JANUARY, 2024 VOL. 4 ISSUE 1

# CIRCUIT TIMES

*The official newsletter of Department of ECE*

SVCE | Sri Venkateswara College of Engineering

**Autonomous Institution, Affiliated to Anna University, Chennai Approved by the AICTE, Accredited by NAAC**

IN THIS ISSUE

IN THIS ISSUE

## 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.

## PROGRAMME 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.

## PROGRAMME SPECIFIC OUTCOMES (PSOS):

**PSO1:** Graduates will gain the high-level competency to design and develop various communication systems involving current emerging technologies.

**PSO2:** Graduates would be able to plan, design, analyze, evaluate and choose the proper communication techniques to meet the global demand in the field of modern communication systems.

FACULTY ARTICLE

# Quantum Cryptography for IoT security

**Mrs.B.Sarala, M.E., (Ph.D),**
*Assistant Professor, Department of Electronics and Communication Engineering,*
*Sri Venkateswara College of Engineering (Autonomous), Sriperumbudur*

Internet of things (IoT) is a developing technology with a lot of scope in the future. It can ease various different tasks for us. On one hand, IoT is useful for us, on the other hand, it has many serious security threats, like data breaches, side-channel attacks, and virus and data authentication. Classical cryptographic algorithms, like the Rivest-Shamir-Adleman (RSA) algorithm, work well under the classical computers. But the technology is slowly shifting towards quantum computing, which has immense processing power and is more than enough to break the current cryptographic algorithms easily. IoT will also be one of the disciplines, which needs to be secured to prevent any malicious activities.

## INTRODUCTION

The Modern computers provide a wide range of services that significantly simplify various tasks in our lives. However, along with their benefits, computers pose security risks in every task they undertake [1]. Therefore, it is crucial for us to prioritize the comprehensive security of our valuable and personal information. Ensuring computer security involves implementing appropriate preventive measures, identifying potential vulnerabilities, addressing possible coercion, and managing incidents [2]. The field of computer security is becoming increasingly important due to the widespread use of the Internet, Wi-Fi, and Bluetooth.

Various forms of misuse can occur on computer networks, such as hacking, phishing, and the spread of viruses, worms, or Trojans. Misuse may also extend to damaging hardware, software, or electronic data sources.

As technology advances, a new area of interest known as the Internet of Things (IoT) is emerging. In this realm, more processes are automated, and user data becomes readily available on the Internet. IoT involves the extending web property from desktops, laptops, Smartphone and tablets.

## SECURITY ISSUES IN IOT SYSTEMS

### a) Data Breaches

The IoT applications collect tons of users' data to operate and function properly. Also, most of the data consist of the user's personal information. So it must be protected by encryption.

### b) Data Authentication

Even when data are successfully encrypted, likelihoods of the device itself being hacked are still there. If there is no way to establish the authenticity of the data communicated to and from an IoT device, the security is conceded.

### c) Side-channel attacks

These are the attacks which are based on the data and information gained from the implementation of a system, rather than the weaknesses in the algorithm of implementation. Power consumption, electromagnetic leak, or sound can be enough to exploit the system.

### d) Irregular/no updates

There are plenty of IoT devices in the world and the number is expected to increase in the near future. While developing the devices, the developers often do not pay much attention to the future updates of the device and hence a device considered to be secure when it was manufactured may not be secure any more after 2 years to 3 years or less if it is not updated regularly.

### e) Malware and ransomware

An example of malware can be the Mirai Botnet which infects the IoT devices that run on Argonaut reduced instruction-set computer core (ARC) processors. If the default username and password combination is not changed for the device, it is very easy for Mirai to infect the device.

## QUANTUM CRYPTOGRAPHY

Quantum cryptography is a field of study that focuses on the use of quantum mechanical phenomena, such as superposition and entanglement, to secure communication. Quantum cryptography involves the use of quantum states to encode and transmit information, and it is based on the principles of quantum mechanics. One of the main advantages of quantum cryptography is that it can provide unconditional security.

This means that it is theoretically impossible for an attacker to intercept and decrypt the transmitted information without being detected. This is because the principles of quantum mechanics ensure that any attempt to intercept the transmitted information will alter the quantum states of the transmitted particles, which can be detected by the sender and receiver. There are several different types of quantum cryptographic protocols, including quantum key distribution (QKD), quantum secure direct communication (QSDC), and quantum private queries (QPQ). These protocols can be used to securely transmit information, establish secure communication channels, and perform secure searches of databases, among other applications.

Overall, quantum cryptography is a promising field of study that has the potential to revolutionize the way we secure communication. However, it is still an active area of research and development, and there are many technical challenges that must be overcome in order to fully realize the potential of quantum cryptography.

Quantum cryptography is a field of study that focuses on the use of quantum mechanical phenomena, such as superposition and entanglement, to secure communication. Quantum cryptography involves the use of quantum states to encode and transmit information, and it is based on the principles of quantum mechanics.

The sender encodes the information they want to transmit into the quantum states of particles, such as photons or atoms. The quantum states of these particles can be manipulated and controlled using specialized equipment. The sender transmits the particles containing the encoded information to the receiver. The receiver measures the quantum states of the particles in order to decode the information.

Because the principles of quantum mechanics ensure that any attempt to intercept the transmitted particles will alter the quantum states of the particles, the receiver can detect any attempts to intercept the transmitted information.

Overall, quantum cryptography works by using the principles of quantum mechanics to encode and transmit information in a way that is theoretically impossible to intercept without being detected. This allows for the secure transmission of information over long distances.

The root of quantum cryptography lies in the fact that it uses the smallest individual particles that exist in nature. i.e. photons.

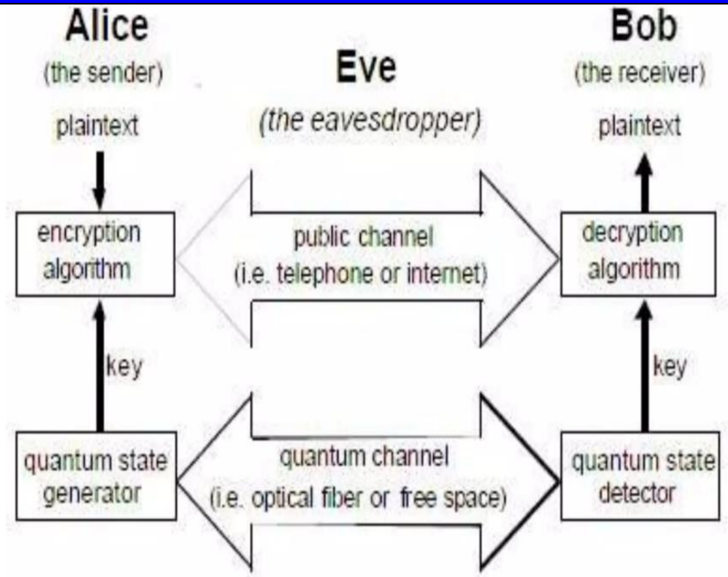


Fig.1 Mechanism of Quantum Cryptography

## FEATURES OF QUANTUM CRYPTOGRAPHY

a) **Secure communication**: One of the main applications of quantum cryptography is the secure transmission of information. Quantum cryptographic protocols, such as quantum key distribution (QKD) can be used to establish secure communication channels between two parties.

b) **Key exchange**: Quantum cryptographic protocols can be used to exchange keys between two parties in a secure manner. This can be used to establish secure communication channels or to secure data that is stored on a computer.

c) **Secure searches**: Quantum cryptographic protocols, such as quantum private queries (QPQ), can be used to perform secure searches of databases. This allows users to search for information without revealing their search queries to the database owner.

d) **Secure identification**: Quantum cryptographic protocols can be used to securely identify individuals or devices. For example, quantum key distribution (QKD) can be used to establish a secure connection between a user's device and a server, allowing the user to authenticate their identity in a secure manner.

e) **Unconditional security**: One of the main benefits of quantum cryptography is that it can provide unconditional security. This means that it is theoretically impossible for an attacker to intercept and decrypt the transmitted information without being detected.

f) **No cloning Theorem**: In quantum mechanics, it is impossible to create an identical copy of an arbitrary unknown quantum state. This theorem is fundamental to quantum key distribution as it prevents an eavesdropper from intercepting and copying the transmitted quantum information without being detected

g) **Tamper-proof**: Quantum cryptographic protocols are tamper-proof, as any attempt to intercept the transmitted information will be detected by the sender and receiver. This makes quantum cryptography highly secure and resistant to tampering.

h) **Long-distance communication:** Quantum cryptographic protocols can be used to securely transmit information over long distances. This is because the principles of quantum mechanics are not affected by distance, allowing quantum cryptographic protocols to be used to securely transmit information across the globe.

i) **Quantum Computers:** Quantum Computers, which are based on quantum mechanical principles, have the potential to solve certain types of problems much faster than classical computers. Quantum cryptographic protocols can be used to secure communication between quantum computers, which could have significant implications for fields such as scientific research and data analysis.

## LIMITATIONS OF QUANTUM CRYPTOGRAPHY

a) **Technical challenges**: Quantum cryptography is still an active area of research and development, and there are many technical challenges that must be overcome in order to fully realize the potential of quantum cryptographic protocols. These challenges include the development of reliable quantum devices and the implementation of scalable quantum cryptographic protocols.

b) **Limited range**: Quantum cryptographic protocols have a limited range, as the transmitted particles can be affected by noise and other factors that can degrade the signal. This limits the distance over which quantum cryptographic protocols can be used to securely transmit information.

c) **Cost**: Quantum cryptographic protocols can be expensive to implement and maintain, as they require specialized equipment and expertise. This may limit their adoption in some situations.

d) **Compatibility**: Quantum cryptographic protocols may not be compatible with all types of communication systems and networks, as they may require specific infrastructure or protocols in order to function properly.

## QUANTUM CRYPTOGRAPHY IMPLEMENTATION WITH IOT

IoT devices have many loopholes in terms of the security of the devices, users, or the network. The current classical architecture of the IoT does not provide any provisions to detect the eavesdropper in the communications channel. Also, there can be some attacks wherein only one device in the whole IoT network can be infected with some virus and other devices trust the infected device and continue communications until it is detected.

## CONCLUSION

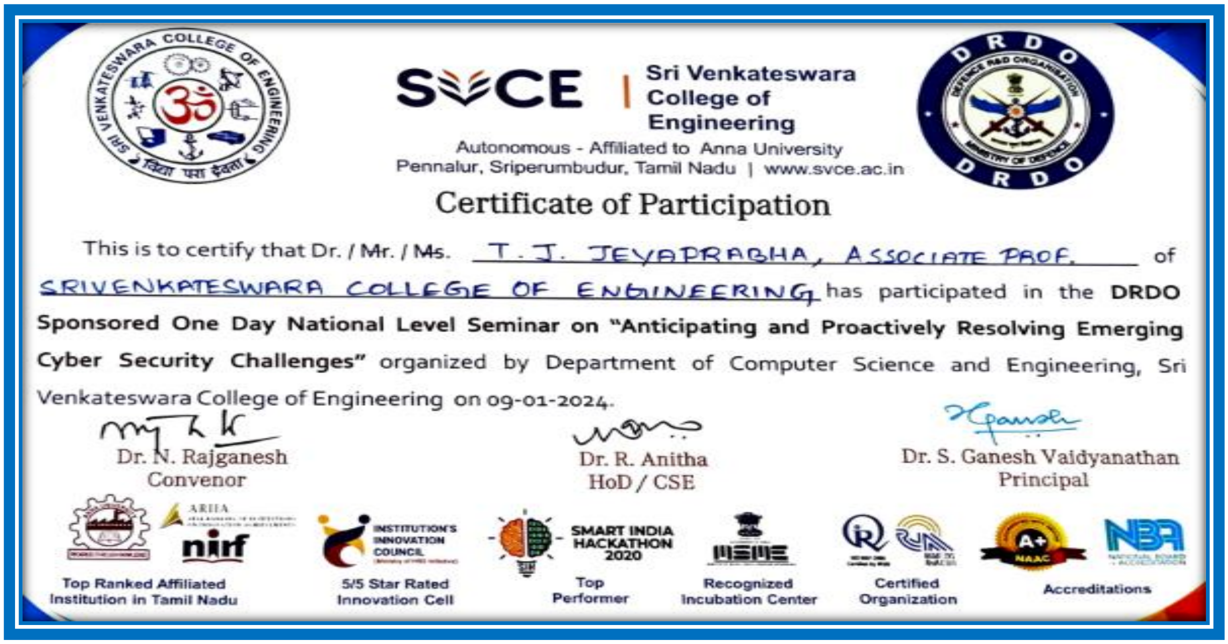
Quantum computing and quantum cryptography have made significant progress, further advancements are necessary to make them a practical reality in commercial systems. Various algorithms, such as the Coherent One Way (COW) quantum key distribution, represent advanced versions aiming to address limitations in the original quantum key distribution algorithm. However, implementing quantum systems for commercial IoT poses a substantial challenge due to the extensive scale and cost of quantum apparatus, which may be beyond the means of many organizations.

## REFERENCES

1. V.Kharchenko, "Reliability and security issues for IoT-based smart business center: Architecture and markov model", Proceedings of the 3rd International Conference on Mathematics and Computers in Sciences and in Industry, China, 2016.
2. J. A. Stankovic, "Research directions for the internet of things," IEEE Internet of Things Journal, vol. 1, no. 1, pp. 3-9, Feb. 2014.
3. R. P. Feynman, "Simulating physics with computers," International Journal of Theoretical Physics, vol. 21, no. 6-7, pp. 467-488, Jun. 1982.
4. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing" Proceedings of the International Conference on Computers, Systems and Signal Processing, Bangalore, 1984, pp. 175-179.

## FACULTY PARTICIPATION (Seminar/FDP/STTP/Workshop/Online Course/Conference):

- **Dr.T.J.Jeyaprabha** attended One Day National Level Seminar **(DRDO Sponsored)** on **"Anticipating and Proactively Resolving Emerging Cyber Security Challenges"** organized by the Department of Computer and Science Engineering, SVCE, Sriperumbudur on 09.01.2024



SVCE | Sri Venkateswara College of Engineering

Autonomous - Affiliated to Anna University

Pennalur, Sriperumbudur, Tamil Nadu | www.svce.ac.in

Certificate of Participation

This is to certify that Dr. / Mr. / Ms. T. J. JEYAPRABHA, ASSOCIATE PROF. of SRIVENKATESWARA COLLEGE OF ENGINEERING has participated in the **DRDO Sponsored One Day National Level Seminar on "Anticipating and Proactively Resolving Emerging Cyber Security Challenges"** organized by Department of Computer Science and Engineering, Sri Venkateswara College of Engineering on 09-01-2024.

Dr. N. Rajganesh
Convenor

Dr. R. Anitha
HoD / CSE

Dr. S. Ganesh Vaidyanathan
Principal

SRI VENKATESWARA COLLEGE OF ENGINEERING
DRDO
ARIIA
nirf
Top Ranked Affiliated Institution in Tamil Nadu
INSTITUTION'S INNOVATION COUNCIL
5/5 Star Rated Innovation Cell
SMART INDIA HACKATHON 2020
Top Performer
MSME
Recognized Incubation Center
Certified Organization
A+ NAAC
NBA
Accreditations

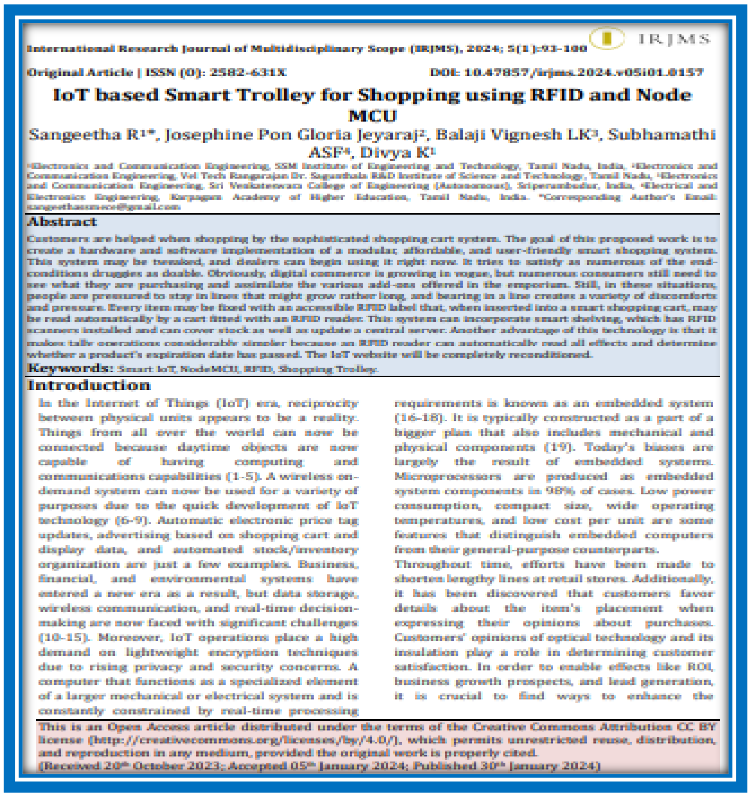
- **Around 32 Faculty Members** from our department attended **BIS Sensitization Programme for Faculty (BSPF)** organized by Standards Club SVCE in collaboration with the Bureau of Indian Standards (BIS), Chennai branch on 10.01.2024
- Mrs.S.Radhika attended ATAL FDP on **AI Evolution: "From Foundations to Generative AI"** organized by AICTE Training and Learning Bureau (AICTE-TLB) in collaboration with Microsoft and SAP & Edunet Foundation from 22.01.2024 to 27.01.2024

## FACULTY PROPOSAL SUBMISSION:

- Dr.P.Jothilakshmi, Mrs.C.Gomatheeswari Preethika and Mr.N.Sathish submitted a proposal titled **"Study of Performance and Safety Parameters of Wearable Compression E-Textile Products"** used for Massaging Applications to BIS.

## FACULTY PUBLICATION:

- Mr.L.K.Balaji Vignesh published a paper titled **"IoT based Smart Trolley for Shopping using RFID and Node MCU"**, in **International Research Journal of Multidisciplinary Scope,** Volume 5, Issue 1, Pages: 93-100, **DOI: https://doi.org/10.47857/irjms.2024.v05i01.0157 (Scopus Indexed)**



International Research Journal of Multidisciplinary Scope (IRJMS), 2024; 5(1):93-100 IRJMS

Original Article | ISSN (O): 2582-631X DOI: 10.47857/irjms.2024.v05i01.0157

# IoT based Smart Trolley for Shopping using RFID and Node MCU

Sangeetha R[1]*, Josephine Pon Gloria Jeyaraj[2], Balaji Vignesh LK[3], Subhamathi ASF[4], Divya K[1]

[1]Electronics and Communication Engineering, SSM Institute of Engineering and Technology, Tamil Nadu, India, [2]Electronics and Communication Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Tamil Nadu, [3]Electronics and Communication Engineering, Sri Venkateswara College of Engineering (Autonomous), Sriperambudur, India, [4]Electrical and Electronics Engineering, Karpagam Academy of Higher Education, Tamil Nadu, India. *Corresponding Author's Email: sangeethassm.ece@gmail.com

## Abstract

Customers are helped when shopping by the sophisticated shopping cart system. The goal of this proposed work is to create a hardware and software implementation of a modular, affordable, and user-friendly smart shopping system. This system may be tweaked, and dealers can begin using it right now. It tries to satisfy as numerous of the end-conditions druggies as doable. Obviously, digital commerce is growing in vogue, but numerous consumers still need to see what they are purchasing and assimilate the various add-ons offered in the emporium. Still, in these situations, people are pressured to stay in lines that might grow rather long, and bearing in a line creates a variety of discomforts and pressure. Every item may be fixed with an accessible RFID label that, when inserted into a smart shopping cart, may be read automatically by a cart fitted with an RFID reader. This system can incorporate smart shelving, which has RFID scanners installed and can cover stock as well as update a central server. Another advantage of this technology is that it makes tally operations considerably simpler because an RFID reader can automatically read all effects and determine whether a product's expiration date has passed. The IoT website will be completely reconditioned.

**Keywords:** Smart IoT, NodeMCU, RFID, Shopping Trolley.

## Introduction

In the Internet of Things (IoT) era, reciprocity between physical units appears to be a reality. Things from all over the world can now be connected because daytime objects are now capable of having computing and communications capabilities (1-5). A wireless on-demand system can now be used for a variety of purposes due to the quick development of IoT technology (6-9). Automatic electronic price tag updates, advertising based on shopping cart and display data, and automated stock/inventory organization are just a few examples. Business, financial, and environmental systems have entered a new era as a result, but data storage, wireless communication, and real-time decision-making are now faced with significant challenges (10-15). Moreover, IoT operations place a high demand on lightweight encryption techniques due to rising privacy and security concerns. A computer that functions as a specialized element of a larger mechanical or electrical system and is constantly constrained by real-time processing requirements is known as an embedded system (16-18). It is typically constructed as a part of a bigger plan that also includes mechanical and physical components (19). Today's biases are largely the result of embedded systems. Microprocessors are produced as embedded system components in 98% of cases. Low power consumption, compact size, wide operating temperatures, and low cost per unit are some features that distinguish embedded computers from their general-purpose counterparts.

Throughout time, efforts have been made to shorten lengthy lines at retail stores. Additionally, it has been discovered that customers favor details about the item's placement when expressing their opinions about purchases. Customers' opinions of optical technology and its insulation play a role in determining customer satisfaction. In order to enable effects like ROI, business growth prospects, and lead generation, it is crucial to find ways to enhance the

(Received 20th October 2023; Accepted 05th January 2024; Published 30th January 2024)

## STUDENT PARTICIPATION (Co-curricular Activities/Extra-curricular Activities):

- Ms.Lakshanaa, Ms.Purvaja, Mr.Mahesh and Mr.Rahul participated in the **Techfest "Shaastra" and demonstrated technical projects** organized by Indian Institute of Technology, Madras on 04.01.2024

GPS Map Camera
Chennai, Tamil Nadu, India
X6RM+V5P, Bonn Ave, Indian Institute Of Technology, Chennai, Tamil Nadu 600036, India
Lat 12.992009°
Long 80.233261°
04/01/24 02:14 PM GMT +05:30
Google

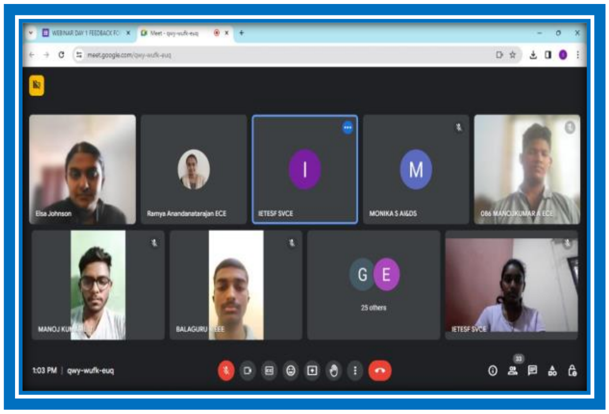
## STUDENT ACHIEVEMENTS:

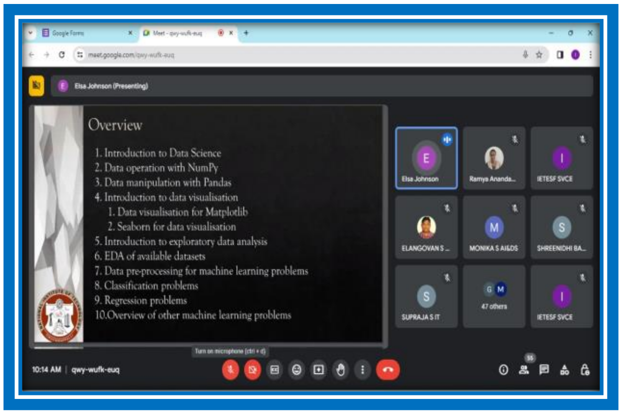
- Our Third year ECE students **(Mr.R.M.Manikandan, Mr.A.Logeshwar, Mr.K.Rahul, Mr.A.S.Praveen)** have won the title of **II Runner up (Team: Tech Titanium)** with a **cash prize of Rs.25,000** in the **Rajasthan Police Hackathon 1.0, 36 hours Hackathon** organized by the RACCAM (Rajasthan Police Cyber Crime Awareness Mission),Government of Rajasthan from 17.01.2024 to 18.01.2024 at Rajasthan International Center, Jaipur.

RACCAM
Rajasthan Police HACKATHON 1.0
Pay Open Category 2nd Runner-up
The Sum of Twenty Five Thousand Only
₹ 25,000

## EVENT ORGANIZED:

- ECEA and RAIC organized Webinar cum Workshop Series on **"Data Analytics and Machine Learning with Python"** from 13.01.2024, followed by 20.01.2024 and 27.01.2024 by Ms.Elsa Sharu Johnson, Prime Minister's Research Fellow, Department of Instrumentation and Control Engineering, NIT, Trichy. The event was coordinated by Dr.T.J.Jeyaprabha, ASP/ECE, Mr.S.Elangovan, AP/ECE and Dr.A.Ramya, AP/ECE.



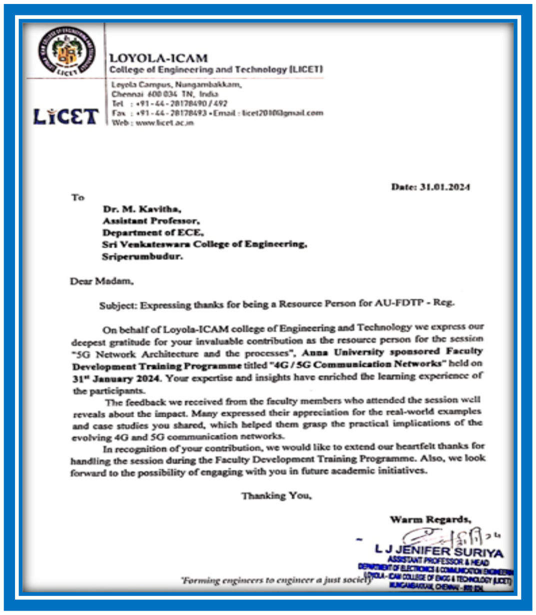


Overview

1. Introduction to Data Science
2. Data operation with NumPy
3. Data manipulation with Pandas
4. Introduction to data visualisation
    1. Data visualisation for Matplotlib
    2. Seaborn for data visualisation
5. Introduction to exploratory data analysis
6. EDA of available datasets
7. Data pre-processing for machine learning problems
8. Classification problems
9. Regression problems
10. Overview of other machine learning problems

## FACULTY ACHIEVEMENTS:

- Dr.M.Bindhu acted as a Resource Person in **Faculty Development Training Program (Anna University Sponsored)** and delivered a talk on **"4G/5G Communication Networks-5G Challenges, Architecture and Techniques"** organized by Loyola ICAM College of Engineering & Technology, Chennai on 30.01.2024
- Dr.K.Kavitha acted as a Resource Person in **Faculty Development Training Program (Anna University Sponsored)** and delivered a talk on **"4G/5G Communication Networks-5G protocols"** organized by Loyola ICAM College of Engineering & Technology, Chennai on 31.01.2024



LOYOLA-ICAM
College of Engineering and Technology (LICET)
Loyola Campus, Nungambakkam,
Chennai 600 034 TN, India
Tel : +91-44-28178490 / 492
Fax : +91-44-28178493 • Email : licet2010@gmail.com
Web : www.licet.ac.in

LICET

**Date: 31.01.2024**

To
**Dr. M. Kavitha,**
**Assistant Professor,**
**Department of ECE,**
**Sri Venkateswara College of Engineering,**
**Sriperumbudur.**

Dear Madam,

Subject: Expressing thanks for being a Resource Person for AU-FDTP - Reg.

On behalf of Loyola-ICAM college of Engineering and Technology we express our deepest gratitude for your invaluable contribution as the resource person for the session "5G Network Architecture and the processes", **Anna University sponsored Faculty Development Training Programme** titled **"4G / 5G Communication Networks"** held on **31st January 2024**. Your expertise and insights have enriched the learning experience of the participants.

The feedback we received from the faculty members who attended the session well reveals about the impact. Many expressed their appreciation for the real-world examples and case studies you shared, which helped them grasp the practical implications of the evolving 4G and 5G communication networks.

In recognition of your contribution, we would like to extend our heartfelt thanks for handling the session during the Faculty Development Training Programme. Also, we look forward to the possibility of engaging with you in future academic initiatives.

Thanking You,

**Warm Regards,**

31/1/24

L J JENIFER SURIYA
ASSISTANT PROFESSOR & HEAD
DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING
LOYOLA-ICAM COLLEGE OF ENGG & TECHNOLOGY (LICET)
NUNGAMBAKKAM, CHENNAI - 600 034.

*"Forming engineers to engineer a just society"*

## Reviewer/Editorial Board Member:

- Dr.T.J.Jeyaprabha, Mr.L.K.Balaji Vignesh acted as reviewer for **IEEE International Conference on Distributed Computing and Optimization Techniques (ICDCOT–2024)** during 15-16 March 2024 in association IEEE Bangalore Section organized by SJB Institute of Technology, Bengaluru.
- Dr.T.J.Jeyaprabha, Mr.L.K.Balaji Vignesh acted as reviewer for **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 organized by H.K.E. Society's S.L.N. College of Engineering, Raichur, Karnataka.

JANUARY, 2024 VOL. 4 ISSUE 1

# EDITORIAL BOARD

# PROGRAMMES OFFERED BY THE DEPARTMENT

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

# TOP RECRUITERS

Infosys
wipro
Ford
FLSmidth
PayPal
verizon
ASHOK LEYLAND
ABB
ThoughtWorks
Tech Mahindra
Atos | Syntel
Capgemini CONSULTING.TECHNOLOGY.OUTSOURCING
HEXAWARE
freshworks
Informatica
HCL
HYUNDAI
Honeywell