Internet Of Things Based Bank Locker With Security Using Keypad And Fingerprint

Dr.K.Durga Prasad[1],Vejendala Chaitanya Bhargav[2],Mudadla Gowri Naidu[3], Siddhi Hema Pratap[4], Syed Abdulla[5]

[2,3,4,5]UG Student,ECE,Chalapathi Institute Of Engineering&Technology Guntur-Andhra Pradesh,India

[5]Associate Professor ECE,Chalapathi Institute Of Engineering&Technology Guntur-Andhra Pradesh,India

***Abstract*—**In todays rapidly evolving technological landscape, ensuring the security of valuable assest stored in bank lockers has become increasingly critical. Traditional locker systems, which rely primarily on mechanical keys and basic authentication m,ethods, are vulnerable to theft, duplication, and unauthorized access. To overcome these limitations, this project proposes an advanced Internet of Things (IoT) based bank locker security system that provides a smart, reliable, and multi layered protection mechanism. The proposed system integrates modern technologies such as electronic locking systems, biometric authentication, and real time monitoring mto enhance the overall security framework. A microcontroller-based architecture, supported by IoT connectivity, enables seamless communication between hardware components and remote monitoring platforms. The system utilizes password verification along with biometric techniques such as fingerprint recognition to ensure that only authorized individuals can access the locker.

Keywords— IoT, Bank Locker Security System, Biometric Authentication, Fingerprint Recognition, Electronic Door Lock, Real time Monitoring, GSM Communication, NodeMCU, Embedded System, Multi Factor Authentication

I. INTRODUCTION

In the modern era, the protection of valuable assets stored in bank lockers has become a major concern due to the rapid advancement of theft techniques and security breaches. Conventional locker systems primarily rely on mechanical keys, PIN-based access, and manual surveillance, which are often prone to duplication, human error, and unauthorized access. As a result, there is a growing need for a more secure, intelligent, and automated solution that can overcome the limitations of traditional systems.

The emergence of the Internet of Things (IoT) has revolutionized various sectors by enabling seamless communication between devices through the internet. IoT technology allows multiple devices to connect, share data, and perform actions intelligently without human intervention. By integrating IoT into bank locker security systems, it becomes possible to design a highly efficient and reliable system that ensures enhanced protection and real-time monitoring of locker activities.

The proposed IoT-based bank locker system introduces a multi-layered security mechanism that combines electronic locking, biometric authentication, and real-time surveillance. Unlike traditional systems, this approach eliminates the dependency on physical keys and introduces advanced authentication techniques such as fingerprint recognition and password verification. These methods ensure that only authorized individuals can access the locker, thereby significantly reducing the chances of unauthorized entry.

A key feature of this system is the use of embedded hardware components such as microcontrollers, sensors, and communication modules. The microcontroller acts as the central processing unit, managing all operations including authentication, monitoring, and communication. Sensors are deployed to detect any abnormal activities such as forced entry or environmental hazards, while communication modules like GSM or Wi-Fi enable instant transmission of alerts and notifications to bank authorities.

Real-time monitoring is another crucial aspect of the system. The IoT-enabled architecture allows continuous tracking of locker status and activities. In case of any suspicious attempt, the system immediately triggers alerts and notifies the concerned personnel through messages or internet-based applications. This ensures quick response and enhances the overall effectiveness of the security system.

Furthermore, the system supports remote access and control, allowing bank officials to monitor locker operations from any location. This not only improves operational efficiency but also provides flexibility in managing multiple locker units simultaneously. The scalable nature of the system

Doi:10.48047/ijiee.2026.16.2.21

makes it adaptable to different banking environments and future technological advancements.

In conclusion, the integration of IoT in bank locker security systems provides a smart and robust solution to address the shortcomings of conventional methods. By combining advanced authentication techniques, real-time monitoring, and remote accessibility, the system ensures a high level of security, reliability, and user convenience. This project demonstrates how modern technology can be effectively utilized to safeguard valuable assets and enhance trust in banking security systems.

II. REVIEW &LITERATURE SURVEY

The rapid growth of technology has significantly influenced the development of advanced security systems, particularly in the banking sector. Over the years, several research works and systems have been proposed to improve the safety of bank lockers. This chapter presents a review of existing literature related to bank locker security systems, focusing on the integration of embedded systems and IoT technologies

Early bank locker security systems were primarily based on mechanical locks and key-based access. Although these systems were simple to implement, they suffered from major drawbacks such as key duplication, lack of monitoring, and vulnerability to physical attacks. To overcome these issues, researchers introduced electronic and digital locking mechanisms using microcontrollers, which improved reliability but still lacked real-time monitoring and remote access capabilities.

One of the significant developments in this domain is the IoT-based bank locker security system, which integrates microcontrollers, sensors, and communication modules. In such systems, only authorized users are allowed to access the locker through authentication mechanisms. A commonly used approach involves a keypad-based password entry combined with mobile-based verification. When a user attempts to access the locker, the system sends a unique password to the registered mobile number. The locker opens only if both the entered password and the received password match, thereby ensuring two-level security. This method enhances protection compared to traditional systems .

Another important contribution in the literature is the use of embedded systems for locker security. These systems employ microcontrollers such as NodeMCU or Arduino along with peripherals like LCD displays, relays, and sensors. The embedded system verifies user credentials and controls the locking mechanism in real time. Additionally, these systems maintain logs of user activities, including entry and exit records, which improves accountability and traceability.

Several studies have also emphasized the importance of integrating fire detection sensors into locker systems. Fire sensors help detect abnormal temperature or smoke conditions and trigger alerts immediately. This feature ensures not only security against theft but also protection against environmental hazards, thereby enhancing the overall safety of stored valuables .

Furthermore, digital security systems with door-lock mechanisms have been developed to provide centralized control and monitoring. These systems allow real-time authentication and quick access for authorized users. The integration of IoT enables these systems to send instant notifications to users or authorities in case of unauthorized access attempts. Mobile applications and web interfaces are often used to monitor locker status remotely, making the system more efficient and user-friendly.

Recent advancements focus on combining multiple authentication techniques such as RFID, biometric verification, and one-time passwords (OTP). Multi-factor authentication significantly increases security by ensuring that even if one method is compromised, additional layers of protection remain intact. These systems also leverage cloud platforms for data storage and remote management, improving scalability and accessibility.

In summary, the literature clearly indicates a transition from traditional mechanical systems to intelligent IoT-based security solutions. While earlier systems provided basic protection, modern approaches incorporate multi-layer authentication, real-time monitoring, and remote accessibility. The proposed IoT-based bank locker system builds upon these advancements by integrating biometric authentication, sensor-based monitoring, and instant alert mechanisms, thereby offering a more secure, reliable, and efficient solution for modern banking needs.

III. RESEARCH METHODOLOGY

The research methodology for the proposed IoT-based bank locker security system focuses on

Doi:10.48047/ijiee.2026.16.2.21

designing, developing, and implementing a secure, reliable, and intelligent system using embedded and IoT technologies. The methodology follows a systematic approach that includes problem identification, system design, hardware and software integration, testing, and performance evaluation .

Initially, the limitations of traditional bank locker systems were analyzed, including their vulnerability to unauthorized access, lack of real-time monitoring, and absence of alert mechanisms. Based on these observations, the need for a multi-layered security system was identified. The proposed solution aims to enhance security by integrating biometric authentication, password verification, and IoT-based monitoring.

The system design phase involves both hardware and software architecture. The hardware components include a microcontroller (NodeMCU), fingerprint sensor, keypad, LCD display, relay module, electronic door lock, and fire sensor. The NodeMCU acts as the central controller, managing all operations and enabling internet connectivity. Sensors and input devices are interfaced with the controller to collect user data and environmental information.

On the software side, the system is developed using the Arduino IDE, where embedded C/C++ programming is used to implement the logic for authentication, communication, and control. The software is responsible for handling fingerprint enrollment and matching, generating one-time passwords (OTP), validating user inputs, and controlling the locking mechanism. Communication protocols such as Wi-Fi and GSM are utilized to send real-time alerts and notifications to authorized personnel.

The working methodology of the system is based on a multi-factor authentication process. When a user attempts to access the locker, the system first verifies the fingerprint. If the fingerprint is successfully matched, an OTP is generated and sent to the registered mobile number. The user must enter the correct OTP through the keypad to gain access. Only when both authentication steps are validated does the system activate the relay to unlock the locker. If authentication fails, the system triggers an alarm and sends alert messages to the concerned authorities.

In addition to access control, the system continuously monitors environmental conditions using sensors such as the flame sensor. If any abnormal condition, such as fire or unauthorized tampering, is detected, the system immediately sends alerts and displays warning messages on the LCD. This ensures both security and safety of the locker environment.

The implementation phase involves assembling the hardware components and integrating them with the programmed microcontroller. Proper interfacing and calibration are carried out to ensure accurate functioning of sensors and modules. The system is then tested under different scenarios, including valid access, invalid authentication, and emergency conditions, to evaluate its performance and reliability.

Finally, the system is evaluated based on parameters such as security strength, response time, reliability, and scalability. The results demonstrate that the proposed system provides enhanced protection through layered authentication, real-time monitoring, and remote alert mechanisms.

In conclusion, the research methodology adopts a structured approach to develop a smart and secure IoT-based bank locker system. By combining embedded systems, biometric technology, and IoT communication, the methodology ensures an efficient and scalable solution that addresses the shortcomings of conventional locker security systems.

IV. EXSITING SYSTEM

The existing bank locker security systems are primarily designed using conventional methods such as mechanical locks, physical keys, and basic password-based access. These systems have been widely used for many years due to their simplicity and low implementation cost. However, with the advancement of technology and increasing security threats, these traditional systems are no longer sufficient to ensure complete protection of valuable assets .

In many current systems, access to bank lockers is controlled through key-based mechanisms or PIN verification. Although these methods provide a basic level of security, they are highly vulnerable to risks such as key duplication, password leakage, and unauthorized access. Additionally, these systems lack proper monitoring capabilities, making

Doi:10.48047/ijiee.2026.16.2.21

it difficult to detect suspicious activities in real time.

To address some of these limitations, modern existing systems have incorporated electronic locking mechanisms and embedded controllers. These systems use microcontrollers along with keypads and displays to authenticate users. In some cases, two-level authentication is implemented, where a password entered through a keypad is verified along with a one-time password (OTP) sent to a registered mobile number. This improves security compared to traditional methods but still has certain drawbacks.

Furthermore, some existing systems include basic sensor integration, such as fire sensors, to detect environmental hazards. When abnormal conditions like fire are detected, the system can trigger alerts to notify authorities. However, these systems often lack advanced features such as continuous real-time monitoring, intelligent threat detection, and centralized control.

Another limitation of existing systems is the absence of full IoT integration. Although certain systems may use GSM modules for sending alerts, they do not provide complete remote monitoring or control capabilities through internet-based platforms. As a result, bank authorities cannot efficiently track locker status or respond quickly to potential threats.

Moreover, existing systems generally do not utilize advanced authentication techniques such as biometric verification or face recognition. This makes them less secure compared to modern multi-factor authentication systems. They also lack scalability and flexibility, making it difficult to integrate with new technologies or expand the system as per future requirements.

In summary, while existing bank locker systems have evolved from purely mechanical designs to partially electronic systems, they still suffer from several limitations, including weak authentication methods, lack of real-time monitoring, limited alert mechanisms, and minimal remote accessibility. These drawbacks highlight the need for a more advanced, IoT-based solution that can provide enhanced security, reliability, and efficiency.

V. PROPOSED METHODOLOGY

The proposed methodology focuses on developing a smart IoT-based bank locker security system that provides enhanced protection through multi-layer authentication, real-time monitoring, and intelligent alert mechanisms. This system is designed to overcome the limitations of existing security systems by integrating advanced technologies such as embedded systems, IoT communication, and biometric verification .

The architecture of the proposed system is based on a centralized microcontroller unit, specifically the NodeMCU (ESP8266), which acts as the core processing and communication module. It connects various hardware components such as the fingerprint sensor, keypad, LCD display, relay module, electronic door lock, and fire sensor. The NodeMCU enables wireless communication through Wi-Fi, allowing seamless integration with IoT platforms for remote monitoring and control.

The system follows a multi-factor authentication approach to ensure maximum security. When a user attempts to access the locker, the process begins with biometric verification using a fingerprint sensor. If the fingerprint is successfully authenticated, the system generates a One-Time Password (OTP) and sends it to the registered mobile number via GSM or internet services. The user must then enter the correct OTP using the keypad. Only when both authentication steps are validated does the system unlock the locker using the relay-controlled electronic lock. This layered approach significantly reduces the chances of unauthorized access.

In addition to authentication, the system continuously monitors the locker environment using sensors. A flame sensor is integrated to detect fire or abnormal temperature conditions. If any unusual activity or threat is detected, the system immediately triggers an alert through buzzer indications and sends notifications to bank authorities via SMS or internet-based alerts. The LCD display provides real-time system status and user interaction feedback.

Doi:10.48047/ijiee.2026.16.2.21

Another important aspect of the proposed methodology is real-time IoT monitoring and remote access. Bank authorities can monitor locker status, receive alerts, and manage the system remotely using cloud-based platforms or mobile applications. This ensures quick response to any security breach and improves operational efficiency.

To ensure data security, the system incorporates encrypted communication between devices and servers. Regular software updates and secure data handling practices are implemented to protect against cyber threats. Additionally, the system is designed with a modular structure, allowing easy scalability and integration with existing banking infrastructure.

The implementation process includes hardware assembly, software programming using Arduino IDE, and proper interfacing of all modules. The system is tested under various conditions such as valid access, invalid attempts, and emergency scenarios to ensure reliability and performance.

In conclusion, the proposed methodology provides a comprehensive and intelligent approach to bank locker security. By combining biometric authentication, OTP verification, IoT connectivity, and sensor-based monitoring, the system ensures a high level of security, real-time responsiveness, and user convenience. This makes it a robust and future-ready solution for modern banking environments.

VI. BLOCK DIAGRAM

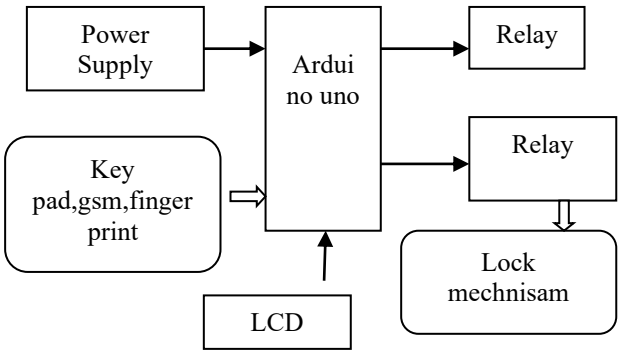

Fig. 6.2. Block Diagram

VII. RESULTS AND OUTCOMES

The implementation of the proposed IoT-based bank locker security system demonstrates significant improvements in security, reliability, and system efficiency compared to conventional locker systems. The system was successfully designed, developed, and tested using embedded hardware and IoT technologies, validating the effectiveness of the proposed approach .

One of the major outcomes of the system is the successful execution of multi-factor authentication. The combination of fingerprint verification and One-Time Password (OTP) validation ensures that only authorized users can access the locker. During testing, the system accurately identified valid users and effectively prevented unauthorized access attempts. This layered authentication mechanism significantly enhances security compared to single-level authentication systems.

The system also demonstrated efficient real-time monitoring and alert capabilities. Whenever an unauthorized attempt was made or incorrect credentials were entered, the system triggered an immediate alert through a buzzer and sent notifications to the registered mobile number. This rapid response mechanism helps in minimizing potential security threats and ensures timely intervention by authorities.

Another important outcome is the reliable functioning of the IoT communication module. The NodeMCU successfully established wireless communication, enabling the system to send real-time updates and alerts through internet or GSM-based services. This feature allows bank officials to monitor locker activity remotely, improving operational control and accessibility.

The integration of environmental monitoring using a fire sensor also proved to be effective. The system was able to detect abnormal conditions such as the presence of fire and promptly generate alerts. This adds an extra layer of safety by protecting valuables not only from theft but also from environmental hazards.

The electronic locking mechanism controlled through the relay module operated efficiently, ensuring smooth locking and unlocking operations. The LCD display provided clear and real-time feedback to users, improving usability and interaction with the system.

In terms of performance, the system exhibited:

- High accuracy in biometric authentication
- Fast response time for OTP generation and verification
- Reliable communication for alerts and notifications

Doi:10.48047/ijiee.2026.16.2.21

- Stable operation under different test conditions

Additionally, the system proved to be scalable and adaptable, meaning it can be extended or integrated with additional features such as cloud storage, face recognition, or advanced analytics in the future.

In conclusion, the results confirm that the proposed IoT-based bank locker system offers a secure, efficient, and intelligent solution. The outcomes highlight its ability to provide enhanced protection, real-time monitoring, and user-friendly operation, making it a suitable replacement for traditional bank locker security systems.

VIII.CONCLUSION

The proposed IoT-based smart greenhouse monitoring and control system provides an efficient and low-cost solution for modern agricultural automation. By integrating Arduino UNO, ESP8266 Wi-Fi module, DHT11 sensor, and soil moisture sensor, the system successfully monitors critical environmental parameters such as temperature, humidity, and soil moisture in real time. The automation logic ensures that irrigation and environmental control are performed only when required, thereby improving resource utilization and reducing manual intervention.

The implementation of IoT technology enables remote monitoring and control of greenhouse conditions through cloud connectivity, making the system more flexible and user-friendly. The inclusion of an I2C LCD display further enhances local monitoring capabilities by providing real-time environmental data.

The experimental results demonstrate that the system effectively maintains optimal conditions for plant growth while significantly reducing water wastage and human effort. This makes the proposed system a reliable and scalable solution for precision agriculture and smart farming applications.

Fig:7.1: OUTPUT

Furthermore, the system can be enhanced in future work by integrating Machine Learning algorithms to enable predictive analysis of environmental conditions. This would allow the system to move beyond rule-based automation toward intelligent decision-making, improving irrigation scheduling and overall agricultural efficiency

Overall, the system contributes significantly to improving flood preparedness and public safety. With further enhancements such as machine learning-based prediction models and integration of additional environmental sensors, the system can be made even more accurate and robust in future implementations.

REFERENCES

1. 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.
2. 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.
3. Vellela, S. S., & Balamanigandan, R. (2024). An efficient attack detection and prevention

Doi:10.48047/ijiee.2026.16.2.21

approach for secure WSN mobile cloud environment. Soft Computing, 28(19), 11279-11293.
4. Vellela, S. S. (2023). Enhanced speckle noise reduction in breast cancer ultrasound imagery using a hybrid deep learning model. Ingénierie des Systèmes d'Information.
5. 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.
6. Praveen, S. P., Nakka, R., Chokka, A., Thatha, V. N., Vellela, S. S., & Sirisha, U. (2023). A novel classification approach for grape leaf disease detection based on different attention deep learning techniques. International Journal of Advanced Computer Science and Applications (IJACSA), 14(6), 2023.
7. 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.
8. 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).
9. Madhuri, A., Jyothi, V. E., Praveen, S. P., Sindhura, S., Srinivas, V. S., & Kumar, D. L. S. (2024). A new multi-level semi-supervised learning approach for network intrusion detection system based on the 'goa'. Journal of Interconnection Networks, 24(supp01), 2143047.
10. Raju, V. V. K., Bhavani, Y. V. K. D., Nandikonda, P., Kareemunnisa, F. N. U., Brahmeswara, K. B., & Sindhura, S. (2026). Iterative and Statistical Analytical Review of Predictive Modeling Approaches in Educational Systems: A Comprehensive Benchmark of AI-Driven Methods. International Journal of Innovative Technology and Interdisciplinary Sciences, 9(1), 490-522.
11. 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.
12. 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).
13. 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.
14. 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.
15. Vellela, S. S., Pushpalatha, D., Sarathkumar, G., Kavitha, C. H., & Harshithkumar, D. (2023). Advanced intelligence health insurance cost prediction using random forest. ZKG International, 8.
16. Vellela, S. S., Babu, B. V., & Mahendra, Y. B. (2024). IoT-based tank water monitoring systems: enhancing efficiency and sustainability. International Journal for Modern Trends in Science and Technology, 10(02), 291-298.
17. 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.

Doi:10.48047/ijiee.2026.16.2.21

18. Vellela, S. S., Chaganti, A., Gadde, S., Bachina, P., & Karre, R. (2022). A Novel Approach for Detecting Automated Spammers in Twitter. Mukt Shabd, 11, 49-53.
19. Vellela, S. S., Narapasetty, S., Somepalli, M., Merikapudi, V., & Pathuri, S. (2022). Fake News Articles Classifying Using Natural Language Processing to Identify in-article Attribution as a Supervised Learning Estimator. Mukt Shabd Journal, 11.
20. Vellela, S. S., Vineeth, S., & Suresh, V. (2024). IoT Based ICU Patient Monitoring System. IoT Based ICU Patient Monitoring System, International Journal for Modern Trends in Science and Technology, 10(02), 265-273.
21. Vellela, S. S., & Balamanigandan, R. (2025). Designing a Dynamic News App Using Python. Available at SSRN 5250912.
22. 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.
23. Vellela, S. S., Singu, K., Kakarla, L. S., Tadikonda, P., & Sattenapalli, S. N. R. (2025). NLP-Driven Summarization: Efficient Extraction of Key Information from Legal and Financial Documents. Available at SSRN 5250908.
24. 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.
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. 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.
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. Vellela, S. S. (2024). A Comprehensive Review of AI Techniques in Serious Games: Decision Making and Machine Learning.
29. 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.
30. 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.
31. Vellela, S. S., Purimetla, N. R., Rao, P. V., Daniel, V. A. A., Koppolu, H. K. R., & Janani, B. (2025). AI-Enabled Wearable Hemodynamic Monitoring System for Early Identification of Thrombotic Events. Vascular and Endovascular Review, 8(16s), 321-336.
32. Venkatesh, N., Maheswari, S., & Triveni, P. (2024). Harnessing IoT for Real-Time Plant Health Monitoring: Challenges and Opportunities.
33. 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

Doi:10.48047/ijiee.2026.16.2.21

Engineering Science (AMATHE) (pp. 1-6). IEEE.
34. 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.
35. Haritha, K., Geethika, N. S., Venkateswarlu, K., Kumar, R. H., & Ramakrishna, Y. Enhancing Public Safety with AI & ML-Based CCTV Surveillance.
36. Haritha, K., Prakash, P. B., Pravallika, D., Venkatesh, K., & Venkatesh, G. Enhancing Object Detection in Autonomous Vehicles Under Low-Light Conditions Using Federated Learning and YOLOv5.
37. Ram, C. S., Vellela, S. S., Sravanthi Javvadi, D. V., Rashid, S. Z., & Madhumathi, S. M. (2025). Integrated Robotic–Imaging Platforms in Endovascular Surgery: Current Capabilities and Future Directions. Vascular and Endovascular Review, 8(16s), 285-298.
38. Roja, D., Navya, G., Srujana, B. S., Mamatha, P., & Sai, C. Y. K. Deep Learning for Hotel Reviews: A Framework for Sentiment Classification and Fake Review Detection.
39. 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.
40. Balamanigandan, R., Vellela, S. S., Gorintla, S., Vuyyuru, L. R., Thanuja, N., & Rao, T. S. (2025, September). Quantum-Enhanced Data Security for Electronic Health Records: A Framework for Post-Quantum Cryptography in Healthcare Systems. In 2025 6th International Conference on Smart Electronics and Communication (ICOSEC) (pp. 1924-1929). IEEE.
41. Roja, D., Amulya, P., Nagasai, M., Prasad, D. D., & Babu, A. V. Machine Learning-Based Early Diagnosis of Fish Diseases via Water Quality Data.
42. Sai, M. B., & Vellela, S. S. (2025, December). Hybrid ML Driven Multi-Cloud Service Work Load Prediction For Financial Systems. In 2025 1st International Conference on Advancement in Futuristic Technologies (ICAFT) (pp. 1-6). IEEE.
43. Kareemunnisa, D., Haritha, K., Ranjani, B. S., Venkateswarlu, K., & Bindu, M. N. H. DUAL-STAGE PRIVACY PROTECTION FOR GRAPH NEURAL NETWORKS AGAINST INFERENCE ATTACKS.
44. 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.

Doi:10.48047/ijiee.2026.16.2.21