iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** III **Month of publication:** March 2026

DOI: https://doi.org/10.22214/ijraset.2026.78459

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

Online Food Ordering System

Chinnu Kollati[1], Lavanya Kunche[2], Adabala Leela Venkata Naresh[3], Adabala Kumar Sai Sandeep[4], Tholeti Ananda Raju[5], Medida Gopal[6], Akula Sai Krishna Veni[7]

[1,2,3,4,5,6]*Department of Computer Science and Engineering, Bonam Venkata Chalamayya Engineering College, Affiliated to JNTU Kakinada, Andhra Pradesh-533210, India*

[7]*Project Guide, Department of Computer Science and Engineering, Bonam Venkata Chalamayya Engineering College, Affiliated to JNTU Kakinada, Andhra Pradesh-533210, India*

Abstract: ***The Online Food Ordering System is a web-based application designed to simplify and automate the process of ordering food from restaurants over the internet. It provides a user-friendly interface where customers can register, browse dynamic menus, customize orders, and make secure payments from any location and at any time. On the business side, the system enables restaurants to manage menus, track incoming orders in real time, update order status, and maintain customer and sales records through an integrated dashboard. By replacing manual order- taking with a digital workflow, the system reduces errors, waiting time, and operational overhead, while improving order accuracy and customer satisfaction. This project demonstrates the analysis, design, and implementation of the system using modern web technologies, with a focus on usability, reliability, and scalability to support the growing demand for online food delivery services.***

Keywords: AES algorithm, RSA algorithm, Cryptography, Data Security, Secure Communication.

I. INTRODUCTION

In today's fast-paced digital world, the Online Food Ordering System revolutionizes how people access their favourite meals, bridging the gap between hungry customers and bustling kitchens with seamless technology. This innovative platform allows users to browse extensive menus from local restaurants, cafes, and cloud kitchens directly from their smartphones or computers, eliminating the need for phone calls or long queues. By leveraging intuitive apps or websites, customers can effortlessly search by cuisine, price, ratings, or dietary preferences, customize orders with add-ons, and schedule deliveries at convenient times. Secure payment gateways integrate options like UPI, cards, or wallets, ensuring quick transactions without hassle. Behind the scenes, restaurant partners receive real-time notifications, manage inventory, and track preparation status to maintain efficiency. Delivery personnel are assigned dynamically via GPS-enabled routing for optimal speed and accuracy. Advanced features like personalized recommendations powered by AI, loyalty rewards, and live order tracking enhance user satisfaction, while analytics dashboards help vendors optimize menus and operations. Embracing trends like contactless delivery post- pandemic, these systems prioritize hygiene with no-touch options and real-time updates. For businesses, it expands reach beyond physical locations, boosting revenue through data-driven insights and promotions. In India, platforms like Zomato and Swiggy exemplify this ecosystem, serving millions daily across urban and semi-urban areas. Ultimately, the Online Food Ordering System not only saves time but transforms dining into a convenient, personalized experience, fuelling the gig economy and supporting local eateries in a competitive market.

II. LITERATURE REVIEW

In today's fast-paced digital world, the Online Food Ordering System revolutionizes how people access their favorite meals, bridging the gap between hungry customers and bustling kitchens with seamless technology. This innovative platform allows users to browse extensive menus from local restaurants, cafes, and cloud kitchens directly from their smartphones or computers, eliminating the need for phone calls or long queues. By leveraging intuitive apps or websites, customers can effortlessly search by cuisine, price, ratings, or dietary preferences, customize orders with add-ons, and schedule deliveries at convenient times. Secure payment gateways integrate options like UPI, cards, or wallets, ensuring quick transactions without hassle. Behind the scenes, restaurant partners receive real-time notifications, manage inventory, and track preparation status to maintain efficiency. Delivery personnel are assigned dynamically via GPS-enabled routing for optimal speed and accuracy. Advanced features like personalized recommendations powered by AI, loyalty rewards, and live order tracking enhance user satisfaction, while analytics dashboards help vendors optimize menus and operations. Embracing trends like contactless delivery post- pandemic, these systems prioritize hygiene with no-touch options and real-time updates. For businesses, it expands reach beyond physical locations, boosting revenue through data-driven insights and promotions.

In India, platforms like Zomato and Swiggy exemplify this ecosystem, serving millions daily across urban and semi-urban areas. Ultimately, the Online Food Ordering System not only saves time but transforms dining into a convenient, personalized experience, fueling the gig economy and supporting local eateries in a competitive market.

Recent scholarly works on online food ordering systems further explore technological architectures and sustainability challenges. Research emphasizes microservices-based designs integrating RESTful APIs for menu management, order processing, and real-time notifications via WebSockets, improving scalability over monolithic systems.[1] Machine learning algorithms enhance personalization by analyzing user data for predictive ordering and dynamic pricing, while blockchain pilots address food traceability and payment security in platforms like Swiggy.[2][3] Sustainability studies critique high packaging waste and carbon emissions from last-mile deliveries, advocating eco-friendly practices like electric fleets and reusable containers, with European models showing 20-30% emission reductions.[4][5] In developing markets, adoption barriers include digital divides and unreliable internet, prompting hybrid offline-online solutions.[6] Economic analyses reveal dual impacts: platforms boost restaurant revenues by 15-25% but impose high commissions (20-35%), sparking regulatory debates in India and the US.[7][8] Future directions highlight AR/VR for virtual dining and metaverse integrations, alongside ethical AI to mitigate biases in recommendation engines.[9] Advanced features like personalized recommendations powered by AI, loyalty rewards, and live order tracking enhance user satisfaction, while analytics dashboards help vendors optimize menus and operations. Embracing trends like contactless delivery post-pandemic, these systems prioritize hygiene with no-touch options and real-time updates. For businesses, it expands reach beyond physical locations, boosting revenue through data-driven insights and promotions. In India, platforms like Zomato and Swiggy exemplify this ecosystem, serving millions daily across urban and semi-urban areas. Ultimately, the Online Food Ordering System not only saves time but transforms dining into a convenient, personalized experience, fueling the gig economy and supporting local eateries in a competitive market. Recent scholarly works on online food ordering systems further explore technological architectures and sustainability challenges.

III. METHODS

A. System Architecture

The system that is proposed has a highly structured client-server architecture. Users will interact with this system through a normal web interface. They will upload files to perform corresponding encryption/decryption operations. This application is developed with front-end tools such as HTML5 and CSS3. Normal web development principles have been used to make this application highly user-friendly. Users will have a good view of system feedback during encryption/decryption operations. The backend layer employs the concept of lightweight and powerful web development technologies like Python Flask. It handles encryption operations and deals efficiently with user authentication and database interactions. It ensures clean separation of concerns. It has built-in security features. MySQL database management will be utilized, storing the users' credentials, encrypted file information, information about the encrypted files, timestamps relating to the encryption process, and log information. The design scheme will enable maintainability, as well as optimize query performance to enable the retrieval of files quickly. User authentication techniques are used to ensure that the users who are accessing the encryption and decryption services are valid. The system utilizes secure password hashing with widely accepted standards and protocols for session handling, with the use of secure cookies for the purpose of retaining the state information of users. Role-based security is used for the administration functions.

Fig.1. System Architecture

A. AES Algorithm Working

AES is a symmetric block cipher that uses a block size of 128 bits, along with a key size of 128, 192, or 256 bits, to encrypt blocks of information, where the larger the key size, the more secure the information will be [1]. Here, a 256-bit key size has been used to ensure maximum security for the information stored in the database, as it can safely counter any present or future kinds of cryptanalysis attacks performed on the information. The process of AES encryption takes place through several rounds of transformation, with 10 rounds for 128bit keys, 12 rounds for 192-bit keys, and 14 rounds of transformation for 256-bit keys. The round consists of four different operations:

1) *SubBytes:* Each byte of the state array in the Rijndael algorithm is replaced by another byte from a pre-defined substitution box. Adding this non-linearity makes it difficult to apply differential and linear cryptanalysis.
2) *ShiftRows:* The rows of the state matrix are shifted in a cyclical way and by different displacements, where row 0 stays unchanged, row 1 shifts left by 1 byte, row 2 by 2 bytes, and row 3 by 3 bytes. This increases dispersion across the algorithm, with a modification in a certain input having also changed several bytes in the output.
3) *MixColumns:* This operation mixes the columns using multiplication of matrices over the Galois Field GF(2^8), which results in more diffusion of data in the block, so each input bit affects many output bits. The MixColumns step is excluded from the last round.
4) *AddRoundKey:* By using XOR operations, the state is combined with one round key, which is derived from the main encryption key. This introduces the key material into each round.

The process of decryption is the inverse of the encryption process. The inverse steps involve InvSubBytes, InvShiftRows, InvMixColumns, and AddRoundKey in the opposite order. The merits of AES include faster encryption rates, better security, measured by resistance to all types of attacks, including differential cryptanalysis and linear cryptanalysis, along with easy implementation in hardware as well as software [2]. The modern processors have been equipped with the AES instruction sets that improve the rate of the encryption and decryption process.

B. RSA Algorithm Working

RSA is a public-key or "asymmetric-key" encryption method that relies upon a pair of mathematically linked keys: a public encryption key may be openly distributed, whereas a private key for decryption must be kept secret [3]. The basis upon which RSA operates is the difficulty in processing the reversal of a product of large prime numbers, a problem for which there is as yet no efficient method or algorithm implemented anywhere in the world in computer systems [1]. Some of the most critical steps in the key generation process are considered to be the selection of two large prime numbers that are often 1024 or 2048 bits long each, the computation of the product of the two prime values as the modulus value ‘n’, the computation of the value represented as $\varphi(n) = (p - 1)(q - 1)$, the selection of the public exponent ‘e’, which is necessarily higher than 65537 for efficiency considerations and is coprime with $\varphi(n)$, and the computation of the private exponent ‘d’, which is needed to satisfy the equation $(d * e) \bmod \varphi(n) = 1$.
During the encryption process, the text message sent is converted into integers. The integer form of the message is then raised to some power e modulo n: C = M^e mod n. While in the process of decrypting the data, the ciphertext that has been sent receives the value of the modular inverse of the original integer raised to some power d modulo n: M = C^d mod n. The basic formula that has been used shows that only the recipient with the matching private key will be able to decrypt any data that has been encrypted with their matching public key [4]. In this case, the RSA algorithm has an important role in key exchange security rather than data encryption. In fact, the key used for encryption by the AES algorithm has to be encrypted using the RSA key of the receiver before the information is actually sent over the channel. In this way, only the authorized party having the corresponding private key can access the actual key for decryption using the AES algorithm.

IV. RESULTS

The experimental environment was a local environment, in which a system that has 8 GB of memory, an Intel i5 processor running at 2.4 GHz, Windows11 as its operating system, along with Python 3.8 and Flask 2.0. The system tested various cases of system performance by testing files of various sizes, from 1KB of plain text up to 10 megabytes of multimedia content. Samples provided indicated that a full encryption/decryption cycle with perfect integrity was achievable. The 1 MB text file took 0.15 seconds to encrypt with AES 256. The RSA file encryption of the 256-bit AES took 0.03 seconds regardless of file size. In terms of decrypt times, this is close to the encrypt times. RSA took 0.04 seconds to decrypt, while AES took 0.15 seconds to decrypt this file. Further, the efficiency of the code is demonstrated by the performance evaluation result that the time consumed for file encryption is directly proportional to the size of the file.

The code maintains consistency in efficiency with various types of files, such as text documents, images, video clips, or compressed files. When the size of the file is considered as 5MB for the pdf file encryption, the code takes a total of 0.68 seconds. When the size of the video file is considered as 10MB, the time consumed is 1.3 seconds. Further, the time consumed for the encryption of the key is constant for any file size or any file type and is considered to be 0.03 seconds.

The file size, as opposed to processing time analysis, demonstrated that it is efficient to handle files of up to 10MB without any noticeable deterioration in performance or any signs of excessive use of memory. The method was seen to be far more efficient and effective as opposed to relying on using RSA for large files alone, which would have seen its processing time 50 -100 times higher and also been limited owing to its maximum message size constraint. Security effectiveness testing has assured us that the encrypted files are completely unreadable without the correct decryption keys. It has been ensured that if incorrect keys are used while attempting to decrypt the files, total failure with proper error messages is achieved. Simulations of brute-force attacks have assured us that attempting such an approach to break the encryption is computationally impossible in any timely fashion. The system has been successful in preventing unauthorized access, data tampering, and replay attacks through the proper implementation of security best practices.

V. DISCUSSION

Results comprehensively demonstrate how the hybrid model of combining AES and RSA outperforms and sustains an effective, practical solution for safe data transmission in web environments. The hybrid approach has been strategically using AES's computational efficiency for encrypting large data volumes by utilizing RSA for its secure key exchange method to address the very symptom-a symmetric key distribution challenge-that has classically hindered the widespread cryptographic deployment. The implementation of the proposed system would therefore offer an optimum balance between the twin requirements of security and performance, compared to existing encryption-based systems that use either symmetric or asymmetric methods exclusively. Systems based on RSA alone for data encryption suffer from severe performance bottlenecks when large files are involved and become practically unusable beyond a few kilobytes because of computational complexity issues. Systems based purely on AES, on the other hand, face problems of secure key distribution, which invariably forces organizations to adopt out- of-band key exchange methods. Accordingly, the advantages of employing both AES as well as RSA are numerous; in line with this fact, the encryption strength provided by 256-bit encryption in AES would effectively act as a barrier to brute-force hacking attempts, the implications of key distribution problems would be effectively handled by employing secure key transmission in RSA encryption, the performance characteristics of this system would facilitate real-time encryption of files with moderate sizes, as well as demonstrate defense in depth because of the layered encryption employed. This system would effectively provide high levels of security for data, including financial data, healthcare data, and confidential business data. There are naturally security/performance compromises to be made here. While the security of the key is very high with an RSA encryption, the computational burden is very low compared to a regular AES encryption. The system attempts to manage this in two ways: the computational burden will not be an issue whatsoever, as the RSA is used only for key encryption rather than data encryption. Naturally, there is a minor increase in memory usage because two contexts are needed: one for AES and another for RSA.

The real-time applicability of the system extends to a variety of practical scenarios, which include secure file sharing within an organization, confidential document transmission between business partners, protected cloud storage in which even the service provider does not have any access to unencrypted data, secure email attachments, healthcare data exchange as per privacy regulations, and financial transaction security. The web-based interface makes advanced cryptography accessible to users without requiring deep technical knowledge, thus promoting wider adoption of security best practices. Some future enhancements to this may include the use of digital signatures for authentication and non-repudiation of messages, inclusion of more encryption algorithms to enable algorithm agility, and integration with enterprise identity management systems. Others include key escrow mechanisms that ensure organizational data recovery, file compression before encryption to minimize costs in storage and transmission, and finally, the development of mobile applications to ensure cross-operability.

VI. CONCLUSION

Overall, the study has effectively created and evaluated a comprehensive internet application that is able to facilitate secure data transmission via a technique employing the best features of both symmetric and asymmetric data encryption. Implementation of the AES technique has proved highly successful for the efficient encryption of data via the utilization of a technique employing the features of both symmetric and asymmetric data encryption.

It can be seen that the proposed system fulfils its proposed objectives with a facility that can perform user-friendly and understandable file encryption as well as decryption, even for users who are not highly proficient in matters of information security. The proposed approach also passed performance evaluations that showed that not only does it perform optimally, but it also ensures that there are strong security standards, enough to counter current cyber threats, with the two concepts covering each other well, as one method does not have what the other lacks. It successfully implemented hybrid encryption using current, open standards for encryption algorithms. The intuitive web interface is easily accessible from any modern browser. It has very efficient processing times for files up to 10 MB, with linear scalability. Key management mechanisms are secure, ensuring protection for the cryptographic keys throughout their life cycle. Authentication and authorization controls are strong, preventing unauthorized access. This system demonstrates how sophisticated cryptographic security can be made available without compromising rigor in security. Future enhancements may be the support for large files by the use of streaming encryption, the use of digital signatures for authentication and non-repudiation, more encryption algorithms to enable algorithm agility, the development of mobile applications for a wider platform support, and the implementation of advanced key management features, including key rotation and escrow mechanisms in enterprise deployments. With this, the web application demonstrates that hybrid cryptography systems show practical and deployable solutions to provide security in modern digital communications; thus, a balance between the two important and competing requirements of security strength and computational efficiency can be well achieved. The research applied therein proves that any efficient and sound cryptographic implementation could be robust for protection while remaining practical for everyday usage.

REFERENCES

[1] Prashant, Md Sohail Haque, Amrinder Kaur, Pankaj Yadav. (2024). Comparative Analysis of AES and RSA with Other Encryption Techniques for Secure Communication. International Journal of Scientific Research in Computer Science, Engineering and Information Technology.
[2] Sood, Kaur, S. A Literature Review on RSA, DES, and AES Encryption Algorithms. SCRS Publications.
[3] Singh, Supriya. A Study of Encryption Algorithms (RSA, DES, 3DES, and AES) for Information Security. International Journal of Computer Applications.
[4] Kumari, Mahato, T. K. (2025). The Evolution of Secure Communication: Analysing Cryptographic Methods from Ancient to Modern Era. International Research Journal.
[5] Globus Toolkit Documentation. Security and Encryption Concepts in Distributed Systems.

BIOGRAPHIES OF AUTHORS

Chinnu Kollati is currently residing at Goditippa, Dr B R Ambedkar Konaseema, Andhra Pradesh-533217. He is a B.Tech student specializing in Computer Science & Engineering at Bonam Venkata Chalamayya Engineering College, Odalarevu, with an expected graduation in May 2026. He aims to secure a position that leverages his strong organizational skills, educational background, and ability to work effectively with others. She possesses key skills in Python, MySQL, HTML, CSS, Machine Learning, ML libraries (pandas, matplotlib), Git/Github. While his professional experience is listed as a student, his proactive approach and skill set indicate a strong potential for growth and contribution in a professional setting. Phone No.: 8919545657 Email: 22221a0549@bvcgroup.in. ORCID: https://orcid.org/0009-00079361-1239

Lavanya Kunche is currently residing at Allavaram, Dr B R Ambedkar Konaseema, Andhra Pradesh-533217. She is a B.Tech student specializing in Computer Science & Engineering at Bonam Venkata Chalamayya Engineering College, Odalarevu, with an expected graduation in May 2026. He aims to secure a position that leverages his strong organizational skills, educational background, and ability to work effectively with others. She possesses key skills in Python, MySQL. While his professional experience is listed as a student, his proactive approach and skill set indicate a strong potential for growth and contribution in a professional setting. Phone No.: 9392752718 Email: 22221a0560@bvcgroup.in. ORCID: https://orcid.org/0009-0009-6784-8384

Leela Venkata Naresh Adabala is currently residing at Kesanapalli, Dr B R Ambedkar Konaseema, Andhra Pradesh- 533244. He is a B.Tech student specializing in Computer Science & Engineering at Bonam Venkata Chalamayya Engineering College, Odalarevu, with an expected graduation in May 2026. He aims to secure a position that leverages his strong organizational skills, educational background, and ability to work effectively with others. He possesses key skills in python, MySQL. While his professional experience is listed as a student, his proactive approach and skill set indicate a strong potential for growth and contribution in a professional setting. Phone No.: 9030153122 Email: 22221a0503@bvcgroup.in. ORCID: https://orcid.org/0009-0007-1203-9382

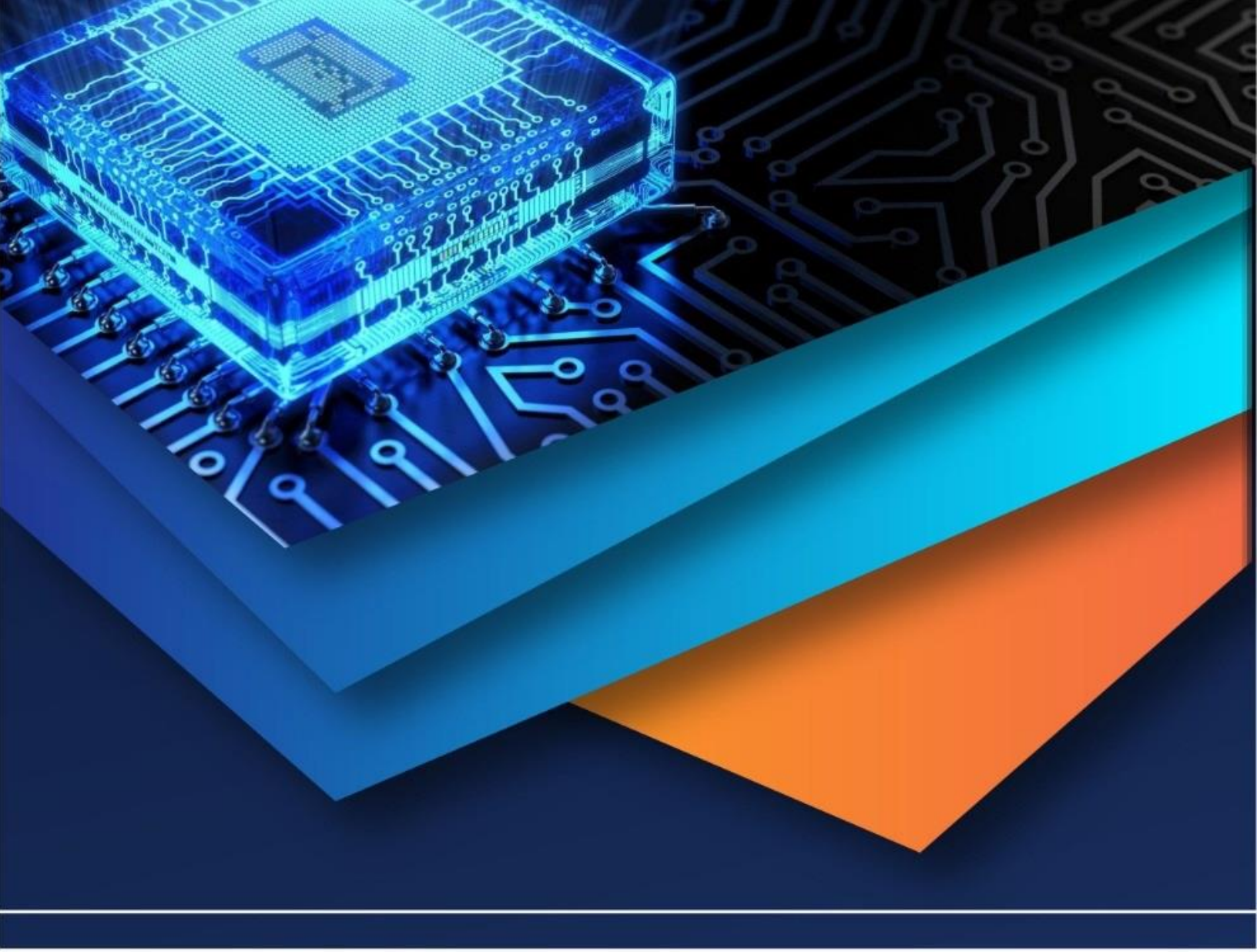
Kumar Sai Sandeep Adabala is currently residing at Ramarajulanka, DR B R Ambedkar Konaseema, Andhra Pradesh- 533253.He is a B.Tech student specializing in Computer Science & Engineering at Bonam Venkata Chalamayya Engineering College, Odalarevu, with an expected graduation in May 2026. He aims to secure a position that leverages his strong organizational skills, educational background, and ability to work effectively with others. He possesses key skills in Python, MySQL. While his professional experience is listed as a student, his proactive approach and skill set indicate a strong potential for growth and contribution in a professional setting. Phone No.:6301732269 Email: 22221a0502@bvcgroup.in. ORCID: https://orcid.org/0009-0001-8525-2789

Ananda Raju Tholeti is currently residing at Komaragiripatnam , DR B R .Ambedkar Konaseema, Andhra Pradesh- 533210.He is a B.Tech student specializing in Computer Science & Engineering at Bonam Venkata Chalamayya Engineering College, Odalarevu, with an expected graduation in May 2026. He aims to secure a position that leverages his strong organizational skills, educational background, and ability to work effectively with others. He possesses key skills in Python, MySQL. While his professional experience is listed as a student, his proactive approach and skill set indicate a strong potential for growth and contribution in a professional setting. Phone No.:7780612524 Email: 22221a05B4@bvcgroup.in.

Gopal Medida.is currently residing at D Ravulapalem , DR B R Ambedkar Konaseema, Andhra Pradesh-533217.He is a B.Tech student specializing in Computer Science & Engineering at Bonam Venkata Chalamayya Engineering College, Odalarevu, with an expected graduation in May 2026. He aims to secure a position that leverages his strong organizational skills, educational background, and ability to work effectively with others. He possesses key skills in Python, MySQL. While his professional experience is listed as a student, his proactive approach and skill set indicate a strong potential for growth and contribution in a professional setting. Phone No.:9951586607 Email: 22221a05D7@bvcgroup.in.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

Sai Krishna Veni Akula Research Scholar at college, Koneru Lakshmaiah Education Foundation (KLEF) Green Fileds, Vaddeswaram also Mrs.Sai Krishna Veni is Assistant Professor at college Bonam Venkata Chalamayya Engineering College,Odalarevu. .Her Research areas are Machine Learning,Deep Learning and Artificial Intelligence.She has number of patents related to machine learning field and industrial designs on her innovatinternational patents and published different articles in international conferences.Email: saikrishnaveni.bvce@bvcgroup.in ORCID: https://orcid.org/0000- 0003-1433-5832



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY