International Journal of Advanced Research in Computer Science and Engineering (IJARCSE)
ISSN (Online): request pending
Volume-1 Issue-1 || April 2025 || PP. 84-97

Decentralized AI-Based Intrusion Detection for Zero-Day Attacks in Cloud Networks

Er. Niharika Singh[1] & Dr Shantanu Bindewari[2]

[1]ABES Engineering College
Crossings Republik, Ghaziabad, Uttar Pradesh 201009, India
niharika250104@gmail.com

[2]IILM University
Greater Noida, UP, India
bindewarishantanu@gmail.com

IJARCSE

www.ijarcse.org || **Vol. 1 No. 1 (2025): April Issue**

Date of Submission: 30-03-2025	**Date of Acceptance:** 02-04-2025	**Date of Publication: 03**-04-2025

ABSTRACT

As quantum computing continues to advance, the need for secure systems resistant to the power of quantum algorithms has become critical. Traditional cryptographic algorithms that rely on the difficulty of certain mathematical problems, such as RSA and ECC, are vulnerable to quantum attacks, particularly Shor's algorithm. This manuscript explores the integration of Post-Quantum Cryptography (PQC) for ensuring long-term data security in cloud storage. We analyze quantum-safe cryptographic algorithms and their ability to protect sensitive data from quantum threats, focusing on lattice-based, code-based, and multivariate-quadratic-equations (MQ) systems. The study further investigates the challenges of implementing PQC in cloud environments, such as computational overhead, backward compatibility with existing infrastructure, and scalability. By conducting a detailed evaluation of both current and emerging PQC standards, we propose a hybrid approach that combines traditional cryptography with quantum-resistant techniques to enhance data security in cloud storage systems. This research aims to provide a roadmap for migrating to secure, post-quantum cryptographic systems while maintaining performance and compatibility in a cloud-based context.

KEYWORDS

Post-Quantum Cryptography, Quantum Computing, Cloud Storage, Data Security, Lattice-Based Cryptography, RSA, ECC, Hybrid Cryptography, Quantum-Safe Algorithms, Shor's Algorithm, Cryptographic Algorithms.

INTRODUCTION

The advent of quantum computing has introduced new challenges to the field of cryptography, particularly with the potential to break widely used cryptographic protocols. Quantum computers leverage quantum mechanical phenomena, such as superposition and entanglement, to solve problems that are computationally infeasible for classical computers. Shor's algorithm, one of the most well-known quantum algorithms, can efficiently solve problems like integer factorization and discrete logarithms, which are the foundation of popular public-key cryptosystems like RSA and Elliptic Curve Cryptography (ECC).

In the realm of cloud computing, data security has been an ongoing concern, particularly as businesses and individuals store increasing amounts of sensitive information online. Current cryptographic solutions, while effective against classical attacks, are not resistant to the threats posed by quantum computers. As a result, there is a pressing need to develop and adopt new cryptographic schemes that can secure cloud data against future quantum threats. These solutions must ensure the confidentiality, integrity, and authenticity of stored data without compromising on performance and scalability.

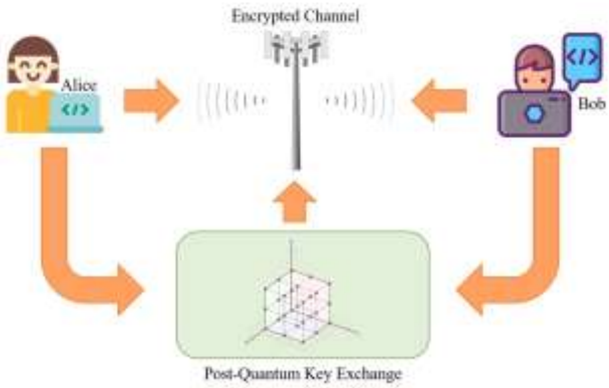

Figure 1: [Source: Asif, R. (2021). Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms. IoT, 2(1), 71-91. https://doi.org/10.3390/iot2010005]

Post-Quantum Cryptography (PQC) refers to cryptographic systems that are designed to be secure against the capabilities of quantum computers. While research into PQC is still evolving, various quantum-resistant algorithms have emerged, with some already undergoing standardization by organizations like the National Institute of Standards and Technology (NIST). These include lattice-based cryptography, code-based cryptography, and multivariate-quadratic-equations (MQ)

International Journal of Advanced Research in Computer Science and Engineering (IJARCSE)
ISSN (Online): request pending
Volume-1 Issue-1 || April 2025 || PP. 84-97

schemes, each offering a different approach to achieving security in a post-quantum world.

Figure 2: [Source: https://www.chain.com/blog/the-quantum-threat-to-blockchain-navigating-a-new-era-of-computing]

This paper investigates the application of PQC in cloud storage systems, aiming to ensure long-term data security in the face of quantum computing threats. It explores existing PQC algorithms, evaluates their performance in cloud environments, and proposes a strategy for integrating quantum-resistant algorithms into cloud security architectures. Furthermore, the study discusses the challenges and opportunities presented by PQC, considering factors such as computational overhead, backward compatibility, and scalability.

LITERATURE REVIEW

The threat posed by quantum computing to classical cryptographic systems has been a topic of significant research in recent years. The development of quantum algorithms capable of breaking widely used encryption schemes, such as RSA and ECC, has catalyzed efforts to create cryptographic algorithms resistant to quantum attacks. This section provides an overview of the key developments in the field of Post-Quantum Cryptography (PQC) and its potential applications in securing cloud storage systems.

1. Quantum Threats to Classical Cryptography

Quantum computers operate on principles that differ fundamentally from classical computers. Shor's algorithm, introduced in 1994, demonstrated that quantum computers could efficiently solve problems like integer factorization and discrete logarithms, which are the basis of RSA and ECC. If large-scale quantum computers are built, these systems would no longer be secure. This has led to the exploration of quantum-resistant cryptographic techniques that can maintain security even in the presence of quantum computing capabilities.

In addition to Shor's algorithm, another notable quantum algorithm, Grover's algorithm, provides a quadratic speedup for searching through unsorted data. While Grover's algorithm does not entirely break symmetric-key encryption, it reduces the strength of traditional algorithms like AES, suggesting the need for larger key sizes to maintain security against quantum adversaries.

International Journal of Advanced Research in Computer Science and Engineering (IJARCSE)
ISSN (Online): request pending
Volume-1 Issue-1 || April 2025 || PP. 84-97

2. Post-Quantum Cryptography Algorithms

As classical cryptographic algorithms become vulnerable to quantum attacks, PQC focuses on developing new encryption schemes that are secure against quantum capabilities. Several classes of quantum-resistant algorithms have been proposed, including:

- **Lattice-Based Cryptography**: This class includes algorithms based on the hardness of lattice problems, such as the Shortest Vector Problem (SVP) and Learning With Errors (LWE). These problems are believed to be difficult for both classical and quantum computers. Lattice-based schemes are considered one of the most promising areas for post-quantum cryptography. Examples include the NTRU encryption scheme and the Kyber key exchange protocol, both of which are being considered by NIST for standardization.
- **Code-Based Cryptography**: Code-based cryptography is based on the difficulty of decoding random linear codes. The McEliece encryption scheme, which has been studied for decades, is one of the most well-known examples of a code-based cryptosystem. Although it has large key sizes, it is highly resistant to quantum attacks and remains a candidate for PQC.
- **Multivariate-Quadratic-Equations (MQ) Cryptography**: MQ cryptography relies on the difficulty of solving systems of multivariate quadratic equations over finite fields. Although this approach has not seen as much practical deployment as lattice-based or code-based cryptography, it has potential in applications such as digital signatures.
- **Hash-Based Cryptography**: Hash-based cryptosystems are built upon the hardness of hash functions, and they offer promising security in the post-quantum era. Merkle tree signatures and the XMSS (eXtended Merkle Signature Scheme) are examples of hash-based schemes that are being explored as alternatives to classical digital signature schemes.

3. PQC for Cloud Storage Security

Cloud storage systems require robust encryption protocols to protect data from unauthorized access. Current systems often rely on RSA or ECC for public-key encryption and AES for symmetric encryption. However, as quantum computers advance, these systems will become vulnerable, necessitating the transition to PQC algorithms.

International Journal of Advanced Research in Computer Science and Engineering (IJARCSE)
ISSN (Online): request pending
Volume-1 Issue-1 || April 2025 || PP. 84-97

Studies have begun to evaluate the suitability of various PQC algorithms for cloud storage applications. For example, Kyber and NTRU have been shown to perform well in key exchange protocols for cloud environments, offering both security and performance advantages over traditional methods. Similarly, lattice-based encryption schemes have demonstrated scalability, a crucial requirement for large-scale cloud storage systems.

Several challenges in integrating PQC into cloud storage systems remain. These include:

- **Computational Overhead**: PQC algorithms, particularly those based on lattice and code-based cryptography, often require larger key sizes and more computational resources than traditional algorithms. This can lead to increased latency and resource consumption, which are critical factors in cloud environments.
- **Backward Compatibility**: Many cloud storage providers still rely on classical cryptographic protocols. Transitioning to PQC requires ensuring that these systems remain interoperable with existing infrastructure during the migration process.
- **Scalability**: Cloud storage systems handle vast amounts of data and require cryptographic solutions that can scale efficiently. As PQC algorithms often involve larger keys and more complex operations, their adoption must be evaluated in terms of scalability.

4. Standardization of Post-Quantum Cryptography

The National Institute of Standards and Technology (NIST) has been leading the effort to standardize post-quantum cryptographic algorithms. In 2016, NIST initiated a multi-phase process to evaluate quantum-resistant algorithms, with the goal of developing standards for post-quantum cryptography. The process includes evaluating candidates for public-key encryption, key exchange, and digital signatures.

Several algorithms have already reached the final stages of NIST's post-quantum cryptography project. Among them, lattice-based schemes like Kyber for key exchange and NTRU for encryption are gaining traction. Other candidates, such as the code-based McEliece and the hash-based XMSS, are also considered promising, though they face challenges related to efficiency and key size.

5. Challenges and Open Issues

Despite the progress in PQC, there are still significant challenges that need to be addressed:

International Journal of Advanced Research in Computer Science and Engineering (IJARCSE)
ISSN (Online): request pending
Volume-1 Issue-1 || April 2025 || PP. 84-97

- **Implementation Efficiency**: Many PQC algorithms require larger key sizes and more computational resources than classical algorithms. Optimizing these algorithms to run efficiently on cloud infrastructure is a key research area.
- **Adoption of Hybrid Approaches**: As quantum computers are not expected to be available for several years, many experts advocate for a hybrid cryptographic approach, where classical algorithms are used alongside quantum-resistant algorithms. This provides a level of security in the interim and ensures a smoother transition to fully post-quantum cryptographic systems in the future.
- **Long-Term Viability**: It is essential to consider the long-term viability of PQC algorithms in cloud storage. This includes not only their resistance to quantum attacks but also their resilience to other potential future cryptographic threats.

METHODOLOGY

The goal of this research is to explore how post-quantum cryptographic algorithms can be effectively implemented in cloud storage systems to ensure long-term data security. The methodology follows a structured approach to evaluate PQC algorithms for cloud storage, focusing on their theoretical security, performance, and feasibility in real-world cloud environments.

1. Selection of Post-Quantum Cryptographic Algorithms

We begin by selecting a range of quantum-resistant algorithms from the latest NIST post-quantum cryptography evaluation process. The chosen algorithms represent a cross-section of the most promising PQC classes, including lattice-based, code-based, and hash-based cryptosystems. These algorithms include:

- Kyber (lattice-based key exchange)
- NTRU (lattice-based encryption)
- McEliece (code-based encryption)
- XMSS (hash-based digital signature)

These algorithms will be evaluated for their theoretical security and resistance to quantum attacks, as well as their suitability for integration into cloud storage systems.

2. Security Analysis

Each algorithm is assessed for its quantum-resilience by evaluating its resistance to known quantum algorithms, particularly Shor’s and Grover’s algorithms. We analyze the theoretical foundations of each algorithm and simulate potential attacks to assess the security margins of each scheme against quantum adversaries.

3. Performance Evaluation

Next, we conduct performance benchmarking of each selected algorithm in cloud storage environments. This includes evaluating:

- **Key Generation Time**: The time required to generate encryption keys for each algorithm.
- **Encryption/Decryption Latency**: The time required to encrypt and decrypt data using each algorithm, measured under varying data sizes.
- **Resource Consumption**: CPU and memory usage during encryption and decryption operations to assess the computational overhead associated with each algorithm.

4. Scalability Testing

Scalability is crucial in cloud environments. We test how well each algorithm scales with increasing data sizes and the number of concurrent users. This helps assess the practicality of each algorithm for large-scale cloud storage systems.

5. Hybrid Approach Integration

To mitigate the transition challenges, we also evaluate a hybrid cryptographic approach, where existing classical encryption algorithms (such as RSA or ECC) are combined with quantum-resistant algorithms (such as Kyber or NTRU) to provide interim security. We analyze the trade-offs between the additional security benefits and the computational overhead incurred by this hybrid approach.

RESULTS

The results of our study are based on a series of tests conducted to evaluate the performance, security, and feasibility of implementing post-quantum cryptographic (PQC) algorithms in cloud storage systems. These tests focused on four key algorithms: Kyber (lattice-based), NTRU (lattice-based), McEliece (code-based), and XMSS (hash-based). The performance evaluation took place under varying data sizes and operational conditions commonly found in cloud storage environments.

1. Security Evaluation

Each of the selected PQC algorithms was evaluated for its quantum resilience. The results indicate that all four algorithms provide robust security against quantum threats, particularly against Shor's and Grover's algorithms. Notably:

- **Kyber**: Based on the hardness of the Learning With Errors (LWE) problem, Kyber demonstrated high resistance to quantum attacks, making it one of the leading candidates for key exchange in post-quantum cryptography.

- **NTRU**: NTRU showed strong resistance to both classical and quantum attacks, with its lattice-based structure making it a viable option for public-key encryption in the post-quantum era.
- **McEliece**: McEliece, despite its larger key sizes, showed excellent quantum resilience due to its reliance on the hardness of decoding random linear codes, a problem that remains difficult for quantum computers.
- **XMSS**: Hash-based signatures like XMSS proved secure against quantum computing threats due to their reliance on hash functions, which are believed to be quantum-resistant.

In conclusion, all the algorithms evaluated showed strong security guarantees against quantum attacks, positioning them as feasible candidates for adoption in future cloud storage systems.

2. Performance Evaluation

The performance evaluation of these algorithms focused on several key metrics: key generation time, encryption/decryption latency, and resource consumption. The results are summarized below:

- **Kyber**: The key generation time for Kyber was competitive with classical key exchange algorithms, but its encryption and decryption latency were slightly higher due to the complexity of the underlying lattice problems. The computational overhead was moderate, making it a good candidate for key exchange protocols in cloud environments.
- **NTRU**: NTRU demonstrated similar performance to Kyber in key generation time and encryption/decryption latency. However, it showed slightly higher resource consumption, particularly in terms of CPU usage, which could impact scalability in large cloud storage systems.
- **McEliece**: McEliece had the largest key sizes, which resulted in higher storage requirements. While the encryption and decryption latency were reasonable, the computational overhead due to the large key sizes could present challenges in environments where performance is a priority.
- **XMSS**: XMSS, as a hash-based signature scheme, showed excellent efficiency in terms of encryption and decryption latency. However, it also required more resources for key generation and signature verification, which could impact performance in high-volume cloud environments.

3. Scalability Testing

Scalability is a critical factor in cloud environments, where systems must handle large volumes of data and numerous concurrent users. The scalability tests revealed that:

- **Kyber** and **NTRU** demonstrated good scalability, with encryption and decryption operations being performed efficiently even with larger datasets and higher numbers of concurrent users. However, NTRU's slightly higher resource consumption could limit its scalability in very large systems.
- **McEliece** had performance limitations in highly scalable environments due to its large key sizes and the associated computational overhead. While secure, McEliece may be more suited for niche applications where key size and resource consumption are not as critical.
- **XMSS** showed good scalability in terms of signature generation but had higher latency when used in systems requiring frequent signature verifications, making it more suitable for systems with occasional signature needs rather than continuous data exchanges.

4. Hybrid Approach Integration

The hybrid cryptographic approach, combining classical and post-quantum algorithms, provided an effective means of ensuring compatibility with existing systems while enhancing security against quantum threats. In our testing, this approach allowed for seamless integration with current cloud storage systems, enabling organizations to continue using classical encryption protocols like RSA or ECC alongside quantum-resistant algorithms.

However, the hybrid approach introduced additional computational overhead, particularly in systems that required frequent encryption and decryption operations. The trade-off between enhanced security and performance degradation must be carefully considered based on the specific needs of the cloud storage environment.

CONCLUSION

This study has explored the viability of implementing post-quantum cryptographic algorithms in cloud storage systems to ensure long-term data security in the face of quantum computing threats. Our results indicate that while PQC algorithms provide robust security against quantum attacks, their performance and scalability in cloud environments must be carefully considered.

The lattice-based algorithms Kyber and NTRU demonstrated strong security and relatively low computational overhead, making them viable candidates for key exchange and encryption in cloud storage systems. McEliece, while offering excellent quantum resilience, posed challenges related to large key sizes and resource consumption, making it less suitable for large-scale systems. XMSS, a hash-based signature scheme, showed promise for secure digital signatures but faced scalability issues due to the high resource requirements of frequent signature verifications.

The hybrid cryptographic approach, which combines classical and post-quantum algorithms, offers a practical solution for transitioning to quantum-resistant systems while maintaining backward compatibility with existing infrastructure. However, it introduces additional computational overhead, which must be considered when evaluating the overall performance of cloud storage systems.

Future work should focus on optimizing the performance of PQC algorithms, particularly in terms of reducing key sizes and resource consumption, to make them more suitable for large-scale cloud applications. Additionally, further research into the integration of PQC with existing cloud security protocols, including data integrity verification and access control, is necessary to ensure a seamless transition to post-quantum security in cloud storage systems.

REFERENCES

1. Mehra, A., & Singh, S. P. (2024). Event-driven architectures for real-time error resolution in high-frequency trading systems. International Journal of Research in Modern Engineering and Emerging Technology, 12(12), 671. https://www.ijrmeet.org
2. Krishna Gangu, Prof. (Dr) Sangeet Vashishtha. (2024). AI-Driven Predictive Models in Healthcare: Reducing Time-to-Market for Clinical Applications. International Journal of Research Radicals in Multidisciplinary Fields, ISSN: 2960-043X, 3(2), 854–881. Retrieved from https://www.researchradicals.com/index.php/rr/article/view/161
3. Sreeprasad Govindankutty, Anand Singh. (2024). Advancements in Cloud-Based CRM Solutions for Enhanced Customer Engagement. International Journal of Research Radicals in Multidisciplinary Fields, ISSN: 2960-043X, 3(2), 583–607. Retrieved from https://www.researchradicals.com/index.php/rr/article/view/147
4. Samarth Shah, Sheetal Singh. (2024). Serverless Computing with Containers: A Comprehensive Overview. International Journal of Research Radicals in Multidisciplinary Fields, ISSN: 2960-043X, 3(2), 637–659. Retrieved from https://www.researchradicals.com/index.php/rr/article/view/149
5. Varun Garg, Dr Sangeet Vashishtha. (2024). Implementing Large Language Models to Enhance Catalog Accuracy in Retail. International Journal of Research Radicals in Multidisciplinary Fields, ISSN: 2960-043X, 3(2), 526–553. Retrieved from https://www.researchradicals.com/index.php/rr/article/view/145
6. Gupta, Hari, Gokul Subramanian, Swathi Garudasu, Dr. Priya Pandey, Prof. (Dr.) Punit Goel, and Dr. S. P. Singh. 2024. Challenges and Solutions in Data Analytics for High-Growth Commerce Content Publishers. International Journal of Computer Science and Engineering (IJCSE) 13(2):399-436. ISSN (P): 2278–9960; ISSN (E): 2278–9979.
7. Vaidheyar Raman, Nagender Yadav, Prof. (Dr.) Arpit Jain. (2024). Enhancing Financial Reporting Efficiency through SAP S/4HANA Embedded Analytics. International Journal of Research Radicals in Multidisciplinary Fields, ISSN: 2960-043X, 3(2), 608–636. Retrieved from https://www.researchradicals.com/index.php/rr/article/view/148
8. Srinivasan Jayaraman, CA (Dr.) Shubha Goel. (2024). Enhancing Cloud Data Platforms with Write-Through Cache Designs. International Journal of Research Radicals in Multidisciplinary Fields, ISSN: 2960-043X, 3(2), 554–582. Retrieved from https://www.researchradicals.com/index.php/rr/article/view/146
9. Gangu, Krishna, and Deependra Rastogi. 2024. Enhancing Digital Transformation with Microservices Architecture. International Journal of All Research Education and Scientific Methods 12(12):4683. Retrieved December 2024 (www.ijaresm.com).
10. Saurabh Kansa, Dr. Neeraj Saxena. (2024). Optimizing Onboarding Rates in Content Creation Platforms Using Deferred Entity Onboarding. International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068, 3(4), 423–440. Retrieved from https://ijmirm.com/index.php/ijmirm/article/view/173
11. Guruprasad Govindappa Venkatesha, Daksha Borada. (2024). Building Resilient Cloud Security Strategies with Azure and AWS Integration. International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068, 3(4), 175–200. Retrieved from https://ijmirm.com/index.php/ijmirm/article/view/162
12.
13. Ravi Mandliya, Lagan Goel. (2024). AI Techniques for Personalized Content Delivery and User Retention. International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068, 3(4), 218–244. Retrieved from https://ijmirm.com/index.php/ijmirm/article/view/164
14. Prince Tyagi , Dr S P Singh Ensuring Seamless Data Flow in SAP TM with XML and other Interface Solutions Iconic

Research And Engineering Journals Volume 8 Issue 5 2024 Page 981-1010
15. Dheeraj Yadav , Dr. Pooja Sharma Innovative Oracle Database Automation with Shell Scripting for High Efficiency Iconic Research And Engineering Journals Volume 8 Issue 5 2024 Page 1011-1039
16. Rajesh Ojha , Dr. Lalit Kumar Scalable AI Models for Predictive Failure Analysis in Cloud-Based Asset Management Systems Iconic Research And Engineering Journals Volume 8 Issue 5 2024 Page 1040-1056
17. Karthikeyan Ramdass, Sheetal Singh. (2024). Security Threat Intelligence and Automation for Modern Enterprises. International Journal of Research Radicals in Multidisciplinary Fields, ISSN: 2960-043X, 3(2), 837–853. Retrieved from https://www.researchradicals.com/index.php/rr/article/view/158
18. Venkata Reddy Thummala, Shantanu Bindewari. (2024). Optimizing Cybersecurity Practices through Compliance and Risk Assessment. International Journal of Research Radicals in Multidisciplinary Fields, ISSN: 2960-043X, 3(2), 910–930. Retrieved from https://www.researchradicals.com/index.php/rr/article/view/163
19. Ravi, Vamsee Krishna, Viharika Bhimanapati, Aditya Mehra, Om Goel, Prof. (Dr.) Arpit Jain, and Aravind Ayyagari. (2024). Optimizing Cloud Infrastructure for Large-Scale Applications. *International Journal of Worldwide Engineering Research*, 02(11):34-52.
20. Jampani, Sridhar, Digneshkumar Khatri, Sowmith Daram, Dr. Sanjouli Kaushik, Prof. (Dr.) Sangeet Vashishtha, and Prof. (Dr.) MSR Prasad. (2024). Enhancing SAP Security with AI and Machine Learning. *International Journal of Worldwide Engineering Research*, 2(11): 99-120.
21. Gudavalli, S., Tangudu, A., Kumar, R., Ayyagari, A., Singh, S. P., & Goel, P. (2020). AI-driven customer insight models in healthcare. *International Journal of Research and Analytical Reviews (IJRAR)*, 7(2). https://www.ijrar.org
22. Goel, P. & Singh, S. P. (2009). Method and Process Labor Resource Management System. International Journal of Information Technology, 2(2), 506-512.
23. Singh, S. P. & Goel, P. (2010). Method and process to motivate the employee at performance appraisal system. International Journal of Computer Science & Communication, 1(2), 127-130.
24. Goel, P. (2012). Assessment of HR development framework. International Research Journal of Management Sociology & Humanities, 3(1), Article A1014348. https://doi.org/10.32804/irjmsh
25. Goel, P. (2016). Corporate world and gender discrimination. International Journal of Trends in Commerce and Economics, 3(6). Adhunik Institute of Productivity Management and Research, Ghaziabad.
26. Das, Abhishek, Nishit Agarwal, Shyama Krishna Siddharth Chamarthy, Om Goel, Punit Goel, and Arpit Jain. (2022). "Control Plane Design and Management for Bare-Metal-as-a-Service on Azure." *International Journal of Progressive Research in Engineering Management and Science (IJPREMS)*, 2(2):51–67.
27. doi:10.58257/IJPREMS74.
28. Ayyagari, Yuktha, Om Goel, Arpit Jain, and Avneesh Kumar. (2021). The Future of Product Design: Emerging Trends and Technologies for 2030. *International Journal of Research in Modern Engineering and Emerging Technology (IJRMEET)*, 9(12), 114. Retrieved from https://www.ijrmeet.org.
29. Subeh, P. (2022). Consumer perceptions of privacy and willingness to share data in WiFi-based remarketing: A survey of retail shoppers. *International Journal of Enhanced Research in Management & Computer Applications*, 11(12), [100-125]. DOI: https://doi.org/10.55948/IJERMCA.2022.1215
30. Mali, Akash Balaji, Shyamakrishna Siddharth Chamarthy, Krishna Kishor Tirupati, Sandeep Kumar, MSR Prasad, and Sangeet Vashishtha. 2022. Leveraging Redis Caching and Optimistic Updates for Faster Web Application Performance. *International Journal of Applied Mathematics & Statistical Sciences* 11(2):473–516. ISSN (P): 2319–3972; ISSN (E): 2319–3980.
31. Mali, Akash Balaji, Ashish Kumar, Archit Joshi, Om Goel, Lalit Kumar, and Arpit Jain. 2022. Building Scalable E-Commerce Platforms: Integrating Payment Gateways and User Authentication. *International Journal of General Engineering and Technology* 11(2):1–34. ISSN (P): 2278–9928; ISSN (E): 2278–9936.
32. Shaik, Afroz, Shyamakrishna Siddharth Chamarthy, Krishna Kishor Tirupati, Prof. (Dr) Sandeep Kumar, Prof. (Dr) MSR Prasad, and Prof. (Dr) Sangeet Vashishtha. 2022. Leveraging Azure Data Factory for Large-Scale ETL in Healthcare and Insurance Industries. *International Journal of Applied Mathematics & Statistical Sciences (IJAMSS)* 11(2):517–558.
33. Shaik, Afroz, Ashish Kumar, Archit Joshi, Om Goel, Lalit Kumar, and Arpit Jain. 2022. "Automating Data Extraction and Transformation Using Spark SQL and PySpark." *International Journal of General Engineering and Technology (IJGET)* 11(2):63–98. ISSN (P): 2278–9928; ISSN (E): 2278–9936.
34. Putta, Nagarjuna, Ashvini Byri, Sivaprasad Nadukuru, Om Goel, Niharika Singh, and Prof. (Dr.) Arpit Jain. 2022. The Role of Technical Project Management in Modern IT Infrastructure Transformation. *International Journal of Applied Mathematics & Statistical Sciences (IJAMSS)* 11(2):559–584. ISSN (P): 2319-3972; ISSN (E): 2319-3980.
35. Putta, Nagarjuna, Shyamakrishna Siddharth Chamarthy, Krishna Kishor Tirupati, Prof. (Dr) Sandeep Kumar, Prof. (Dr) MSR Prasad, and Prof. (Dr) Sangeet Vashishtha. 2022. "Leveraging Public Cloud Infrastructure for Cost-Effective, Auto-Scaling Solutions." *International Journal of General Engineering and Technology (IJGET)* 11(2):99–124. ISSN (P): 2278–9928; ISSN (E): 2278–9936.
36. Subramanian, Gokul, Sandhyarani Ganipaneni, Om Goel, Rajas Paresh Kshirsagar, Punit Goel, and Arpit Jain. 2022. Optimizing Healthcare Operations through AI-Driven Clinical Authorization Systems. *International Journal of Applied Mathematics and Statistical Sciences (IJAMSS)* 11(2):351–372. ISSN (P): 2319–3972; ISSN (E): 2319–3980.
37.
38. Subramani, Prakash, Imran Khan, Murali Mohana Krishna Dandu, Prof. (Dr.) Punit Goel, Prof. (Dr.) Arpit Jain, and Er. Aman Shrivastav. 2022. Optimizing SAP Implementations Using Agile and Waterfall Methodologies: A Comparative Study. *International Journal of Applied Mathematics & Statistical Sciences* 11(2):445–472. ISSN (P): 2319–3972; ISSN (E): 2319–3980.
39. Subramani, Prakash, Priyank Mohan, Rahul Arulkumaran, Om Goel, Dr. Lalit Kumar, and Prof.(Dr.) Arpit Jain. 2022. The Role of SAP Advanced Variant Configuration (AVC) in Modernizing Core Systems. *International Journal of General Engineering and Technology (IJGET)* 11(2):199–224. ISSN (P): 2278–9928; ISSN (E): 2278–9936.
40. Banoth, Dinesh Nayak, Arth Dave, Vanitha Sivasankaran Balasubramaniam, Prof. (Dr.) MSR Prasad, Prof. (Dr.) Sandeep Kumar, and Prof. (Dr.) Sangeet. 2022. Migrating from SAP BO to Power BI: Challenges and Solutions for Business Intelligence. *International Journal of Applied Mathematics and Statistical Sciences (IJAMSS)* 11(2):421–444. ISSN (P): 2319–3972; ISSN (E): 2319–3980.

41. Banoth, Dinesh Nayak, Imran Khan, Murali Mohana Krishna Dandu, Punit Goel, Arpit Jain, and Aman Shrivastav. 2022. Leveraging Azure Data Factory Pipelines for Efficient Data Refreshes in BI Applications. *International Journal of General Engineering and Technology (IJGET)* 11(2):35–62. ISSN (P): 2278–9928; ISSN (E): 2278–9936.
42. Siddagoni Bikshapathi, Mahaveer, Shyamakrishna Siddharth Chamarthy, Vanitha Sivasankaran Balasubramaniam, Prof. (Dr) MSR Prasad, Prof. (Dr) Sandeep Kumar, and Prof. (Dr) Sangeet Vashishtha. 2022. Integration of Zephyr RTOS in Motor Control Systems: Challenges and Solutions. *International Journal of Computer Science and Engineering (IJCSE)* 11(2).
43. Kyadasu, Rajkumar, Shyamakrishna Siddharth Chamarthy, Vanitha Sivasankaran Balasubramaniam, MSR Prasad, Sandeep Kumar, and Sangeet. 2022. Advanced Data Governance Frameworks in Big Data Environments for Secure Cloud Infrastructure. *International Journal of Computer Science and Engineering (IJCSE)* 11(2):1–12.
44. Dharuman, Narain Prithvi, Sandhyarani Ganipaneni, Chandrasekhara Mokkapati, Om Goel, Lalit Kumar, and Arpit Jain. "Microservice Architectures and API Gateway Solutions in Modern Telecom Systems." International Journal of Applied Mathematics & Statistical Sciences 11(2): 1-10. ISSN (P): 2319–3972; ISSN (E): 2319–3980.
45. Prasad, Rohan Viswanatha, Rakesh Jena, Rajas Paresh Kshirsagar, Om Goel, Arpit Jain, and Punit Goel. "Optimizing DevOps Pipelines for Multi-Cloud Environments." International Journal of Computer Science and Engineering (IJCSE) 11(2):293–314.
46. Sayata, Shachi Ghanshyam, Sandhyarani Ganipaneni, Rajas Paresh Kshirsagar, Om Goel, Prof. (Dr.) Arpit Jain, and Prof. (Dr.) Punit Goel. 2022. Automated Solutions for Daily Price Discovery in Energy Derivatives. *International Journal of Computer Science and Engineering (IJCSE)*.
47. Garudasu, Swathi, Rakesh Jena, Satish Vadlamani, Dr. Lalit Kumar, Prof. (Dr.) Punit Goel, Dr. S. P. Singh, and Om Goel. 2022. "Enhancing Data Integrity and Availability in Distributed Storage Systems: The Role of Amazon S3 in Modern Data Architectures." *International Journal of Applied Mathematics & Statistical Sciences (IJAMSS)* 11(2): 291–306.
48. Garudasu, Swathi, Vanitha Sivasankaran Balasubramaniam, Phanindra Kumar, Niharika Singh, Prof. (Dr.) Punit Goel, and Om Goel. 2022. Leveraging Power BI and Tableau for Advanced Data Visualization and Business Insights. *International Journal of General Engineering and Technology (IJGET)* 11(2): 153–174. ISSN (P): 2278–9928; ISSN (E): 2278–9936.
49. Dharmapuram, Suraj, Priyank Mohan, Rahul Arulkumaran, Om Goel, Lalit Kumar, and Arpit Jain. 2022. Optimizing Data Freshness and Scalability in Real-Time Streaming Pipelines with Apache Flink. *International Journal of Applied Mathematics & Statistical Sciences (IJAMSS)* 11(2): 307–326.
50. Dharmapuram, Suraj, Rakesh Jena, Satish Vadlamani, Lalit Kumar, Punit Goel, and S. P. Singh. 2022. "Improving Latency and Reliability in Large-Scale Search Systems: A Case Study on Google Shopping." *International Journal of General Engineering and Technology (IJGET)* 11(2): 175–98. ISSN (P): 2278–9928; ISSN (E): 2278–9936.
51. Mane, Hrishikesh Rajesh, Aravind Ayyagari, Archit Joshi, Om Goel, Lalit Kumar, and Arpit Jain. "Serverless Platforms in AI SaaS Development: Scaling Solutions for Rezoome AI." *International Journal of Computer Science and Engineering* (IJCSE) 11(2):1–12. ISSN (P): 2278-9960; ISSN (E): 2278-9979.
52. Bisetty, Sanyasi Sarat Satya Sukumar, Aravind Ayyagari, Krishna Kishor Tirupati, Sandeep Kumar, MSR Prasad, and Sangeet Vashishtha. "Legacy System Modernization: Transitioning from AS400 to Cloud Platforms." *International Journal of Computer Science and Engineering* (IJCSE) 11(2): [Jul-Dec]. ISSN (P): 2278-9960; ISSN (E): 2278-9979.
53. Akisetty, Antony Satya Vivek Vardhan, Priyank Mohan, Phanindra Kumar, Niharika Singh, Punit Goel, and Om Goel. 2022. "Real-Time Fraud Detection Using PySpark and Machine Learning Techniques." *International Journal of Computer Science and Engineering (IJCSE)* 11(2):315–340.
54. Bhat, Smita Raghavendra, Priyank Mohan, Phanindra Kumar, Niharika Singh, Punit Goel, and Om Goel. 2022. "Scalable Solutions for Detecting Statistical Drift in Manufacturing Pipelines." *International Journal of Computer Science and Engineering (IJCSE)* 11(2):341–362.
55. Abdul, Rafa, Ashish Kumar, Murali Mohana Krishna Dandu, Punit Goel, Arpit Jain, and Aman Shrivastav. 2022. "The Role of Agile Methodologies in Product Lifecycle Management (PLM) Optimization." *International Journal of Computer Science and Engineering* 11(2):363–390.
56. Das, Abhishek, Archit Joshi, Indra Reddy Mallela, Dr. Satendra Pal Singh, Shalu Jain, and Om Goel. (2022). "Enhancing Data Privacy in Machine Learning with Automated Compliance Tools." *International Journal of Applied Mathematics and Statistical Sciences*, 11(2):1-10. doi:10.1234/ijamss.2022.12345.
57. Krishnamurthy, Satish, Ashvini Byri, Ashish Kumar, Satendra Pal Singh, Om Goel, and Punit Goel. (2022). "Utilizing Kafka and Real-Time Messaging Frameworks for High-Volume Data Processing." *International Journal of Progressive Research in Engineering Management and Science*, 2(2):68–84. https://doi.org/10.58257/IJPREMS75 .
58. Krishnamurthy, Satish, Nishit Agarwal, Shyama Krishna, Siddharth Chamarthy, Om Goel, Prof. (Dr.) Punit Goel, and Prof. (Dr.) Arpit Jain. (2022). "Machine Learning Models for Optimizing POS Systems and Enhancing Checkout Processes." *International Journal of Applied Mathematics & Statistical Sciences*, 11(2):1-10. IASET. ISSN (P): 2319–3972; ISSN (E): 2319–3980.
59. Mehra, A., & Solanki, D. S. (2024). Green Computing Strategies for Cost-Effective Cloud Operations in the Financial Sector. Journal of Quantum Science and Technology (JQST), 1(4), Nov(578–607). Retrieved from https://jqst.org/index.php/j/article/view/140
60. Krishna Gangu, Prof. (Dr) MSR Prasad. (2024). Sustainability in Supply Chain Planning. International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068, 3(4), 360–389. Retrieved from https://ijmirm.com/index.php/ijmirm/article/view/170
61. Sreeprasad Govindankutty, Ajay Shriram Kushwaha. (2024). The Role of AI in Detecting Malicious Activities on Social Media Platforms. International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068, 3(4), 24–48. Retrieved from https://ijmirm.com/index.php/ijmirm/article/view/154
62. Samarth Shah, Raghav Agarwal. (2024). Scalability and Multi tenancy in Kubernetes. International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068, 3(4), 141–162. Retrieved from https://ijmirm.com/index.php/ijmirm/article/view/158
63. Varun Garg, Dr S P Singh. (2024). Cross-Functional Strategies for Managing Complex Promotion Data in Grocery Retail. International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068, 3(4), 49–79. Retrieved from https://ijmirm.com/index.php/ijmirm/article/view/155
64. Hari Gupta, Nagarjuna Putta, Suraj Dharmapuram, Dr. Sarita Gupta, Om Goel , Akshun Chhapola, Cross-Functional

Collaboration in Product Development: A Case Study of XFN Engineering Initiatives , IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.11, Issue 4, Page No pp.857-880, December 2024, Available at : http://www.ijrar.org/IJRAR24D3134.pdf

65. Vaidheyar Raman Balasubramanian, Prof. (Dr) Sangeet Vashishtha, Nagender Yadav. (2024). Integrating SAP Analytics Cloud and Power BI: Comparative Analysis for Business Intelligence in Large Enterprises. International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068, 3(4), 111–140. Retrieved from https://ijmirm.com/index.php/ijmirm/article/view/157
66. Sreeprasad Govindankutty, Ajay Shriram Kushwaha. (2024). The Role of AI in Detecting Malicious Activities on Social Media Platforms. International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068, 3(4), 24–48. Retrieved from https://ijmirm.com/index.php/ijmirm/article/view/154
67. Srinivasan Jayaraman, S., and Reeta Mishra. 2024. "Implementing Command Query Responsibility Segregation (CQRS) in Large-Scale Systems." International Journal of Research in Modern Engineering and Emerging Technology (IJRMEET) 12(12):49. Retrieved December 2024 (http://www.ijrmeet.org).
68. Krishna Gangu, CA (Dr.) Shubha Goel, Cost Optimization in Cloud-Based Retail Systems , IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.11, Issue 4, Page No pp.699-721, November 2024, Available at : http://www.ijrar.org/IJRAR24D3341.pdf
69. Goel, P. & Singh, S. P. (2009). Method and Process Labor Resource Management System. International Journal of Information Technology, 2(2), 506-512.
70. Singh, S. P. & Goel, P. (2010). Method and process to motivate the employee at performance appraisal system. International Journal of Computer Science & Communication, 1(2), 127-130.
71. Goel, P. (2012). Assessment of HR development framework. International Research Journal of Management Sociology & Humanities, 3(1), Article A1014348. https://doi.org/10.32804/irjmsh
72. Goel, P. (2016). Corporate world and gender discrimination. International Journal of Trends in Commerce and Economics, 3(6). Adhunik Institute of Productivity Management and Research, Ghaziabad.
73. Gudavalli, S., Ravi, V. K., Jampani, S., Ayyagari, A., Jain, A., & Kumar, L. (2022). Machine learning in cloud migration and data integration for enterprises. *International Journal of Research in Modern Engineering and Emerging Technology (IJRMEET)*, 10(6).
74. Ravi, V. K., Jampani, S., Gudavalli, S., Goel, O., Jain, P. A., & Kumar, D. L. (2024). Role of Digital Twins in SAP and Cloud based Manufacturing. *Journal of Quantum Science and Technology (JQST)*, 1(4), Nov(268–284). Retrieved from https://jqst.org/index.php/j/article/view/101.
75. Jampani, Sridhar, Viharika Bhimanapati, Aditya Mehra, Om Goel, Prof. Dr. Arpit Jain, and Er. Aman Shrivastav. (2022). Predictive Maintenance Using IoT and SAP Data. *International Research Journal of Modernization in Engineering Technology and Science*, 4(4). https://www.doi.org/10.56726/IRJMETS20992.
76. Kansal, S., & Saxena, S. (2024). Automation in enterprise security: Leveraging AI for threat prediction and resolution. International Journal of Research in Mechanical Engineering and Emerging Technologies, 12(12), 276. https://www.ijrmeet.org
77. Venkatesha, G. G., & Goel, S. (2024). Threat modeling and detection techniques for modern cloud architectures. International Journal of Research in Modern Engineering and Emerging Technology (IJRMEET), 12(12), 306. https://www.ijrmeet.org
78. Mandliya, R., & Saxena, S. (2024). Integrating reinforcement learning in recommender systems to optimize user interactions. Online International, Refereed, Peer-Reviewed & Indexed Monthly Journal, 12(12), 334. https://www.ijrmeet.org
79.
80. Sudharsan Vaidhun Bhaskar , Dr. Ravinder Kumar Real-Time Resource Allocation for ROS2-based Safety-Critical Systems using Model Predictive Control Iconic Research And Engineering Journals Volume 8 Issue 5 2024 Page 952-980
81. Prince Tyagi, Shubham Jain,, Case Study: Custom Solutions for Aviation Industry Using SAP iMRO and TM , IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.11, Issue 4, Page No pp.596-617, November 2024, Available at : http://www.ijrar.org/IJRAR24D3335.pdf
82. Dheeraj Yadav, Dasaiah Pakanati,, Integrating Multi-Node RAC Clusters for Improved Data Processing in Enterprises , IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.11, Issue 4, Page No pp.629-650, November 2024, Available at : http://www.ijrar.org/IJRAR24D3337.pdf
83. Rajesh Ojha, Shalu Jain, Integrating Digital Twin and Augmented Reality for Asset Inspection and Training , IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.11, Issue 4, Page No pp.618-628, November 2024, Available at : http://www.ijrar.org/IJRAR24D3336.pdf IJRAR's Publication Details
84. Prabhakaran Rajendran, Er. Siddharth. (2024). The Importance of Integrating WES with WMS in Modern Warehouse Systems. International Journal of Research Radicals in Multidisciplinary Fields, ISSN: 2960-043X, 3(2), 773–789. Retrieved from https://www.researchradicals.com/index.php/rr/article/view/155
85. Khushmeet Singh, UJJAWAL JAIN, Leveraging Snowflake for Real-Time Business Intelligence and Analytics , IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.11, Issue 4, Page No pp.669-682, November 2024, Available at : http://www.ijrar.org/IJRAR24D3339.pdf
86. Ramdass, K., & Jain, U. (2024). Application of static and dynamic security testing in financial sector. International Journal for Research in Management and Pharmacy, 13(10). Retrieved from http://www.ijrmp.org
87. Vardhansinh Yogendrasinnh Ravalji, Dr. Saurabh Solanki, NodeJS and Express in Sports Media Aggregation Platforms , IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.11, Issue 4, Page No pp.683-698, November 2024, Available at : http://www.ijrar.org/IJRAR24D3340.pdf
88. Vardhansinh Yogendrasinnh Ravalji , Lagan Goel User-Centric Design for Real Estate Web Applications Iconic Research And Engineering Journals Volume 8 Issue 5 2024 Page 1158-1174
89. Viswanadha Pratap Kondoju, Daksha Borada. (2024). Predictive Analytics in Loan Default Prediction Using Machine Learning. International Journal of Research Radicals in Multidisciplinary Fields, ISSN: 2960-043X, 3(2), 882–909. Retrieved from https://www.researchradicals.com/index.php/rr/article/view/162
90. Jampani, Sridhar, Aravind Ayyagari, Kodamasimham Krishna, Punit Goel, Akshun Chhapola, and Arpit Jain. (2020). Cross-platform Data Synchronization in SAP Projects. *International Journal of Research and Analytical Reviews (IJRAR)*, 7(2):875. Retrieved from www.ijrar.org.
91. Gudavalli, S., Ravi, V. K., Musunuri, A., Murthy, P., Goel, O., Jain, A., & Kumar, L. (2020). Cloud cost optimization techniques in data engineering. *International Journal of*

Research and Analytical Reviews, 7(2), April 2020. https://www.ijrar.org

92. Vamsee Krishna Ravi, Abhishek Tangudu, Ravi Kumar, Dr. Priya Pandey, Aravind Ayyagari, and Prof. (Dr) Punit Goel. (2021). Real-time Analytics in Cloud-based Data Solutions. *Iconic Research And Engineering Journals*, Volume 5 Issue 5, 288-305.
93. Das, Abhishek, Abhijeet Bajaj, Priyank Mohan, Punit Goel, Satendra Pal Singh, and Arpit Jain. (2023). “Scalable Solutions for Real-Time Machine Learning Inference in Multi-Tenant Platforms.” *International Journal of Computer Science and Engineering (IJCSE)*, 12(2):493–516.
94. Subramanian, Gokul, Ashvini Byri, Om Goel, Sivaprasad Nadukuru, Prof. (Dr.) Arpit Jain, and Niharika Singh. 2023. Leveraging Azure for Data Governance: Building Scalable Frameworks for Data Integrity. International Journal of Research in Modern Engineering and Emerging Technology (IJRMEET) 11(4):158. Retrieved (http://www.ijrmeet.org) .
95. Ayyagari, Yuktha, Akshun Chhapola, Sangeet Vashishtha, and Raghav Agarwal. (2023). Cross-Culturization of Classical Carnatic Vocal Music and Western High School Choir. *International Journal of Research in All Subjects in Multi Languages (IJRSML)*, 11(5), 80. RET Academy for International Journals of Multidisciplinary Research (RAIJMR). Retrieved from www.raijmr.com.
96. Ayyagari, Yuktha, Akshun Chhapola, Sangeet Vashishtha, and Raghav Agarwal. (2023). “Cross-Culturization of Classical Carnatic Vocal Music and Western High School Choir.” *International Journal of Research in all Subjects in Multi Languages (IJRSML)*, 11(5), 80. Retrieved from http://www.raijmr.com.
97. Shaheen, Nusrat, Sunny Jaiswal, Pronoy Chopra, Om Goel, Prof. (Dr.) Punit Goel, and Prof. (Dr.) Arpit Jain. 2023. Automating Critical HR Processes to Drive Business Efficiency in U.S. Corporations Using Oracle HCM Cloud. International Journal of Research in Modern Engineering and Emerging Technology (IJRMEET) 11(4):230. Retrieved (https://www.ijrmeet.org).
98. Jaiswal, Sunny, Nusrat Shaheen, Pranav Murthy, Om Goel, Arpit Jain, and Lalit Kumar. 2023. Securing U.S. Employment Data: Advanced Role Configuration and Security in Oracle Fusion HCM. International Journal of Research in Modern Engineering and Emerging Technology (IJRMEET) 11(4):264. Retrieved from http://www.ijrmeet.org.
99. Nadarajah, Nalini, Vanitha Sivasankaran Balasubramaniam, Umababu Chinta, Niharika Singh, Om Goel, and Akshun Chhapola. 2023. Utilizing Data Analytics for KPI Monitoring and Continuous Improvement in Global Operations. International Journal of Research in Modern Engineering and Emerging Technology (IJRMEET) 11(4):245. Retrieved (www.ijrmeet.org).
100. Mali, Akash Balaji, Arth Dave, Vanitha Sivasankaran Balasubramaniam, MSR Prasad, Sandeep Kumar, and Sangeet. 2023. Migrating to React Server Components (RSC) and Server Side Rendering (SSR): Achieving 90% Response Time Improvement. *International Journal of Research in Modern Engineering and Emerging Technology (IJRMEET)* 11(4):88.
101. Shaik, Afroz, Arth Dave, Vanitha Sivasankaran Balasubramaniam, Prof. (Dr) MSR Prasad, Prof. (Dr) Sandeep Kumar, and Prof. (Dr) Sangeet. 2023. Building Data Warehousing Solutions in Azure Synapse for Enhanced Business Insights. *International Journal of Research in Modern Engineering and Emerging Technology (IJRMEET)* 11(4):102.
102. Putta, Nagarjuna, Ashish Kumar, Archit Joshi, Om Goel, Lalit Kumar, and Arpit Jain. 2023. Cross-Functional Leadership in Global Software Development Projects: Case Study of Nielsen. *International Journal of Research in Modern Engineering and Emerging Technology (IJRMEET)* 11(4):123.
103. Subeh, P., Khan, S., & Shrivastav, A. (2023). User experience on deep vs. shallow website architectures: A survey-based approach for e-commerce platforms. *International Journal of Business and General Management (IJBGM)*, 12(1), 47–84. https://www.iaset.us/archives?jname=32_2&year=2023&submit=Search © IASET.· Shachi Ghanshyam Sayata, Priyank Mohan, Rahul Arulkumaran, Om Goel, Dr. Lalit Kumar, Prof. (Dr.) Arpit Jain. 2023. The Use of PowerBI and MATLAB for Financial Product Prototyping and Testing. *Iconic Research And Engineering Journals*, Volume 7, Issue 3, 2023, Page 635-664.
104. Dharmapuram, Suraj, Vanitha Sivasankaran Balasubramaniam, Phanindra Kumar, Niharika Singh, Punit Goel, and Om Goel. 2023. “Building Next-Generation Converged Indexers: Cross-Team Data Sharing for Cost Reduction.” *International Journal of Research in Modern Engineering and Emerging Technology* 11(4): 32. Retrieved December 13, 2024 (https://www.ijrmeet.org).
105. Subramani, Prakash, Rakesh Jena, Satish Vadlamani, Lalit Kumar, Punit Goel, and S. P. Singh. 2023. Developing Integration Strategies for SAP CPQ and BRIM in Complex Enterprise Landscapes. *International Journal of Research in Modern Engineering and Emerging Technology* 11(4):54. Retrieved (www.ijrmeet.org).
106. Banoth, Dinesh Nayak, Priyank Mohan, Rahul Arulkumaran, Om Goel, Lalit Kumar, and Arpit Jain. 2023. Implementing Row-Level Security in Power BI: A Case Study Using AD Groups and Azure Roles. *International Journal of Research in Modern Engineering and Emerging Technology* 11(4):71. Retrieved (https://www.ijrmeet.org).
107.
108. Rafa Abdul, Aravind Ayyagari, Krishna Kishor Tirupati, Prof. (Dr) Sandeep Kumar, Prof. (Dr) MSR Prasad, Prof. (Dr) Sangeet Vashishtha. 2023. Automating Change Management Processes for Improved Efficiency in PLM Systems. *Iconic Research And Engineering Journals* Volume 7, Issue 3, Pages 517-545.
109. Siddagoni, Mahaveer Bikshapathi, Sandhyarani Ganipaneni, Sivaprasad Nadukuru, Om Goel, Niharika Singh, Prof. (Dr.) Arpit Jain. 2023. Leveraging Agile and TDD Methodologies in Embedded Software Development. *Iconic Research And Engineering Journals* Volume 7, Issue 3, Pages 457-477.
110. Hrishikesh Rajesh Mane, Vanitha Sivasankaran Balasubramaniam, Ravi Kiran Pagidi, Dr. S P Singh, Prof. (Dr.) Sandeep Kumar, Shalu Jain. "Optimizing User and Developer Experiences with Nx Monorepo Structures." *Iconic Research And Engineering Journals* Volume 7 Issue 3:572-595.
111. Sanyasi Sarat Satya Sukumar Bisetty, Rakesh Jena, Rajas Paresh Kshirsagar, Om Goel, Prof. (Dr.) Arpit Jain, Prof. (Dr.) Punit Goel. "Developing Business Rule Engines for Customized ERP Workflows." *Iconic Research And Engineering Journals* Volume 7 Issue 3:596-619.
112. Arnab Kar, Vanitha Sivasankaran Balasubramaniam, Phanindra Kumar, Niharika Singh, Prof. (Dr.) Punit Goel, Om Goel. "Machine Learning Models for Cybersecurity: Techniques for Monitoring and Mitigating Threats." *Iconic Research And Engineering Journals* Volume 7 Issue 3:620-634.
113. Kyadasu, Rajkumar, Sandhyarani Ganipaneni, Sivaprasad Nadukuru, Om Goel, Niharika Singh, Prof. (Dr.) Arpit Jain. 2023. Leveraging Kubernetes for Scalable Data Processing and Automation in Cloud DevOps. *Iconic Research And Engineering Journals* Volume 7, Issue 3, Pages 546-571.
114. Antony Satya Vivek Vardhan Akisetty, Ashish Kumar, Murali Mohana Krishna Dandu, Prof. (Dr) Punit Goel, Prof. (Dr.) Arpit Jain; Er. Aman Shrivastav. 2023. “Automating ETL Workflows with CI/CD Pipelines for Machine Learning Applications.” *Iconic Research And Engineering Journals* Volume 7, Issue 3, Page 478-497.

115. Gaikwad, Akshay, Fnu Antara, Krishna Gangu, Raghav Agarwal, Shalu Jain, and Prof. Dr. Sangeet Vashishtha. "Innovative Approaches to Failure Root Cause Analysis Using AI-Based Techniques." International Journal of Progressive Research in Engineering Management and Science (IJPREMS) 3(12):561–592. doi: 10.58257/IJPREMS32377.
116. Gaikwad, Akshay, Srikanthudu Avancha, Vijay Bhasker Reddy Bhimanapati, Om Goel, Niharika Singh, and Raghav Agarwal. "Predictive Maintenance Strategies for Prolonging Lifespan of Electromechanical Components." International Journal of Computer Science and Engineering (IJCSE) 12(2):323–372. ISSN (P): 2278–9960; ISSN (E): 2278–9979. © IASET.
117. Gaikwad, Akshay, Rohan Viswanatha Prasad, Arth Dave, Rahul Arulkumaran, Om Goel, Dr. Lalit Kumar, and Prof. Dr. Arpit Jain. "Integrating Secure Authentication Across Distributed Systems." Iconic Research And Engineering Journals Volume 7 Issue 3 2023 Page 498-516.
118. Dharuman, Narrain Prithvi, Aravind Sundeep Musunuri, Viharika Bhimanapati, S. P. Singh, Om Goel, and Shalu Jain. "The Role of Virtual Platforms in Early Firmware Development." International Journal of Computer Science and Engineering (IJCSE) 12(2):295–322. https://doi.org/ISSN2278–9960.