OPTIMIZED SECURE CLOUD STORAGE USING ATTRIBUTE-BASED KEYWORD SEARCH

[1]Yoheswari S
[1] Department of Computer Science & Engineering, K.L.N College of Engineering, Pottapalayam – 630612, Tamilnadu, India
[1]yoheswari1988@gmail.com

Abstract: In the modern digital era, cloud storage has become an indispensable service due to its scalability, accessibility, and cost-effectiveness. However, with the vast amount of sensitive information stored on cloud platforms, ensuring data security and privacy remains a critical challenge. Traditional encryption techniques, while secure, often hinder efficient data retrieval, especially when using keyword searches. To address this, attribute-based keyword search (ABKS) offers a promising solution by allowing secure, fine-grained access control and efficient keyword searches over encrypted data. This paper delves into the integration of optimization techniques within ABKS to enhance search efficiency and data security in cloud storage environments. We explore various optimization strategies, such as index compression, query processing enhancement, and encryption optimization, which aim to reduce computational overhead while maintaining robust security measures. Through a comprehensive analysis, the paper illustrates how these techniques can significantly improve the performance of cloud storage systems, ensuring both security and usability. Experimental results demonstrate that optimized ABKS not only accelerates search queries but also reduces storage costs, making it a viable solution for modern cloud storage challenges. Future research directions include exploring advanced machine learning algorithms for predictive search optimizations and further improving the resilience of ABKS against emerging security threats.

Key words: Attribute-Based Keyword Search (ABKS), Secure Cloud Storage, Data Encryption, Access Control, Search Optimization

Corresponding Author: Yoheswari S
K.L.N. College of Engineering, Pottapalayam, Tamil Nadu, India
Mail: yoheswari1988@gmail.com

Introduction:

Cloud computing has revolutionized the way organizations and individuals manage and store their data, offering unparalleled advantages in terms of scalability, flexibility, and cost-effectiveness. However, the rapid adoption of cloud storage services has also led to increasing concerns about data security and privacy. As sensitive information is outsourced to third-party cloud providers, the need to ensure that this data is protected from unauthorized access

becomes paramount. Traditional encryption methods, while effective at securing data, present significant challenges in terms of data retrieval. Specifically, conducting efficient searches over encrypted data without compromising security remains a complex problem.

Attribute-Based Keyword Search (ABKS) has emerged as a promising solution to this challenge. ABKS allows users to search over encrypted data using keywords, while also enabling fine-grained access control based on user attributes. This ensures that only authorized users can perform searches and retrieve relevant data, thereby safeguarding the privacy of the data stored in the cloud. However, the practical implementation of ABKS is not without its challenges. One of the key issues is the computational overhead associated with the encryption and decryption processes, which can significantly slow down search queries, especially in large-scale cloud environments.

To address these challenges, optimization techniques can be employed to enhance the performance and efficiency of ABKS. These techniques aim to reduce the computational burden, improve query processing times, and minimize storage requirements, all while maintaining robust security protocols. For instance, index compression techniques can be used to reduce the size of the encrypted index, thereby speeding up the search process. Similarly, query processing enhancements, such as parallel processing and caching strategies, can significantly reduce the time required to execute search queries.

In addition to these technical optimizations, the integration of machine learning algorithms offers a novel approach to further enhance the efficiency of ABKS. By predicting user search behavior and optimizing search queries accordingly, machine learning can help reduce the computational load and improve the overall user experience. Moreover, advances in encryption techniques, such as homomorphic encryption and lightweight cryptography, provide additional avenues for optimizing ABKS in cloud storage environments.

Despite these advancements, several challenges remain. The balance between security and efficiency is a delicate one, and optimizing ABKS requires careful consideration of various trade-offs. Furthermore, the dynamic nature of cloud environments, with their varying workloads and user demands, adds an additional layer of complexity to the optimization process. As such, ongoing research is essential to develop more effective optimization techniques that can address these challenges and ensure the secure and efficient storage of data in the cloud.

This paper seeks to explore the various optimization techniques that can be applied to ABKS, with the aim of improving its performance and usability in cloud storage environments. By providing a comprehensive analysis of these techniques, we aim to contribute to the ongoing efforts to secure cloud storage systems while also enhancing their efficiency. In doing so, we hope to pave the way for more robust and scalable solutions that can meet the evolving needs of users and organizations in the digital age.

Data Encryption and Index Creation:

The first step in the secure cloud storage process involves the encryption of data before it is uploaded to the cloud. Encryption is a critical component that ensures that data remains confidential, even if unauthorized access occurs. Advanced encryption techniques, such as homomorphic encryption or symmetric key encryption, are typically employed to safeguard the data. Once the data is encrypted, an encrypted index is generated based on the keywords associated with the data. This index serves as a map, linking encrypted data to the keywords, thus facilitating efficient keyword searches. The creation of this index is vital for enabling users to search over encrypted data without decrypting the entire dataset, thereby preserving both security and efficiency. The encrypted index must be designed carefully to ensure that it does not reveal any sensitive information about the data it references. Techniques like searchable encryption or order-preserving encryption may be utilized to strike a balance between search efficiency and data security. The index is stored alongside the encrypted data in the cloud, ready to be queried by authorized users. This phase of the workflow lays the groundwork for the secure storage and retrieval of data, establishing a foundation that integrates encryption with searching.

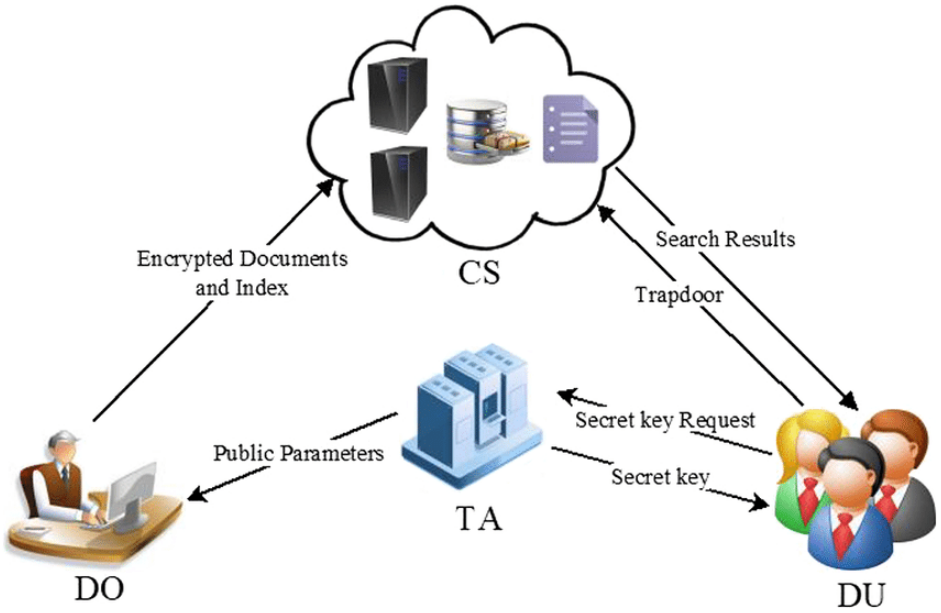

Fig.1. Architecture of attribute-based searchable encryption:

Attribute-Based Access Control:

Once the data is encrypted and the index is created, the next step is to establish access control mechanisms that regulate who can search and retrieve the data. Attribute-based access control (ABAC) is implemented to ensure that only authorized users can perform searches on the encrypted data. Unlike traditional access control models that rely on fixed roles, ABAC offers a more flexible approach by granting permissions based on user attributes. These attributes could include user roles, organizational hierarchy, security clearance levels, or specific project assignments. For instance, a user might only be allowed to search for data if they have a particular job title or are working on a specific project. This ensures that access is tailored to individual users, reducing the risk of unauthorized data exposure. The attributes are evaluated against the access control policies defined by the data owner. If the user's attributes meet the required criteria, they are granted permission to perform keyword searches on the encrypted data. This method enhances data security by providing fine-grained access control and ensuring that only those with legitimate reasons can access sensitive information. Additionally, the attribute-based model is scalable and adaptable, making it suitable for dynamic cloud environments where user roles and permissions frequently change.

Optimization Techniques:

Optimizing the efficiency of the attribute-based keyword search (ABKS) system is crucial for ensuring that it operates effectively in real-world cloud environments. The first optimization technique involves index compression, which reduces the size of the encrypted index. A smaller index requires less storage space and can be searched more quickly, thus speeding up the entire search process. Index compression can be achieved through techniques like prefix encoding, dictionary-based compression, or advanced algorithms like Huffman coding. By reducing the storage overhead, index compression not only improves search performance but also lowers the cost of cloud storage. In parallel, query processing enhancements are introduced to accelerate search operations. Techniques such as parallel processing, where multiple queries are executed simultaneously, and caching strategies, where frequently searched terms are stored for quick retrieval, are employed to minimize query response times. Additionally, machine learning algorithms are integrated into the ABKS framework to predict user search patterns. By analyzing previous search behavior, these algorithms can optimize query execution, prefetch relevant data, and prioritize resources for high-probability searches. This predictive approach reduces computational load and improves user experience by delivering faster search results. Together, these optimization techniques transform the ABKS system into a more efficient and cost-effective solution, capable of handling large-scale data searches without compromising security.

Search and Retrieval Process:

The final step in the workflow involves the actual search and retrieval process, where authorized users interact with the ABKS system to retrieve encrypted data. Users submit their keyword queries, which are processed by the ABKS framework using the optimized techniques discussed earlier. The system first verifies the user's attributes to ensure they are authorized to perform the search. If the user passes the access control check, the system proceeds to search the encrypted index for matches to the keyword query. Thanks to the optimizations in index compression and query processing, this search is conducted efficiently, even for large datasets. Once the relevant encrypted data is identified, it is retrieved from the cloud and provided to the user. At this point, the user decrypts the data locally, using their decryption keys. This ensures that the data remains encrypted throughout the search and retrieval process, minimizing the risk of unauthorized access during transmission. The entire process is designed to be seamless, secure, and efficient, allowing users to quickly find and retrieve the information they need without compromising the security of the stored data. The combination of encryption, access control, and optimization ensures that the search and retrieval process meets the high demands of modern cloud storage systems, providing a robust solution for secure data management.

Conclusions:

This paper has demonstrated the potential of optimization techniques in enhancing the performance of attribute-based keyword search systems in secure cloud storage environments. By integrating these optimizations, such as index compression, query processing improvements, and machine learning-based predictive algorithms, we can achieve significant improvements in both search efficiency and data security. However, the ongoing evolution of cloud technologies presents new challenges and opportunities. Future research should focus on further refining these techniques and exploring new approaches, such as quantum-resistant encryption algorithms and more sophisticated machine learning models, to ensure that ABKS remains a viable solution in the face of emerging security threats.

Reference:

1. Ramesh, G., Gorantla, V. A. K., & Gude, V. (2023). A hybrid methodology with learning based approach for protecting systems from DDoS attacks. *Journal of Discrete Mathematical Sciences and Cryptography*, *26*(5), 1317-1325.
2. Logeshwaran, J., Gorantla, V. A. K., Gude, V., & Gorantla, B. (2023, September). The Smart Performance Analysis of Cyber Security Issues in Crypto Currency Using Blockchain. In *2023 6th International Conference on Contemporary Computing and Informatics (IC3I)* (Vol. 6, pp. 2235-2241). IEEE.
3. Komatireddy, S. R., Meghana, K., Gude, V., & Ramesh, G. (2023, December). Facial Shape Analysis and Accessory Recommendation: A Human-Centric AI Approach. In *2023 3rd*

International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) (pp. 182-191). IEEE.

4. Sriramulugari, S. K., Gorantla, V. A. K., Gude, V., Gupta, K., & Yuvaraj, N. (2024, March). Exploring mobility and scalability of cloud computing servers using logical regression framework. In *2024 2nd International Conference on Disruptive Technologies (ICDT)* (pp. 488-493). IEEE.
5. Gorantla, V. A. K., Gude, V., Sriramulugari, S. K., Yuvaraj, N., & Yadav, P. (2024, March). Utilizing hybrid cloud strategies to enhance data storage and security in e-commerce applications. In *2024 2nd International Conference on Disruptive Technologies (ICDT)* (pp. 494-499). IEEE.
6. Bharathi, G. P., Chandra, I., Sanagana, D. P. R., Tummalachervu, C. K., Rao, V. S., & Neelima, S. (2024). AI-driven adaptive learning for enhancing business intelligence simulation games. *Entertainment Computing*, *50*, 100699.
7. Rao, S. D. P. (2024). HARNESSING AI FOR EVOLVING THREATS: FROM DETECTION TO AUTOMATED RESPONSE.
8. Rao, S. D. P. (2022). PREVENTING INSIDER THREATS IN CLOUD ENVIRONMENTS: ANOMALY DETECTION AND BEHAVIORAL ANALYSIS APPROACHES.
9. Rao, S. D. P. (2022). THE SYNERGY OF CYBERSECURITY AND NETWORK ARCHITECTURE: A HOLISTIC APPROACH TO RESILIENCE.
10. Rao, S. D. P. (2022). MITIGATING NETWORK THREATS: INTEGRATING THREAT MODELING IN NEXT-GENERATION FIREWALL ARCHITECTURE.
11. Rao, S. D. P. (2023). RANSOMWARE DEFENSE IN THE CLOUD ENVIRONMENTS: ADAPTIVE STRATEGIES FOR EVOLVING THREATS.
12. Sanagana, D. P. R., & Tummalachervu, C. K. (2024, May). Securing Cloud Computing Environment via Optimal Deep Learning-based Intrusion Detection Systems. In *2024 Second International Conference on Data Science and Information System (ICDSIS)* (pp. 1-6). IEEE.
13. Kanth, T. C. (2023). EXPLORING SERVER-LESS COMPUTING FOR EFFICIENT RESOURCE MANAGEMENT IN CLOUD ARCHITECTURES.
14. Kanth, T. C. (2023). SECURING DATA PRIVACY IN CLOUD NETWORK SYSTEMS: A COMPARATIVE STUDY OF ENCRYPTION TECHNIQUES.
15. Kanth, T. C. (2023). EFFICIENT STRATEGIES FOR SEAMLESS CLOUD MIGRATIONS USING ADVANCED DEPLOYMENT AUTOMATIONS.
16. Kanth, T. C. (2023). CONTEMPORARY DEVOPS STRATEGIES FOR AUGMENTING SCALABLE AND RESILIENT APPLICATION DEPLOYMENT ACROSS MULTI-CLOUD ENVIRONMENTS.
17. Thangapalani, L., Dharini, R., & Keerthana, R. (2023, May). Securing Medical Image Transmission using Memetic Algorithm. In *2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)* (pp. 1-8). IEEE.

18. Vennila, D., Vinotha, C., Shanthakumari, A., & Thangapalani, L. Convex Optimization Algorithm for Product Recommendation Using Microblogging Information. *Journal of Data Mining and Management*, *2*(1).
19. Lawan, L. A., & Roy, S. K. Assessing the Predictive Capability of the Theory of Planned Behavior in the Nigerian Context: A Study of Intention to Founding New Business. In *Constructive Discontent in Execution* (pp. 231-248). Apple Academic Press.
20. Ibrahim, M., & Roy, S. K. (2023). Advancement of Nonlife Insurance in Both Public and Private Sectors in Bangladesh. In *Constructive Discontent in Execution* (pp. 209-230). Apple Academic Press.
21. Jain, M. B., & Roy, S. K. (2022). Student Motivation in Online Learning. *International Journal of Early Childhood*, (01), 4339-4346.
22. Jain, B., & Roy, S. K. (2022). Exploring the Pros and Cons of Promoting Interaction in Online Learning. *NeuroQuantology*, *20*(5), 5401.
23. Ibrahim, M., & Roy, S. K. (2022). Assessment of Profitability Achievement of Stateowned Non-life Insurance in Bangladesh. *NeuroQuantology*, *20*(6), 2883.
24. Roy, S. K. (2014). Factors Affecting (CRM) Practices in Commercial Banks a Case of Select Banks in India. *International journal of current research*, *6*(11), 10344-10351.
25. Gupta, R. C., & Roy, S. K. (1970). Studies on the pollen grains of Urena lobata Linn. *Cur Sci*.
26. Alikhan, J. S., Alageswaran, R., & Amali, S. M. J. (2023). Self-attention convolutional neural network optimized with season optimization algorithm Espoused Chronic Kidney Diseases Diagnosis in Big Data System. *Biomedical Signal Processing and Control*, *85*, 105011.
27. Alikhan, J. S., Alageswaran, R., & Amali, S. M. J. (2023). Dingo optimization based network bandwidth selection to reduce processing time during data upload and access from cloud by user. *Telecommunication Systems*, *83*(2), 189-208.
28. Rokade, U. S., Doye, D., & Kokare, M. (2009, March). Hand gesture recognition using object based key frame selection. In *2009 International Conference on Digital Image Processing* (pp. 288-291). IEEE.
29. Kshirsagar, K. P. (2015). Key Frame Selection for One-Two Hand Gesture Recognition with HMM. *International Journal of Advanced Computer Research*, *5*(19), 192.
30. Kumbhar, K., & Kshirasagar, K. P. (2015). Comparative study of CCD & CMOS sensors for image processing. *International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering*, *3*, 194-196.
31. Kshirsagar, K. P., & Doye, D. (2010, October). Object Based Key Frame Selection for Hand Gesture Recognition. In *2010 International Conference on Advances in Recent Technologies in Communication and Computing* (pp. 181-185). IEEE.

32. Ingle, A., Gour, A., & Kshirsagar, K. (2017). DDoS attack detection algorithms based on pattern classification and machine learning. *J Univ Shanghai Sci Technol. ISSN*, 1007-6735.
33. Kshirsagar, K. P., & Shinde, R. A. (2017, October). Comparing techniques of segmenting hand region. In *2017 2nd International Conference on Communication and Electronics Systems (ICCES)* (pp. 721-724). IEEE.
34. Rokade, R., Kshirsagar, K., Sonawane, J., & Munde, S. (2019). Analysis of Human-Machine Interaction Through Facial Expression and Hand-Gesture Recognition. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, *8*(9S3).
35. Kshirsagar, K. P., Rokade, R., & Kamble, D. (2019). IoT based gesture recognition for smart controlling. *International Journal of Recent Technology and Engineering (IJRTE)*, *8*(4).
36. Kshirsagar, K. P., & Doye, D. D. (2015). Comparing key frame selection for one-two hand gesture recognition using different methods. *International Journal of Signal and Imaging Systems Engineering*, *8*(5), 273-285.
37. Kshirsagar, K. P., Sahu, R. M., Bankar, S. M., Moje, R. K., & Doye, D. D. (2013). K one hand gesture recognition. *Int. J. Innov. Res. Electr. Electron. Instrum. Control Eng*, *1*(7), 330-334.
38. Gujarkar, P., Lonkar, S., Jain, T., Nigal, S., Patil, P., Deshpande, P., ... & Ratnaparkhi, A. (2023, March). IoT based Smart Attendance System. In *2023 International Conference on Emerging Smart Computing and Informatics (ESCI)* (pp. 1-6). IEEE.
39. Chishty, S., Langare, A., Sawant, S., & Kshirsagar, K. Industrial Data Acquisition. *International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)*, *11*(12), 14590-14594.
40. Raikwar, A. R., Sadawarte, R. R., More, R. G., Gunjal, R. S., Mahalle, P. N., & Railkar, P. N. (2018). Long-Term and Short-Term Traffic Forecasting Using Holt-Winters Method.
41. Kshirsagar, K. P. (2015). Segmentation Of One And Two Hand Gesture Recognition Using Key Frame Selection. *Segmentation of One and Two Hand Gesture Recognition using Key Frame Selection*.
42. Mukati, N., Namdev, N., Dilip, R., Hemalatha, N., Dhiman, V., & Sahu, B. (2023). Healthcare assistance to COVID-19 patient using internet of things (IoT) enabled technologies. *Materials today: proceedings*, *80*, 3777-3781.
43. Bansal, B., Jenipher, V. N., Jain, R., Dilip, R., Kumbhkar, M., Pramanik, S., ... & Gupta, A. (2022). Big data architecture for network security. *Cyber Security and Network Security*, 233-267.
44. Shrivastava, A., Nayak, C. K., Dilip, R., Samal, S. R., Rout, S., & Ashfaque, S. M. (2023). Automatic robotic system design and development for vertical hydroponic farming using IoT and big data analysis. *Materials Today: Proceedings*, *80*, 3546-3553.

45. Pandey, J. K., Jain, R., Dilip, R., Kumbhkar, M., Jaiswal, S., Pandey, B. K., ... & Pandey, D. (2022). Investigating role of iot in the development of smart application for security enhancement. In *IoT Based Smart Applications* (pp. 219-243). Cham: Springer International Publishing.
46. Gupta, N., Janani, S., Dilip, R., Hosur, R., Chaturvedi, A., & Gupta, A. (2022). Wearable sensors for evaluation over smart home using sequential minimization optimization-based random forest. *International Journal of Communication Networks and Information Security*, *14*(2), 179-188.
47. Gite, P., Shrivastava, A., Krishna, K. M., Kusumadevi, G. H., Dilip, R., & Potdar, R. M. (2023). Under water motion tracking and monitoring using wireless sensor network and Machine learning. *Materials Today: Proceedings*, *80*, 3511-3516.
48. Dilip, R., & Bhagirathi, V. (2013). Image processing techniques for coin classification using LabVIEW. *OJAI 2013*, *1*(1), 13-17.
49. Krishna, K. M., Borole, Y. D., Rout, S., Negi, P., Deivakani, M., & Dilip, R. (2021, September). Inclusion of cloud, blockchain and iot based technologies in agriculture sector. In *2021 9th international conference on cyber and IT service management (CITSM)* (pp. 1-8). IEEE.
50. Dilip, R. (2019). DESIGN AND DEVELOPMENT OF INTELLIGENT SYSTEM FOR HUMAN BODY DESIGN AND DEVELOPMENT OF INTELLIGENT SYSTEM FOR HUMAN BODY. *no. July*, 0-3.
51. Veeraiah, V., Thejaswini, K. O., Dilip, R., Jain, S. K., Sahu, A., Pramanik, S., & Gupta, A. (2024). The Suggested Use of Big Data in Medical Analytics by Fortis Healthcare Hospital. In *Adoption and Use of Technology Tools and Services by Economically Disadvantaged Communities: Implications for Growth and Sustainability* (pp. 275-289). IGI Global.
52. Dilip, R., Milan, R. K., Vajrangi, A., Chavadi, K. S., & Puneeth, A. S. (2021, November). Jumping robot: a pneumatic jumping locomotion across rough terrain. In *Journal of Physics: Conference Series* (Vol. 2115, No. 1, p. 012008). IOP Publishing.
53. Dilip, R., Borole, Y. D., Sumalatha, S., & Nethravathi, H. M. (2021, September). Speech based biomedical devices monitoring using LabVIEW. In *2021 9th International Conference on Cyber and IT Service Management (CITSM)* (pp. 1-7). IEEE.
54. Rekha, C. M., Shivakumar, K. S., & Dilip, R. (2020, October). Comparison of spacefactor, capacitance value and impregnated temperature in mpp oil impregnated polypropylene film AC capacitors. In *2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)* (pp. 544-547). IEEE.
55. Dilip, R., & Bhagirathi, V. (2013). LAN Based Industrial Automation with GSM Connectivity. ICSEM-2013 Conference Proceedings.
56. Janani, S., Dilip, R., Talukdar, S. B., Talukdar, V. B., Mishra, K. N., & Dhabliya, D. (2023). IoT and Machine Learning in Smart City Healthcare Systems. In *Handbook of Research on Data-Driven Mathematical Modeling in Smart Cities* (pp. 262-279). IGI Global.

57. Dilip, R., Solabagoudar, M. P., Chapi, N., & Vaidya, P. B. (2023). A Review of Surveillance and Fire Fighter Drone. *International Journal of Unmanned Systems Engineering*, *5*(2), 123-145.
58. Janani, S., Dilip, R., Talukdar, S. B., Talukdar, V. B., Mishra, K. N., & Dhabliya, D. (2023). IoT and Machine Learning in Smart City Healthcare Systems. In *Handbook of Research on Data-Driven Mathematical Modeling in Smart Cities* (pp. 262-279). IGI Global.
59. Dilip, R., & Ramesh, K. B. (2020). Development of Graphical System for Patient Monitoring using Cloud Computing.
60. Mathuravalli, S. M. D., Narayanansamy Rajendran, D. K. B., Dilip, R., Ranjan, A., Das, I., & Chauhan, A. (2023). Deep Learning Techniques For Exoticism Mining From Visual Content Based Image Retrieval. *Journal of Pharmaceutical Negative Results*, 925-933.
61. Dilip, R., Samanvita, N., Pramodhini, R., Vidhya, S. G., & Telkar, B. S. (2022, February). Performance Analysis of Machine Learning Algorithms in Intrusion Detection and Classification. In *International Conference on Emerging Technologies in Computer Engineering* (pp. 283-289). Cham: Springer International Publishing.
62. Begum, M. B., & Venkataramani, Y. (2012). LSB based audio steganography based on text compression. *Procedia Engineering*, *30*, 703-710.
63. Begum, M. B., Deepa, N., Uddin, M., Kaluri, R., Abdelhaq, M., & Alsaqour, R. (2023). An efficient and secure compression technique for data protection using burrows-wheeler transform algorithm. *Heliyon*, *9*(6).
64. Manikandan, A., Madhu, G. C., Flora, G. D., Parvez, M. M., & Begum, M. B. (2023). Hybrid Advisory Weight based dynamic scheduling framework to ensure effective communication using acknowledgement during Encounter strategy in Ad-hoc network. *International Journal of Information Technology*, *15*(8), 4521-4527.
65. Althaf, M. M., & Begum, M. B. (2012, April). Handwritten characters pattern recognition using neural networks. In *International Conference on Computing and Control Engineering* (Vol. 4, No. 7).
66. Begum, M. B., & Venkataramani, Y. (2011). An efficient text compression for massive volume of data. *International Journal of Computer Applications*, *975*, 8887.
67. Abirami, C., & Begum, M. (2016). Biometric cryptosystem based on Delaunay quadrangle structure for fingerprint template protection and person identification. *Middle-East Journal of Scientific Research*, *24*(S2), 53-57.
68. Begum, M. B., & Venkataramani, Y. (2013). A new compression scheme for secure transmission. *International Journal of Automation and Computing*, *10*, 578-586.
69. Begum, M. B., Sivakannu, G., Eindhumathy, J., Priya, J. S., Mahendran, M., & Kumar, R. R. (2023, August). Enhancing Agricultural Productivity with Data-Driven Crop Recommendations. In *2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)* (pp. 1055-1063). IEEE.

70. Begum, M., Aziz, F. B., Islam, R., Hasan, M. M., Parvez, M. M., & Sarkar, S. (2018). Anti-diabetogenic impact of bitter melon (Momordica charantia) and mahogany (Swietenia macrophylla) on alloxan induced diabetic rabbit model. *Asian-Australasian Journal of Bioscience and Biotechnology*, *3*(2), 136-142.
71. Swathi, T., & Begum, M. B. Maximum Connected Load Balancing Cover Tree Algorithm for Wireless Sensor Network. *Journal of Switching Hub*, *3*(3).
72. Begum, M. B., & Venkataramani, Y. (2012). A Novel Multidictionary Based Text Compression. *Journal of Computer Science*, *8*(12), 1940.
73. Kumar, V. S., Thansekhar, M. R., Saravanan, R., & Amali, S. M. J. (2014). Solving multi-objective vehicle routing problem with time windows by FAGA. *Procedia Engineering*, *97*, 2176-2185.
74. Selvan, M. A., & Amali, S. M. J. (2024). RAINFALL DETECTION USING DEEP LEARNING TECHNIQUE.
75. Sudha, S., Baskar, S., Amali, S. M. J., & Krishnaswamy, S. (2015). Protein structure prediction using diversity controlled self-adaptive differential evolution with local search. *Soft Computing*, *19*, 1635-1646.
76. Kadhar, K. M. A., Baskar, S., & Amali, S. M. J. (2015). Diversity Controlled Self Adaptive Differential Evolution based design of non-fragile multivariable PI controller. *Engineering Applications of Artificial Intelligence*, *46*, 209-222.
77. Sivaramkumar, V., Thansekhar, M. R., Saravanan, R., & Miruna Joe Amali, S. (2018). Demonstrating the importance of using total time balance instead of route balance on a multi-objective vehicle routing problem with time windows. *The International Journal of Advanced Manufacturing Technology*, *98*, 1287-1306.
78. Brindha, S. (2021). A robust and adaptive fuzzy logic based differential evolution algorithm using population diversity tuning for multi-objective optimization. *Engineering Applications of Artificial Intelligence*, *102*, 104240.
79. Sivaramkumar, V., Thansekhar, M. R., Saravanan, R., & Miruna Joe Amali, S. (2017). Multi-objective vehicle routing problem with time windows: Improving customer satisfaction by considering gap time. *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture*, *231*(7), 1248-1263.
80. Zhang, J., Chen, C., Xiang, Y., Zhou, W., & Xiang, Y. (2012). Internet traffic classification by aggregating correlated naive bayes predictions. *IEEE transactions on information forensics and security*, *8*(1), 5-15.
81. Kirubahari, R., & Amali, S. M. J. (2024). An improved restricted Boltzmann machine using Bayesian optimization for recommender systems. *Evolving Systems*, *15*(3), 1099-1111.
82. Jemimah, J. P. P., & Miruna Joe Amali, S. (2024). An efficient PCCM masking scheme for PAPR reduction and encryption in OFDM-VLC system. *Telecommunication Systems*, 1-31.
83. Rekha, K. S., Amali, M. J., Swathy, M., Raghini, M., & Darshini, B. P. (2023). A steganography embedding method based on CDF-DWT technique for data hiding

application using Elgamal algorithm. *Biomedical Signal Processing and Control*, *80*, 104212.

84. Sashi Rekha, K., & Miruna Joe Amali, S. A. (2022). Efficient feature subset selection and classification using levy flight-based cuckoo search optimization with parallel support vector machine for the breast cancer data. *International Journal of Imaging Systems and Technology*, *32*(3), 869-881.
85. Kiran, A., Kalpana, V., Madanan, M., Ramesh, J. V. N., Alfurhood, B. S., & Mubeen, S. (2023). Anticipating network failures and congestion in optical networks a data analytics approach using genetic algorithm optimization. *Optical and Quantum Electronics*, *55*(13), 1193.
86. Lalithambigai, M., Kalpana, V., Kumar, A. S., Uthayakumar, J., Santhosh, J., & Mahaveerakannan, R. (2023, February). Dimensionality reduction with DLMNN technique for handling secure medical data in healthcare-IoT model. In *2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS)* (pp. 111-117). IEEE.
87. Kalpana, V., Mishra, D. K., Chanthirasekaran, K., Haldorai, A., Nath, S. S., & Saraswat, B. K. (2022). On reducing energy cost consumption in heterogeneous cellular networks using optimal time constraint algorithm. *Optik*, *270*, 170008.
88. Kalpana, V., & Karthik, S. (2020). Route availability with QoE and QoS metrics for data analysis of video stream over a mobile ad hoc networks. *Wireless Personal Communications*, *114*(3), 2591-2612.
89. Kalpana, V., & Karthik, S. (2018, February). Bandwidth Constrained Priority Based Routing Algorithm for Improving the Quality of Service in Mobile Ad hoc Networks. In *2018 International Conference on Soft-computing and Network Security (ICSNS)* (pp. 1-8). IEEE.