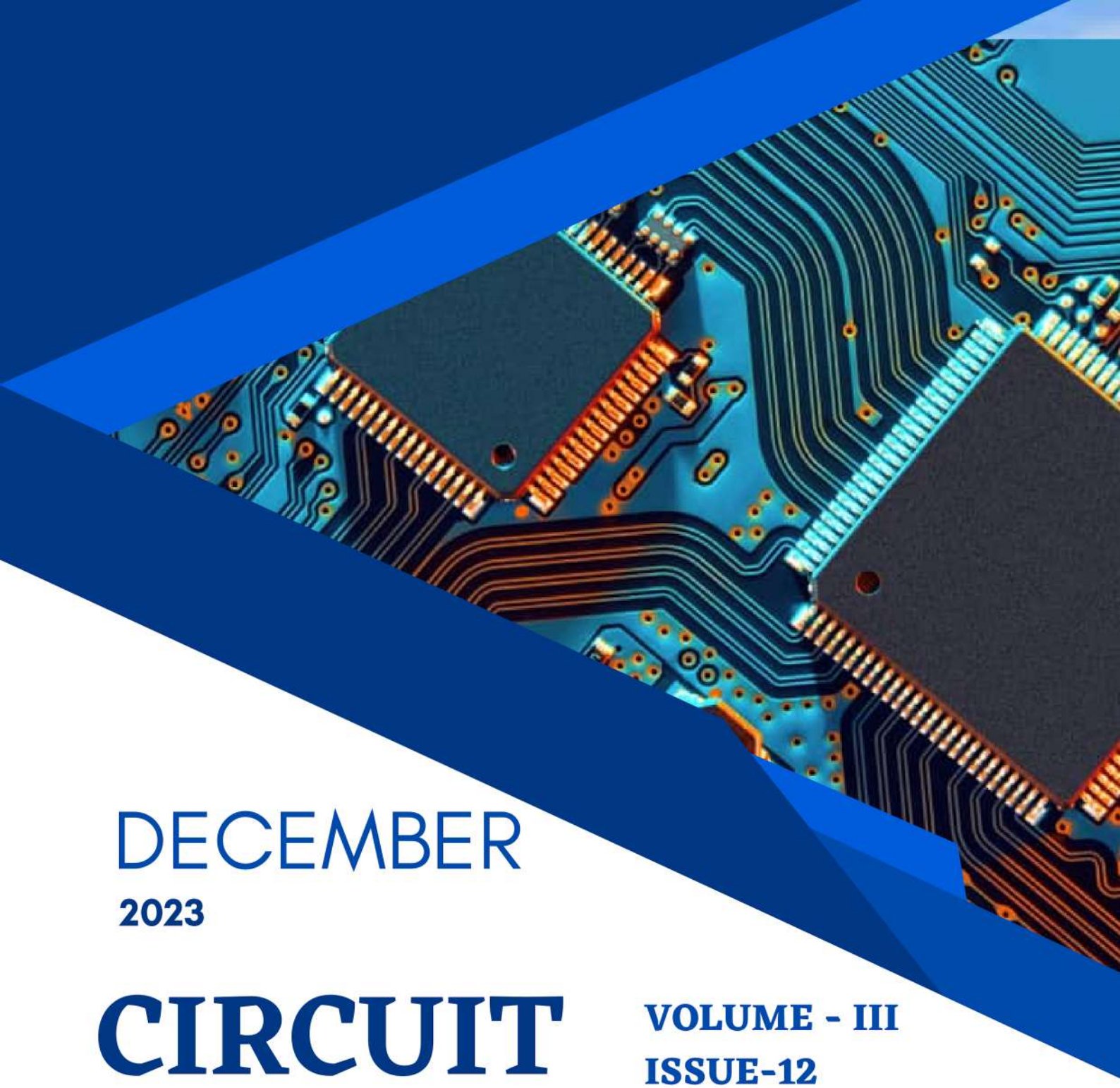

DECEMBER

2023

CIRCUIT TIMES

VOLUME - III
ISSUE-12

SVCE | SRI VENKATESWARA COLLEGE OF ENGINEERING

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

IN THIS ISSUE

ARTICLE

- A PRAGMATIC SURVEY ON SECURITY IN EMERGING 6G COMMUNICATION: CHALLENGES AND COUNTERMEASURES

ACHIEVEMENTS

- FACULTY PARTICIPATION
- STUDENT PARTICIPATION
- STUDENT ACHIEVEMENTS
- FACULTY ACHIEVEMENTS
- REVIEWER/EDITORIAL BOARD MEMBER
- EVENTS ORGANISED
- PARENT TEACHERS MEETING

VISION OF THE DEPARTMENT

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

MISSION OF THE DEPARTMENT

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

Program Educational Objectives (PEOs)

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

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

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

Program Specific Outcomes (PSOs)

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

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

FACULTY ARTICLE

A PRAGMATIC SURVEY ON SECURITY IN EMERGING 6G COMMUNICATION: CHALLENGES AND COUNTERMEASURES

Ms.R. Kousalya, Assistant Professor - Department of ECE,
Sri Venkateswara College of Engineering, Sriperumbudur.

1.INTRODUCTION

The evolution of wireless communication technologies started with the first generation of cellular networks (1G) in the 1980s. By then, significant advancements have been added to the telecommunication and networking industries during 2G, 3G, and 4G cellular networks. The era of fifth-generation (5G) wireless technologies has been deployed since 2020, and it is yet to evolve mostly on software-based till 2025 with full coverage. The Internet of Everything (IoE), Virtual Reality (VR), Three-Dimensional (3D) media, Artificial Intelligence (AI), Machine-to-Machine (M2M) communication, enhanced Mobile BroadBand (eMBB), and other developing applications and industries have evolved rapidly, which will need 6G capabilities to be realized at scale to be commercially feasible. The most remarkable feature of 5G is the cloudification of networks with the microservice-based architecture. This provides an abstraction of physical resources to virtual and logical environments introducing on-demand automated learning management functions. Figure 1 depicts the security evolution of mobile communication.

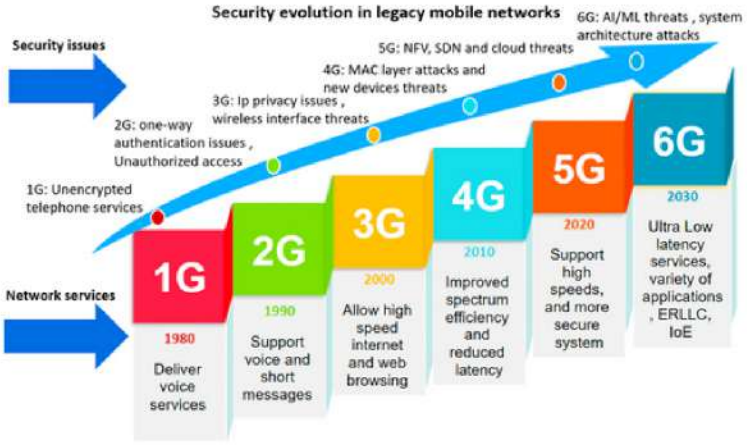

Figure 1 Security evolution of cellular mobile communications [1]

2. THREAT MODELS

A threat model [2] is a structured representation of potential threats to a system and the vulnerabilities that could be exploited by those threats. It helps identify, prioritize, and address security risks effectively. A taxonomy of threat models includes Confidentiality, Integrity, Availability, Authentication and Access Control shown in Figure 2.

2.1Confidentiality

Confidentiality, keeping information secret from unauthorized access, is probably the most common aspect of information security.

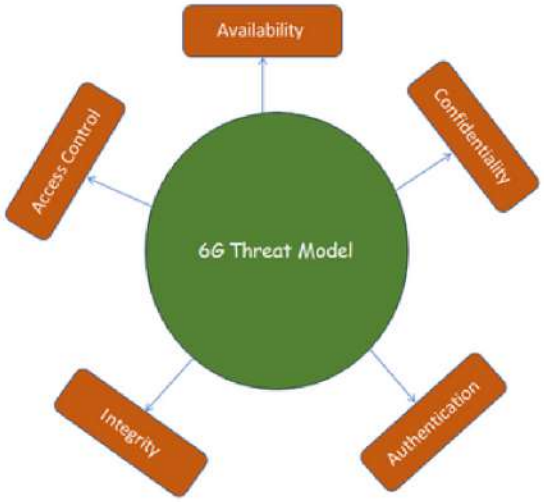

Figure 2 Taxonomy of Threats in 6G Communications

2.2 Integrity

Information needs to be changed constantly. In a bank, when a customer deposits or withdraws money, the balance of their account needs to be changed. Integrity means that changes should be done only by authorized users and through authorized mechanisms.

2.3 Availability

The information created and stored by an organization needs to be available to authorized users and applications. Information is useless if it is not available.

2.4 Authentication

Authentication is the process of verifying the identity of a user, system, or entity to ensure that they are who they claim to be.

2.5 Access Control

Access control is a security measure that regulates and restricts access to specific resources or areas within a system. The primary goal of access control is to protect sensitive information, prevent unauthorized access, and ensure that only authorized users or systems can interact with certain resources.

3. SECURITY CHALLENGES

With the increased data transfer rates and connectivity in 6G, there may be a higher risk of privacy breaches. Massive amounts of data could be transmitted, raising concerns about the unauthorized collection and use of personal information. 6G is expected to introduce network slicing, which allows the creation of multiple virtual networks on a shared physical infrastructure. Ensuring the security of these slices and preventing unauthorized access between them will be crucial. The integration of Artificial Intelligence (AI) and Machine Learning (ML) in 6G networks may introduce new security challenges [3,4].

Adversarial attacks targeting AI models, for example, could compromise the functionality and reliability of the network. With more devices and users connected to the 6G network, robust authentication mechanisms will be crucial. Security threats may arise from compromised credentials, unauthorized access, or inadequate identity management. The Internet of Things (IoT) is expected to play a significant role in 6G networks. Securing a vast number of connected devices and ensuring their resilience against cyber threats will be a key challenge. Figure 3 explains the security challenges in 6G networks.

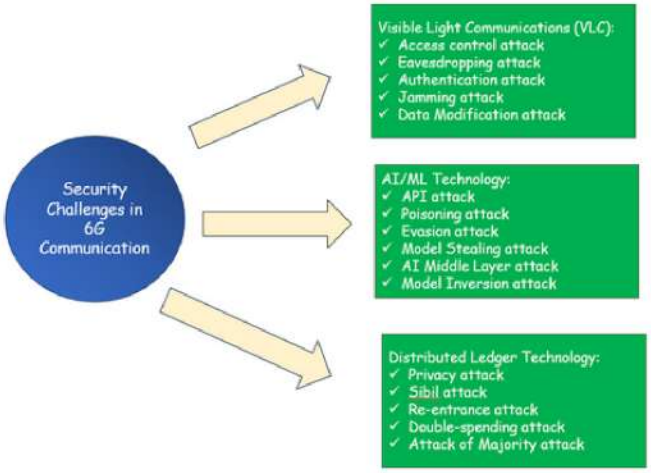

Figure 3 Security Challenges

3.1 Visible Light Communication (VLC)

An important technology that needs to be highlighted is the Visual Light Communication (VLC) system, which can provide transmission similar to that of fiber optics. Optical fiber is a thin, highly flexible medium made of silica that is used to transmit data. Because fiber optics transmits light, it can transmit data at higher transmission rates and bandwidths than a number of other methods.

3.2 AI/ML Technology

AI and ML have recently been identified as critical components of the network architecture of all 6G network technologies. As a result, artificial intelligence has garnered a lot of attention in the 6G networking industry. AI/ML in 5G networks is implemented in places with large amounts of training data and powerful computer cores. However, AI/ML has emerged as a crucial component of 6G networks. AI and machine learning are being used to secure various frames of 6G security defense and protection. The application of AI and machine learning in security makes security solutions more autonomous and accurate, with predictive capabilities for security analytics.

3.3 Distributed Ledger Technology (DLT)

The anticipated collaboration between DLT and 6G may have an implicit impact on the security issues in blockchain and smart contracts in 6G networks. Such attacks arise as a result of issues in software development, language constraints, and network connection security issues.

4.CRYPTOGRAPHY-BASED COUNTERMEASURES

Cryptography plays a fundamental role in securing communication systems, including those in 6G networks. Here are some cryptography-based countermeasures [5] that can be employed to enhance security in 6G communication:

4.1 Quantum-Resistant Cryptography

Quantum computers pose a potential threat to traditional cryptographic algorithms, such as RSA and ECC. To counter this, 6G networks may adopt quantum-resistant cryptographic algorithms, which are designed to remain secure even in the presence of powerful quantum computers.

4.2 Post-Quantum Cryptography

Post-quantum cryptography involves using cryptographic algorithms that are believed to be secure against quantum attacks. As quantum computers advance, 6G systems may transition to post-quantum cryptographic standards to ensure long-term security.

4.3 Homomorphic Encryption

Homomorphic encryption allows computations to be performed on encrypted data without decrypting it. This can enhance the privacy and security of sensitive information in 6G networks, especially when outsourcing computation tasks to third parties.

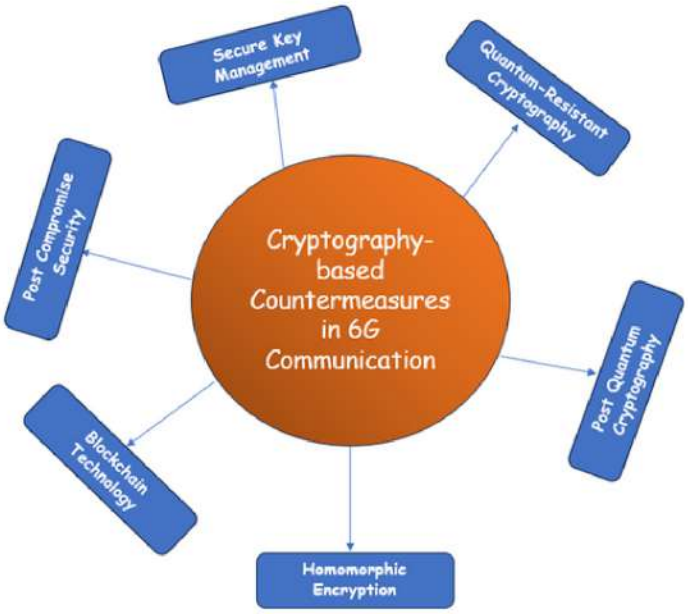

Figure 4 Cryptography-based countermeasures

4.4 Blockchain Technology

Blockchain, with its decentralized and tamper-evident nature, can be employed for secure transactions and data integrity in 6G networks. Smart contracts on blockchain platforms can provide automated and secure execution of predefined rules.

4.5 Post-Compromise Security

In addition to preventing unauthorized access, 6G systems may implement post-compromise security measures. For example, encrypted communication channels combined with intrusion detection systems can help detect and respond to security breaches in real time.

4.6 Secure Key Management

Robust key management is crucial in any cryptographic system. 6G networks should employ secure key exchange protocols and periodically update encryption keys to mitigate the risk of key compromise.

5. CONCLUSION

This article surveyed possible challenges to effectively implement 6G mobile networks and discussed the various countermeasures performed in cryptographic techniques. The future research directions include privacy preservation in 6G network-based 3D fog computing, 6G-enabled privacy-protected smart infrastructures, and SDN-based secure architecture in 6G networks

REFERENCES

[1] Shimaa A. Abdel Hakeem, Hanan H. Hussein, HyungWon Kim, (2022) "Security Requirements and Challenges of 6G Technologies and Applications", Sensors, 22(5), 1969; https://doi.org/10.3390/s22051969

[2] Pawani Porambage, Gürkan Gür, Diana Pamela Moya Osorio, Madhusanka Liyanage, Andrei Gurtov, (2021) "The Roadmap to 6G Security and Privacy", IEEE Open Journal of the Communications Society (Volume: 2), DOI: 10.1109/OJCOMS.2021.3078081, 1094 - 1122.

[3] Mohammed Banafaa, Ibraheem Shayea, Jafri Din, Marwan Hadri Azmi, Abdulaziz, Alashbi, Yousef Ibrahim Daradkeh, Abdulraqeb Alhammadi, (2023) "6G Mobile Communication Technology: Requirements, Targets, Applications, Challenges, Advantages, and Opportunities", Alexandria Engineering Journal 64, 245–274, https://doi.org/10.1016/j.aej.2022.08.017

[4] Syed Hussain Ali Kazmi, Rosilah Hassan, Faizan Qamar, Kashif Nisar, Ag Asri Ag Ibrahim, (2023) "Security Concepts in Emerging 6G Communication: Threats, Countermeasures, Authentication Techniques and Research Directions" Symmetry, 15, 1147. 4.4 Blockchain Technology

[5] Shimaa A. Abdel Hakeem, Hanan H. Hussein, HyungWon Kim, (2022) "Vision and research directions of 6G technologies and applications", Journal of King Saud University - Computer and Information Sciences, Volume 34, Issue 6, 2419-2442.

ACHIEVEMENTS

FACULTY PARTICIPATION

(Seminar/FDP/STTP/Workshop/Online Course/Conference):

- Dr.M.Bindhu, Mrs.K.S.Subhashini, Mr.S.Senthil Rajan participated in the six days Faculty Development Programme on "Applications of Internet of Things Networks in 5G and Beyond" (ATAL Sponsored) organized by Rajalakshmi Engineering College, Chennai held from 11th December to 16th December 2023.

- Mrs.R.Kousalya, Mrs.B.Sarala participated in the the six days Faculty Development Programme on "OUTCOME-BASED RESEARCH: VLSI DESIGN AND MODELING" (ATAL Sponsored) organized by Bharat Institute of Science and Technology, Chennai held from 11th December to 16th December 2023.

- Dr.T.J.Jeyaprabha participated in the two days National level Seminar on "Technological upgradation for Improved Efficiency in Broadband Wireless Systems" (SERB Sponsored) organized by SA Engineering College, Chennai held from 14th December to 15th December 2023.

- Mr.L.K..Balaji Vignesh participated in the six days Faculty Development Programme on "Design Challenges and Realization of Wearable Antennas from an antenna Engineer Perspective" (ATAL Sponsored) organized by Velalar College of Engineering and Technology, Erode held from 18th December to 23th December 2023.

- Dr.S.Vijayanand, Mr.K.Venkatesh participated in the International Level Faculty Development Programme on "Modern Research Convergence in Next Generation Computing" organized by Sri Krishna College of Engineering and Technology, Coimbatore held from 18th December to 22nd December 2023.

- Mrs.S.Mary Cynthia participated in the Online Faculty Development Programme on "Medical Image Processing" organized by Alpha College of Engineering, Chennai held from 27th December to 29th December 2023.

STUDENT PARTICIPATION:

- Jeevitha K (Team Leader), Anishaa S, Bhuvaneshwari N S, Dhanshrepriya P C, Dharani A, Gogulapriya A from Third year ECE A batch participated in the Grand Finale of Smart India Hackathon 2023- Hardware Edition (5 days) held at Galgotias University, Greater Noida, Uttar Pradesh from 19th to 23rd December 2023, under the mentorship of Dr.D.Menaka, ASP/ECE and Mr.D.Silambarasan, AP/ECE. The team was shortlisted for the Grand Finale after many rounds of initial evaluation.

STUDENT ACHIEVEMENTS:

- Our team from III year ECE emerged as the 2nd runner-up in the Atomquest2023 competition held at Techfest, IIT Bombay.

FACULTY ACHIEVEMENTS:

- Dr.T.J.Jeyaprabha acted as a Resource Person during the 2 days National level Seminar on “Technological upgradation for Improved Efficiency in Broadband Wireless Systems" sponsored by SERB from 14-12-2023 to 15-12-2023 at SA Engineering College, Chennai and gave an expert delivery on “Challenges and Solutions to Broadband Access”.

- Dr.A.Prasanth served as Resource Person for a Research Talk titled “Crafting Excellence: A Guide to High-Impact Research Paper Writing” organized by Loyola-ICAM College of Engineering & Technology (LICET), Chennai held on 09-12-2023

REVIEWER/EDITORIAL BOARD MEMBER:

- Dr.T.J.Jeyaprabha acted as Reviewer for SJB Institute of Technology, Bengaluru which is organizing IEEE International Conference on Distributed Computing and Optimization Techniques (ICDCOT–2024) during 15-16 March 2024 in association IEEE Bangalore Section.

- Dr.T.J.Jeyaprabha acted as a Reviewer for the manuscript “Using a Privacy-Enhanced Authentication Process to Secure IoT-based Smart Grid Infrastructure”, published by The Journal of Supercomputing, Springer Nature SNAPP during Dec 2023.

- Dr.T.J.Jeyaprabha acted as Reviewer for H.K.E. Society's S.L.N. College of Engineering, Raichur, Karnataka is organizing Second IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS - 2024) during 23rd & 24th February 2024 in association with IEEE Bangalore Section and IEEE North Karnataka Subsection.

- Mr.L.K.Balaji Vignesh reviewed one paper titled “Comparative Analysis of Microstrip Antenna Arrays with Diverse Feeding Techniques” for Journal of Engineering Research and Reports.

EVENTS ORGANISED

- Dr T J Jeyaprabha, ASP/ECE organized an encryption and decryption based event ENIGMA under ECEA, IETE & RAIC on 18th December 2023 for the first year ECE students of SVCE.

PARENT TEACHERS MEETING:

- Parents Teacher Meeting for first Year students will be held on 23th December 2023.
- Parents said PTM was very useful and faculty advisors are maintaining their wards records as of date. Moreover, they are encouraging their wards to participate in all activities.
- Parents felt great about their interaction with all subject-handling faculties regarding their ward's discipline and subject understanding inside their respective classes.

EDITORIAL BOARD

CHIEF EDITOR

Dr.G.A.SATHISH KUMAR
HOD/ECE

CO-EDITORS

Dr. A. PRASANTH
ASSISTANT PROFESSOR, ECE

Mr. L.K. BALAJI VIGNESH
ASSISTANT PROFESSOR, ECE

STUDENT EDITORS

Mr. V.S.PRITHIVIRAJ - IV Year ECE

Ms.P.VARSHA - II YEAR ECE

Programme Offered By Department of Electronics and Communication Engineering

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

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

TOP RECRUITERS