International Journal for Modern Trends in Science and Technology
Volume 12, Special Issue 01, pages 1150-1157
ISSN: 2455-3778 online
Available online at: http://ijmtst.com/ICRCSET2026.html
DOI: https://doi.org/10.5281/zenodo.19769846

Smart IOT Bicycle Anti-Theft and GPS Tracking Alaram System

Sai Srinivas Vellela, N. Dhana Lakshmi, P. Uma Shankar, N. Ananya, Shaik Adam Shafi

Department of CSE – Data Science, Chalapathi Institute of Technology, Guntur-522016, A.P, India

To Cite this Article
Sai Srinivas Vellela, N. Dhana Lakshmi, P. Uma Shankar, N. Ananya & Shaik Adam Shafi (2026). Smart IOT Bicycle Anti-Theft and GPS Tracking Alaram System. International Journal for Modern Trends in Science and Technology, 12(SI01), 1150-1157. https://doi.org/10.5281/zenodo.19769846

Article Info
Received: 12 March 2026; Revised: 07 April 2026; Accepted: 10 April 2026.

KEYWORDS

ESP32 Electric Vehicles (EV), Battery Management System (BMS), Arduino Uno, State of Charge (SoC), Overcharge Protection.

ABSTRACT

The system integrates multiple technologies, including Internet of Things(IoT), GPS tracking, and sensor-based detection, to provide a comprehensive and intelligent security solution. Sensors such as vibration or accelerometer modules are employed to detect unauthorized movement or tampering. Upon detection of suspicious activity, the system immediately activates an audible alarm to deter theft and simultaneously transmits real time location data to the user via GSM/GPRS or cloud-based communication platforms. Experimental analysis demonstrates that the proposed system significantly enhances bicycle security by combining detection, alerting, tracking, and monitoring functionalities into a single integrated platform. This work contributes to the advancement of smart security systems and demonstrates the effective application of IoT in real world anti-theft solutions.Bicycle usage as an economical and eco-friendly mode of transportation has led to a corresponding rise in bicycle theft, highlighting the limitations of traditional security mechanisms such as locks and chains. These conventional methods fail to provide real-time monitoring, alert systems, or recovery solutions. To address this issue, this project proposes a Smart IoT-Based Bicycle Anti-Theft and GPS Tracking System using the Raspberry Pi as the central processing unit

I. INTRODUCTION

In recent years, bicycles have gained significant popularity as a cost-effective, eco-friendly, and convenient mode of transportation. They are widely used for daily commuting, fitness, and short-distance travel. However, the increasing number of bicycles has also led to a rise in theft incidents, making security a major concern for bicycle owners. Traditional security measures such as mechanical locks and chains provide only a basic level of protection and can be easily bypassed by skilled thieves. Moreover, these conventional methods do not offer any mechanism for tracking or recovering a stolen bicycle [1].

With the rapid advancement of the Internet of Things (IoT), smarter and more efficient security systems have

become possible. IoT enables devices to communicate and share data over the internet, allowing real-time monitoring and control. By leveraging IoT technology, it is possible to design intelligent anti-theft systems that not only detect unauthorized access but also provide instant alerts and location tracking capabilities [2].

In this project, a smart bicycle anti-theft system is developed using the Raspberry Pi as the core processing unit. The system integrates various components such as motion or vibration sensors to detect tampering, a GPS module to determine real-time location, and communication modules to send alerts to the user. When any suspicious activity is detected, the system triggers an alarm to deter the thief and simultaneously notifies the owner with the bicycle's location details.

Furthermore, advanced features such as camera integration can be incorporated to capture images or videos of the intruder, enhancing security through evidence collection. The system is designed to be compact, energy-efficient, and cost-effective, making it suitable for real-world applications. By combining detection, alert mechanisms, and tracking into a single platform, the proposed system aims to overcome the limitations of existing solutions and provide a reliable and intelligent approach to bicycle security.

This project demonstrates how modern IoT-based technologies can be effectively utilized to address real-world problems, improving both prevention and recovery in bicycle theft scenarios.

2. REVIEW LITERATURE SURVEY

In recent years, significant research has been carried out in the field of vehicle and bicycle security systems, particularly with the integration of the Internet of Things (IoT). Early anti-theft systems primarily relied on GSM and GPS technologies, where the location of the vehicle was obtained using a GPS module and transmitted to the user via SMS. These systems were relatively simple and cost-effective; however, they lacked continuous real-time monitoring, automation, and user-friendly interfaces, limiting their overall effectiveness [1].

With advancements in embedded systems, researchers began incorporating microcontrollers and single-board computers such as the Raspberry Pi to develop more intelligent and flexible security solutions. These modern systems utilize sensors such as vibration sensors, accelerometers, and motion detectors to identify unauthorized access or tampering. When suspicious activity is detected, alerts are generated instantly, improving the chances of preventing theft at an early stage [2].

Further developments in IoT-based security systems introduced cloud computing and mobile applications, enabling users to monitor their vehicles remotely in real time. These systems provide features such as live tracking, push notifications, and historical data analysis through intuitive dashboards. One important advancement is geo-fencing, where users receive alerts if the vehicle moves outside a predefined safe zone, thereby adding an extra layer of security and control [3].

Recent studies have also explored the integration of camera modules and image processing techniques to enhance security systems. In such implementations, images or videos of the intruder are captured and stored in cloud platforms or sent directly to the user via email or mobile applications. This feature is particularly useful for evidence collection and assists in identifying suspects during investigations [2].

In addition, researchers have focused on improving power efficiency and system reliability, especially for compact applications like bicycles. Techniques such as rechargeable battery systems and low-power components have been implemented to ensure continuous operation without frequent maintenance. Despite these advancements, many existing systems suffer from limitations such as high cost, complex design, or lack of integration of multiple features into a single platform [1].

Therefore, there is a clear need for a comprehensive, cost-effective, and integrated solution that combines real-time tracking, intelligent sensing, alert mechanisms, and evidence collection. The proposed system aims to address these limitations by providing a unified IoT-based bicycle anti-theft solution that enhances both theft prevention and recovery efficiency.

3. RESEARCH METHODOLOGY

The proposed Smart IoT-Based Bicycle Anti-Theft and GPS Tracking System is developed using a systematic methodology that integrates hardware and software components to achieve real-time monitoring, detection, and tracking. The methodology involves system design, component integration, data processing, and communication mechanisms to ensure efficient operation.

1. System Design and Architecture

The system is designed around the Raspberry Pi, which acts as the central processing unit. It interfaces with various modules such as sensors, GPS, communication modules, and output devices. The architecture follows an IoT-based model where data is collected from sensors, processed locally, and transmitted to the user through network communication [1].

2. Data Acquisition (Sensing Mechanism)

To detect unauthorized access or tampering, sensors such as vibration sensors or accelerometers are used. These sensors continuously monitor the movement of the bicycle. When abnormal motion is detected beyond a predefined threshold, the sensor sends a signal to the Raspberry Pi for further processing [2].

3. Data Processing and Decision Making

The Raspberry Pi processes the input data from the sensors using programmed algorithms. The system distinguishes between normal movement (e.g., user activity) and suspicious activity (e.g., theft attempt). If a potential theft is detected, the system triggers predefined actions such as activating an alarm and initiating tracking.

4. Alert and Notification System

Once a theft attempt is identified, the system immediately activates a buzzer to produce an audible alarm, which acts as a deterrent. Simultaneously, notifications are sent to the user through GSM/GPRS or internet-based services. These notifications may include SMS alerts or app-based messages containing real-time information about the incident [1].

5. GPS-Based Tracking

A GPS module is integrated into the system to provide real-time location data. Upon detection of theft, the GPS module continuously retrieves the geographical coordinates of the bicycle. This data is transmitted to the user, allowing live tracking through mapping services such as Google Maps [2].

6. Image Capture and Evidence Collection (Optional Feature)

For enhanced security, a camera module can be incorporated into the system. When triggered, it captures images of the surrounding environment or the intruder. These images are then stored or sent to the user via cloud storage or email, providing useful evidence for identification and investigation.

7. Communication and IoT Integration

The system uses IoT technology to enable communication between the device and the user. Data is transmitted through wireless communication modules such as Wi-Fi or GSM. A cloud platform or mobile application can be used to monitor the bicycle remotely, providing features like live tracking, alerts, and status updates.

8. Power Management

The entire system is powered using a rechargeable battery to ensure portability and continuous operation. Power-efficient components and optimized programming are used to reduce energy consumption, making the system suitable for long-term usage without frequent recharging.

4. PROPOSED METHODOLOGY

The proposed system introduces an integrated IoT-based smart bicycle anti-theft and tracking solution that combines real-time detection, alert mechanisms, and location tracking into a single efficient platform. The system is built around the Raspberry Pi, which acts as the central processing unit and coordinates all hardware and software operations. It continuously monitors the condition of the bicycle using sensors such as vibration sensors or accelerometers to detect unauthorized movement. These sensors are programmed with threshold values to differentiate between normal usage

and suspicious activity, ensuring accurate detection of theft attempts [1].

When abnormal movement is detected, the Raspberry Pi processes the input data and immediately triggers a buzzer alarm to alert nearby individuals and deter the intruder. Simultaneously, the system sends real-time notifications to the user through GSM or internet-based communication modules, ensuring that the user is informed instantly regardless of their location. In addition to alert mechanisms, the system incorporates a GPS module that continuously tracks the bicycle's geographical coordinates. This location data is transmitted to the user and can be viewed through mapping platforms such as Google Maps, enabling effective tracking and recovery of the stolen bicycle [2].

Furthermore, the system utilizes IoT technology to enable remote monitoring through cloud platforms or mobile applications. This allows users to access real-time updates, track movement history, and monitor the status of their bicycle from anywhere. For enhanced security, an optional camera module can be integrated to capture images or videos during a theft attempt, which are then stored or sent to the user as evidence. The entire system is powered by a rechargeable battery and is designed with power-efficient components to ensure long-term operation. Overall, the proposed methodology provides a comprehensive, cost-effective, and intelligent solution by integrating detection, alerting, tracking, and monitoring into a unified system, thereby significantly improving bicycle security compared to existing methods.

WORKING PRINCIPLE

The working principle of the proposed smart bicycle anti-theft and tracking system is based on continuous monitoring, intelligent detection, and real-time communication using IoT technology. The system is centered around the Raspberry Pi, which acts as the main controller and processes data received from various connected modules. A vibration sensor or accelerometer is mounted on the bicycle to continuously monitor its movement. Under normal conditions, the system remains in a standby mode; however, when unauthorized movement or tampering is detected beyond a predefined threshold, the sensor sends a signal to the Raspberry Pi for further action [1].

Upon receiving this signal, the Raspberry Pi analyzes the data and identifies it as a potential theft attempt. Immediately, it activates a buzzer alarm to alert nearby individuals and discourage the thief. At the same time, the system initiates the communication process by sending a notification to the user through GSM or internet-based services. This notification typically includes an alert message along with the real-time location of the bicycle [2].

The GPS module plays a crucial role by continuously acquiring the geographical coordinates of the bicycle. These coordinates are transmitted to the user and can be viewed on mapping applications such as Google Maps, enabling live tracking of the bicycle's position. Additionally, if a camera module is integrated, it captures images or video during the theft attempt, which are then stored or sent to the user for evidence purposes.

The entire system operates using a rechargeable power source and is designed for low power consumption to ensure continuous functionality. Through the integration of sensing, processing, alerting, and tracking mechanisms, the system effectively prevents theft and enhances the chances of recovery, making it a reliable and intelligent security solution.

BLOCK DIAGRAM

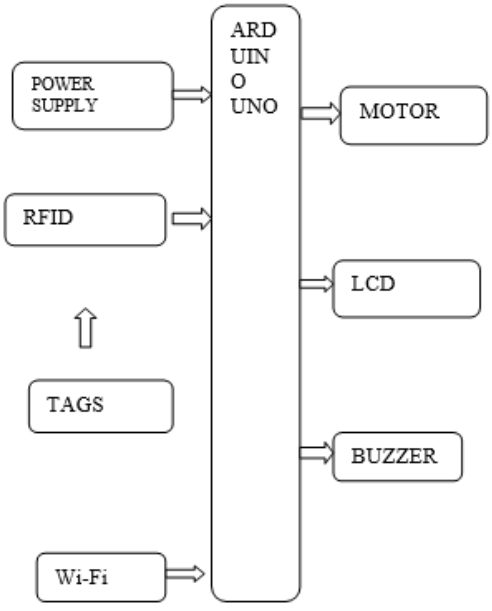

Fig 4.1: Block Diagram

5. RESULTS AND OUTCOMES

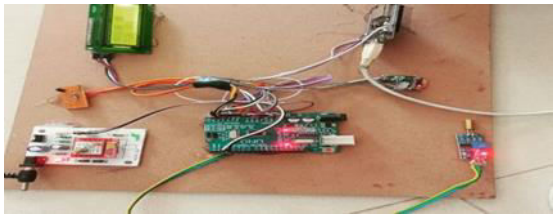

Fig 5.1: Output 1

The implementation of the proposed smart bicycle anti-theft and tracking system demonstrates effective performance in terms of real-time detection, alert generation, and location tracking. The system successfully detects unauthorized movement using vibration or motion sensors, and the Raspberry Pi accurately processes the sensor data to identify potential theft attempts. Upon detection, the buzzer alarm is activated instantly, which helps in deterring intruders and drawing attention to the bicycle [1].

The GPS module provides reliable and accurate real-time location data, enabling continuous tracking of the bicycle. The transmitted coordinates can be easily accessed by the user through mobile devices and visualized using mapping platforms, ensuring quick response and recovery. The alert notification system also performs efficiently by sending immediate messages to the user through GSM or internet-based communication, minimizing the delay between detection and user awareness [2].

The integration of IoT technology allows remote monitoring and control, improving the overall usability of the system. The optional camera module, when implemented, successfully captures images during suspicious activity, which can be used as supporting evidence. The system operates with low power consumption and maintains stable performance over extended periods using a rechargeable battery.

The integration of IoT technology allows remote monitoring and control, improving the overall usability of the system. The optional camera module, when implemented, successfully captures images during suspicious activity, which can be used as supporting evidence. The system operates with low power consumption and maintains stable performance over extended periods using a rechargeable battery.

CONCLUSION

The proposed Smart IoT-Based Bicycle Anti-Theft and GPS Tracking System provides an effective and reliable solution to address the increasing problem of bicycle theft. By integrating advanced technologies such as IoT, real-time sensing, and GPS tracking, the system overcomes the limitations of traditional security methods that lack monitoring and recovery capabilities. The use of the Raspberry Pi as the central controller enables efficient processing of sensor data and seamless coordination between different modules [1].

The system successfully detects unauthorized movement using sensors and responds immediately by activating an alarm and sending real-time notifications to the user. The integration of GPS tracking ensures accurate location monitoring, which significantly improves the chances of recovering a stolen bicycle. Additionally, features such as IoT-based remote monitoring and optional camera integration enhance the overall security by providing continuous updates and evidence collection [2].

The results of the project demonstrate that the system is cost-effective, compact, and energy-efficient, making it suitable for practical real-world applications. By combining detection, alerting, tracking, and monitoring into a single platform, the proposed solution offers a comprehensive approach to bicycle security. In conclusion, this project highlights the potential of IoT-based systems in improving personal asset security and contributes to the development of smart and intelligent transportation safety solutions.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] K. K. . Kommineni and A. . Prasad, “A Review on Privacy and Security Improvement Mechanisms in MANETs”, Int J Intell Syst Appl Eng, vol. 12, no. 2, pp. 90–99, Dec. 2023.

[2] Kommineni, K.K., Prasad, A. Enhancing Data Security and Privacy in SDN-Enabled MANETs Through Improved Data Aggregation Protection and Secrecy. Wireless Pers Commun 139, 855–882 (2024). https://doi.org/10.1007/s11277-024-11635-w

[3] “Blockchain-Enabled Secure Data Aggregation for SDN-Enabled Ad-Hoc Networks,” International Journal of Intelligent Engineering and Systems, vol. 18, no. 5, pp. 704–717, Jun. 2025, doi: https://doi.org/10.22266/ijies2025.0630.49.

[4] K. K. Kommineni, P. Ande, "Blockchain-driven key management and privacy-preserving data Aggregation Scheme for SDN-enabled MANETs," International Journal of Intelligent Engineering and Systems, vol. 18–18, no. 9, pp. 601–615, 2025, doi: 10.22266/ijies2025.1031.39.

[5] Kumar, K. K., Kumar, S. G. B., Rao, S. G. R., & Sydulu, S. S. J. (2017, November). Safe and high secured ranked keyword searchover an outsourced cloud data. In 2017 International Conference on Inventive Computing and Informatics (ICICI) (pp. 20-25). IEEE.

[6] K. K. Kommineni, S. J. Basha, M. Sandeep, P. S. Vadana, T. S. R. Sai and D. S. Kumar, "A Review on IoT-based Defensive Devices for Women Security," 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2023, pp. 99-104, doi: 10.1109/ICACCS57279.2023.10113015.

[7] Vellela, S. S., & Balamanigandan, R. (2024). Optimized clustering routing framework to maintain the optimal energy status in the wsn mobile cloud environment. Multimedia Tools and Applications, 83(3), 7919-7938.

[8] Vellela, S. S., & Balamanigandan, R. (2023). An intelligent sleep-awake energy management system for wireless sensor network. Peer-to-Peer Networking and Applications, 16(6), 2714-2731.

[9] Vellela, S. S., & Balamanigandan, R. (2022, December). Design of Hybrid Authentication Protocol for High Secure Applications in Cloud Environments. In 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS) (pp. 408-414). IEEE.

[10] Vellela, S. S., Balamanigandan, R., & Praveen, S. P. (2022). Strategic survey on security and privacy methods of cloud computing environment. Journal of Next Generation Technology, 2(1).

[11] Reddy, N. V. R. S., Chitteti, C., Yesupadam, S., Desanamukula, V. S., Vellela, S. S., & Bommagani, N. J. (2023). Enhanced Speckle Noise Reduction in Breast Cancer Ultrasound Imagery Using a Hybrid Deep Learning Model. Ingenierie des Systemes d'Information, 28(4), 1063.

[12] Vellela, S. S., & Balamanigandan, R. (2024). An efficient attack detection and prevention approach for secure WSN mobile cloud environment. Soft Computing, 28(19), 11279-11293.

[13] Polasi, P. K., Vellela, S. S., Narayana, J. L., Simon, J., Kapileswar, N., Prabu, R. T., & Rashed, A. N. Z. (2026). Data rates transmission, operation performance speed and figure of merit signature for various quadurature light sources under spectral and thermal effects. Journal of Optics, 55(1), 633-643.

[14] Vellela, S. S., & Krishna, A. M. (2020). On Board Artificial Intelligence With Service Aggregation for Edge Computing in Industrial Applications. Journal of Critical Reviews, 7(07).

[15] Vellela, S. S., Rao, M. V., Mantena, S. V., Reddy, M. J., Vatambeti, R., & Rahman, S. Z. (2024). Evaluation of Tennis Teaching Effect Using Optimized DL Model with Cloud Computing System. International Journal of Modern Education and Computer Science (IJMECS), 16(2), 16-28.

[16] Biyyapu, N., Veerapaneni, E. J., Surapaneni, P. P., Vellela, S. S., & Vatambeti, R. (2024). Designing a modified feature aggregation model with hybrid sampling techniques for network intrusion detection. Cluster Computing, 27(5), 5913-5931.

[17] Vuyyuru, L. R., Purimetla, N. R., Reddy, K. Y., Vellela, S. S., Basha, S. K., & Vatambeti, R. (2025). Advancing automated street crime detection: a drone-based system integrating CNN models and enhanced feature selection techniques. International Journal of Machine Learning and Cybernetics, 16(2), 959-981.

[18] Praveen, S. P., Vellela, S. S., & Balamanigandan, R. (2024). SmartIris ML: harnessing machine learning for enhanced multi-biometric authentication. Journal of Next Generation Technology (ISSN: 2583-021X), 4(1).

[19] Vellela, S. S., Roja, D., Purimetla, N. R., Thalakola, S., Vuyyuru, L. R., & Vatambeti, R. (2025). Cyber threat detection in industry 4.0: Leveraging GloVe and self-attention mechanisms in BiLSTM for enhanced intrusion detection. Computers and Electrical Engineering, 124, 110368.

[20] Vellela, S. S., Varshini, K., Jeevana, M., Kadheer, S. K., & Kumar, T. P. (2024). Iot based smart irrigation and controlling system. IoT Based Smart Irrigation and Controlling System, International Journal for Modern Trends in Science and Technology, 10(02), 77-85.

[21] Vellela, S. S., Manne, V. K., Trividha, G., Chaithanya, L., & Shaik, A. (2025). Intelligent transportation systems ai and iot for sustainable urban traffic management. Available at SSRN 5250812.

[22] Vindhya, A. S., Vellela, S. S., Malathi, N., Vullam, N. R., Vuyyuru, L. R., & Rao, T. (2025, September). Integrating Quantum Computing with Genomic Data Analysis: A Next-Generation Approach for Predicting Disease Susceptibility. In 2025 4th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) (pp. 1168-1173). IEEE.

[23] Vellela, S. S., Rao, M. V., Krishna, C. V. M., Rao, T. S., & Dasthavejula, R. (2026). Piezoelectric and Shape-Memory Materials for Actuators and Energy Harvesting in Mechanical, Electronics, and Biomedical Engineering Using AI-Based Design. In Advanced Materials for Biomedical Devices (pp. 195-206). CRC Press.

[24] Vellela, S. S., Malathi, N., Vuyyuru, L. R., Javvadi, S., Rao, T. S., Bindu, M. N. H., & Rao, K. N. (2025, August). Improving Medical Image Analysis with Convolutional Neural Networks (Cnns). In 2025 International Conference on Intelligent and Secure Engineering Solutions (CISES) (pp. 579-584). IEEE.

[25] Roja, D., Jidugu, S. K., Rao, T. S., Vuyyuru, L. R., Vellela, S. S., & Ranjani, B. S. (2025, December). High-Fidelity Image Synthesis using Enhanced Generative Adversarial Networks with Attention Mechanisms. In 2025 International Conference on NexGen Networks and Cybernetics (IC2NC) (pp. 885-890). IEEE.

[26] Pakalapati, S., Rani, C. J., Vellela, S. S., Thanuja, N., & Bindu, M. N. H. (2025, November). Progressive GAN-based Framework for Realistic Image Generation and Style Transfer. In 2025 5th International Conference on Evolutionary Computing and Mobile Sustainable Networks (ICECMSN) (pp. 474-479). IEEE.

[27] Yanamadala, N., & Vellela, S. S. (2025, June). Ensuring Authenticity and Confidentiality in Images using SHA-ECC Fusion. In 2025 Second International Conference on Networks and Soft Computing (ICNSoC) (pp. 684-689). IEEE.

[28] Rao, M. V., Sreeraman, Y., Mantena, S. V., Gundu, V., Roja, D., & Vatambeti, R. (2024). Brinjal Crop yield prediction using Shuffled shepherd optimization algorithm based ACNN-OBDLSTM model in Smart Agriculture. Journal of Integrated Science and Technology, 12(1), 710-710.

[29] Reddy, B. V., Kumar, A. H., Gopi, C., Prasad, Y. V. D., Vellela, S. S., & Roja, D. (2025, April). Machine learning based automated liver fibrosis stage diagnosis with prediction. In 2025 International Conference on Advances in Modern Age Technologies for Health and Engineering Science (AMATHE) (pp. 1-6). IEEE.

[30] Burra, R. S., APCV, G. R., & Vellela, S. S. (2024). Enhancing Ddos Detection Through Semi-Supervised Machine Learning: A Novel Approach for Improved Network Security. International Research Journal of Modernization in Engineering Technology and Science, 6.

[31] Vellela, S. S., Vullam, N. R., Gorintla, S., Rao, T. S., & Harinadh, T. (2025, July). Exploring the Anti-Inflammatory Potential of Green-Synthesized Pyrazolines. In 2025 6th International Conference on Data Intelligence and Cognitive Informatics (ICDICI) (pp. 814-819). IEEE.

[32] Vellela, S. S., Chandra, S. S., Thommandru, R., Mastan Basha, S., & Sri Ram, D. (2023). Novel Approach to Mitigate Starvation in Wireless Mesh Networks. Available at SSRN 5262254.

[33] Praveen, S. P., Vellela, S. S., Sharma, K., & Dalavai, L. Quantitative Evaluation of Smart Textile Adoption in Rural Weaving Communities using Machine Learning. Journal of the Textile Association, 86(3), 277-284.

[34] Mandava, R., Dalavai, L., Vellela, S. S., Purimetla, N. R., Mohan, B. K., & Harinadh, T. (2025, June). An In-Depth Study on the Integration of Explainable AI Techniques to Enhance Interpretability in Clinical Risk Prediction Models. In 2025 Second International Conference on Networks and Soft Computing (ICNSoC) (pp. 43-47). IEEE.

[35] Rao, M. V., Krishna, C. V. M., Vellela, S. S., Vara, J., Paul, K. J., & Rao, K. N. (2025, March). Enhancement and Blind Image Restoration for Quality Improvements of Camera Captured Pictures/Videos. In 2025 7th International Conference on Intelligent Sustainable Systems (ICISS) (pp. 791-796). IEEE.

[36] Vellela, S. S., Anusha, P., Vullam, N. R., Jala, J., Bellapu, V. S., & Vindhya, A. S. (2025, October). Quantum Cryptography and Key Distribution for Secure Communication in the Post Quantum World. In 2025 International Conference on Sustainable Communication Networks and Application (ICSCN) (pp. 619-624). IEEE.

[37] Vellela, S. S., Vuyyuru, L. R., Jidugu, S. K., Rao, M. P., & Srinivas, B. R. (2025, November). The Impact Of Quantum Computing On Blockchain Security And Quantum Resistant Protocols. In 2025 2nd International Conference on Intelligent Systems for Cybersecurity (ISCS) (pp. 1-6). IEEE.

[38] Kumar, M. S., Vellela, S. S., Gorintla, S., Malathi, N., Rao, T. S., & Rani, N. R. (2025, October). Intelligent Resource Allocation in Wireless Sensor Networks: A Hybrid Optimization Approach for Energyconstrained Environments. In 2025 2nd International Conference on Electronic Circuits and Signaling Technologies (ICECST) (pp. 724-729). IEEE.

[39] Krishna, T. V., Rani, N. R., Ranjani, B. S., & Vellela, S. S. (2025). Distributed Big-Data Analytics with PySpark for Personalized Restaurant Recommendation Systems. Journal of Next Generation Technology (ISSN: 2583-021X), 5(6).

[40] Harinadh, T., Anusha, P., Roja, D., Vellela, S. S., & Muthukumar, P. (2025). PySpark Orchestrated Machine Learning Paradigms for Advanced Network Intrusion Detection. Journal of Next Generation Technology (ISSN: 2583-021X), 5(6).

[41] Mandava, R., Haritha, K., Vellela, S. S., Purimetla, N. R., Mohan, B. K., & Harinadh, T. (2025, June). Analysing User Perceptions of Trust in Financial Systems Using Explainable AI. In 2025 Second International Conference on Networks and Soft Computing (ICNSoC) (pp. 26-30). IEEE.

[42] Burra, R. S., APCV, G. R., & Vellela, S. S. (2024). Strategic Insights: Unleashing the Power of Big Data Analytics for Credit Investigation and Risk Mitigation in Commercial Banking. International Journal of Progressive Research in Engineering Management and Science, 4(01), 458-464.

[43] Vellela, S. S., Purimetla, N. R., Vindhya, A. S., Vullam, N. R., Srinivas, B. R., & Vuyyuru, L. R. (2025, October). Design and Simulation of Quantum Error Correction Codes for Scalable Quantum Architectures. In 2025 7th International Conference on Innovative Data Communication Technologies and Application (ICIDCA) (pp. 1570-1575). IEEE.

[44] Devana, V. K. R., Beno, A., Devadoss, C. P., Sukanya, Y., Ravi Sankar, C. V., Balamuralikrishna, P., ... & Babu, K. V. (2024). A compact self isolated MIMO UWB antenna with band notched characteristics. IETE Journal of Research, 70(8), 6677-6688.

[45] Potti, Dr Balamuralikrishna. "Characteristic Mode Analysis of Two Port Semi-circular Arc-Shaped Multiple-Input-Multiple-Output Antenna With High Isolation for 5G Sub-6 GHz and Wireless Local Area Network Applications." Int J Commun Syst (2022): e5257.

[46] Srija, V., & Krishna, P. B. M. (2015). Implementation of agricultural automation system using web & gsm technologies. International Journal of Research in Engineering and Technology, 4(09), 385-389.

[47] Potti, B., Subramanyam, M. V., & Prasad, K. S. (2013). A packet priority approach to mitigate starvation in wireless mesh network with multimedia traffic. International Journal of Computer Applications, 62(14).

[48] Potti, B., Subramanyam, M. V., & Satya Prasad, K. (2016). Adopting Multi-radio Channel Approach in TCP Congestion Control Mechanisms to Mitigate Starvation in Wireless Mesh Networks. In Information Science and Applications (ICISA) 2016 (pp. 85-95). Springer Singapore.

[49] Potti, D. B., MV, D. S., & Kodati, D. S. P. (2015). Hybrid genetic optimization to mitigate starvation in wireless mesh networks. Hybrid Genetic Optimization to Mitigate Starvation in Wireless Mesh Networks, Indian Journal of Science and Technology, 8(23).

[50] Devana, V. K. R., Beno, A., Alzaidi, M. S., Krishna, P. B. M., Divyamrutha, G., Awan, W. A., ... & Alathbah, M. (2024). A high bandwidth dimension ratio compact super wide band-flower slotted microstrip patch antenna for millimeter wireless applications. Heliyon, 10(1).

[51] Doss, B., Balamuralikrishna, P., Nagaraju, C. H., Lakshmaiah, D., & Naresh, S. Blockchain-Based Secure Big Data Storage on the Cloud. In Blockchain Technology for IoT and Wireless Communications (pp. 11-18). CRC Press.

[52] Kapileswar, N. and Simon, J., 2025, October. A Hybrid Acoustic-Optical Communication Technique for Ultra-Low Latency Underwater IoT Network. In 2025 2nd International Conference on Electronic Circuits and Signaling Technologies (ICECST) (pp. 468-473). IEEE.

[53] Simon, J. and Kapileswar, N., 2025, June. Federated deep learning-driven cloud-IoT framework for real-time healthcare monitoring and privacy-preserving anomaly detection. In 2025 3rd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS) (pp. 1866-1871). IEEE.

[54] Kapileswar, N. and Simon, J., 2025, June. Quantum-Resilient Consensus Mechanisms for Scalable Blockchain Networks using Lattice-based Cryptography. In 2025 6th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) (pp. 1849-1854). IEEE.

[55] Kapileswar, N. and Simon, J., 2025, August. DeepCurrent: An Attention-Driven Graph Neural Network for Energy-Efficient Routing and Data Aggregation in UIoT Networks. In 2025 International Conference on Modern Sustainable Systems (CMSS) (pp. 716-720). IEEE.

[56] Sathish, K., 2025, February. Dynamic Topology Optimizing Magnetic Circuits for Underwater Systems for Improved Performance and Efficiency. In 2025 International Conference on Electronics and Renewable Systems (ICEARS) (pp. 433-438). IEEE.

[57] Sathish, K., 2025, September. Adaptive Fusion and Feature Refinement for Visibility Enhancement in Turbid Underwater Scenes. In 2025 3rd International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI) (pp. 456-460). IEEE.

[58] R. Saravanakumar et al., "Dual-band performance enhancement of square wheel antennas with FR4 substrate for sub-7 GHz applications," in Proc. ACROSET, IEEE, Sept. 2024, pp. 1–7.

[59] D. N. Ravikiran and C. G. Dethe, "Improvements in routing algorithms to enhance lifetime of wireless sensor networks," Int. J. Comput. Netw. Commun., vol. 10, no. 2, pp. 23–32, 2018.

[60] R. Thommandru and R. Saravanakumar, "Performance analysis of circularly polarised MIMO antenna for wireless applications," in Proc. ICICNIS, IEEE, Dec. 2024, pp. 513–518.

[61] D. N. Ravikiran et al., "Secure visual data processing: Image encryption and decryption through reversible logic gates in VLSI design," Int. J. Mod. Trends Sci. Technol., vol. 10, no. 2, 2024.
[62] R. Saravanakumar et al., "Cross scoop fractal antenna design with notch at 15 degree for emerging applications at 5.2 GHz," in Proc. RAEEUCCI, IEEE, Apr. 2024, pp. 1–7.