Ajay Agarwal	Co-Chairman
Dr M H Kori	Member
Brig V K Panday (Retd)	Member
Prof J K Mandal	Member
Dr K Gnaneshwar Rao	Member
Dr D C Pande	Member
Dr A Sarveswara Rao	Member
Dr C P Dwivedi	Member
Dr K Seetha Ram Babu	Member
Shri G Narendra Nath	Member
Prof Gajendra Pal Singh	Member
Dr Ajay Kumar	Co-opted
Dr Shiv Kumar	Co-opted

C-6 CORPORATE TRAINING & COLLABORATION COMMITTEE (CTCC)

Shri C Satyanandan	Chairman
Dr S Arumuga Perumal	Co-Chairman
Col Balraj Anand (Retd)	Member
Dr K Jaya Sankar	Member
Shri Ramesh Gorantala	Member
Ms Anupma Sharma	Member
Ms Meenakshi Vij	Member
Dr K Seetha Ram Babu	Member
Dr C V Ravishankar	Member
Ms Sharmila Ghosh	Member
Dr Shivaji B Ghungrad	Member

C-7 ACCESSIBILITY AND INCLUSIVITY OF ENGINEERS COMMITTEE (AIEC)

Dr K Seetha Ram Babu	Chairman
Dr K Jaya Sankar	Co-Chairman
Dr Shiv Kumar	Member
Dr J K Mandal	Member
Col Balraj Anand (Retd)	Member
Ms Meenakshi Vij	Member
Dr Ajay Agarwal	Member
Shri Hari Kumar R	Member
Dr C V Ravishankar	Member
Prof Gajendra Pal Singh	Member

THE INSTITUTION OF
ELECTRONICS AND TELECOMMUNICATION ENGINEERS

सह वीर्यं करवावहै

Conferment of Honorary Fellowship 2025-26

on

Shri Shashi Shekhar Vempati

Padma Shri Awardee | Chairperson, Central Board of Film Certification | Former CEO, Prasar Bharati, GoI

CITATION

*The Institution of Electronics and Telecommunication Engineers is proud to confer its **Honorary Fellowship** on **Shri Shashi Shekhar Vempati**, a distinguished technocrat, media leader, technology strategist and public policy professional whose career represents a remarkable confluence of technology, digital innovation, public broadcasting, media and national communication.*

An alumnus of the Indian Institute of Technology Bombay, Shri Vempati brings over two decades of rich professional experience spanning technology consulting, corporate leadership, digital transformation, media and public policy. He began his career in the technology sector and spent over a decade with Infosys, where he worked in technology strategy and digital innovation in the areas of wireless data, mobility, RFID and wireless sensors. His pioneering work in technology is reflected in patents relating to real-time business event management within wireless sensor networks.

He subsequently made a significant transition into the digital media domain, serving as Chief Digital Officer and later Chief Executive Officer of Niti Digital, where he contributed to the adoption of digital technologies for citizen participation and communication during the 2014 General Elections.

In 2017, Shri Vempati was appointed Chief Executive Officer of Prasar Bharati, becoming the first non-bureaucrat to hold this position and one of the youngest leaders of India's public broadcasting organisation. During his tenure from 2017 to 2022, he provided transformative leadership to Doordarshan and All India Radio, advancing their modernisation, digital convergence, technology adoption and expansion of digital outreach. He also served as Chief Executive Officer of Rajya Sabha TV from 2017 to 2019.

His contributions extend well beyond broadcasting. Shri Vempati has played an important role in advancing science communication, educational media and technology policy, having chaired the Committee for Science & Technology Communication of the Department of Science and Technology and the Educational Media Experts Committee for the UGC. He has also contributed to the governance and development of prominent institutions and organisations, including the Indian Institute of Mass Communication and the Broadcast Audience Research Council.

A strong proponent of India's emerging technology ecosystem, Shri Vempati has been associated with initiatives aimed at strengthening India's capabilities in artificial intelligence and deep technology. As Co-Founder of the DeepTech for Bharat Foundation (AI4India), he has contributed to the advancement of an indigenous technology ecosystem. He has also served as an Independent Director of the BharatGen Technology Foundation, established at IIT Bombay under the IndiaAI Mission. Through his writings, public engagements and thought leadership, he has contributed significantly to contemporary discourse on technology, artificial intelligence, digital platforms, media, public policy and strategic communication. His contribution to conceptualising and initiating the development of indigenous Direct to Mobile D2M technology, along with the creation of its supporting ecosystem, is highly commendable and deeply appreciated.

In recognition of his distinguished contributions in the field of Literature and Education, the Hon'ble President of India conferred upon Shri Shashi Shekhar Vempati the Padma Shri in 2026. In May 2026, he was appointed Chairperson of the Central Board of Film Certification (CBFC) for a three-year term, entrusting him with an important national responsibility in the field of media and public communication.

The Institution of Electronics and Telecommunication Engineers proudly recognizes Shri Shashi Shekhar Vempati for his distinguished leadership, technological vision and outstanding contributions to India's digital transformation, public broadcasting, media, science communication and emerging technology ecosystem.

25th Sept 2026
Kolkata

Manju Mam
Secretary General

Sunil
President

THE INSTITUTION OF ELECTRONICS AND TELECOMMUNICATION ENGINEERS

सह वीर्यं करवावहै

IETE has a great pleasure in awarding

Lieutenant General (Dr) A K S Chandele, PVSM, AVSM (Retd)

Distinguished Fellow, IETE | President Emeritus, IETE | Former Director General EME, Indian Army

IETE Life-Time Achievement Award 2025-26

CITATION

*IETE is proud to confer its **Lifetime Achievement Award** on **Lieutenant General (Dr) A K S Chandele, PVSM, AVSM (Retd),** a distinguished military engineer, technocrat, institution builder and industry leader, with an illustrious career spanning advanced defence technologies, engineering systems and professional institutions.*

Commissioned into the Corps of Electronics and Mechanical Engineers (EME), Indian Army, in June 1970, Lt Gen Chandele specialized in electronics, radar and control systems, air defence, anti tank missiles and biomedical engineering. He is a graduate of the Defence Services Staff College and has undergone the Higher Command Course at the Army War College and the prestigious National Defence College, New Delhi. He rose to the position of Director General EME, providing strategic leadership to the corps responsible for the repair, maintenance and overhaul of the complete range of vehicles, weapon systems and equipment of the Indian Army.For his distinguished service he was awarded the prestigious Ati Vishisht Seva Medal (AVSM) and Param Vishist Seva Medal (PVSM) by the President of India.

Beyond his military career, Lt Gen Chandele has made enduring contributions to India's engineering, technology and professional institutions. A Distinguished Alumnus of IIT Roorkee, he is a Distinguished Fellow and President Emeritus of IETE and a Distinguished Engineer of the Institution of Engineers (India). Elected a Distinguished Fellow of IETE in 2013–14, he served as President of IETE during 2016–17, providing visionary leadership to the Institution.

Throughout his over three decades of association with IETE, Lt Gen Chandele has made sustained and valuable contributions to the growth of the Institution. As a member of the IETE Governing Council and subsequently as President, he actively participated in and supported the initiatives and programmes of IETE Headquarters and its Centres. He played a particularly important role in strengthening IETE's engagement with the Defence Forces engineering community and in fostering institutional linkages with organisations and professional bodies sharing IETE's objectives. His efforts were instrumental in facilitating the establishment of IETE Sub-Centres at Meerut and Agra, thereby extending the Institution's professional outreach.

Following his tenure on the Governing Council, Lt Gen Chandele has continued to remain closely associated with IETE and has consistently extended his guidance, experience and support to its programmes and activities. His unwavering commitment to the Institution exemplifies the spirit of professional service and leadership.

Lt Gen Chandele has continued to contribute to India's industrial and technology ecosystem through leadership and advisory roles with organisations including Larsen & Toubro (L&T) and Ashok Leyland. Currently, he is serving as the President – Defence, Internal Security & Public Safety, Geospatial World, Chairman of the Geospatial World Chamber of Commerce and Senior Advisor to the Electronics Industries Association of India (ELCINA). He has also served as Director of the Electronics Sector Skills Council of India (ESSCI).

IETE recognizes Lieutenant General A K S Chandele for his exceptional leadership in defence engineering and technology and his sustained and significant contributions to the growth, outreach and professional advancement of the Institution of Electronics and Telecommunication Engineers.

25th Sept 2026
Kolkata

Manju Mam
Secretary General

Sunil
President

THE INSTITUTION OF ELECTRONICS AND TELECOMMUNICATION ENGINEERS

सह वीर्यं करवावहै

IETE has a great pleasure in awarding

Prof (Dr) G S N Raju

Chancellor, Centurion University, Andhra Pradesh | Former Vice-Chancellor, Andhra University, Visakhapatnam

IETE Life-Time Achievement Award 2025-26

CITATION

*IETE is proud to confer the **IETE Lifetime Achievement Award** on **Prof (Dr) G S N Raju**, a distinguished academician, researcher and administrator, for his outstanding contributions to teaching, research, academic leadership and professional service in Electronics and Communication Engineering, and for his dedicated and sustained service to IETE.*

An alumnus of Andhra University, Prof Raju secured First Class with Distinction and First Rank in B E and M E, earned his PhD from IIT Kharagpur in Communication and Radar Engineering. He was also a DAAD Fellow and served as Visiting Professor at the Universities of Karlsruhe and Paderborn, Germany.

With over four decades of distinguished academic and professional service, Prof Raju served Andhra University for 34 years, rising to the position of Professor and subsequently holding several key academic and administrative positions, including Principal, AU College of Engineering (A), Dean, Faculty of Engineering, Dean (R&D) and Vice-Chancellor of Andhra University. He also served as In-Charge Vice-Chancellor of Damodaram Sanjivayya National Law University, Visakhapatnam. Under his leadership, Andhra University achieved significant recognition in academic excellence, research, accreditation, employability and national and international rankings.

A prolific researcher and mentor, Prof Raju has published over 500 research papers, guided 60 PhD scholars and more than 200 postgraduate theses, and successfully completed several R&D and consultancy projects supported by DRDO, MHRD and AICTE, among others.

Prof Raju is the author of 11 textbooks in areas including Antennas and Wave Propagation, Electromagnetic Field Theory, Electronic Devices and Circuits, Microwave Engineering, and Radar Engineering, contributing significantly to engineering education and professional learning.

His distinguished contributions have been recognised through several honours, including the State Best Teacher Award (1999), Best Research Award (1994), Prof Aiya Memorial IETE Award for Best Research Guidance (2005), Dr Sarvepalli Radhakrishnan Award for Best Academician (2007), National EMC Engineer of the Year Award (2008), Eminent Electronics and Communication Engineer Award (2012), National Award for Teaching Excellence, National Award for Research Excellence, and the ISTE Lifetime Achievement Award (2025), among numerous other academic and professional distinctions.

Prof Raju has made significant and sustained contributions to IETE for over four decades as a Life Member and Fellow. He has served as Vice-Chairman and Chairman of the IETE Visakhapatnam Centre and played a pivotal role in strengthening IETE's activities in the region. His efforts contributed to the establishment of an exclusive IETE building at the Andhra University Engineering College Campus, supporting IETE's academic, examination, seminar and training activities. He also contributed to the expansion of IETE Student Forums, enhancement of student membership and wider recognition of IETE qualifications for postgraduate admissions.

IETE is proud to confer its Lifetime Achievement Award on Prof (Dr) G S N Raju for his outstanding contributions to Electronics, Communication and Electromagnetic Engineering, and for his dedicated efforts in strengthening IETE activities and advancing the engineering profession.

25th Sept 2026
Kolkata

Manju Mam
Secretary General

Sunil
President

THE INSTITUTION OF ELECTRONICS AND TELECOMMUNICATION ENGINEERS

सह वीर्यं करवावहै

Conferment of Distinguished Fellowship 2025-26

on

Prof (Col) S L Kapoor (Retd)

CITATION

Prof (Col) S L Kapoor (Retd), a distinguished professional, educator and long-standing member of IETE, began his career after completing his M.Sc. in Physics by joining the Indian Army Corps of Signals in 1973. He subsequently obtained his B.Tech. from the Military College of Telecommunication Engineering, Mhow, and his M.Tech. from IIT Kanpur in 1986. He also holds an MBA in Human Resources from IGNOU.

During his distinguished military career, Prof. Kapoor served at Army Headquarters and was closely involved in the development and induction of advanced communication systems for the Indian Army, in coordination with premier organisations such as LRDE and BEL, Bengaluru. He commanded his unit during Operation Vijay (Kargil) and, thereafter, moved to the Defence Research and Development Organisation (DRDO), Bengaluru. He retired from the Indian Army/DRDO service in 2005.

He is having a long and distinguished association with the Institution of Electronics and Telecommunication Engineers (IETE) spanning approximately four decades. He has contributed actively to various activities and initiatives of the Institution over the years. He became a member of the IETE Council in 2008, following his tenure as Chairman of the IETE Noida Centre. He was subsequently elected to the IETE Governing Council on three occasions and completed his final tenure in 2025.

At present, Prof (Col) S L Kapoor is serving as a Professor at Ajay Kumar Garg Engineering College, Ghaziabad, where he continues to contribute to technical education, mentoring and the development of young engineering professionals.

His distinguished career, spanning the Indian Army, DRDO, academia and IETE, reflects his unwavering commitment to technology, professional excellence, institutional development and the service of the engineering community.

IETE is proud to confer the Distinguished Fellowship of the Institution to Prof (Col) S L Kapoor for his substantive and distinguished contributions to IETE.

Kolkata
25 Sep 2026

Manju Mam
Secretary General

Sunil
President

THE INSTITUTION OF ELECTRONICS AND TELECOMMUNICATION ENGINEERS

सह वीर्यं करवावहै

Conferment of Distinguished Fellowship 2025-26

on

Prof (Dr) Jagdish W Bakal

CITATION

Prof (Dr) Jagdish W Bakal is a distinguished Academician and Researcher with 40 years of experience. He is presently serving as Principal, Pillai HOC College of Engineering and Technology, Rasayani. He was the first Director of the School of Engineering and Applied Sciences, University of Mumbai, Kalyan, where he established a Research Centre for Science and Technology. He has also held several important academic positions at the University of Mumbai, including Chairman of Boards of Studies in Computer Engineering, Information Technology and Computer Science, and has served on various academic and research committees.

He has an impressive record of research, publications and mentoring. He holds 10 patents, has published 200+ research papers in international journals and conferences, authored 4 book chapters, and has guided 29 Ph.D scholars, besides mentoring more than 50 M.Tech students.

He has received several prestigious honours, including the B. R. Batra Award of IETE, the Achievement in Education Excellence Award by NEHRDO, New Delhi, and the Best Principal of the Year Award (2022) by IARDO. He is a Fellow of IETE and a member/senior member of several professional bodies, including IEEE, IE, CSI and other international professional societies.

His contribution to IETE has been significant. He served as President of IETE during 2019–2021, was Governing Council member during 2013–2016 and served as Chairman of the Academic Committee. He was again elected to the Governing Council for 2018–2021 and served as Vice President. He also served as Chairman, Vice Chairman and Honorary Secretary of the IETE Mumbai Centre and contributed to several major IETE initiatives and programmes.

IETE is proud to confer the Distinguished Fellowship of the Institution to Prof (Dr) Jagdish W Bakal for his substantive and distinguished contributions to IETE.

Kolkata
25 Sep 2026

Manju Mam
Secretary General

Sunil
President

IETE AWARDEES 2026

It is with great pleasure that IETE announces the recipients of the IETE Awards for the year 2025–2026. IETE extends its heartfelt congratulations and best wishes to all the distinguished awardees on this well-deserved recognition of their outstanding contributions and achievements.

- ***IETE MAIN AWARDS***
- ***IETE CORPORATE AWARDS***
- ***IETE BEST PAPER AWARDS***
- ***IETE ACADEMIC AWARD***

This year, IETE witnessed an unprecedented response to its Main Awards**,** receiving the highest-ever number of nominations**.** A stringent screening process was undertaken to ensure fairness and adherence to the prescribed criteria, resulting in the rejection or disqualification of nominations that did not fulfil the stipulated eligibility requirements.

The **IETE Award Ceremony 2026** will be held during the **69th Annual IETE Convention in Kolkata, September 25–26, 2026**. The final list of **IETE Awards 2026 recipients** is given below.

IETE will separately communicate the **ceremony details, programme schedule, and other arrangements** to all awardees.

IETE warmly congratulates all the awardees and looks forward to honouring their outstanding contributions.

S.No.	IETE MAIN AWARDEES-2026	
1.	**IETE - Ram Lal Wadhwa Award -2026** **Awardee** **Dr Binoy Kumar Das**, Electronics & Communication Systems (ECS), Defence Research & Development Organization (DRDO), Bengaluru	
2.	**IETE - Hari Ramji Toshniwal Award-2026** **Awardee** **Dr Faruk AS Kazi,** Dept of Electrical Engineering**,** Veermata Jijabai Technological Institute (VJTI), Mumbai	
3.	**IETE – Bimal Bose Award-2026** **Awardee** **Shri Manmath Kumar Badapanda,** Dept of Atomic Energy, Raja Ramanna Centre for Advanced Technology, Indore	

S.No.	IETE MAIN AWARDEES-2026	
4.	**IETE - Lal C Verman Award-2026** **Joint Awardee(s)** **Dr Surender Singh Saini,** Central Scientific Instruments Organisation-CSIO, Chandigarh **and** **Dr Anesh Kumar Sharma,** Electronics Corporation India Ltd (ECIL), Hyderabad	 
5.	**IETE - Flt Lt Tanmaya Singh Dandass Memorial Award-2026** **Awardee** **Dr G Sivakumar**, Aerospace Electronics & Systems Division, CSIR-National Aerospace Laboratories, Bangalore	
6.	**IETE - Prof K Sreenivasan Memorial Award-2026** **Awardee** **Prof A Arockia Bazil Raj,** Dept of Electronics Engineering, Defence Institute of Advanced Technology (DIAT), DRDO, Pune	
7.	**IETE - Prof SVC Aiya Memorial Award-2026** **Awardee** **Prof Chinmoy Saha,** Dept of Avionics, Indian Institute of Space Science and Technology (IIST) Dept of Space, Govt of India, Trivandrum	
8.	**IETE - Prof S N Mitra Memorial Award-2026** **Awardee** **Shri Chakresh Kumar Jain,** Former Dy Director General, Prasar Bharati (All India Radio & Doordarshan).	
9.	**IETE-CEOT Award (Biennial) -2026** **Joint Awardee(s)** **Dr Simranjit Singh,** Dept of Electronics and Communication Engineering, Punjab Engineering College (PEC), Chandigarh **and** **Dr Sanjeev Kumar Raghuwanshi,** Dept of Electronics Engineering, Indian Institute of Technology (ISM), Dhanbad, Jharkhand	 

S.No.	IETE MAIN AWARDEES-2026	
10.	**IETE - B V Baliga Memorial Award-2026** **Awardee** **Shri K Venkateswara Rao,** Microwave Tube Research and Development Centre, Defence Research & Development Organization (DRDO), Bangalore	
11.	**IETE-NV Gadadhar Memorial Award -2026** **Awardee** **Dr Suraj Srivastava,** Dept of Electronics Engineering, Indian Institute of Technology (IIT), Jodhpur	
12.	**IETE - B R Batra Memorial Award-2026** **Awardee** **Ms Preeti Agrawal,** Technical Consultant, M/s Aimtron, Vadodara, Gujarat	
13.	**IETE - R S Khandpur Award-2026** **Awardee** **Dr Neelesh Kumar,** Biomedical Instrumentation Unit, CSIR-CSIO, Chandigarh	
14.	**IETE – Brig M L Anand Award-2026** **Awardee** **Shri Raju Gupta,** Samsung Research & Development Institute, Bangalore, Bengaluru	
15.	**IETE – Biman Behari Sen Memorial Award-2026** **Awardee** **Dr Bhaskar Kanseri,** Dept of Physics, Indian Institute of Technology, Hauz Khas, Delhi	
16.	**IETE-Lifetime Achievement Award-2026** **Joint Awardee(s)** **Lt Gen (Dr) AKS Chandele, PVSM, AVSM (Retd),** President Emeritus & Distinguished Fellow, IETE, Noida **and** **Prof GSN Raju,** Chancellor, Centurion University, AP	 

S.No.	IETE MAIN AWARDEES-2026	
17.	**IETE- Smt Manorama Rathore Memorial Award-2026** **Awardee** **Dr Taimoor Khan,** Dept of Electronics and Communication Engineering, National Institute of Technology (NIT) Silchar, Silchar Assam	
18.	**IETE-Smt Ranjana Pal Memorial Award-2026** **Awardee** **Prof Binod Kumar Kanaujia**, B R Ambedkar National Institute of Technology, Jalandhar	
19.	**IETE-Smt Triveni Devi Gupta Memorial Award-2026** **Awardee** **Dr Sangeeta Narendra Kale,** Defence Institute of Advanced Technology (DIAT), Pune	
20.	**IETE-Technomedia Award for Young Women in Engineering-2026** **Awardee** **Dr Anubha Goel**, Dept of Electronics and Communication Engineering, Maharaja Agrasen Institute of Technology, New Delhi	
21.	**IETE-Shri Devi Singh Tyagi Memorial Award-2026** **Awardee** **Dr C S Madhusudhana**, Programme Planning & Evaluation Group, (PPEG), U R Rao Satellite Centre, ISRO, Bengaluru	
22.	**IETE-Shri P P Malhotra Memorial Award-2026** (For IETE Organisational Member) **Awardee** **Sri Sai Ram Engineering College** (G00586), Chennai **Principal- Dr J Raja**	
23.	**IETE- Dr Sudhakar Rao Award-2026** **Awardee** **Dr Gopi Ram,** Dept of Electronics & Communication Engineering, National Institute of Technology (NIT), Warangal	

S.No.	IETE MAIN AWARDEES-2026	
24.	**IETE – Sri C Viswanatha Reddy Memorial Award-2026** **Awardee** **Dr Giuseppe Labate,** Netherlands Organization for Applied Scientific Research, Netherlands	
25.	**IETE – Smt C Ranganayakamma Memorial Award-2026** **Awardee** **Dr Garima Chopra,** Dept of Electronics & Communication Engineering, Chitkara University, Punjab	
26.	**IETE- Yasodamma and Sarasavani Award-2026** **Awardee** **Prof Vinay Chamola,** Dept of Electrical & Electronics Engineering, Birla Institute of Technology and Science (BITS) Pilani, Rajasthan	
27.	**IETE – Prof Anita Gopal Dandekar Award-2026** **Awardee** **Dr Manas Kamal Bhuyan,** Dept of Electronics and Electrical Engineering, Indian Institute of Technology (IIT) Guwahati, Assam	
28.	**IETE – Dr K D Pavate Memorial Award-2026** **Joint Awardee(s)** **Shri Jyotheswar Jettipalli,** Central Research Laboratory, Bharat Electronics Ltd (BEL), Bangalore **and** **Dr Manish Narwaria,** Dept of Electrical Engineering, Indian Institute of Technology, IIT Jodhpur **and** **Dr V Thulasi Bai,** Dept of Electronics & Communication Engineering KCG College of Technology, Chennai	  

S.No.	IETE MAIN AWARDEES-2026	
29.	**IETE – Shri Mantej Singh Mangat Memorial Award-2026** **Awardee** **Shri Balaji Salem Balasundram**, Amazon Web Services Inc., USA	
30.	**IETE – Poojya Dr Sharnbaswappa Appaji Award for Women in Technology and Innovation-2026** **Awardee** **Dr Sriparna Saha,** Dept of Computer Science and Engineering, Indian Institute of Technology (IIT) Patna	

IETE CORPORATE AWARDEES-2026	
IETE–Corporate Award for Performance in Development of Software (MSME)- 2026 **Awardee** **byteXL TechEd Private Limited**, Bangalore **Shri Karun Tadepalli**, Co-Founder & CEO	
IETE-Corporate Award for Performance in Electronic Components (MSME) -2026 **Joint Awardee(s)** **Phytec Embedded Private Limited**, Bangalore **Shri Baipalli Vallab Rao (Vasu)**, Managing Director **and** **SSD Polymers**, Machilipatnam, AP **Dr P V Datta Prasad**, Director Technical	 
IETE Corporate Award for Performance in Electronic Instruments and Instrumentation (MSME) - 2026 **Awardee** **Conformity Testing Labs Pvt Ltd,** New Delhi **Shri Arun Sachdeva**, Managing Director	

IETE BEST PAPER AWARDEES-2026

Awards	Best Paper(s)/Awardees	
IETE SK Mitra Memorial Award- **The best research-oriented paper**	**Memcapacitor Emulator Based on Voltage Differencing Buffered Amplifiers by Mustafa Konal & Firat Kacar, published in *IETE Journal of Research,* Vol 71 no 4 April 2025 issue, pp 1411–1421.**	 
IETE J C Bose Memorial Award- **The best engineering-oriented paper**	**Frequency Diverse Array Radar Application for Drone Detection by Venugopal Kulkarni, A. Vengadarajan & K. P. Ray, published in *IETE Journal of Research* Vol 71 no 4 April 2025 issue, pp 1298–1314.**	  
IETE M N Saha Memorial Award- **The best application-oriented paper**	**High-Quality Factor Ultrathin Polarization-Insensitive Wide Angular Stable Elliptical-Shaped Microwave Absorber with Reconfigurability Features by Garima Tiwari, Manshree Mishra, Pramod Kumar Gupta, Trivesh Kumar and Biswajeet Mukherjee, *IETE Journal of Research* Vol 71 no 3 March 2025 issue, pp 960-968.**	  

Awards	Best Paper(s)/Awardees	
		 
IETE K S Krishnan Memorial Award- **The best system-oriented paper**	**Improving Human Activity Recognition in Smart Healthcare with Ensemble Deep Learning by Vaibhav Soni, Himanshu Yadav, Vijay Bhaskar Semwal & Sudhakar Tripathi, published in *IETE Journal of Research* Vol 71 no 3, March 2025 issue, pp 894–908.**	   
IETE CDIL Award for Industry- **The best paper contributed by authors working in Industry**	**AI-Powered Robotic Cloud Automation-Based Dynamic Task Allocation and Process Optimization Using E-WFO and C²DRBM by Rajya Lakshmi Gudivaka, Dinesh Kumar Reddy Basani, Raj Kumar Gudivaka, Sri Harsha Grandhi, Basava Ramanjaneyulu Gudivaka, Sundarapandian Murugesan and M M Kamruzzaman published in *IETE Journal of Research* Vol 71 no 9, Sep 2025 issue, pp 2988-3001.**	 

Awards	Best Paper(s)/Awardees	
		    
IETE Gowri Memorial Award- **The best paper on topic of general Interest**	**FedHFP: A Federated Deep Learning Framework for Heart Failure Prediction by Anu Lohachab and Kuldeep Kumar published in IETE Journal of Research Vol 71 no 2, Feb 2025 issue, pp 479-491**	 

Awards	Best Paper(s)/Awardees	
IETE Journal of Education Award- **Two best papers from *IETE Journal of Education***	**i) WiFi Security - A Tutorial by P V Ananda Mohan and N Sarat Chandra Babu published in *IETE Journal of Education* Vol 66 no 2, Jul-Dec 2025 issue, pp 95-110**	 
	ii) Teaching of Engineering Mathematics in the Era of Data Science and Artificial Intelligence by C P Ravikumar and Radha Gupta published in *IETE Journal of Education* Vol 66 no 2, July-Dec 2025 issue, pp 130-143	 

IETE ACADEMIC AWARDEE-2026

AMIETE CATEGORY

AMIETE Council Award-III for securing the highest percentage with 6.5 GPA and above marks and completing Part II of Section B (except project) in one attempt without exemptions.

	GPA	Mem. No.	Name
Dec 2025	9.5	SG-177150	Shri Ajay Rawat

E & T Stream

****

IETE-IRSI (83) MAIN AND YOUNG SCIENTIST AWARDS 2025-26

DECLARED

The IETE-IRSI (83) Awards Committee for the year 2025–26 met on 04 September 2026 in Bengaluru to consider and evaluate the nominations received for the IETE-IRSI (83) Main Award and the IETE-IRSI (83) Young Scientist Award.

Based on its deliberations and evaluation, the Committee has declared the following awardees:

S.N.	IETE-IRSI (83) MAIN AWARDEES-2026	
1.	**IETE - IRSI (83) Main Award-2026** **Awardee**: **Prof Shobha Sundar Ram,** Indraprastha Institute of Information Technology, New Delhi.	
	IETE-IRSI (83) YOUNG SCIENTIST AWARDS	
2.	**IETE - IRSI (83) Young Scientist Awardees-2026:** **Joint Awardee(s):** **Shri Nirbhay Kumar Singh,** Centre of Excellence-Radar and Weapon System / PDIC, Bharat Electronics Limited (BEL), Bangalore **and** **Shri Ruchit MS,** Bharat Electronics Limited (BEL), Bangalore	 

IETE extends its warmest congratulations to all the distinguished recipients of the IETE-IRSI (83) Main and Young Scientist Awards for the year 2025–26. The Institution wishes them continued success and many more significant achievements in their future professional endeavours.

IETE-IRSI (83) MAIN AND YOUNG SCIENTIST AWARDS-2024-25

During the 68th Annual IETE Convention (AIC), the 2025 IETE Award ceremony took place at the CSIR-Central Scientific Instruments Organization (CSIO), Sector 30, Chandigarh. It took place on September 27 and 28, 2025. Unfortunately, the IETE-IRSI (83) Awards Committee was unable to meet earlier, thus the 2024–2025 IETE-IRSI (83) Awards winners could not be announced alongside the other winners.

The Committee recently convened in Bangalore and announced their results. Along with the 2025–2026 winners, the newly declared names of the 2024–2025 winners will also receive their awards this year. As soon as the date and location are confirmed, the recipients will be shared details.

IETE extends its warmest congratulations to both recipients of IETE-IRSI (83) Awards of 2024-25.

IETE-IRSI (83) MAIN AND YOUNG SCIENTIST AWARDEES (2024-25)

IETE - IRSI (83) Main Award-2025 **Awardee: Prof Ram Mohan Narayanan,** Distinguished Professor of Electrical Engineering The Pennsylvania State University PA 16802, USA	
IETE - IRSI (83) Young Scientist Award-2025 **Awardee: Ms Sherry Gomez** Bharat Electronics Limited, Bangalore	

IETE BEST CENTRE / SUB-CENTRE AWARDEES-2026

CENTRES

- IETE Kolkata Centre
- IETE Vijayawada Centre

SUB-CENTRE

- IETE Nashik Sub-Centre

BEST ISF AWARDEES (2025-26)

NORTH ZONE

I. B K Birla Institute of Engg. & Technology, Jhunjhunu, Rajasthan

II. Manav Rachna University, Faridabad

SOUTH ZONE

I. Sri Sairam Engineering College, Chennai

II. KKR & KSR Institute of Technology and Sciences, Guntur, AP

WEST ZONE

I. JSPM's Bhivarabai Sawant Institute of Technology and Research, Pune

II. Military College of Telecommunication Engineering (MCTE), Mhow

EAST ZONE

I. Narula Institute of Technology, Kolkata

II. Dinabandhu Andrews Institute of Tech. & Manag., Kolkata

AIC IETE 2026

Patrons:

- Shri Sunil, President
- Dr D C Pande, President Elect (2026-27)

General Chairs

- Dr Shiv Kumar, Chairman TPOC & Zonal Mentor (N)
- Dr Jyotsna Kumar Mandal, Zonal Mentor (E)

Program Chairs:

- Prof Debashis De, GC (Elec), IETE
- Dr Jyoti Sekhar Banerjee, Chairman CSI, Kolkata

Program Co-Chairs:

- Dr Amartya Mukherjee, IETE Kolkata
- Dr Abhijit Das, IETE Kolkata
- Dr Debashis Mondal, Dean (RI), RCCIIT
- Dr Indrajit Pan,Dean (A), RCCIIT
- Dr Hiranmoy Roy, President, (IIC), RCCIIT

Organizing Chair

- Dr Anindita Ganguly, Director of Technical Education, Govt of West Bengal
- Dr P P Sarkar, Chairman, IETE Kolkata Centre

Organizing Co-Chair

- Prof (Dr) Ashoke Mondal, Principal-in Charge, RCCIIT
- Ms Sharmila Ghosh, IETE Kolkata

National Advisory Committee

- Prof (Dr) A K Saini, President Emeritus-I
- Prof (Dr) V Gunasekhar Reddy, DIG of Police (Retd) President Emeritus-II
- Dr M H Kori, Vice President
- Prof (Dr) Ajay Kumar, Vice President
- Dr R D Kharadkar, Vice President & Zonal Mentor (W)
- Brig V K Panday (Retd) - Hony Treasurer
- Prof K Jaya Sankar
- Col Balraj Anand (Retd)
- Shri G Narendra Nath
- Prof Baswaraj Gadgay
- Prof H S Bhatia
- Dr K Seetha Ram Babu
- Shri Ramesh Gorantala
- Dr C P Dwivedi
- Ms Anupma Sharma
- Dr R K Sinha
- Dr R K Upadhyay
- Shri Hari Kumar R
- Shri R N Lahiri - Ex-Chairman, IETE Kolkata
- Prof (Dr) Ajay Kumar Ray - Ex Director, IIEST Shibpur
- Shri Taranjit Singh - MD, JIS Group
- Shri P S Biswas - Ex-Chairman, IETE Kolkata
- Prof (Dr) Paramartha Dutta - Visva Bharati, Santiniketan, Bolpur
- Prof (Dr) Ujjal Moulik - JU, Kolkata
- Dr Satyam Roy Choudhuri - Techno India Group
- Dr Satyajit Chakraborty - VC, UEM Kolkata
- Shri Pavan Vovveti, Seattle, USA
- Shri Sairamakrishna Buchi Reddy Karri, USA, Michigan

Technical Programme Committee (TPC)

- Dr Shiv Kumar
- Prof Ajay Agarwal
- Dr R D Kharadkar
- Dr K Gnaneshwar Rao
- Dr S Arumuga Perumal
- Shri Satyanandan
- Dr A Sarveswara Rao
- Ms Meenakshi Vij
- Dr S S Saini
- Dr N Srinivasa Rao
- Dr Shivajai B Ghungrad
- Shri G P Singh
- Dr Tarun Kumar Rawat
- Dr Sandip Patil
- Shri R K Khetan
- Dr Debashis De
- Dr P P Sarkar
- Dr Jyoti Sekhar Banerjee
- Dr Soumen Mukherjee, RCCIIT
- Dr Arpan Deyasi, RCCIIT
- Mr Arup Kumar Bhattacharjee, RCCIIT
- Mr Snehasis Banerjee
- Mr Sandeep Sengupta
- Dr Sudipta Sahana
- Dr Radha Krishna Bar
- Dr Raktim Chakraborty

Publicity Committee (IETE Kolkata Centre)

- Dr Jyotsna Kumar Mandal
- Shri Partha Sarathi Biswas
- Dr P P Sarkar
- Dr Aniruddha Nag
- Ms Sharmila Ghosh, Immdt Chairperson, Kolkata Centre

Resource Generation Committee

- Shri P S Biswas, Past Chairman, IETE Kolkata Centre
- Dr Aniruddha Nag, IETE Kolkata Centre
- Dr Soumya Paul, IETE Kolkata Centre

Organizing Committee

- Dr Partha Pratim Sarkar
- Mr Sandip Saha, Registrar, RCCIIT
- Dr Tapasi Bhattacharjee
- Dr Debarati Dey Roy
- Dr Soma Bandyopadhyay
- Dr Priti Deb
- Dr Rajeev Chatterjee
- Mr Arijit Majumdar, SA, RCCIIT
- Dr Subhram Das
- Dr Subhankar Bhattacharjee
- Shri Niladri Roy
- Shri Soumya Ray
- Shri Snehasis Banerjee
- Shri Dibyendu Majumder
- Shri Shibendra N Roy Chowdhuri
- Dr Aniruddha Nag

IETE - Ram Lal Wadhwa Awardee - 2026

Dr B K Das

Director General (Electronics & Communication Systems), DRDO
Bangalore
Email: bkdas@yahoo.com

Title: Modern Warfare & India's Preparedness

Abstract

The character of warfare is undergoing a profound transformation and becoming predominantly digital. The battlefields of today and tomorrow extend far beyond conventional domains, encompassing cyber space, outer space, the electromagnetic spectrum, information and cognitive domains, autonomous systems, artificial intelligence, unmanned platforms, precisioan weapons, and increasingly interconnected command-and-control networks. Technological superiority, speed of decision-making, resilience of critical infrastructure, and the ability to integrate multiple domains are becoming decisive factors in national security.

This talk, **"Modern Warfare & India's Preparedness,"** examines the changing nature of conflict and the implications of emerging technologies for India's defence preparedness. It will explore how mission sensors, electronic warfare, directed energy systems, artificial intelligence, drones and counter-drone systems, space-based capabilities, quantum technologies, advanced communications, and sensor networks are reshaping military operations. Particular emphasis will be placed on the convergence of these technologies and the emergence of network-centric, multi-domain warfare.

The talk will also underline the critical role that engineers, researchers, technologists, entrepreneurs, and professional institutions can play in strengthening India's technological and strategic autonomy.

The central message is that preparedness for modern warfare is not simply a question of acquiring advanced weapon systems; it is a comprehensive national endeavour requiring technology, talent, innovation, resilience, integration, and strategic foresight. India's ability to harness its vast scientific and engineering capabilities will be a key determinant of its security and strategic autonomy in the decades ahead.

✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧

Speaker's Biography

Dr B K Das is presently serving as Director General (Electronics & Communication Systems), DRDO, since 2022. Earlier, he served as Director, Integrated Test Range (ITR), Chandipur, for five years and Director, IRDE and DEAL, Dehradun, for two years. He has made significant contributions to the Indian Missile Program for over three decades, particularly in Test and Evaluation of advanced missile systems.

Dr Das holds a BTech in Electronics & Communication Engineering from University College of Engineering, Burla, where he was University Topper and received the Best Graduate Gold Medal. He obtained his MTech in Computer Engineering and PhD in Image Processing from IIT Kharagpur, securing the Institute Topper position and Best Thesis Award.

Under his leadership, major indigenous capabilities were developed in radar systems**,** electro-optics, telemetry, electronic warfare, directed-energy weapons, communication systems, missile test systems and counter-drone technologies. He played a key role in transforming ITR into a highly advanced indigenous test range and established state-of-the-art test facilities.

As DG (ECS), he has driven several strategic defence programs and strengthened collaboration among DRDO, academia and industry, facilitating transfer of advanced technologies to Indian industry and contributing significantly to the *Atmanirbhar Bharat* initiative.

Dr Das has received numerous national and international honours, including the Distinguished Alumnus **Award of IIT Kharagpur (2026)**, Fellow of INAE, several Honorary Doctorates and prestigious national awards for excellence in defence technology, engineering, image processing and electro-optics.

IETE - IRSI (83) Main Awardee - 2025

Dr. Ram M. Narayanan

Distinguished Professor of Electrical Engineering
The Pennsylvania State University
University Park, PA 16802, USA
Email: ram@engr.psu.edu

Title: Nonlinear and Harmonic Radar

Abstract

Nonlinear radar exploits the difference in frequency between radar waves that illuminate and are reflected from electromagnetically nonlinear targets. Nonlinear radar differs from traditional linear radar by offering high clutter rejection and is particularly suited to the detection of devices containing metals and semiconductors. Examples include tags for tracking insects, tags worn by humans for avoiding collisions with vehicles, or for monitoring vital signs. Such tags contain a radio-frequency (RF) nonlinearity, often a Schottky diode, connected to a suitable antenna. Targets with inherent nonlinearities, such as metal contacts, semiconductors, transmission lines, antennas, filters, and ferroelectrics, also respond to nonlinear radar. A nonlinear radar can be used to locate devices whose emissions exceed permitted limits, allow security personnel to detect unauthorized radio electronics in restricted areas, or enable first-responders to locate personal electronics during emergencies. Harmonic radar is a special type of nonlinear radar that transmits one or multiple frequencies and listens for frequencies at or near their harmonics.

The talk will address the design and application of nonlinear and harmonic radar, their advantages and limitations compared to conventional linear radar, and some unique applications of harmonic radar systems.

✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧ ✧✧✧

Speaker's Biography

Professor Ram Narayanan received his B.Tech. from the IIT Madras in 1976, and his Ph.D. from the UMass Amherst in 1988, both in electrical engineering. From 1976–1983, he was an R&D engineer at Bharat Electronics Ltd., Ghaziabad, where he developed microwave communications subsystems and equipment. His Ph.D. research focused on millimeter-wave radar scattering from natural surfaces such as vegetation and snow. In 1988, he joined the Electrical Engineering Department at the University of Nebraska where he last served as Blackman and Lederer Professor. Since 2003, he is a Professor of EE at Pennsylvania State University, recently elevated to Distinguished Professor. He has coauthored over 200 journal articles and over 500 conference publications. He is a Fellow of IEEE, SPIE, and IETE. He received the 2017 IEEE Warren White Award for Excellence in Radar Engineering and the 2025 IETE-IRSI (83) Award for his contributions to radar. He received the 2003 Distinguished Alumnus Award from IIT Madras. His current research interests are cognitive radar, harmonic radar, noise radar, through-barrier detection and imaging, and information processing.

5th International Conference

on

Network Security and Blockchain Technology

(ICNSBT 2026)

In Conjunction with AIC 2026

Jointly organized by

The Institution of Electronics and Telecommunication Engineers (IETE), Kolkata Centre

and

Computer Society of India, Kolkata Chapter

In association with

RCC Institute of Information Technology (RCCIIT), Kolkata

Venue

Dr Jaya Deb Roy Auditorium
RCC Institute of Information Technology (RCCIIT)
Canal South Road, Beliaghata
Kolkata-700015, West Bengal, India

on

September 25 - 26, 2026

Technical Co-Sponsors

Academic Partner

Kolkata Chapter

ABSTRACT

Table of Contents

Adversarial Attack Detection in Software-Defined Network (SDN) using Explainable AI and Graph Neural Networks (GNN)

Yeddula Bhaskar Reddy[1], (bhaskar1884@grietcollege.com)
[1]Department of AIML, Assistant Professor, GRIET, Telangana, India
K geetha[2], (kgeethapapers@gmail.com)
[2]Department of AIML, Assistant Professor, GNU, Telangana, India
Divya Sri Koppolu[3], (divyasri90koppolu@gmail.com)
[3]Department of AIML, Assistant Professor, GNU, Telangana, India

Abstract

Although it is extremely susceptible to DDoS attacks, software-defined networking (SDN) has lately surfaced as a new, adaptable, and programmable network architecture. Traditional machine learning algorithms are vulnerable to adversarial assaults and are unable to effectively recognize the complex relationships seen in network traffic. This research proposes a unique robust SDN-based model for adversarial attack detection using GNN and XAI.

First, GCN-based categorization is carried out after the network traffic is converted to a graph using K-nearest neighbor (KNN) relations. We created adversarial samples using FGSM and PGD techniques to assess the robustness of our model. In order to differentiate between genuine and altered traffic, an adversarial detector was also trained using the acquired embeddings. First, GCN-based categorization is carried out after the network traffic is converted to a graph using K-nearest neighbor (KNN) relations. We created adversarial samples using FGSM and PGD techniques to assess the robustness of our model. In order to differentiate between genuine and altered traffic, an adversarial detector was also trained using the acquired embeddings.

The findings of our experiment show that the proposed framework maintains its robustness against adversarial perturbations and produces superior classification accuracy of 99.61% sans hostile attacks. With an accuracy of 96.36%, an adversarial detector trained on our model is able to distinguish between antagonistic traffic.

Keywords **— Software-Defined Networking (SDN), Graph Neural Networks (GNN), Explainable Artificial Intelligence (XAI), Cybersecurity, Adversarial Attacks, Network Traffic Analysis, Intrusion Detection, Real-Time Monitoring.**

A Blockchain Based Framework for Land Registry System

Swati Sri Thingbaijam[1] and Oinam Bidyapati Chanu[2]
[1]National Institute of Technology, Manipur, India
thingbaijamswatisri@gmail.com
[2]oinambidyapati@nitmanipur.ac.in

Abstract

Land registry systems in many countries, particularly in India, continue to rely on centralized and paper based processes that are vulnerable to fraud, corruption, data tampering and ownership disputes. This paper proposes a blockchain based decentralized application (DApp) framework named LandChain for land registration and ownership transfer, designed to eliminate the inefficiencies of traditional land registry systems. The proposed system leverages Ethereum smart contracts to enable transparent, immutable and tamper proof recording of land ownership and transactions. The framework incorporates five core functional modules accessible through a role based dashboard: land registration, administrative verification, verified lands management, land explorer and ownership transfer confirmation. Each module is implemented as a Solidity smart contract function and exposed through a React based DApp interface using MetaMask wallet integration. The system ensures that only administratively verified land records are made available for transfer and all historical ownership data remains permanently and immutably accessible on the blockchain. Experimental evaluation on a local Ganache blockchain with sample land records from Manipur demonstrates that the proposed system significantly improves transparency, reduces fraudulent transactions and eliminates dependency on trusted third parties in land administration.

Keywords **- Blockchain · Land Registry · Smart Contracts · Ethereum · Decentralized Application · DApp · Land Ownership Transfer · Meta-Mask · LandChain**

A Secure Multimodal Biometric System Using Quantum Key-Based Cancelable Templates and Blockchain Integrity

Diptadip Maiti[1] and Madhuchhnda Basak[2]
[1]MCKV Institute of Engineering, Liluah, Howrah, West Bengal, India-711204
diptadip.maiti@mckvie.edu.in
[2]Techno International New Town, Newt own, Kolkata, West Bengal-700156
madhuchhanda.basak@tint.edu.in

Abstract

Traditional biometric authentication systems have issues with template compromise, weak revocability, and spoo_ng vulnerability. This study proposes a quantum-inspired cancelable multimodal biometric sys-tem that integrates_ngerprint and iris modalities to enhance security and performance. Deep convolutional neural networks are used to ex- tract discriminative features, which are then transformed into secure binary templates using a key-dependent cancelable transformation. A quantum-inspired key generation method that produces unlinkable, re-vocable, and non-invertible templates guarantees high entropy. Feature- level fusion combines complementary biometric features, and e_ective authentication is achieved by Hamming distance-based matching. The results of the experiment demonstrate strong AUC, low EER, and high accuracy. Ablation and security investigations demonstrate the e_ective- ness and robustness of the proposed strategy against inversion, linking, and key compromise attacks. The framework provides a secure and e_cient solution for high-security real-world applications.

Keywords **- Multimodal Biometrics · Cancelable Biometrics · Quantum- Inspired Security · Deep Learning · Feature-Level Fusion · Hamming Distance Matching.**

Dynamic Cryptographic Algorithm Adaptation in Heterogeneous IoT-Blockchain-Cloud Environments: A Trustless Orchestration Framework

Naina Parmar[1], Vatsal Shah[2]
[1]Gujarat Technological University (GTU), Ahmedabad, Gujarat, India
[1] Charusat University, Changa, Anand, Gujarat, India
[2] Birla Vishvakarma Mahavidyalaya, Anand, Gujarat, India
Corresponding author: naina.parmar@charusat.ac.in

Abstract

Due to conflicting trust models, evolving threat landscapes, and varying resource constraints, the convergence of blockchain, cloud computing, and the Internet of Things (IoT) poses previously unseen security challenges. Current static cryptographic systems do not meet the dynamic security requirements of this convergent environment. CryptoAdapt, a blockchain-orchestrated system that dynamically modifies cryptographic algorithms across IoT, blockchain, and cloud layers, is proposed in this study. The framework presents a three-tier adaptation engine that uses real-time contextual factors, such as threat intelligence feeds, device resource availability, data sensitivity classification, and regulatory jurisdiction requirements, to automatically choose, deploy, and validate cryptographic algorithms. CryptoAdapt facilitates safe, well-coordinated cryptographic transitions without generating exploitable vulnerabilities during migration windows by utilizing smart contracts as trust anchors and unchangeable policy enforcers. We implement a proof-of-concept using Hyperledger Fabric 2.4 and heterogeneous IoT hardware (ESP32, Raspberry Pi 4), present a formal security model based on the Universal Composability (UC) framework with full simulator construction, and assess performance overhead through extensive testbed experiments and large-scale simulation (10,000 nodes). The findings show that CryptoAdapt maintains a reasonable performance overhead (less than 15%) across all device categories while reducing security compromise windows by 73% when compared to static alternatives. Superior security-performance trade-offs are confirmed by comparative analysis against three cutting-edge baselines. The framework makes autonomic security for convergent cyber-physical systems more advanced.

Keywords- **Cryptographic Agility · Blockchain Orchestration · IoT Security · Adaptive Cryptography · Smart Contracts · Trustless Systems · Universal Composability · Post-Quantum Readiness.**

High-Integrity EHR Systems Powered by Intelligent Blockchain System

Pawar Bharat Ramdas [1], Dr. Sathyasri B.[2]
[1] Research Scholar, Department of Electronics and Communication Engineering,Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, 400 feet Outer Ring Road, Avadi, Chennai–600062, Tamil Nadu, India.
[2] Associate professor, Department of Electronics and Communication Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, 400 feet Outer Ring Road, Avadi, Chennai – 600062, Tamil Nadu, India.
bharat.pawar14@gmail.com[1], sathyasrib@veltech.edu.in[2]

Abstract

In today's era Managing electronic health records (EHRs) in a secure confident and private way is still a biggest challenge because patient data is very sensitive and cyber threats are getting more advanced and advnced.To tackle these issues, we have, we suggest a single, privacy-focused system that combines blockchain, lightweight encryption methodology and deep learning for detecting unusual activity or malicious activity .This system uses a hybrid blockchain setup with edge devices.A permissioned Ethereum blockchain is used to keep a tamper-proof or unchangeable record and allow decentralized control, while the edge devices handle simple encryption tasks to make the blockchain more efficient and reliable. Patient data is protected using symmetric encryption, and the keys are shared securely through Decentralised Attribute-Based Encryption , which lets you control who can access specific parts of the data based on their attributes of system.To make sure only (CIA) authorized people can change or view EHRs, the system also uses Attribute-Based Signatures to check that all actions are done by the right people in right way.

Keywords **- Blockchain, security, TCN, EHR**

A Decentralized Trust Management Framework for VANETs Using SUMO Simulation and Blockchain Smart Contracts

Umesh Bodkhe
Department of Computer Science and Engineering, School of Technology, Nirma University, Ahmedabad, Gujarat, India [umesh.bodkhe@nirmauni.ac.in]

Abstract

Vehicular Ad-hoc Networks (VANETs) are increasingly relied upon for safety-critical applications such as collision warnings, congestion alerts, and road-side coordination. Conventional VANET architectures depend on centralized trusted authorities for message validation and storage, introducing single points of failure, latency bottlenecks, and vulnerability to Sybil and message-spoofing attacks. This paper presents a decentralized VANET framework that integrates microscopic traffic simulation (SUMO) with an Ethereum-based Decentralized Application (DApp) through a TraCI-to-Web3 bridge. To enhance a baseline smart contract architecture, we introduce two key mechanisms: a priority-aware off-chain batching scheme that stores low-priority telemetry data through Merkle root hash commitments while ensuring immediate blockchain submission of safety-critical alerts, and an on-chain reputation-scoring mechanism for real-time identification of misbehaving vehicles. The effectiveness of the proposed framework is validated using a realistic OpenStreetMap-derived road network simulated in SUMO, with vehicular event streams connected to a private Ethereum test network (Ganache) via Web3.py. Our experimental results across vehicle densities of 50–500 demonstrate up to 56% reduction in average transaction confirmation latency and up to 54% reduction in gas cost for non-critical events compared to a naive per-event on-chain submission baseline, while the reputation mechanism achieves a true positive misbehavior-detection rate exceeding 90% at a 10% false-positive rate. These results indicate that selective on-chain anchoring combined with reputation-based filtering can make blockchain-backed VANETs practically scalable without compromising the integrity guarantees that motivate decentralization in the first place.

Keywords**- VANET · Blockchain · Decentralized Application · SUMO · TraCI · Smart Contracts · V2X Security.**

Cutting the Right Links: Intelligent Edge Pruning with Attention and Pattern Mining for Rumor Control

Akash M and Himansu Sekhar Pattanayak
National Institute of Technology Kurukshetra, India

Abstract

Rumors can travel fast and uncontrollably through online social networks, posing serious threats to public discourse, institutional trust and societal stability. Existing rumor containment approaches either blindly block the whole nodes or score edges by a single topological property, without considering the joint optimization of rumor suppression and structure preservation. In this paper, we propose a novel framework, called FGTHEP (FP-Growth Transformer Hybrid Edge Pruning), to effectively determine and prune the network edges to achieve the maximum reduction of rumors while ensuring the connectivity of the graph. We propose an approach that builds an 8-dimensional feature representation for each candidate edge, encoding Independent Cascade spread frequency, Jaccard neighborhood redundancy, PageRank-based endpoint influence, normalized degree, local clustering coefficient, bridgepenalty estimation, spread-influence coupling and FP-Growth-mined coactivation scores. Each of these features is characterized by one of the four-head attention mechanisms, like the transformer architecture, with each head optimizing a specific feature: Propagation targeting, Redundancy exploitation, Bridge-Avoidance regularization, and Co-occurrence pattern selection. The per-edge attention weights are produced by the global softmax normalisation and then aggregated with the weighted aggregation to create a composite removal score. Experiments on various real-world Facebook network under the Independent Cascade model show that FGTHEP effectively improves rumor reduction compared to random removal and a standalone three-head attention approach (MHAEP), while guaranteeing less number of disconnected components that cannot be guaranteed by any competing baseline.

***Keywords*- Rumor minimization, social network, edge pruning, multihead attention, Independent Cascade model, FP-Growth, frequent pattern mining, graph connectivity, bridge detection, influence minimization, network robustness.**

A Hybrid AI Model Based on Explainable Graph Transformers for Enhancing Financial Security and Operational Resilience in Banking Fraud Detection Systems

Yousef Alasadi[1],, Hamid Ali Abed AL-Asadi[2], Zaid Ameen Abduljabbar[3], Vincent Omollo Nyangaresi[4]*
[1]Alkunoze University, Basrah 61004, Iraq yousifalasadi8@gmail.com
[2]Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq {hamid.alasadi, zaid.ammen}@uobasrah.edu.iq
[3]Huazhong University of Science and Technology, Shenzhen Institute Shenzhen, China
[4]Department of Computer Science and Software Engineering Jaramogi Oginga Odinga University of Science and Technology, Bondo, Kenya
**Corresponding Author*

Abstract

The conventional fraud detection systems are unable to balance between real-time performance, adaptability and interpretability, which tends to be an opaque black-box model, restraining regulatory compliance and confidence of stakeholders. The paper presents an AI hybrid model, which is Explainable Graph Transformers, as a way of maximizing financial safety and operational robustness within banking fraud detection systems. The given model embodies the banking ecosystem as a knowledge graph that is dynamic, meaning nodes that describe and maintain it represent accounts, customers and devices and edges are determined by transactional and relationship interactions. Graph Transformer is the composite detection engine that is useful in modeling of topology-sensitive and convoluted fraud patterns. This ensures flexibility to any new and zero-day fraud methods by dynamically changing the model parameters based on real-time feedbacks. The framework is expected to enhance resilience under stress conditions and improve regulatory trust through interpretable and auditable decision-making processes.

***Keywords*- Banking Fraud Detection, Graph Learning, Deep Reinforcement Learning, Explainable AI, Operational Resilience, Financial Security.**

PhishCRC: Conformal Risk-Controlled Cascades for Phishing URL Detection

Kritik Mishra and Priyanka Ahlawat
Department of Computer Engineering
National Institute of Technology Kurukshetra, Haryana, India
kritikmishra1301@gmail.com, priyankaahlawat@nitkkr.ac.in

Abstract

State-of-the-art phishing URL detectors report single-number accuracy on IID test splits but expose neither (i) a distribution-free guarantee on the false-negative rate that a security operator can contract against, (ii) a principled abstain-and-defer mechanism that trades a small fraction of cloud calls for hard guarantees, nor (iii) an evaluation against the emerging threat of phishing URLs generated on the fly by large language models. We present PhishCRC, a conformal riskcontrolled cascade for phishing URL detection. PhishCRC wraps three classical edge classifiers (logistic regression, LightGBM, random forest)

in split, Mondrian, and risk controlling prediction sets [23,19,4] to obtain a per-tier confidence assessment with marginal coverage $1 - \alpha$ guaranteed for any data-generating distribution that is exchangeable with the calibration set. We extend the design to streaming phishing feeds with Gibbs-Candès adaptive conformal inference [8], which keeps the longrun miscoverage close to the target α even under temporal drift. Finally, we construct the first benchmark of LLM-generated adversarial phishing URLs (2 000 URLs across 32 brands and 10 evasion techniques generated by a seeded procedural attacker, with a Llama-3.1 8B drop-in path also released) and show that nonconformity scores transfer naturally to flag this out-of-distribution attack. On a 1.6M-URL corpus assembled from URLhaus, the Phishing.Database mirror, OpenPhish, a Kaggle URL set, and the Cisco-Umbrella, Tranco, and Majestic benign toplists, PhishCRC delivers the target marginal coverage to within `}0.005 across α ε {0.005, . . . , 0.10}, controls the FNR below 0.005 at $\delta = 0.05$, and resolves 44% of requests at the cheapest tier with end-to-end p95 latency ≈ 3 ms while preserving the global coverage guarantee.

Keywords- **Phishing URL detection · conformal prediction · risk controlling prediction sets · adaptive conformal inference · cloud-edge cascade · LLM-generated phishing · distribution-free guarantees.**

Lightweight Certificate-Based Authentication Protocol for Vehicular Ad Hoc Networks

Rezq Raad[1], Zaid Ameen Abduljabbar[1,2,], Vincent Omollo Nyangaresi[3,4], Samson Abura[3], Hamid Ali Abed AL-Asadi[4], Abdulla J. Y. Aldarwish[5], Zaid Alaa Hussien[6], Ali Hasan Ali[7,8,9]*
[1]Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq
{rezq.raad, zaid.ameen, hamid.abed, abdullajas}@uobasrah.edu.iq
[2]Shenzhen Institute, Huazhong University of Science and Technology, Shenzhen, China
[3]Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science and Technology, Bondo 40601, Kenya.
{vnyangaresi@jooust.ac.ke, sba.abura@gmail.com}
[4]Department of Applied Electronics, Saveetha School of Engineering, SIMATS, Chennai 602105, Tamil Nadu, India
[5]Department of Management and Marketing, College of Industrial Management for Oil and Gas, Basrah University for Oil and Gas, Basrah 61004, Iraq
mustafa.alsibahee@buog.edu.iq
[6]Information Technology Department, Management Technical College, Southern Technical University, Basrah 61004, Iraq
zaid.alaa@stu.edu.iq
[7]Department of Mathematics, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq
[8]Technical Engineering College, Al-Ayen University, Thi-Qar 64001, Iraq
[9]Institute of Mathematics, University of Debrecen, Pf. 400, H-4002 Debrecen, Hungary.
ali.hasan@science.unideb.hu
[*]Corresponding Author

Abstract

Smart cities have enhanced remote monitoring and control of intelligent transportation systems, home appliances and sensory devises, which has helped enhance comfort, efficiency and quality of life. Nevertheless, the transmission of sensitive information across public channels exposes the smart city networks to numerous external and internal threats. In addition, the openness of the transmission channel implies that there are possibilities of unauthorized access which can threaten the confidentiality of sensitive data. To mitigate against these security threats, robust authentication mechanisms must be implemented in these intelligent home networks. To this end, numerous authentication schemes have appeared in literature, based on a myriad of cryptographic mechanisms. Unfortunately, the authentication and session key negotiation phases of these existing protocols in characterized with inefficiencies in terms of computational and communication overheads. In this paper, a lightweight authentication protocol is developed which effectively balances between low overheads and robust security. As such, it is suitable for deployment in intelligent homes where smart devices such as sensors are resource-limited. In particular, it incurs the least computation overheads at relatively low communication costs. In addition, it is demonstrated to resist a wide range of typical smart city security threats such as impersonations, eavesdropping, replays and session key compromise.

Keywords- **Smart homes, security, attacks, privacy, authentication, efficiency, intelligent homes.**

DGS-LOM: A Decentralized Group Signature Framework for Secure Blockchain-Based Land Ownership Management

Yogesh Sharma[1] and Sanjay Sharma[2]
[1]Department of Mathematics and Computer Applications, Maulana Azad National Institute of Technology, Bhopal, Madhya Pradesh - 462003, Bharat
yogeshs.scs@gmail.com
[2]sanjaysharma.nitb@gmail.com

Abstract

The development of blockchain technology has been seen as a potential solution to enhance transparency, integrity and auditability in land administration systems. Traditional blockchain-based land registration systems, however, tend to reveal land ownership data to other network participants, raising privacy concerns and hindering the adoption of these systems in actual governance contexts. In order to solve the above problem, we proposed a group signatures framework that allows land owners to prove ownership of a land transaction without revealing their identity, avoids the single point of trust of a group manager, and increases the transparency of governance. To facilitate land registration, an Ethereum-compatible smart contract implementation was developed. The practical gas consumption and low transaction latency are shown by performance analysis, and the throughput is stable even when the workload increases. The findings suggest that the proposed framework provides a good balance between privacy protection, accountability, and operational efficiency, making it a potential solution for secure blockchain-based ownership management systems.

***Keywords*- Blockchain · Land Registry · Privacy Preservation · Decentralized Group Signatures · Smart Contracts · Digital Governance · Ethereum.**

CredChain: An Efficient Hybrid Blockchain Framework for Secure Digital Credential Verification

Subhranil Nandy, Harshit Kumar, Pallab Mandal, and Indrajit Banerjee
Indian Institute of Engineering Science and Technology, Shibpur, India
iamsubhranil.nandy@gmail.com

Abstract

Organizational digital revolution requires secure, verifiable, and immutable solution to credential verification. Centralized databases utilized by governmental bodies, enterprises, and educational institutions have a single point of failure, risk of data manipulation, and slow interorganizational verification process. This paper describes a blockchain framework for credential verification. Management of Decentralized Identifiers (DIDs) and Role-Based Access Control (RBAC) is performed using Ethereum smart contracts for authorized access. To reduce costs and optimize efficiency, the hybrid approach stores the document data off-chain and its Keccak-256 hash on-chain. Wallet-based signing eliminates the server-side security issues associated with private keys. Dynamic QRcode based procedure allows third-party validation for authenticity. The approach consumes around 430,000 gas for credential issuance and reduces total costs by about 34% (saving over 218,000 gas per transaction). Credential issuance and verification take around 420 ms and 325 ms respectively.

***Keywords*- Blockchain-based credential verification · Decentralized Identifiers (DIDs)· Hybrid Off-Chain Storage · Ethereum Smart Contracts · Role-Based Access Control (RBAC).**

A Synergistic PSO-WOA Optimized SVD-DWT Framework for Robust Digital Image Watermarking

Santa Singh (Vidyasagar University) santasingh807@gmail.com
Partha Chowdhuri (Vidyasagar University) prc.email@gmail.com
Pabitra Pal (Swami Vivekananda University, Kolkata) pabipaltra@gmail.com
Sukhendu Bikash Giri (Vidyasagar University) sbgiri999@gmail.com

Abstract

This work presents a resilient watermarking strategy for digital images utilizing Singular Value Decomposition (SVD) with the combination of Particle Swarm Optimization (PSO), and the Whale Optimization Algorithm (WOA). In this method the host image is partitioned into appropriate blocks for embedding and then the singular values are altered using the SVD to embed the watermark. Suitable block locations are determined for watermark embedding based on the metrics related to imperceptibility and robustness using PSO. The scaling factor β is optimized by the WOA. The proposed SVD-PSO-WOA method is verified by various standard metrics. The experimental results reveal that PSNR is about 56.34 dB, SSIM is equal to 0.9994, NCC is equal to 0.9988, BER is equal to 0.0013, and MSE is equal to 0.1514. The experimental results clearly illustrate that the suggested approach achieves exceptional imperceptibility while guaranteeing the robust and reliable extraction of the embedded watermark.

***Keywords*- Discrete Wavelet Transform (DWT) · Particle Swarm Optimization (PSO) · Whale Optimization Algorithm (WOA) · Singular Value Decomposition (SVD) · Image Watermarking.**

HalluciGuard: A Multi-Agent Verification Framework for Explainable Hallucination Detection in Large Language Models

Varun Shukla[1], Badiea Abdulkarem Mohammed[2], Neelam Srivastava[3], Atul[1], and Mehul Kumar Das[1]
Allenhouse Institute of Technology, Kanpur, Uttar Pradesh, India
University of Ha'il, Ha'il, Saudi Arabia
Institute of Engineering and Technology, Lucknow, Uttar Pradesh, India
varun.shuklaa@gmail.com, b.alshaibani@uoh.edu.sa,
neelam.srivastava@ietlucknow.ac.in, atulverma15704@gmail.com,
dasmehulkumar08@gmail.com

Abstract

Large Language Models (LLMs) are widely used for question answering, education, healthcare, software development, and decision support,but they frequently generate hallucinations: fluent responses that are factually incorrect, unsupported, or logically inconsistent. This paper implements and evaluates HalluciGuard, a multi-agent verification framework for explainable hallucination detection. The framework decomposes verification into response generation, evidence retrieval, factual verification, logical reasoning, confidence estimation, explanation generation, and decision fusion. Instead of returning only a binary prediction, HalluciGuard produces a hallucination label, hallucination risk estimate, and evidence-based explanation. The proposed model combines semantic evidence similarity, factual consistency, logical consistency, and confidence scoring into a unified decision rule. We evaluate the implementation on TruthfulQA, HaluEval, FaithDial, and FActScore, and compare it with RAG, SelfCheckGPT, Chain-of-Verification, self-consistency verification, and single-agent fact verification. Results are reported using classification, explainability, ablation, and latency metrics. The work contributes a compact, modular, and interpretable verification architecture for improving the reliability of LLM-generated content.

***Keywords*- Large language models · Hallucination detection · Multiagent systems · Explainable AI · Fact verification.**

XMal-Edge: An Explainable Malware Detection and Response Framework for Edge Computing Using LLM-Augmented Ensemble Learning

*Nandan Sharma[1], Sree Pranathi Pallela[2], Sanatya Singh[3], Somnath Banerjee[*4], Sohail Saif[4]*
[1]BC Public Service, Canada
[2]Elanco,USA
[3]Munich Reinsurance, USA
[4]Maulana Abul Kalam Azad University of Technology, West Bengal, India
*somnathbanerjeedwbi@gmail.com (*Corresponding Author)*

Abstract

The rapid growth of Internet of Things (IoT) devices and edge computing has increased malware threats while imposing stringent latency and resource constraints that limit the effectiveness of cloudbased security solutions. This paper presents XMal-Edge, an explainable malware detection framework that integrates large language model (LLM)-augmented feature extraction, heterogeneous stacking ensemble learning, SHapley Additive exPlanations (SHAP), and adaptive Next-Generation Firewall (NGFW) policy orchestration for real-time edge security. The proposed framework combines TF-IDF representations with CodeBERT contextual embeddings to capture both statistical and semantic characteristics of API call sequences and network payloads. Malware detection is performed using a stacking ensemble of Random Forest, Gradient Boosting Machine, and LightGBM classifiers with a Logistic Regression meta-learner, while TreeSHAP provides interpretable feature attribution for automated NGFW policy generation. Experimental evaluation on the CIC-MalMem-2022, EMBER-2018, and EdgeMal-2024 datasets (801,443 samples) demonstrates 98.47% accuracy, 97.89% precision, 98.12% recall, 98.00% F1-score, and 0.997 AUC, outperforming existing approaches. Furthermore, the proposed framework reduces the false positive rate by 34.2% and achieves 42.1 ms inference latency with a 19.6 MB quantized model on an NVIDIA Jetson AGX Xavier, demonstrating its suitability for accurate, interpretable, and resource-efficient edge malware detection.

***Keywords*- Edge Malware Detection, CodeBERT, SHAP, Stacking Ensemble Learning , NGFW.**

Homophily-Validated Feature-Similarity Graphs for GraphSAGE-Based Phishing Website Detection

Shubhranshu Gorai (National Institute of Technology, Durgapur) gorai17subho@gmail.com
Saibal Majumder (Dr. B.C. Roy Engineering College, Durgapur) saibal.majumder.1729@gmail.com
Suchandra Banerjee (Dr. B.C. Roy Engineering College, Durgapur) mailnmeetsuchandra@gmail.com
Chandan Bandyopadhyay (Dr. B.C. Roy Engineering College, Durgapur) chandanb.iiest@gmail.com
Diganta Das (Sathyabama Institute of Science and Technology, Chennai) mr.diganta.das@gmail.com

Abstract

Phishing websites remain a serious cybersecurity threat because they deceive users into revealing sensitive information through manipulated URLs and webpages. Traditional machine learning models can detect phishing websites using URL, domain, hyperlink, and webpage related features, but they usually treat each sample independently and ignore relationships among similar website samples. This paper proposes a graph-enhanced phishing website detection framework that combines machine learning baselines, GraphSAGE-based graph learning, and probability-level fusion. A weighted KNN feature-similarity graph is constructed from standardized website features using cosine similarity and validated through edge-label homophily. All evaluated graph settings achieved homophily values above 0.88, indicating meaningful class-related neighborhood structure. GraphSAGE is used to learn neighbourhoodaware website representations, and its predictions are combined with Gradient Boosting using validation-selected fusion weight and decision threshold. Experiments were performed on a balanced phishing website dataset containing 11,430 samples and 81 numerical features after preprocessing. GraphSAGE achieved the highest F1-Macro score of 0.9598, while the hybrid model achieved the highest phishing recall of 0.9772. The results show that feature-similarity graph learning provides useful neighborhood information for phishing detection, particularly by reducing missed phishing websites.

***Keywords*- Phishing Detection · GraphSAGE · Graph Neural Network · Gradient Boosting · Cybersecurity.**

A Crypto-Agile Zero Trust Framework for Quantum-Safe CBDC Transaction Processing Using NIST PQC Standards

Krishnaveni Palanivelu [1]
Independent Researcher, Dallas, TX, USA
krishnavenipalanivelu@gmail.com

Abstract

Central Bank Digital Currencies (CBDCs) are moving from pilots to national-scale deployment across more than 130 countries. Their cryptographic foundations, ECDSA signatures and RSA-based key exchange, are vulnerable to quantum attack via Shor's algorithm, and adversaries are already executing "Harvest Now, Decrypt Later" (HNDL) strategies, archiving encrypted CBDC data today to decrypt once cryptographically relevant quantum computers (CRQCs) arrive. Existing CBDC frameworks address quantum-resistant cryptography or Zero Trust access control in isolation, without a cohesive architecture enforcing both while retaining the agility to track the evolving NIST PQC landscape. This paper proposes CA-ZT-CBDC, a Crypto-Agile Zero Trust Framework for Quantum-Safe CBDC Transaction Processing aligned with NIST FIPS 203 (CRYSTALS-Kyber), 204 (CRYSTALS-Dilithium), and 205 (SPHINCS+). A modular Cryptographic Abstraction Layer (CAL) decouples signing and key exchange from specific PQC implementations, enabling algorithm rotation without application-layer disruption, while Zero Trust enforcement combines SPIFFE workload identity, OPA authorization, and hybrid classical-PQC TLS 1.3. An analytical evaluation grounded in published PQC and Hyperledger Fabric benchmarks projects elimination of HNDL exposure, ~90-second algorithm rotation, and ~3.2 ms mean latency overhead, within the sub-10 ms retail threshold. To our knowledge, this is the first work to jointly address crypto-agility, Zero Trust enforcement, and NIST PQC alignment for CBDC transaction processing.

***Keywords*- Crypto-Agility · Zero Trust Architecture · CBDC Security · Post-Quantum Cryptography · NIST PQC · CRYSTALS-Dilithium · CRYSTALS-Kyber · Blockchain · Digital Currency · HNDL.**

Comparative Analysis of Hybrid Convolutional Neural Networks and Adversarial DCT Autoencoders for Trustworthy Digital Watermark Detection

Prasenjit Patra
(IIT, KGP) prasenjitkumarpatra@gmail.com

Abstract

The protection of digital media requires strong, understandable, and secure authentication systems. The difficulty of unambiguously classifying invisible watermarks lies in their level of imperceptibility and high sensitivity to conventional image processing operations. The proposed paper considers nine Convolutional Neural Networks (CNNs) that systematically combine spatial, statistical, and frequency-domain data to classify watermarked and original images. The analysed models include baseline networks that use pure pixel data, full-raw-pixel networks, and Deep CNNs (DCNNs) with specific feature fusions, e.g., edge entropy, spatial Kullback-Leibler divergence (KLD), and discrete wavelet transform (DWT). Moreover, we present and discuss a new Discrete Cosine Transform (DCT)-based autoencoder model, which serves as a detection and adversarial embedding pipeline. It has been shown experimentally that conventional CNN classifiers are not very effective at detecting subtle structural changes, with a baseline validation accuracy of only 72%. Conversely, the DCNN combined with the Spatial KLD achieves a validation accuracy of 94%, demonstrating better generalisation and greater interpretability. The experiment demonstrates that latent-space autoencoding and feature-level fusion significantly enhance detection security and robustness, providing a highly reliable architecture for authenticating media.

***Keywords* - Convolutional Neural Networks· Trustworthy AI· Digital Watermark Detection · Spatial Kullback-Leibler Divergence · Discrete Wavelet Transform · DCT Autoencoder.**

Anomaly Detection for IoT Networks using Hybrid GAT-GCN with Dynamic Contextual Similarity and Tuned Behavioral Drift Score Analysis

Shubham Kumar[1], Pari Gupta[2], Shenbaga Krithika Nb, Menaka Pushpa Ab, Radha Sa
[1]School of Advanced Sciences, Vellore Institute of Technology, Chennai Campus, Chennai, 600127, India
[2]School of Computer Science and Engineering, Vellore Institute of Technology, Chennai Campus, Chennai, 600127, India

Abstract

Modern cybersecurity threats that focus on the growing trend of insider threats pose serious obstacles to business security designs, which calls for a need for innovative solutions that detect anomalies. The sophistication and scale of network traffic instances may surpass the capacities of conventional detection systems, hence the necessity to consider contextual, temporal, and relational aspects when detecting fraud. In our work, we represent network flow instances through graph nodes and utilize contextual and behavioral similarities in edge representation to reflect intricate network relations. Through reconstructing the graph structure, the Hybrid GAT-GCN which is based on GCNs (Graph Convolutional Network), learns expressive latent node representations, recognizing anomalies based on graph structure irregularities. Tuned Behavioral Drift Score (TBDS) quantify the node deviation using feature and graph reconstruction errors. Compared to previous methods, this model provides superior anomaly detection performance and better interpretability. This work presents the potential of using graph-based methods for detecting insider threats. For the complete evaluation of the proposed method, we use the UNSW-NB15 Cybersecurity Dataset with comprehensive records of IoT network traffic flows. The implementation results also done with feature subset selection algorithms Correlation-based Feature Selection, Recursive Feature Elimination, Sequential Forward Selection, SelectFromModel, and combined feature selection strategies to find the best subset to achieves the remarkable outcomes. The results highlights that Hybrid GAT-GCN performs better than the baseline Graph Auto Encoder.

***Keywords*- Hybrid GAT-GCN, Cybersecurity, Temporal and Behavioral Similarity, Adversarial Robustness, Graph Neural Networks (GNNs), Graph Autoencoders (GAEs), Insider Threats and Anomaly Detection.**

A Robust Authentication Framework for Privacy and Security Preservation in Industrial Monitoring

Noor Ahmed Al-Mohammed[1] , Zaid Ameen Abduljabbar[1,2,] Vincent Omollo Nyangaresi[3,4] Samson Abura[3], Hamid Ali Abed AL-Asadi[1], Abdulla J. Y. Aldarwish[1], Zaid Alaa Hussien[6], Ali Hasan Ali[7,8,9]*
[1]Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq
{ noor.salem, zaid.ameen, hamid.abed,abdullajas}@uobasrah.edu.iq
[2]Shenzhen Institute, Huazhong University of Science and Technology, Shenzhen, China
[3]Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science and Technology, Bondo 40601, Kenya.
{vnyangaresi@jooust.ac.ke, sba.abura@gmail.com}
[4]Department of Applied Electronics, Saveetha School of Engineering, SIMATS, Chennai 602105, Tamil Nadu, India
[5]Department of Management and Marketing, College of Industrial Management for Oil and Gas, Basrah University for Oil and Gas, Basrah 61004, Iraq
mustafa.alsibahee@buog.edu.iq
[6]Information Technology Department, Management Technical College, Southern Technical University, Basrah 61004, Iraq
zaid.alaa@stu.edu.iq
[7]Department of Mathematics, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq
[8]Technical Engineering College, Al-Ayen University, Thi-Qar 64001, Iraq
[9]Institute of Mathematics, University of Debrecen, Pf. 400, H-4002 Debrecen, Hungary.
ali.hasan@science.unideb.hu

Abstract

The Industrial Internet of Things (IIoT) amalgamates various Internet of Things (IoT) and information communication technologies into industrial sectors to interconnect an assortment of devices, sensors and user end points. As such, IIoT is characterized with the generation of high volumes of sensitive industrial data. The surging number of smart devices interlinked in IIoT has led to the exchange of massive sensitive data in industrial sectors such as logistics management, smart cities, and smart manufacturing. The sheer vast amount of devices and heterogeneity in this IIoT ecosystem render the provision of secure and efficient communication among devices and users quite challenging. Nevertheless, the reliance on open wireless communication channels expose users, devices and networks to various privacy and security threats. In addition, the limited computational capabilities at the IIoT devices render it infeasible to deploy complicated cryptographic schemes. As such, the existing authentication protocols have continued to exhibit numerous vulnerabilities or high resource requirements. Any successful attack in this ecosystem can potentially lead to significant economic losses or operational disruptions. In this paper, a lightweight authentication framework has been developed that is demonstrated to be resistant against typical IIoT security threats such as impersonations, ephemeral secret leakages and key compromise attacks. In terms of performance, it is shown to incur the lowest communication and computation complexities.

***Keywords*- Authentication, WSN, IoT, IIoT, security, privacy, remote monitoring.**

Hybrid Machine Learning Framework for Insider Threat Detection and Response in Enterprise Systems

Dhinakaran M
Department of Electronics and Communicatiion Engineering
Government Polytechnic College
Thiruvallur
dhinakaran2612@gmail.com
Dr. P. Vinayagam
Department of Computer Science Engineering
Saveetha Engineering College
Chennai
vinayagamap@gmail.com

Abstract

Intrusions by insiders cause 30-50% of data intrusions, and their costs average over 15 million dollars. Thus, cybersecurity is an important issue in this field. This paper proposes a system based on federated learning, graph-based context analysis, reinforcement learning-based mitigation, and deep temporal modeling for detecting and responding to insider threats in a real-time manner. This system uses federated variational auto-encoders based on role to build behavioral baselines to keep privacy safe. It detects sequential anomalies using attention-based LSTM and records user-resource interaction patterns using GAT. A quantum mechanically inspired algorithm for optimal fusion of scores from various anomalous modalities is also proposed, and a Deep Q-Network is proposed to decide upon an optimal course of action in response to an anomaly in real-time. Using the proposed framework on Kaggle and Kilthub datasets, PR-AUC scores of 0.986 and 0.982, F1-scores of 0.981 and 0.978, and FPR @ 95% Recall of 0.018 are achieved, with an average detection latency of less than 0.91 seconds. As this system is better in response efficiency, generalization, and false positives compared to previous systems, it is optimal for real-time deployment in enterprises.

***Keywords*- Federated VariationalAutoencoder, Attention-based LSTM, Graph Attention Network, Quantum-inspired Risk Fusion, Deep Q-Network Mitigation, Cross-dataset Generalization, Role-based Behavioral Modeling.**

DRDS-Chain: An Adaptive Trust-Driven Explainable Federated Learning Framework with Blockchain-Verified Aggregation for Privacy-Preserving Malware and Intrusion Detection in Healthcare IoT Networks

Reeta Mishra
IILM University, Greater Noida
Ree76shok@gmail.com

Abstract

The rapid adoption of Internet of Things (IoT) devices in healthcare has transformed clinical workflows, remote patient monitoring, and real-time diagnostics. However, conventional intrusion detection systems typically rely on centralized machine learning, requiring sensitive clinical data to be transferred to remote servers, thereby increasing privacy risks and limiting compliance with regulations such as HIPAA and GDPR. Although Federated Learning (FL) enables decentralized model training without sharing raw data, existing FL-based solutions remain vulnerable to model poisoning attacks, unreliable client participation, and limited model interpretability. To address these challenges, this paper proposes **DRDS-Chain**, a secure and explainable federated intrusion detection framework that integrates dynamic client trust scoring, a permissioned blockchain-inspired hash-chained ledger for secure model update verification, trust-weighted federated aggregation, and SHAP-based explainability. The proposed framework is implemented and evaluated using a simulated five-hospital federated environment with non-IID data distribution on three publicly available benchmark datasets: UNSW-NB15, CIC-IDS2017, and N-BaIoT, where the latter serves as a behavioral proxy for IoMT device compromise.

Experimental results demonstrate strong detection performance, achieving F1-scores of 0.938, 0.988, and 0.9999 on the three datasets, respectively, while the blockchain ledger consistently provides tamper-evident verification of model updates. An extensive ablation study highlights the key contribution of the framework. Under mild poisoning (one malicious client among five), trust-weighted aggregation performs similarly to conventional equal-weight aggregation. However, under severe coordinated poisoning (two malicious clients with 90% label corruption), conventional aggregation degrades dramatically to an F1-score of 0.038, whereas DRDS-Chain maintains an F1-score of 0.923, representing an improvement of 88.5 percentage points. These findings demonstrate that integrating trust-aware aggregation with blockchain-based validation substantially enhances the robustness, security, and reliability of federated intrusion detection for privacy-preserving healthcare IoT environments while maintaining transparent and reproducible model decisions.

***Keywords*- Federated Learning, Blockchain, Trust-Aware Aggregation, Explainable AI, SHAP, Healthcare IoT, Malware Detection, Intrusion Detection, Model Poisoning, Privacy Preservation.**

Listen-and-Click: An Audio-Linked Graphical Password Scheme to Prevent Shoulder Surfing Attacks

Rajarajan Srinivasan (SASTRA Deemed University) srini.rajarajan@gmail.com
Vikash V (SASTRA Deemed University) viks892005@gmail.com
Manikandan R (SASTRA DEEMED UNIVERSITY) srmanimt75@gmail.com

Abstract

Graphical passwords are valued for their ease of memorability and enhanced security. They offer users a wide range of possibilities to create unique and personalized passwords. As a result, there has been growing interest among researchers in developing secure and user-friendly graphical password schemes. While graphical passwords are generally more secure than textual ones, they remain vulnerable to shoulder surfing attacks (SSA), where an attacker can observe and replicate the sequence of clicks on the password images. To address this issue, this paper proposes a novel audio-enhanced graphical password scheme designed to resist shoulder surfing. In the proposed method, users must listen to an audio cue while entering their password and are required to click on the password points precisely when their selected audio segment is played. This synchronization ensures that, even if an attacker observes or records the click locations as they are entered by users, they cannot determine the correct audio segments to be associated with the click locations to successfully accomplish the authentication process. To ascertain the security of our proposed scheme, we carried out user study on the model of the scheme. The results proved that the proposed scheme effectively resists SSA

Keywords **- User authentication, Password attacks, Internet banking,Shoulder-surfing, Graphical passwords; Hardening Passwords, Shoulder surfing, Authentication systems.**

Binary Classification of Malware Using Graph Convolutional and Graph Isomorphism Networks

Aditya Alok[1], Arya Kumari[1], Dr. A. Menaka Pushpa[2], and Dr. Rohit Tanwar[1]
[1]School of Computer Science and Engineering, SMVDU, Katra, India
romitkumar912@gmail.com, aryakumari1964@gmail.com,
rohit.tanwar@smvdu.ac.in
[2]School of Computer Science and Engineering, VIT Chennai, India
menakapushpa.a@vit.ac.in

Abstract

The rapid evolvement of malware requests advanced techniques to detect and classify them. Graph representation learning provides global and local dependencies among malware families that makes the classification task easier. In this work, we present an architecture for binary malware classification using Graph Neural Networks (GNNs). Especially, we examine the performance of Graph Convolutional Networks (GCN) and Graph Isomorphism Networks (GIN) in differentiating malicious android applications from benign applications. We have analyzed the system performance with various associated factors in the graph representation learning. We evaluated several graph weighting strategies such as unweighted, call frequency, method length, and hybrid weighting schemes. All of these strategies have been evaluated on balanced datasets which build from different sources; AndroZoo and CICAndMal2017. We have used robust evaluation metrics such as Precision, Recall, F1-score and ROC-AUC to observe the performances of the graph based malware classification system. This work more focuses on the foundation for feature engineering, model architecture, and evaluation methodology in GNN-based malware classification.

Keywords**- Malware Classification · Graph Neural Networks · Graph Convolutional Network · Graph Isomorphism Network · Function call Graph.**

A Blind Robust Image Watermarking Scheme for Copyright Protection Using Hadamard Transform and Quantization Index Modulation

Piyali Singh[1], Rahul Mandal[2], Jaydeb Bhaumik[3] and Supriyo De[4]
[1](Department of Computer Applications, Maulana Abul Kalam Azad University of Technology, Nadia 741 249) piyalisingh49@gmail.com
[2](Department of Computer Applications, Maulana Abul Kalam Azad University of Technology, Nadia 741 249) mrahul786605@gmail.com
[3](Department of Electronics and Telecommunication Engineering, Jadavpur University, Kolkata 700 032) jaydeb.bhaumik@jadavpuruniversity.in
[4](MAKAUT) supriyo.de@makautwb.ac.in

Abstract

Protecting the ownership of digital images has become increasingly important as image sharing continues to grow across online platforms. This work introduces a blind image watermarking scheme that combines the Hadamard Transform (HT), Quantization Index Modulation (QIM), and a chaos-driven block selection technique. The chaosbased pseudo-random sequence is used to select the non-overlapping blocks in the cover image, where the embedding process is performed.

Each selected non-overlapping block has been decomposed by HT, and the obtained DC coefficient has been modified using the QIM technique according to the state of the secret bit. Finally, the watermarked image has been reconstructed by applying the inverse Hadamard Transformation. The proposed scheme is assessed using PSNR, WPSNR, SSIM, NC, and BER together under various image processing attacks, including JPEG compression, filtering, noise, scaling, rotation, sharpening, cropping etc. The experimental outcomes demonstrate that the proposed scheme achieves a satisfactory trade-off between imperceptibility and robustness.

***Keywords*- Blind image watermarking · Hadamard Transform · QIM · H´enon map · Robustness · Imperceptibility.**

Physiological Manifold Authentication via Normalizing-Flow Density Scoring: A Multi-Modal Contactless Biometric Framework Robust to Autonomous Adversarial Agents

Arpan Adhikari (Ramakrishna Mission Vidyamandira) arpanadhikari@vidyamandira.ac.in
Arindam Sarkar (Ramakrishna Mission Vidyamandira) arindam.vb@gmail.com

Abstract

Biometric authentication built on discriminative attack cata-logues fails silently against novel synthesis pipelines whose artefacts were never seen at training time. The rise of autonomous adversarial agents_ software that probes an interface at machine speed, learns which attacks succeed, and synthesises novel variants without human intervention_ sharpens this weakness. We introduce BioFlow-Auth (BFA), a multi-modal authenticator that scores each attempt by its density under the genuine physiological distribution. BFA fuses five concurrent streams through a Real-NVP normalizing flow scorer (L=8 coupling layers) trained only on genuine sequences: three-view facial landmark geometry; three- region contactless rPPG with SpO2 and inter-regional phase consistency; a ≈111-bit active gaze-and-speech challenge; dual synthetic-media detectors; and elastic weight consolidation for drift adaptation. BFA attains Equal Error Rate 1.12 Rs} 0.07% on OULU-NPU Protocol IV and HTER 1.84 Rs}0.08% on an author-collected corpus against eight recent baselines. No evaluated real-time attack satisfied the multi-channel conjunction within an 800 ms window. Cross-dataset AUC degradation (mean 4.5 pp) is less than half that of the strongest discriminative baseline (9.4 pp). Genuine behaviour occupies a compact manifold (silhouette 0.78), and density scoring over it yields authentication that is simultaneously more accurate on seen attacks and more robust to out-of-distribution and autonomous adversarial attacks than the evaluated discriminative alternatives.

***Keywords* - Biometric authentication · Normalizing-_ow density estimation · Out-of-distribution robustness · Autonomous adversarial agents · Contactless rPPG liveness · Active challenge-response.**

An IWT-DCT Based Hybrid Watermarking Scheme Using LBP For Image Authentication

Souvik Sasmal (Maulana Abul Kalam Azad University of Technology) study.souvik2002@gmail.com
Pabitra Pal (Swami Vivekananda University, Kolkata) pabipaltra@gmail.com
Partha Chowdhuri (Vidyasagar University) prc.email@gmail.com
Soamdeep Singha (Vidyasagar University) soamdeep.singha0@gmail.com

Abstract

This research introduces an effective semi-blind digital image authentication framework that synergistically combines Integer Wavelet Transform (IWT), Discrete Cosine Transform (DCT), and Local Binary Pattern (LBP) techniques. The proposed methodology extracts textural features from the watermark image by dividing it into 3×3 non-overlapping blocks and applying LBP operators. Simultaneously, the host image undergoes n-level IWT decomposition, with the LL subband partitioned into 8×8 non-overlapping blocks. DCT is then applied to these blocks, facilitating watermark embedding by modifying the first eight AC coefficients using least significant bit (LSB) substitution. During authentication, the extraction process reverses these steps to obtain the embedded LBP pattern, which is compared with the original watermark's LBP using Normalized Cross-Correlation (NCC). Images with NCC values below 0.95 are classified as tampered, while those above this threshold are deemed authentic. Experimental results demonstrate excellent imperceptibility with a Peak Signal-to-Noise Ratio (PSNR) reaching up to 59.32 dB, along with a tamper detection accuracy of 0.99928, while maintaining high sensitivity to detect various tampering operations. Notably, the proposed framework demonstrates strong fragility even under extremely localized alterations such as single pixel changes, achieving a favourable trade-off between high imperceptibility and fine-grained tamper sensitivity that is often difficult to attain simultaneously. The system's semi-blind nature, requiring only the original watermark for verification, makes it particularly suitable for applications demanding rigorous authentication protocols, such as medical imaging, legal evidence verification, and secure document management. Our approach offers a valuable balance between imperceptibility and tamper detection capabilities while addressing the increasing concerns of digital content authenticity in today's information landscape.

***Keywords*- Integer Wavelet Transform, Discrete Cosine Transform, Local Binary Pattern, Semi-blind image watermarking, Fragile watermarking, SHA-256 checksum, Private Key.**

A Secure Encrypted Steganographic Framework Using BLAKE3-Based Stream Encryption with LWT for Confidential Image Communication

Suparnesh Bhattacharyya (Swami Vivekananda University, Kolkata) suparneshbhattacharyya@gmail.com
Pabitra Pal (Swami Vivekananda University, Kolkata) pabipaltra@gmail.com
Sanjay Nag (Swami Vivekananda University, Kolkata) sanjaynag75@gmail.com

Abstract

In this research, a new encrypted picture steganography scheme is suggested using Modified Dynamic Key Stream 256 (MDKS-256) encryption algorithm and Lifting Wavelet Transform (LWT). The proposed MDKS-256 architecture is a new dynamic state-update mechanism that includes three novel modifications: the use of BLAKE3 for master key generation, the adaptive rotation, the nonlinear mixing, the dynamic generation of round constant, the parallel update of the state, and the dynamic generation of the keystream. The proposed encryption engine uses 16 rounds of transformation, which leads to more diffusion, perplexity and defences against statistical and differential assaults.

In proposed architecture for data hiding is based on Lifting Wavelet Transform that disintegrates and split the image into the LL, LH, HL, and HH frequency sub-bands. The bit stream is encrypted then adaptively embedded in the HL sub-band for high embedding capacity and excellent visual quality. The integer-to-integer property of LWT guarantees lossless reconstruction, low computation complexity and better imperceptibility than the traditional DWT-based methods.

Standard benchmark image datasets are employed to evaluate the proposed framework and standard image processing techniques are implemented to analyze it with PSNR, SSIM, MSE, entropy, histogram uniformity, NPCR, UACI, correlation coefficient, embedding capacity, and execution time. The proposed MDKS-256 with LWT framework is shown to be more secure, high imperceptibility, more robust and efficient in computation than some other known encrypted steganographic schemes by experimental analysis.

***Keywords*— Image Encryption, Image Steganography, MDKS-256, BLAKE3, LWT, Secure Communication, Stream Cipher, Keystream Generation, Information Hiding.**

Q-SCION: Reliability-First Quantum-Inspired Sine–Cosine Optimisation for Latent-Space Ensemble Intrusion Detection in Smart-City Cyber-Physical Systems

Arindam Bhar (Ramakrishna Mission Vidyamandira) arindam.bhar.ju@gmail.com
Arindam Sarkar (Ramakrishna Mission Vidyamandira) arindam.vb@gmail.com

Abstract

Smart-City Cyber-Physical Systems (CPS) sustain high-velocity intrusion campaigns whose taxonomies reach 34 mechanistically distinct classes under severe (≥ 103:1) imbalance, at flow volumes exceeding 25×106 records. An operational Intrusion Detection System (IDS) must reconcile three requirements that prior work satisfies only pairwise: near-saturated detection on dominant classes, analyst-interpretable priority-stratified alerts, and sub-millisecond inference. Natureinspired (NI) ensemble optimisers suit the non-differentiable, non-convex, black-box macro-F1 surface, but every NI-IDS optimiser surveyed here is adopted without a measurable base-method justification and without a restart-to-restart reliability check, so an apparent mean-objective gain can mask an optimiser that simply fails less often on one benchmark than on the rest. This work makes two contributions that stand independently of each other. First, a Structural Ceiling Theorem bounds the macro-F1 any deterministic classifier can achieve on a class-imbalanced taxonomy, showing that the 0.5659 macro-F1 observed on the 34-class CICIoT-2023 benchmark already sits at 71.3% of a provable maximum (0.794) – a property of the benchmark's support distribution,not of any optimiser tested against it. Second, a full, honestly reported reliability audit of a quantum-inspired augmentation of the Sine–Cosine Algorithm (SCA), termed Q-SCION, which couples a Quantum-Inspired L´evy Flight (QILF) for stagnation escape with a Chaotic Logistic Map (CLM) renewal for diversity injection, applied to the ensemble-weight problem for a heterogeneous XGBoost–LightGBM detector over a 128-dimensional BiLSTM–contrastive–attention latent space. Across four NetFlow benchmarks the deployed ensemble attains 0.9996 macro Area Under the Receiver Operating Characteristic curve (AUC-ROC) and a macro-F1 of 0.9554 on NF-ToN-IoT-v3, with sub-millisecond inference latency (0.037–0.156 ms) on every benchmark. The audit's central, and deliberately unflattering, finding is reported in full: across 30 independent restarts, Q-SCION ties exactly with equal weighting, SCA, Particle Swarm Optimisation (PSO), Grey Wolf Optimiser (GWO), and a Chaotic-Aquila baseline on three of the four benchmarks, where the ensemble weight surface is close to flat, and shows a measurable effect on only the fourth, CICIoT-2023, where its restart-to-restart variance is significantly lower than SCA's ($p = 0.0253$) without a correspondingly large mean-accuracy gain. The two contributions are reported side by side – a general theoretical bound that holds regardless of which optimiser is used, and a narrow, honestly delimited empirical case for when a specific optimiser augmentation helps – together with a dataset-by-dataset separation of proven from empirical claims, including the three benchmarks on which no reliability difference between optimisers is observed.

***Keywords*- structural ceiling theorem · quantum-inspired metaheuristic · Sine–Cosine Algorithm · convergence reliability · intrusion detection · cyber-physical systems · latent-space ensemble optimisation.**

HMAC-Secured QR Payment Verification with Multi-Layer Fraud Detection for UPI Ecosystems

Jude D'Souza[1], Rishika Kapasi[2], Archit Gupta[3], and Deepa Krishnan[4]
Department of Computer Engineering,
Mukesh Patel School of Technology, Management and Engineering,
SVKM's NMIMS, Mumbai, India
judeds2005@gmail.com, rishika04kapasi@gmail.com,
architgupta062@gmail.com, deepa.krishnan@nmims.edu

Abstract

QR codes have become the de facto payment interface for India's Unified Payments Interface (UPI) payment system, handling more than 13 billion transactions per month as of 2024. In doing so, it has created a lucrative attack vector known as the QR overlay attack, where attackers superimpose fake QR stickers over the QR code of genuine merchants to redirect payments without alerting the users. Current UPI applications do not offer any means of pre-payment authentication of merchants' identities, leaving everything in the hands of the user. This paper proposes a simple and mobile-friendly payment verification gateway for QR payments which adds a cryptographic pre-payment security pipeline to the mix. It embeds an HMAC-SHA256 integrity token into the payload of the QR code, verifies its authenticity in constant time on the server side against the GST registry of merchants and assigns risk scores based on their types for arbitrary QR inputs. Our proof-of-concept implementation in Python/Flask delivered via HTTPS has proven successful at detecting all considered attacks out of 60 controlled trials. Measured latencies on dedicated hardware reveal average end-to-end verification times of 267 ms with tunnelled HTTPS and projected below 50 ms with co-located production setup.

***Keywords*- QR fraud detection · UPI security · HMAC authentication · GST registry verification · mobile payment security · cryptographic integrity · digital payment fraud · India fintech.**

A Blockchain-Anchored Trust Verification Layer for OIDC/OAuth Misconfiguration Detection in Distributed IoT Microservice Meshes

Ketankumar Savajiyani (Independent Researcher) imketan@gmail.com

Abstract

Distributed IoT microservice meshes rely on OpenID Connect and OAuth 2.0 for device and service authentication, yet misconfigurations such as insecure redirect URIs, missing PKCE, and over-scoped tokens remain common and difficult to verify across dynamically scaling, short-lived service instances. Existing scanners report point-in-time findings with no tamper-evident record of detection or remediation, which limits their value for multi-party auditing across mesh boundaries. This paper presents BATV, a blockchain-anchored trust verification layer that pairs continuous OIDC/OAuth misconfiguration scanning with an append-only ledger of attestation records. Each mesh node's authentication posture is periodically hashed into a Merkle-tree attestation and committed to a permissioned ledger, letting a relying service verify configuration integrity through an inclusion proof rather than a repeated scan. We describe the BATV architecture, a threat model for the attestation layer, and an evaluation on a synthetic IoT mesh testbed showing sub-second attestation latency at mesh sizes up to 1600 nodes.

***Keywords*- OpenID Connect, OAuth 2.0, blockchain, trust attestation, IoT, microservices, misconfiguration detection.**

Threat-Resilient Blockchain Audit Layer for Trust Verification in Federated IoT Networks: A Security Analysis

Turan Jafarzade (Azerbaijan University of Languages) turanjafarzade1@gmail.com

Abstract

Permissioned blockchain audit layers are increasingly used as a trust foundation for Federated Learning (FL) in IoT edge networks, yet their security completeness is rarely examined beyond functional demonstration. We conduct a security-focused analysis of a blockchain-anchored trust verification protocol for FL in IoT networks, formalizing an ex- tended threat model that separates client-side attacks (Sybil, replay, temporal-adaptive poisoning) from infrastructure-side attacks against the audit layer itself (malicious block producers, ordering-service manipulation, partition-induced liveness loss) _ a category unaddressed by prior blockchain-FL work. We prove replay-attack prevention and trust-history integrity as safety properties independent of the ordering service's fault-tolerance class, and characterize the gap between the crash-fault-tolerant (CFT) guarantees of Raft-based ordering (e.g., Hyperledger Fabric v2.5) and the Byzantine-fault-tolerant (BFT) guarantees needed against a malicious producer. A comparative analysis of Raft, PBFT, and Proof-of-Authority substrates, together with experimental validation (100% replay-attack rejection; contained insider trust manipulation, 4.2% vs. 31.2% attack success), substantiates these claims.

Keywords **- Federated learning · Blockchain security · Byzantine fault tolerance · Trust verification · Consensus protocols · IoT edge networks.**

A Robust Approach for Secure Multi-Cloud Data Management with Privacy and Integrity Protection

Saranya A[1], Garima Shukla[2], M. Mageshwari[3], Mandalapu Manjunadha[4],
Ankush Ghosh[5], Tarun Kumar Chatterjee[6]*
[1,2,4]Department of Computer Science and Engineering, Amity School of Engineering and Technology,
Amity University Maharashtra, Mumbai-410206, India.
[3]Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, Tamil Nadu, India
[5]University Center for Research & Development (UCRD), Chandigarh University, Mohali, Punjab, India
[6]Presidio, USA*
saranya.arnise@gmail.com[1], garimashukla0719@gmail.com[2], drmageshwarim@veltech.edu.in[3], manjunadhamclx@gmail.com[4],
ankushghosh@gmail.com[5], reachtarunchatterjee@gmail.com[6*]

Abstract

Protecting data is essential in the cloud. It already has a secure infrastructure, but when we store information on a single cloud provider, it exposes user's privacy risk, service outages, and integrity tampering. Sometimes the cloud provider often leaks the metadata or depend on trusting the provider for encryption. Decentralization of multi cloud storage using Shamir' secret sharing algorithm on Client-Side Encryption was an option. However, when we executed this algorithm on client side, it introduced a problem of computation, which causes a browser to be freeze and gets memory exhaustion for files more than 50 MB. It is difficult to manage multiple simultaneous cloud connections. To overcome problem, we have built the architecture where the Client-Side device encrypts the file and add padding to protect the metadata and send to the proxy server, where the algorithm is applied and transmitted to multiple cloud providers. The suggested solution is reduced computational bottlenecks, improve data confidentiality, data integrity, reduce metadata leakage, zero tampering, and resilience, all while keeping a simple and straightforward interface. We also have discussed about how we can expand the solution to a zero-knowledge secure recovery key and secure file sharing. The Multi Cloud Storage architecture has wide range of applications. There are numerous benefits to employing the multi-Cloud idea for data backup, storage and Encryption depending on system architecture.

Keywords **- Client-Side Encryption, Multi Cloud Storage, Zero Trust Security, Secret Sharing, Data Confidentiality, Data Integrity, Privacy Preserving Storage.**

AI-Powered Code Review Assistant: Eliminating LLM Pipeline Using AST-Enhanced Hallucination to Analyze Pull Requests Automatically

Sairamakrishna BuchiReddy Karri[1], Ravi Prakash Srivastava[2] Kiran Kumar Kadimi Chenchu[3], Ravina Marilyn Banze[4], and Ryan Banze[5]
[1]Ford Motor Company, Farmington Hills, MI 48335, USA
sairamakrishna.karri@gmail.com
[2]SS Software Solutions LLC, Hyderabad, India raviprakashshrivastav7@gmail.com
[3]Individual Researcher, 8642 Shady Pine Dr, Frederick, MD 21704, USA
[4]reachkadimi@gmail.com
[5]Independent Researcher ravina82@gmail.com
[6]Data Analyst and Automation, University of Massachusetts Amherst, Amherst, MA, USA rybosco@gmail.com
[7]AI Leader, Liberty Systems and Analytics

Abstract

A code review process is one of the most vital parts in software development nowadays, which is rather slow. Traditional static code checkers, for instance, SonarQube, are able only to detect syntactical problems, but they cannot understand the actual purpose of code blocks. Inexperienced engineers can get lots of bugs from LLMs because of providing plain code as input data without any structural information. The current paper describes an autonomous system for code review that is based on Java 21 and Spring Boot 3.2 frameworks. The proposed code review pipeline utilizes structural analysis techniques using JavaParser library (for example, calculating cyclomatic complexity and identifying God Classes, magic numbers, and OWASP vulnerabilities) in conjunction with Groq LLaMA 3.3 inference engine (70B). Using an appropriate injection technique with additional structural metadata, it generates strictly formatted JSON reports, including the overall quality score and ranked issues list. Moreover, the code review tool is connected with GitHub by the help of webhooks, works asynchronously, and uses H2 database. Experimental results confirm accurate detection of SQL injection vulnerabilities (CRITICAL), architectural anti-patterns (God Method), and clean-code verification without hallucination.

***Keywords*- Code Review Automation · Abstract Syntax Tree · Large Language Models · Cyclomatic Complexity · GitHub Webhooks · Spring Boot · Groq LLaMA · OWASP Security · Static Analysis.**

A Hybrid Metaheuristic Framework for Feature Selection in AI-Based Cyber Network Intrusion Detection

Maryam Mahdi Alhusseini[1], Yasir al-adhami[1], Fadhil Abbas Fadhil[2], Mohammad-Reza Feizi-Derakhshi[3], Alireza Rouhi[4], Zaid Ameen Abduljabbar[5,6], Vincent Omollo Nyangaresi[7],
[1]Polytechnic College of Engineering-Baghdad, Middle Technical University, Baghdad, Iraq.
mariammahdi@mtu.edu.iq,
yasir_isam@mtu.edu.iq
[2]College of Computer Science, University of Technology, Baghdad, Iraq,
fadhil.a.fadhil@uotechnology.edu.iq
[3]Computerized Intelligence Systems Laboratory, Department of Computer Engineering, University of Tabriz, Tabriz, Iran
mfeizi@tabrizu.ac.ir
[4]Faculty of Information Technology and Computer Engineering, Azarbaijan Shahid Madani University, Tabriz, Iran
rouhi@azaruniv.ac.ir
[5]Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, Iraq.
[6]Shenzhen Institute, Huazhong University of Science and Technology, Shenzhen, China
zaid.ameen@uobasrah.edu.iq
[7]Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science & Technology, Bondo, Kenya
[8]Department of Applied Electronics, Saveetha School of Engineering, SIMATS, Chennai, Tamilnadu, India
vnyangaresi@jooust.ac.ke

Abstract

Cybersecurity presents a significant challenge for Intrusion Detection Systems (IDSs) due to the large size and high dimensionality of datasets, compounded by skewed data distributions and poor classification model performance. This article presents a novel Energy Valley Optimizer (EVO)-based feature selection (FS) and dimensionality reduction approach that improves the effectiveness of IDS. The CSE-CIC-IDS2018 dataset is large and highly dimensional, so EVO was chosen to reduce the feature set, making IDS models more efficient and less computationally expensive. The proposed EVO technique is employed for feature selection to illustrate its efficacy in enhancing IDS input data, model efficiency, and classification outcomes. The suggested method uses Support Vector Machine (SVM), Random Forest (RF), Decision Tree (D_Tree), and K-Nearest Neighbors (KNN) machine learning (ML) models. Downsampling improves model accuracy in distinguishing benign and malicious traffic. EVO reduced the number of features from 80 to 43 in our testing, boosting classification accuracy, precision, and recall across all models. These results show that EVO's specific feature selection technique reduces data complexity and boosts IDS detection rates. The findings imply that EVO improves feature selection and IDS performance in cybersecurity domains.

***Keywords*- Cybersecurity; Metaheuristics; Feature selection.**

A Lightweight and Energy-Efficient Multi-Prime RSA Algorithm using Carmichael's λ(n) for Resource-Constrained Devices

Partha Sarker[1], Ashifuddin Mondal[1], Papri Ghosh[1], Debrupa Pal[1], and Subhram Das[1]
[1]Narula Institute of Technology, Kolkata, India
pscsedu1989@gmail.com, ashifuddin.nit@gmail.com, paprighosh06@gmail.com,
dppalit@gmail.com, subhram@gmail.com

Abstract

Resource-constrained devices demand cryptographic methods that are secure with the requirement of minimal energy and fast decryption. Traditional RSA is computationally expensive on limited hardware. This paper proposes a lightweight, energy-efficient multi-prime algorithm that uses four primes along with Carmichael's λ(n) function. The method randomly generates four equal-length primes *a, b, c, d,* computes the modulus $n = a \times b \times c \times d$, and employs $\lambda(n) = \text{lcm}(a-1, b-1, c-1, d-1)$ instead of Euler's totient. Decryption is accelerated by Garner's algorithm, which decomposes the operation into four modular exponentiations. Experimental results demonstrate a reduction in decryption energy (6000 μJ compared to 32500 μJ for traditional RSA) and also minimum time for decryption with key sizes from 512 to 3000 bits. The proposed scheme maintains a security level of 87.5% relative to traditional RSA and improves energy efficiency and decryption speed by 18.7%. This proposal serves as a viable alternative to ECC. Future work will integrate this algorithm with blockchain frameworks for secure, lightweight transactions and extend it with post-quantum cryptographic primitives to resist upcoming quantum attacks.

***Keywords*- Multi-Prime RSA · Carmichael function · energy-efficient cryptography · lightweight cryptography · resource-constrained devices.**

A Novel Generic Digital Circuit Based Symmetric Key Cryptography Using Session Based Key

*Joyita Goswami Ghosh1, Manas Paul[1], and Abhishek Bhattacharyya[2]
[1]Research Scholar, Sister Nivedita University, and Assistant Professor, Department of BCA, Global Institute of Management & Technology
[1*]joyitagoswami@gmail.com
[2]Professor, Department of CSE, Global Institute of Management & Technology
[2]drmanaspaul@gmail.com
[3]Professor, Department of CSE, Sister Nivedita University
[3]abhishek.bh@snuniv.ac.in

Abstract

The symmetric key cryptography technique is introduced in this paper and named as "XNOR_L". In this paper the plain text is considered as a finite number of binary bits and its chopped into blocks of variable lengths. Binary representation of each bit is XNOR-ed with another bit and the LSB bit is XNOR-ed with the low volt (i.e: 0) by using the digital circuit. The session key is randomly generated by the chopping information of plain text. Twenty files of different size and type has been taken to calculate the result. The results of XNOR_L are compared with the existing symmetric cryptographic algorithm AES and TDES with respect to the encryption and decryption time, Avalanche and Strict Avalanche values, Bit independence value, and Chi- square values.

***Keywords*- XNOR_L, AES, TDES, symmetric key, session key.**

Adaptive Confidence-Based Hybrid Fusion for Robust Cyberbullying Detection Using Machine Learning and Transformer Models

Manik Patra1 and Chanchal Patra1
Dept. of Information Technology, Maulana Abul Kalam Azad University of Technology, West Bengal, India
manikpatra409@gmail.com

Abstract

As malicious actors continually adapt their strategies to evade detection, moderating online platforms has become increasingly difficult. A common tactic involves intentionally misspelling toxic terms, which easily bypasses conventional keyword filters. While classical machine learning models utilizing character-level features demonstrate resilience against these obfuscation attempts, they often struggle to grasp subtle contextual nuances. Conversely, advanced transformer models excel at semantic understanding but frequently falter when confronted with heavily masked vocabulary. Recognizing this inherent trade-off, we present a hybrid framework that dynamically balances the strengths of both approaches. Our system processes input through a parallel architecture: a stacking ensemble relying on character and word features, alongside a RoBERTa transformer integrated with a CNN-BiLSTM head. Rather than employing static weight averaging, the framework evaluates the absolute confidence of each pipeline for every instance. When lexical distortion causes the transformer's certainty to drop, the system adaptively prioritizes the character-aware ensemble. We evaluated this approach on a harmonized corpus of 31,356 comments. The model achieved an F1- score of 0.9930 and an ROC-AUC of 0.9998. Beyond these strong baseline metrics, our dynamic confidence gating successfully maintained high predictive integrity against simulated obfuscation attacks, ensuring robust moderation suitable for high-throughput environments.

***Keywords* - Cyberbullying Detection · Natural Language Processing · Adaptive Hybrid Fusion · Deep Learning · Transformer Models · Machine Learning · Lexical Obfuscation · Stacking Ensemble.**

An Innovative Distance-Metrics–Guided Clustering Method for Stratifying Cardiovascular Risk in Asymptomatic Populations: A Proof-of-Concept Analysis

Utsab Bhattacharyya (Ramakrishna Mission Vidyamandira) ubh.chem@gmail.com:
Arindam Sarkar (Ramakrishna Mission Vidyamandira) arindam.vb@gmail.com

Abstract

Cardiovascular disease remains the leading cause of death worldwide and typically advances without symptoms, so conventional pathways driven by clinical presentation or by costly investigation reach the asymptomatic population least well. Photoplethysmography (PPG) offers a low-cost, non-intrusive alternative, but the continuous recordings produced by consumer wearables are overwhelmingly unlabelled, which frustrates the supervised classifiers that dominate this literature. We present a proof-of-concept framework that converts raw wrist-worn PPG into ordered, interpretable cardiovascular risk zones without using any disease labels. Physiological descriptors extracted from the WildPPG corpus are aggregated into stable 15-minute profiles and expressed as proportional deviations from published healthy reference intervals; each profile is then reduced to a single scalar by its distance from an idealised healthy reference vector. Constraining clustering to that one-dimensional deviation axis, rather than to the full feature space, yields zones that are monotonically ordered by severity and thresholds that are directly interpretable. A systematic sweep over four distance metrics, five clustering algorithms and three to six clusters, adjudicated by a composite of the Silhouette, Cali´nski–Harabasz and Davies–Bouldin indices, selects a Euclidean four-component Gaussian mixture (composite score 2.4608) with boundaries at 2.21956, 3.08403 and 4.06057. On four held-out user records the framework recovers deteriorating and improving trajectories, attributes each to specific physiological drivers, flags abrupt anomalies by standardised score, and forecasts zone-transition times analytically from the fitted trend.

***Keywords*- Photoplethysmography (PPG), early detection of heart disease, risk stratification, artificial intelligence in health monitoring, preventive and predictive cardiology.**

The Latency Price of Scale: A Security–Latency–Parallelism Frontier for Sharded Blockchains

Sarvagya Jha (University of Massachusetts, Amherst) jhasarvagya@gmail.com

Abstract

In the random-assignment model no sharding protocol can scale throughput better than O(N/ log N)— a bound that presumes unbounded confirmation latency, whereas on a probabilistic-finality chain the safety error decays only exponentially in the confirmation delay. We show the two constraints interact, and that their interaction binds at realistic parameters. Abstracting each shard by a settlement profile (A, γ, ρmax), both error sources are governed by one parameter, the internal corruption threshold ρ a shard is provisioned for: raising ρ sharpens the shard-capture exponent, for which we give the sharp finite-population form, and flattens the settlement exponent. For longest-chain shards we prove the profile with prefactor A = 1 uniformly in ρ. Eliminating ρ yields a frontier with an achievability bound at integral shard counts and a converse. The attainable shard count is non-decreasing in the latency budget and reaches its ceiling only as latency diverges; once the epoch duty cycle is priced, the attainable parallelism instead has an interior optimum. Any gain requires latency strictly exceeding a lower-bound benchmark for unsharded settlement, and under a mobile τ -adaptive adversary the attainable factor degrades monotonically, equalling 1 below an explicit delay τ0. At N = 20,000, a 20% adversary and a 40-bit target the best attainable parallelism is 10.6×, at a latency near 9 × 104 block times.

***Keywords*- Blockchain sharding · Security–latency trade-off · Nakamoto consensus · Adaptive adversary · Cross-shard atomic commit · Large deviations.**

K2A-Hash: A Novel Diagonal Block Perceptual Hashing Algorithm for Blockchain-Based CCTV Video Evidence Verification

Kumar Tejash
Department of Computing Technologies SRM Institute of Science and Technology Kattankulathur, Chennai, India kmrtejash@gmail.com
Abhigyan Shukla
Department of Computing Technologies SRM Institute of Science and Technology Kattankulathur, Chennai, India as3148@srmist.edu.in
Dr. Kavitha R
Department of Computing Technologies SRM Institute of Science and Technology Kattankulathur, Chennai, India
kavithar14@srmist.edu.in

Abstract

Evidence systems based on blockchain store SHA256 hash which identifies CCTV evidence. Deepfakes are capable of editing files at the level of bytes, but are oblivious to tampering with perception. and frame substitution. We introduce K2AHash, a new algorithm of perceptual hashing that satisfies four properties unavailable to other methods at the same time uniform 8-by-8 block-grid diagonal pixel extraction, directional bit compression with asymmetric thresholds, complement-based self-checking with no external secret, and temporal frame-index coupling to frame-level edits. K2A-Hash generates a 256-bit output that can be directly stored in Solidity bytes 32, which makes it possible to have a dual-hash record of evidence in which both SHA-256 and K2A are stored on-chain as immutable. The hamming distance that is less than 8 bits indicates the presence of authentic content; more than 8 indicates the presence of modification. K2A-Hash takes about 81 ms to compute on 60 clips in six categories of crime scenarios. According to the tests, the average Hamming distance of true re-encodings is 0.58 bits and the average Hamming distance of brightness-manipulated clips is 27.7 bits of the evidence that is signs of authentic and evidence of tampering.

***Index Terms*—Blockchain, CCTV, Perceptual Hashing, Video Forensics, Ethereum, Deepfake Detection, K2A-Hash**

Governed Cloud Data Fabric for Scalable Analytics Engineering and Intelligent Feature Lifecycle Automation

Narendra Mangala[1]
[1]*Princeton University, Princeton NJ 08544, USA, mangalanarendra2@gmail.com*

Abstract

Seamlessly bridged analytical and operational data environments as part of a governed cloud data fabric supporting scalable analytics engineering and intelligent feature lifecycle automation. Cloud data fabrics promote a continuum between operational and analytical data systems. Cloud infrastructure enables fabric scaling to meet the evolving demands of big data, advanced analytics, and machine learning. However, the pursuit of fully automated data fabric governance still remains relative. Scalable analytics engineering and intelligent feature lifecycle automation further facilitate the translation of analytic insights into automated operational actions. These requirements are being realised through the unification of enterprise source control and deployment capabilities with version-controlled data pipelines across the do-it-yourself analytic domain.

A simple data-layered approach centred on central oversight is no longer tenable. A modular fabric underpinned by event-driven data products, engineered by feature management capabilities, allows a decentralised analytics engineering model to flourish. Central governance and/or quality checks are retained for essential infrastructure components and other sensitive domains. The principal objective of the supporting engineering framework is the observability of all data assets and associated strategic decisions, thus enabling confidence in the decisions taken by others.

***Keywords*- Cloud data fabric, governed data platform, analytics engineering, data pipelines, reproducibility, feature engineering, automation, metadata, lineage.**

Workshop on Aerial Robotics and UAV Systems

The **Institution of Electronics and Telecommunication Engineers (IETE), Kolkata Centre**, organized a technical **Workshop on Aerial Robotics and UAV Systems** under the **IETE Tutorial Series** on **24 September 2026**, from **2:30 PM to 4:30 PM**, at **IEM, Salt Lake, Godrej Genesis Building, 15th Floor, Sector 5, Kolkata**. The workshop was designed to provide participants with an understanding of the scientific and technological foundations of drones and aerial robotic systems, with particular emphasis on practical learning, real-time training, and emerging applications of UAV technology. The event brought together academic experts and industry professionals to discuss the design, operation, intelligence, and application of modern aerial systems.

The technical programme featured **Prof. Dr. Debashis De**, Professor, Department of Computer Science and Engineering, Maulana Abul Kalam Azad University of Technology, Kolkata, West Bengal; **Prof. Dr. Amartya Mukherjee**, Associate Professor and HOD of CSE (AIML), CSBS, IEM Salt Lake; **Prof. Banashree Mandal**, Assistant Professor, Department of CSE (AIML), CSBS, IEM Salt Lake; and **Mr. Soumanka Sarkar**, Senior System Analyst. The speakers brought complementary perspectives from academia and industry, covering both the theoretical foundations and practical aspects of aerial robotics and UAV systems.

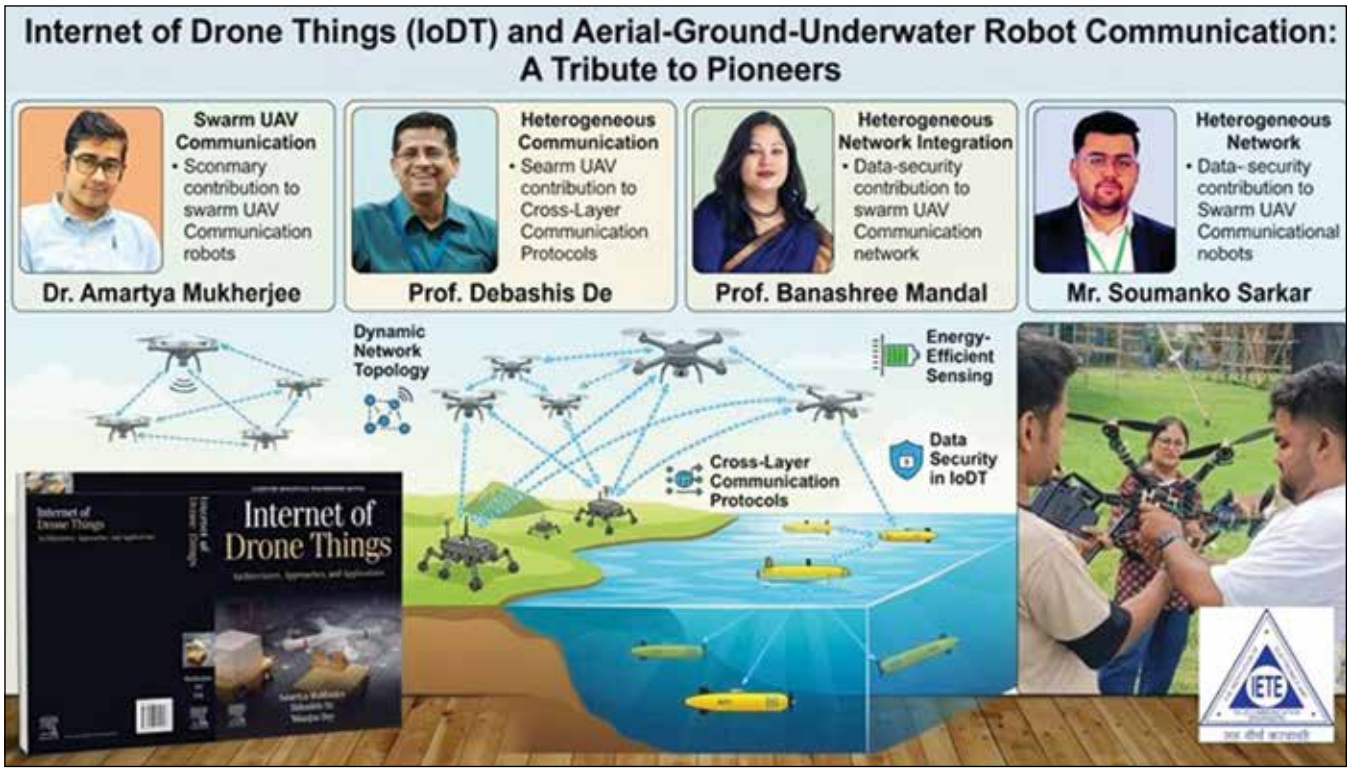


Figure 1: Flyer of the workshop

The workshop addressed the fundamental architecture of **Unmanned Aerial Vehicles (UAVs)** and their transformation from remotely operated platforms into intelligent autonomous robotic systems. A UAV typically integrates propulsion, flight-control systems, onboard processors, sensors, communication modules, navigation mechanisms, and power systems. Understanding the interaction among these components is essential for achieving stable flight, accurate positioning, autonomous decision-making, and reliable mission execution. The sessions therefore provided a technical foundation for understanding how hardware and software components work together within an aerial robotic platform.

Particular attention was given to **flight control, navigation, and autonomous operation**. Flight-control algorithms are responsible for maintaining UAV stability and regulating parameters such as altitude, orientation, velocity, and trajectory. Navigation systems combine information from sensors and positioning technologies to estimate the UAV's state and guide it toward a desired location. These capabilities become increasingly important in autonomous missions where the UAV must follow planned trajectories, respond to environmental conditions, avoid obstacles, and accomplish mission objectives with limited human intervention.

Figure 2: UAV/drone operating in an outdoor environment during flight.
The figure may be inserted here to illustrate the practical deployment of aerial robotic systems.

The practical relevance of UAV technology was further demonstrated through its application to real-world domains. UAVs can serve as mobile sensing and robotic platforms for **agriculture, surveillance, search and rescue, disaster management, infrastructure inspection, smart-city services, environmental monitoring, and defence applications**. Their ability to rapidly access large or difficult-to-reach areas makes them particularly useful for aerial observation, data acquisition, mapping, monitoring, and emergency response. The integration of cameras, environmental sensors, communication technologies, and onboard intelligence further expands the range of missions that can be performed by UAV systems.

An important technical dimension of the workshop was the emerging area of **multi-UAV and swarm-based aerial robotics**. In a swarm, multiple UAVs can cooperate to perform a common mission through distributed coordination, communication, task allocation, and collective decision-making. Such systems can improve spatial coverage and enable parallel execution of complex missions. However, swarm operation also introduces challenges related to collision avoidance, communication reliability, distributed control, synchronization, localization, energy management, and coordination among autonomous agents. These aspects connect aerial robotics with broader research areas such as multi-agent systems, distributed computing, artificial intelligence, and swarm intelligence.

The Institution of Electronics and Telecommunication Engineers
2, Institutional Area, Lodi Road,
New Delhi-110 003
Tel : +91-11- Ph: 45142153, 44467525 Extn:213
E-mail: mgeditor.iete@gmail.com

सह वीर्यं करवावहै

IETE ADVERTISEMENT TARIFFS

IETE Journal of Research **(Monthly),** ***IETE Technical Review*** **(Bi-monthly),** ***IETE Journal of Education*** **(Bi-annually) and** ***IETE News Letter*** **a**re the publications of the Institution of Electronics and Telecommunication Engineers with print & online circulation and are also available on IETE website www.iete.org. IETE News Letter is four monthly publication and has an online circulation to over 30000 members. The rate of advertisement in any of the publications is as follows:-

Advt. Position	Colour		B/W	
	Rs	US$	Rs	US$
Back Cover (full page) (available only in IETE Newsletter)	35,000	2,100	21,000	1,750
Inside back Cover (full page)	25,000	1,840	17,000	1,350
Any other Full page (Inside anywhere)	15,000	1,250	10,000	875
Any other Half page (vertical/horizontal)	-	-	7,000	550
Any other Quarter page (vertical/horizontal)	-	-	4,000	300

Advertisement Material	
Technical specifications: Ad size (Height mm × Width mm)	
Full Page	250 × 170
Half Page (Vertical)	250 × 85
(horizontal)	125 × 170
Quarter Page (Vertical)	250 × 42.5
(horizontal)	62.5 × 170

- **Special discount to IETE Organizational Members** Organizational Members of the Institution are entitled to a special discount of **20%** on full page advertisement tariffs only if the order is received directly by IETE.
- **Discount to IETE Centres/ Sub-Centres/ ISFs/PACs 10%** discount could be availed by the above IETE units for bringing in advertisements for IETE journals.

IETE Journal of Research (IETE JR), IETE Technical Review (IETE TR) **and** ***IETE Journal of Education (IETE JE)***

These publications of the Institution of Electronics and Telecommunication Engineers (either monthly or bimonthly or six monthly) have a circulation of 600 copies (print) and 30000(online) each for JR, TR and JE). IETE journals are available on its website "www.iete.org" with free access to its members. IETE JR & TR are indexed in SCI, Web of Science and EBSCO, IETE JE is included on the UGC Care list.

Advertising with us has its own set of advantages: Published in association with M/s Taylor & Francis of England, IETE publications are widely read by academics, industry, and research and development facilities worldwide. IETE journals are moving forward and creating new benchmarks for excellence, and are respected for their good standards. People and institutions across the nation are more likely to see and recognize IETE's print/ online platforms. Decision-makers and influential individuals will consequently notice your brand more frequently.

We strongly recommend that you use our advertising options in your overall marketing strategy.

Yes, I would like to advertise in:

- **IETE Journal of Research (IETE JR)**
- **IETE Technical Review (IETE TR)**
- **IETE Journal of Education (IETE JE)**
- **IETE News Letter**

Mr./Mrs./Ms ……

……

Products/Services ……

Company Name ……

Designation ……

Address ……

City …… Pin……

Telephone ……

Email …… Website……

Payments are accepted through:

i) At par Cheques /Demand Drafts payable at New Delhi, in favour of IETE, New Delhi.

ii) Online Bank details:-
Institution of Electronics & Telecommunication Engineers (IETE)
Indian Overseas Bank
SB A/c No: 149801000001800
IFS Code: IOBA0001498
Address: 20 Lok Kala Manch, Lodi Road,
New Delhi-110 003

Mail to: **Assistant Secretary (Awards & Publications) IETE, 2, Institutional Area, Lodi Road, New Delhi-110 003**

The Institution of Electronics & Telecommunication Engineers

Subscription Rates-2027

Subscribe to the IETE JOURNALS to stay abreast on new technologies.

1. There have been unprecedented advances in science and technology in recent years. New inventions and innovations are being reported in quick succession. The industry is becoming highly research-oriented and competitive. Growth of knowledge is increasing at such a rapid rate that a professional has an uphill task keeping oneself up-to-date in the area of one's specialization. Towards this end, IETE caters to the needs of electronics, telecommunication and IT professionals by publishing highly informative journals. IETE assists a professional through dissemination of current knowledge thereby enabling him / her to contribute substantially towards the profession and match the changing requirements of society. **The IETE journals are indexed by reputed national and international abstracting agencies**.
2. Leading organizations within the country and abroad including R&D establishments, educational institutions, polytechnics and libraries subscribe to the IETE journals. **The non-member readers are invited to subscribe to IETE Journals.** The brief scope of journals is asunder:
   - ***IETE Journal of Research*** **(Monthly):** contains R&D type articles, original research and review papers covering state-of-the-art technologies. ISSN 0377-2063 (Print) & E-ISSN 0974-780X (Online) **Impact Factor- 1.4**
   - ***IETE Technical Review*** **(Bi-monthly):** contains informative and general interest articles, reviews of technologies/products/designs. ISSN 0256-4602 (Print) & E-ISSN 0974-5971 (Online) **Impact Factor-2.3**
   - ***IETE Journal of Education*** **(Six Monthly):** contains(but are not restricted to) research articles, tutorial articles, review/survey articles, new interpretations or extensions of known concepts, new design ideas, innovative laboratory practices, innovative teaching methodologies, and appraisal of new technologies.ISSN-2455-4383 (Print) & E-ISSN:0974-7338(Online). The Journal has been indexed and abstracted with UGC- CARE List (India) from July 2022 onwards.
3. *The following Annual Subscription Rates (**Effective from 1st January 2027**) for IETE Journals are inclusive of inland delivery charges by Regd Book Post.* **No partial subscriptions will be accepted.** Payments are accepted via following modes-

   I) At par Cheques /Demand Drafts in favour of IETE, New Delhi; payable at New Delhi.

   ii) Through Online with bank details as follow:-Institution of Electronics & Telecommunication Engineers (IETE),

   Indian Overseas Bank, SB A/c No: 149801000001800,

   IFS Code: IOBA0001498; Address: 20, Lok Kala Manch, Lodi Road, New Delhi-110003

   IMPORTANT NOTE: This information may be treated asan invoice where needed as no separate invoice will be issued.

IETE Journals	Inland Subscription (Rs) PRINT COPY	Print+E-Journals (Rs)	Foreign Subscription including Surcharge (only for SAARC) countriesin US$	IMPORTANT INFORMATION FOR SUBSCRIBERS *Subscription Discount :* 10% discount if subscribed for 3 years & 15% discount if subscribed for 5 years
IETE Journal of Research, IETE Technical Review & IETE Journal of Education (in combo)	12000	19500	375	➢ Subscription Number will be allotted and journals will be mailed after receipt of payment in advance in full. ➢ All journals to paid subscribers will be dispatched within the country by Registered Parcel only. ➢ Non-receipt complaints become time-barred after two months of publication. The same queries will not be attended repeatedly. ➢ We Donot Have Any Policy of Refunds/ Replacements / Sending of Backissues. ➢ Kindly check the periodicity before claiming on- receipt for any issue. ➢ Non receipt complaints will only be entertained on extra payment and also if return copies are available in stock. ➢ Names & addresses of end users are a must for bulk / agency subscribers.
IETE Journal of Research & IETE Technical Review (in combo)	9500	15000	300	
IETE Journal of Research	6000	10000	200	
IETE Technical Review	6000	10000	200	
IETE Journal of Education	2500	4200	75	
IETE Journal of Education for Corporate Members of IETE	750		40	

IETE Corporate members& Organizational Members can access the *IETE Journals Online.* ISF Students can access IETE Journal of Education online. IETE Newsletter is available on IETE website (Publications) and is also sent through email.

http://iete-elan.ac.in/elan/membership/journalsTF.jsp?button=Click+to+Access+IETE+Journals

For any information or assistance to place an order, please Email at –mgeditor.iete@gmail.com

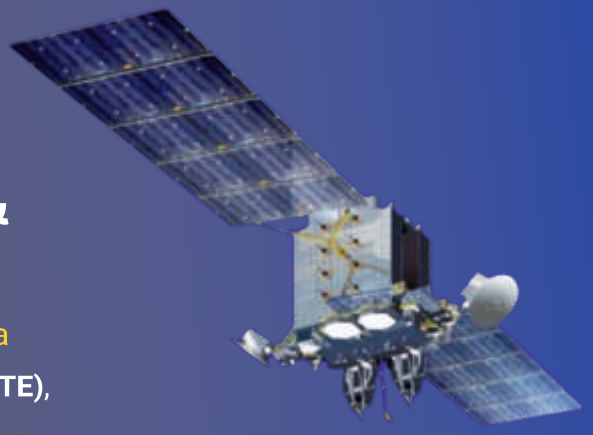
Ph:011-45142106&104 Extn:213(M)9868493445

IEEE Advancing Technology for Humanity | IEEE AP-S Antennas and Propagation Society | WAMS | SASI Institute of Technology & Engineering Autonomous, Tadepalligudem, West Godavari Dist., A.P

WAMS 2027

IEEE Conference Record Number #73032

6th Wireless, Antenna, & Microwave Symposium



June 28 - July 01, 2027, Andhra Pradesh, India

Sasi Institute of Technology and Engineering (SITE), Tadepalligudem, Andhra Pradesh, India

Committees

Patrons
B. Venugopala Krishna
M. Narendra Krishna

Co-Patrons
Sudhakar Rao
Dhaval Pujara

General Chair
Mohammad Ismail

General Co-Chair
Sivakumar Perumal

Organising Chairs
P. N. Malleswari
P. Hema Chandu

Technical Program Committee
Anantha Bharathi
Winny Elizabeth Philip

Track Chairs
Koushik Datta
M. D. Selvaraj
S. Kirubakaran
Abhishek Kumar Jha
Shiv Narayan

Advisory Committee
Ajay Poddar
Rajeev Jyoti
Puneet Mishra
Ke Wu
Qammer Abbasi
Danilo Erricolo
P. Satish Rama Chowdary
T. Rama Rao
Nacer Chahat
Balamati Choudhury
Philip Venerzia
Prabhakar Pathak
Nelson Fonseca
Hao Xin
Hema Singh
Sanjeev Reddy
Jawad Siddique
Debatosh Guha
A. Harish

Executive Committee
C. J. Reddy
Francesco Andriulli
Christophe Fumeaux
Sudhakar Rao
Dhaval Pujara
Satish Sharma
Bharathi Anantha
Mahesh Appajappa
Sameer Chakravarthy
Keerthipriya Satish
Anupama Naidu
Somak Bhattacharyya
Desmond Sim
Priyanka Dalal

Publication Committee
T V Krishna Moorthy
Puli Kishore
N. Kusuma

Finance Committee
Sameer Chakravarthy
V. V. N. Sujit

Local Organizing Committee
C R S Hanuman
T V Raghu
Shaik Mohammed Rafee
P Kiran Kumar
L B Bharath Raju
K Subash Bhagavan
A Praveena
K. Uma
U. Uma Maheswara Rao
S. Sri Ramya
A Akshaya kranth
Suresh Angadi
Ch Jayaprakash
P Srinivas
P R Mahidhar
P Sivadurgarao
N Sannajaji
T Venkateswara Reddy
M. Ravi Sankar
SK Fatima
Shaik.M.Unnishabegum
K Avinash
Mohammad Subhani
M V Kiran Kumar
M Venu
SK Salman Basha

About WAMS

6th Wireless, Antenna and Microwave Symposium (WAMS) is planned as a multidisciplinary symposium held annually in an academic institute. It is focused on providing an affordable yet state-of-the-art international forum for students and young professionals to interact with the leading domain experts around the world. The 6th edition of WAMS, WAMS 2027, will be held at the Sasi Institute of Technology and Engineering in Tadepalligudem of South India, AP during June 28 - July 01, 2027. WAMS 2027 provides an excellent opportunity for sharing and exchanging information on the cutting-edge research and scientific achievements in wireless, antenna, & microwave engineering and sciences along with establishing and strengthening professional networks.
WAMS 2027 begins the collaboration between the IEEE AP Society and WAMS Society where APS is the 100% financial sponsor.

About SITE

Sasi Institute of Technology & Engineering is a nationally accredited NAAC A+ Autonomous DSIR-SIRO & ISO 21001:2018 certified Institution affiliated to Jawaharlal Nehru Technological University, Kakinada, and recognized by All India Council of Technical Education, New Delhi. The college offers Diploma, Under graduate, Post Graduate and doctoral programs in the core and emerging is technologies, and where the students are groomed with life skills to make them globally competent responsible individuals. The campus spreads across 30 acres of green lush ambience has Drone Technology Lab that offers Drone pilot licensing, Robotics lab, Intel Certified AI lab, AR/VR Lab & AICTE Idea lab that support ideation to prototyping. The Institution organizes as a calendar activity one International Conference under their IEEE or Springer affiliation to provide opportunities for young researcher to collaborate globally.

Call for Papers

WAMS 2027 invites original contributions relevant to the themes of the symposium falling under one of the following tracks (but not limited to):

Wireless
- Wireless 5G & 6G Communication
- 5G AI/ML in Signal Processing
- Digital & Image Processing
- Antennas & Propagation
- Communication
- SDR/Cognitive Radio
- Wireless Sensor Networks
- Vehicular Communications
- IoT & Data Analytics
- Nano Electronics
- Communication
- Underwater Network

Antenna
- Antennas Microwave and Millimeter Wave
- Antenna Theory
- Antenna Array Design
- Satellite Antennas
- Array Antennas
- Metamaterials
- Measurement and Applications
- Antennas on handheld & ground terminals
- Antenna
- Measurements & RCS
- EM Wave
- Computational EM
- Reflector and reflectarray antennas

Microwave
- RF and Microwave
- RF/Microwave Circuits
- RF Devices and Components
- Millimeter Wave Design
- Microwave Imaging
- Wireless Power Transmission
- Electromagnetic Interference and Compatibility
- Design and Optimization of
- Amplifiers & Oscillators

Paper Submission Link
https://cmt3.research.microsoft.com/WAMS2027/

Website Link
wams27.sasi.ac.in

Contact
wams2027@sasi.ac.in
8074480076, 88767 67676,
85001 08141

Important Dates

Submission Deadline	: December 31, 2026
Acceptance Notification	: March 31, 2027
Camera-Ready Paper Submission	: April 10, 2027
Conference Dates	: **June 28-July 01, 2027**