International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802474

Privacy-Enhanced File Hosting With Multi-Factor Authentication and QR-Code-Based Access Tracking

Mr. E. Rajamanickam[1], Ms Swetha v[2]

Assistant Professor, Dept. of Master of Computer Applications, Er.Perumal Manimekalai College of Engineering, Hosur, Tamil Nadu, India[1]

(II-MCA), Dept. of Master of Computer Applications, Er.Perumal Manimekalai College of Engineering, Hosur, Tamil Nadu, India[2]

Publication History: Received: 25.02.2026; Revised: 20.03.2026; Accepted: 25.03. 2026; Published: 28.03.2026.

ABSTRACT: File sharing is essential for digital communication, but existing methods face security risks like unauthorized access and data breaches. Traditional systems often lack strong authentication and encryption, making them vulnerable to attacks. This project enhances file security by integrating secure authentication, encryption, and QR code-based access control. Users authenticate with Two-Factor Authentication (2FA) before uploading files, which are encrypted and linked to a QR code. The recipient scans the QR code to retrieve the file, with decryption keys securely shared via email. Expiry time and scan limits further enhance security, ensuring a reliable and protected file-sharing system.

KEYWORDS: Privacy-Enhanced File Hosting, Multi-Factor Authentication (MFA), QR-Code-Based Access Tracking , Secure File Sharing, Data Security, Cloud Storage Security, User Authentication, Access Control, Encryption, Cybersecurity

I. INTRODUCTION

File sharing plays a crucial role in digital communication, enabling seamless data exchange. Traditional methods face security threats like unauthorized access, data interception, and weak encryption. Lack of strong authentication mechanisms increases the risk of breaches and cyber attacks. Secure file sharing requires encryption, authentication, and controlled access mechanisms. This project enhances security using encryption, Two-Factor Authentication (2FA), and QR code-based access control

1.1 Need for Privacy-Enhanced File Hosting System

- Increasing use of cloud storage services
- Risk of unauthorized file access
- Need for secure file sharing
- Protection of confidential information
- Requirement for strong user authentication

1.2 Challenges in Existing Systems

- Weak password-based authentication
- Lack of privacy protection
- Vulnerability to cyberattacks
- Unauthorized file downloads
- Poor access monitoring mechanisms

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802474

II. RELATED WORK

Several existing file hosting systems provide cloud storage and sharing functionalities. Traditional systems mainly depend on password-based authentication methods, which are vulnerable to hacking and phishing attacks. Some cloud storage platforms implement encryption techniques, but they may still lack proper authentication and access tracking features.

Recent research works focus on secure authentication mechanisms such as OTP verification, biometric authentication, and encryption-based cloud storage systems. Multi-Factor Authentication has become an effective approach for improving account security and preventing unauthorized access.
However, many existing systems still face limitations such as:

- Lack of complete privacy protection
- Weak access control mechanisms
- Limited authentication security
- Inadequate user activity tracking

The proposed system overcomes these limitations by integrating secure authentication, encrypted storage, and user access monitoring.

III. METHODOLOGY

3.1 User Registration

- Users create accounts using username, email, and password
- Passwords are securely stored using encryption techniques
- Email verification is performed during registration
- User information is maintained in a secure database

3.2 Multi-Factor Authentication

- Users enter login credentials
- OTP is generated and sent to registered email/mobile
- User must verify OTP successfully
- Authentication is completed only after all verification steps
- Enhances account security and prevents unauthorized access

3.3 Secure File Upload

- Authenticated users can upload files securely
- Files are encrypted before storage
- File metadata is stored in the database
- Supports secure cloud-based file management

3.4 Secure File Access and Download

- Only authorized users can access files
- Access permissions are verified before download
- Files are decrypted only for authenticated users
- Prevents unauthorized file sharing and leakage

3.5 Access Tracking and Monitoring

- Records user login and file access activities
- Maintains logs for uploads and downloads
- Helps identify suspicious activities
- Improves accountability and system monitoring

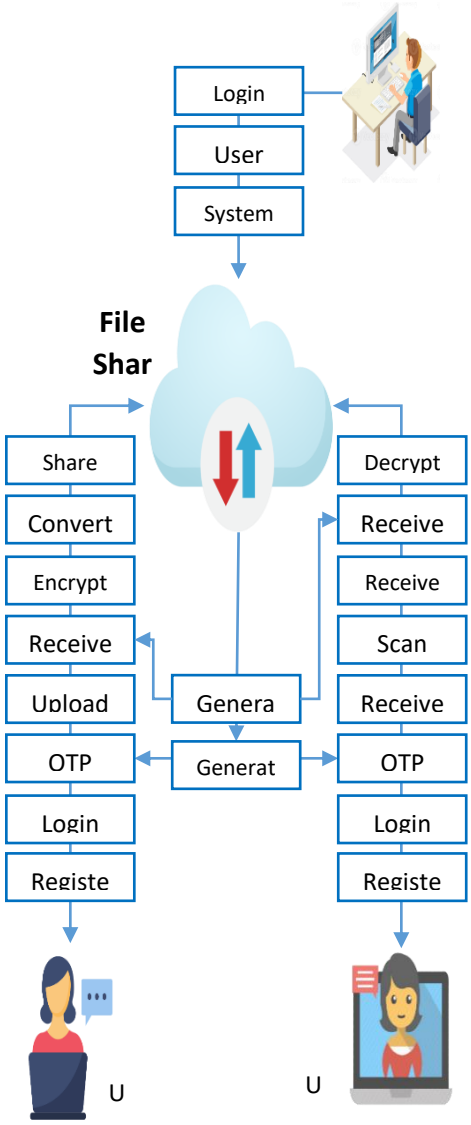
International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802474

IV. SYSTEM ARCHITECTURE



V. SYSTEM MODULES

5.1 End User

This module defines two types of users: Admin and User.

Admin

Responsible for managing user accounts, monitoring file-sharing activities, enforcing security policies, and maintaining access logs. The admin ensures compliance with security protocols and manages expired or inactive QR codes.

User

Uploads and shares encrypted files through the system. The recipient must authenticate to scan the QR code and decrypt the file, ensuring a secure and restricted access mechanism.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802474

5.2 Authentication

To prevent unauthorized access, users must log in using Two-Factor Authentication (2FA), which consists of:

- **Username & Password:** Used for primary authentication.
- **OTP Verification:** A one-time password (OTP) is sent to the user's registered email or mobile number, ensuring an additional security layer before
- file access or QR code generation.

5.3 Key Generation

A unique AES encryption key is generated for each file upon upload.
This key is necessary for decryption and is securely managed within the system, preventing unauthorized access or interception during transmission.

5.4 File Encryption

Before storage, uploaded files are encrypted using AES-256 (Advanced Encryption Standard), ensuring strong encryption that prevents unauthorized decryption.
The encrypted file is then stored in a secure cloud or local server for retrieval by authorized recipients.

5.5 QR Code Generation

A QR code is generated dynamically for each encrypted file.
The QR code contains the secure file access link embedded with metadata, including the encrypted file's location and authentication requirements.
To ensure data integrity and scanning accuracy, Reed-Solomon error correction is applied to the QR code.

VI. IMPLEMENTATION

6.1 Technologies Used

- Python
- Django / Flask
- HTML, CSS, JavaScript
- MySQL
- AES Encryption
- OTP Authentication

6.2 System Setup

- Install Python
- Install required libraries
- Configure database
- Setup authentication modules
- Run web server

6.3 Sample Code

```
from cryptography.fernet import Fernet

key = Fernet.generate_key()
cipher = Fernet(key)

message = b"Secure File Data"
encrypted = cipher.encrypt(message)

print("Encrypted Data:", encrypted)
```

VII. RESULTS AND ANALYSIS

7.1 Performance

- Secure authentication achieved
- Fast file upload and download

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802474

- Successful OTP verification
- Secure encrypted storage implemented

7.2 Observations

- Prevents unauthorized access effectively
- Improves user privacy and security
- Reduces risk of data leakage
- Provides reliable authentication mechanism

VIII. ADVANTAGES

- Ensures secure file sharing with encryption and 2FA.
- QR codes with expiry time and scan limits prevent misuse.
- Simplifies secure file sharing without manual key exchange.
- Prevents unauthorized modifications during transmission.

Can be integrated into various secure communication platforms

IX. LIMITATIONS

Dependence on Internet Connectivity
The system requires stable internet access for cloud-based operations and OTP verification.

OTP Delivery Delay
Network issues may delay OTP delivery during authentication.

Initial Setup Complexity
Configuring encryption and authentication systems may require technical expertise.

Storage Limitations
Large file storage may require additional server resources.

X. FUTURE ENHANCEMENTS

Blockchain Integration – Implementing blockchain technology to create a tamper-proof record of file transactions, ensuring transparency and security.
Biometric Authentication – Enhancing security by integrating fingerprint or facial recognition for user authentication instead of or in addition to OTP-based 2FA.
Cloud Storage Integration – Allowing users to store encrypted files on secure cloud platforms, enabling seamless access across multiple devices.
Role-Based Access Control (RBAC) – Introducing customized access permissions based on user roles to improve security in enterprise environments.

XI. CONCLUSION

In Conclusion, this project provides a secure and efficient file-sharing system by integrating AES-256 encryption, Two-Factor Authentication (2FA), and QR code-based access control. Unlike traditional file-sharing methods, which are often vulnerable to unauthorized access, interception, and weak encryption, this system ensures data confidentiality and integrity. With AES-256 encryption, files are protected from unauthorized access, while secure key transmission ensures that only intended recipients can decrypt them. The use of QR codes with Reed-Solomon error correction enhances reliability by ensuring accurate scanning, even in suboptimal conditions. Additionally, expiry control mechanisms, such as time-based expiration and limited scans, provide further security. The system ensures seamless and protected data exchange, making it an ideal solution for organizations and individuals requiring highly secure file transmission.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802474

REFERENCES

1. S. Yusupova, B. Ishmetov, R. Baltayev, B. Nurmetova, O. Allayorov and B. Ortiqov, "Recognition of QR Codes Resistant to Affine Transformations", 2024 IEEE 25th International Conference of Young Professionals in Electron Devices and Materials (EDM), pp. 2590-2593, 2024.
2. Benito-Altamirano, D. Martínez-Carpena, O. Canals, C. Fábrega, A. Waag and J. Prades, "Back-compatible Color QR Codes for colorimetric applications", Pattern Recognit., vol. 133, 2023.
3. T. Shindo et al., "Super Resolution for QR Code Images", 2022 IEEE 11th Global Conference on Consumer Electronics (GCCE), pp. 274-277, Oct. 2022.
4. C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor &Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011. DOI: 10.1080/15325008.2010.541746
5. C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of Electrical Engineering, Vol.63 (6), pp.365-372, Dec.2012. DOI: 10.2478/v10187-012-0054-2
6. C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011. DOI 10.1007/s00202-011-0203-9
7. S.Tamilselvi, R.Prakash, C.Nagarajan,"Solar System Integrated Smart Grid Utilizing Hybrid Coot-Genetic Algorithm Optimized ANN Controller" Iranian Journal Of Science And Technology-Transactions Of Electrical Engineering, DOI10.1007/s40998-025-00917-z,2025
8. S.Tamilselvi, R.Prakash, C.Nagarajan," Adaptive sliding mode control of multilevel grid-connected inverters using reinforcement learning for enhanced LVRT performance" Electric Power Systems Research 253 (2026) 112428, doi.org/10.1016/j.epsr.2025.112428
9. S.Thirunavukkarasu, C. Nagarajan, 2024, "Performance Investigation on OCF and SCF study in BLDC machine using FTANN Controller," Journal of Electrical Engineering And Technology, Volume 20, pages 2675–2688, (2025), doi.org/10.1007/s42835-024-02126-w
10. C. Nagarajan, M.Madheswaran and D.Ramasubramanian- 'Development of DSP based Robust Control Method for General Resonant Converter Topologies using Transfer Function Model'- *Acta Electrotechnica et Informatica Journal* , Vol.13 (2), pp.18-31,April-June.2013, DOI: 10.2478/aeei-2013-0025.
11. C.Nagarajan and M.Madheswaran - 'DSP Based Fuzzy Controller for Series Parallel Resonant converter'- *Springer, Frontiers of Electrical and Electronic Engineering*, Vol. 7(4), pp. 438-446, Dec.12. DOI 10.1007/s11460-012-0212-0.
12. C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- *Iranian Journal of Electrical & Electronic Engineering*, Vol.8 (3), pp.259-267, September 2012.
13. C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007
14. Suganthi Mullainathan, Ramesh Natarajan, "An SPSS and CNN modelling based quality assessment using ceramic materials and membrane filtration techniques", Revista Materia (Rio J.) Vol. 30, 2025, DOI: https://doi.org/10.1590/1517-7076-RMAT-2024-0721
15. M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022
16. K. Pena-Pena, D. L. Lau, A. J. Arce and G. R. Arce, "Qrnet: fast learning-based qr code image embedding", Multimed. Tools Appl., pp. 1-20, 2022.
17. M. Xu, Q. Li, J. Niu, H. Su, X. Liu, W. Xu, et al., "Art-up: A novel method for generating scanning-robust aesthetic qr codes", ACM Trans. Multimed. Comput. Commun. Appl., vol. 17, no. 1, pp. 1-23, 2021.
18. Anand, L., Maurya, M., Seetha, J., Nagaraju, D., Ravuri, A., & Vidhya, R. G. (2023, July). An intelligent approach to segment the liver cancer using Machine Learning Method. In 2023 4th international conference on electronics and sustainable communication systems (ICESC) (pp. 1488-1493). IEEE.
19. Rajendran, S., Sundarapandi, A. M. S., Krishnamurthy, A., & Thanarajan, T. (2022). An intelligent face recognition technology for iot-based smart city application using condition-cnn with foraging learning pso model. International Journal of Pattern Recognition and Artificial Intelligence, 36(14), 2256018.
20. Murugeshwari, B., & Sujatha, R. (2014). Preservation of Privacy for Multiparty Computation System with Homomorphic Encryption. International Journal of Emerging Technology and Advanced Engineering, 4(3), 530-535.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802474

21. Sugumar, R. (2025). Unified AI Framework for Predictive Data Engineering and Real Time Prescription and Billing Systems. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 8(5), 17261.
22. Samrat, B., Thomas, P. K., Kumar, S., Benila, A., Bhardwaj, R., & Vigenesh, M. (2024, December). Industrial informatics in optimizing software-defined vehicles for logistics. In 2024 IEEE 2nd International Conference on Innovations in High Speed Communication and Signal Processing (IHCSP) (pp. 1-9). IEEE.
23. Soundappan, S. J. (2024). AI-driven customer intelligence in enterprise lakehouse systems Sentiment Mining Governance-Aware Analytics and Real-Time Data Synchronization. International Journal of Advanced Engineering Science and Information Technology.
24. Rajasekar, M. (2024). AI-Powered Cyber-Secure Federated Learning on AWS for Next-Generation Digital Banking Analytics. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(3).
25. Deivendran, P., Babu, P. S., Malathi, G., Anbazhagan, K., & Kumar, R. S. (2023). Emotion Recognition for Challenged People Facial Appearance in Social using Neural Network. arXiv preprint arXiv:2305.06842.
26. Sugumar, R., & Murugeshwari, B. (2016). An Efficient MChord based Authentication for Vehicular Ad-Hoc Networks.
27. Pandey, V. K., Mishra, S., Rengarajan, A., Savita, & Roomi, M. M. (2024, March). Enhancing Weather Forecasting with Machine Learning Techniques. In International Conference on Renewable Power (pp. 147-156). Singapore: Springer Nature Singapore.
28. Mathew, A., & Alex, H. (2025). Federated Learning for Secure Genomic Research: Privacy-Preserving AI Solutions for Precision Medicine. Science and Technology: Developments and Applications Vol. 9, 36-43.
29. Selvi, G. V., Anbarasan, A. B., Murthy, B. A., & Prabavathy, S. (2023). An Application Oriented Integrated Unequal Clustering Algorithm for Wireless Sensor Network. In Underwater Vehicle Control and Communication Systems Based on Machine Learning Techniques (pp. 140-154). CRC Press.
30. Soundappan, S. J. (2025). Next Generation AI Enabled Holistic Cognitive Platform for Secure Cloud Network Intelligence Enterprise Systems and Digital Trust Optimization. International Journal of Computer Technology and Electronics Communication, 8(5), 11534-11542.
31. Rajasekar, M. (2024). Real-Time Predictive DevOps Intelligence for Risk-Aware Digital Business Processes in Cloud and SAP Ecosystems. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(4), 10713-10718.
32. Jagadeesh, S., & Sugumar, R. (2017). A comparative study on artificial bee colony with modified ABC algorithm. European Journal of Applied Sciences, 9(5), 243–248.
33. Murugeshwari, B., Sarukesi, K., & Jayakumar, C. (2010, March). An efficient method for knowledge hiding through database extension. In 2010 International Conference on Recent Trends in Information, Telecommunication and Computing (pp. 342-344). IEEE.
34. Reddy, K. V. V. K., & Vimal, V. R. (2024, July). A novel approach on improved segmentation and classification of remote sensing images using AlexNet compared over linear discriminant analysis with improved accuracy. In 2024 Second International Conference on Advances in Information Technology (ICAIT) (Vol. 1, pp. 1-6). IEEE.
35. Gowthami, D., & Vigenesh, M. (2024). Distributed and Lightweight Intrusion Detection for IoT: A Lightweight Pyramidal U-Net With Tri-Level Dual Inception-Based Framework. In The Convergence of Self-Sustaining Systems With AI and IoT (pp. 154-173). IGI Global Scientific Publishing.
36. Anand, P. V., & Anand, L. (2023, December). An Enhanced Breast Cancer Diagnosis using RESNET50. In 2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES) (pp. 1-5). IEEE.
37. Mathew, A. (2022). Leveraging Big Data Analytics to Power AI and ML (Machine Learning) Automation. Educational Research (IJMCER), 4(5), 131-134.
38. Dhinakaran, D. (2022). Joe Prathap P. M, Selvaraj D, Arul Kumar D and Murugeshwari B," Mining Privacy-Preserving Association Rules based on Parallel Processing in Cloud Computing,". International Journal of Engineering Trends and Technology, 70(3), 284-294.
39. Poornima, G., & Anand, L. (2024, April). Effective Machine Learning Methods for the Detection of Pulmonary Carcinoma. In 2024 Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM) (pp. 1-7). IEEE.
40. Rengarajan, A., Jayakumar, C., & Sugumar, R. (2012). Optimization Of Recent Attacks Using Internet Protocol. National Journal of System and Information Technology, 5(1), 8.
41. Mathew, A., & Romasco, L. (2024). Forensic Investigation of Artificial Intelligence Systems. Research Updates in Mathematics and Computer Science Vol. 4, 154-164.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802474

42. Vekariya, V., Kumar, S., & Rengarajan, A. (2024). A distinctive and smart agricultural knowledge-based framework using ontology. In Sustainability in Digital Transformation Era: Driving Innovative & Growth (pp. 207-213). CRC Press.
43. Soundappan, S. J. (2020). Big data analytics in healthcare: Applications for pandemic forecasting. International Journal of Advanced Research in Computer Science & Technology, 3.
44. Sugumar, R. (2024). AI-Augmented Quality Engineering for Performance Optimization and Test Orchestration in Distributed Systems. International Journal of Science, Research and Technology, 7(5), 12835-12846.
45. Soundappan, S. J., & Sugumar, R. (2016). Optimal knowledge extraction technique based on hybridisation of improved artificial bee colony algorithm and cuckoo search algorithm. International Journal of Business Intelligence and Data Mining, 11(4), 338–356.
46. Mathew, A. (2025). Ahead of the breach: Predictive threat intelligence in aviation inspired by Scattered Spider attacks. Multidisciplinary International Journal of Research and Development (MIJRD), 4(6), 54–58.
47. Soundappan, S. J. (2021). DataOps: Orchestrating Reliable ML Data Pipelines. International Journal of Research and Applied Innovations, 4(4), 5533-5537.
48. Garg, V. K., Soundappan, S. J., & Kaur, E. M. (2020). Enhancement in intrusion detection system for WLAN using genetic algorithms. South Asian Research Journal of Engineering and Technology, 2(6), 62–64.
49. Anand, L., Tyagi, R., & Mehta, V. (2024, January). Food recognition using deep learning for recipe and restaurant recommendation. In Proceedings of Eighth International Conference on Information System Design and Intelligent Applications (pp. 269-279). Singapore: Springer Nature Singapore.
50. Kumar, A., & Anand, L. (2025). A Novel EEG-Based Deep Learning Framework for Enhancing Communication in Locked-In Syndrome Using P300 Speller and Attention Mechanisms. KSII Transactions on Internet and Information Systems (TIIS), 19(11), 3841-3855.
51. Soundappan, S. J. (2022). AI-Based Fault Detection and Isolation for Reliability in Modern Power Systems. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(4), 7106-7110.
52. Chandra, S., Rengarajan, A., Sahoo, G. S., & Sharma[4], S. (2024, October). Identifying Neuronal Damage and Plasticity by Analyzing Changes in Diffusion Tensor. In Proceedings of the 5th International Conference on Data Science, Machine Learning and Applications; Volume 2: ICDSMLA 2023, 15–16 December, Hyderabad, India (Vol. 2, p. 433). Springer Nature