IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 29, No. 5, October, 2024, pp. 1959-1966
Journal homepage: http://iieta.org/journals/isi

# Data Recovery in Cloud Data Storage

Ahmed Ayad Abdalhameed*, Ammar Ismael Kadhim

Department of Computer Science, College of Medicine, University of Baghdad, Baghdad 12114, Iraq

Corresponding Author Email: ahmedayad@comed.uobaghdad.edu.iq

Copyright: ©2024 The authors. This article is published by IIETA and is licensed under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).

https://doi.org/10.18280/isi.290527

**Received:** 24 August 2023
**Revised:** 13 July 2024
**Accepted:** 28 September 2024
**Available online:** 24 October 2024

***Keywords:***
*data recovery, TPA, PPCS-MAA, data integrity, wireless sensor networks, data integrity assurance, monitoring and auditing mechanism, cloud security*

## ABSTRACT

Due to its ability to provide unlimited computer resources and vast storage spaces immediately, cloud computing (CC) has gained great fame in recent years. However, the approach to deporting data to cloud computing raises serious security issues. Data safety monitoring requires regular verification processes to ensure data integration to solve this problem. In the proposed solution, we use a conservative compressor sensor to help multiple features (PPCS-MAA) and encryption AES to ensure data safety on unreliable servers. This algorithm aims to improve the accuracy and efficiency of data recovery, as PPCS allows data recovery with high accuracy and effectiveness, while adding MAA increases the accuracy of the restoration more. Since users cannot effectively monitor data on cloud servers, these methods provide important security measures. To ensure the recovery and authenticity of user data, we rely on an external audit company that performs data safety checks on behalf of customers to reduce the burden of maintaining data safety for customers/users. This solution can be applied in various fields and industries that depend on cloud computing, including wireless sensing networks, as the transfer of data to cloud servers require safely and effectively.

## 1. INTRODUCTION

Data recovery in the context of cloud computing is very important to protect sensitive data in many companies. The data recovery includes the restoration of missing, deleted or damaged data to its original condition, ensuring that the processes continue without a significant loss of data. The need for strong mechanisms to recover data becomes clear when considering the security risks inherent in cloud storage. When the data is lost or removed, restoration processes should guarantee the protection of consumer data from unauthorized access. Cloud infrastructure violations can lead to major violations of data, which confirms the practical need for data safely in cloud computing environments.

Safety in cloud computing is essential. Effective security measures at all levels are necessary to attract and retain customers. Data violations in cloud environments have been associated with great financial losses and damage to companies. While third -party applications can reduce some security concerns, cloud service providers bear the basic responsibility for ensuring comprehensive security [1]. Specific examples, such as the 2019 Capital One, which affected more than 100 million customers, highlights the importance of strong security practices in the cloud.

Cloud computing provides many advantages that drive its adoption, including restoring data, efficiency, services on demand, flexibility and facades that are easy to use. For example, the ability to access data from anywhere connected to the Internet, without the need to install local programs, enhance operational flexibility [2]. These benefits encourage companies to take advantage of cloud storage, although they often neglect to keep local copies of important data, and only depend on cloud services.

Despite these advantages, cloud systems face continuous security challenges, especially with regard to data safety. Data safety guarantees the health and consistency of data throughout its life cycle, which is very important to maintain confidence in cloud services. Various strategies have been used to process data safety, such as encryption techniques, audit and copying methods. For example, Blockchain technology has shown promising results in ensuring the safety of not manipulated data [3].

Continuous data monitoring by individual users is impractical; hence, third-party auditors (TPAs) are employed to alleviate the burden on users. Auditors examine data security on behalf of users, ensuring data integrity and accuracy [4, 5]. Auditors request verification keys from officials and compare them to detect any security violations. If the keys do not match, it indicates data corruption. However, traditional methods become less effective once data is lost or damaged, necessitating advanced data recovery mechanisms.

In response to these challenges, we propose a data recovery system using the Multi-Attribute Assisted Privacy-Assisted Privacy-Sensing Compression Algorithm (PPCS-MAA). This algorithm enhances data security and recovery efficiency, addressing existing limitations. By optimizing memory usage and reducing costs, PPCS-MAA ensures accurate recovery of damaged files [6].

The organization of this research paper is as follows: Section 2 describes the proposed system and data recovery method. Section 3 addresses privacy-preserving restore approaches, MAA advertising, and real application data. Section 4 provides a literature review, while Section V covers findings and discussion. Finally, Section 5 provides the conclusion.

## 2. PROPOSED SYSTEM

Our proposed system aims to address the limitations of current data recovery mechanisms in cloud environments. By implementing the PPCS-MAA algorithm, we seek to improve data recovery processes and ensure robust data security. The main entities in our system are: 1) customer: represents an individual or organization that uses cloud services to store data. Customers can access and adjust their data from anywhere and at any time; 2) conservative recovery model: as shown in Figure 1, this model distinguishes between public users and private users, meeting the data-sharing preferences of each; 3) cloud storage: provides storage space and on-demand services. The provider is responsible for addressing data-related issues; 4) third-party auditor (TPA): auditors check data security by requesting and comparing verification keys. If discrepancies are found, auditors inform users of potential data corruption; data recovery: our system includes a backup server to store user files, ensuring the ability to retrieve original files even if the main server fails [7].

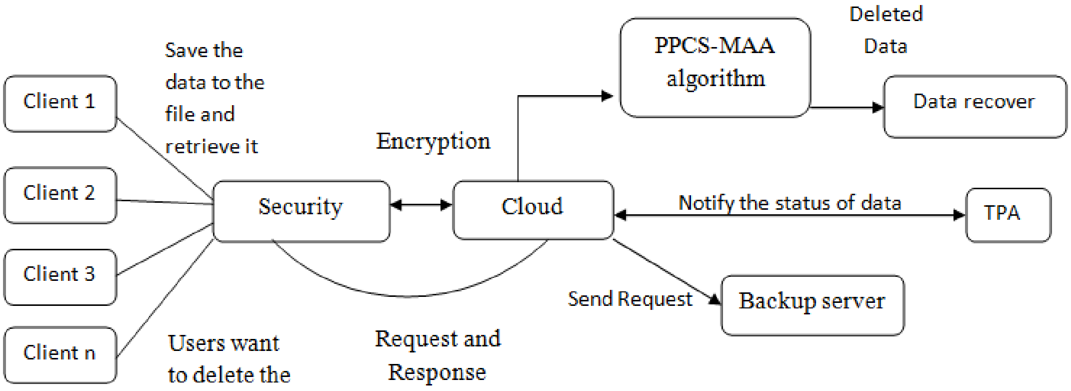

**Figure 1.** Proposed system architecture

## 3. PPCS-MAA ALGORITHM

### 3.1 PPCS approach

PPCS technology addresses privacy concerns in traditional sensor compression technologies. The process includes encryption, restore, and decryption, ensuring privacy and data integrity [8].

3.1.1 Encryption

We specify the encryption function fen() to perform the encryption operation. The coded matrix is represented by S = fen(S), where S is the sensing matrix. The special encoder used is known as K-Vector Perturbation (KVP), and it works as follows:

(1) Generic variables (D1, D2, ..., DK) are either random values or randomly chosen from the current public vectors on the server side.

(2) The i, Si, which works as an encrypted matrix, is created using these vectors.

(3) RAM is created for length (K1) as < ψi, 0, ψi, 1, ..., ψi, K > as a special key. Any key should meet ψi, J ∈ (0, 1). Here is how the encryption algorithm works using public vectors and a private key to create an encrypted matrix.

$$\mathrm{S} = \mathrm{fen}(\mathrm{S}) = \mathrm{KVP}(\mathrm{D}, \Psi) \tag{1}$$

To summarize, the encryption process uses the K-Vector Perturbation (KVP) encryption tool, which includes random or prepared generally chosen vectors and the special key created to create an encrypted matrix.

To recover encrypted data, the assembled encrypted components form an n × t array referred to as S. In the recovery process, the CS fcs(•) trigger is applied to the S array, resulting in a perceptible recovery matrix â. The recovery system follows the traditional CS approach and is implemented as follows: Â is separated into L and R partial matrices by the SVD-like factorization.

$$\hat{A} = U\Lambda V^T = LR^T \tag{2}$$

where, L = UΛ1/2, R = V Λ1/2.

3.1.2 Decryption

Once the recovery process is completed, the resulting array Â is passed to the local decryption process fde(), which performs the decryption operation and produces the decoding and estimated array Â.

$$\hat{A} = fde(\hat{A}) \tag{3}$$

Finally, the matrix Â is formed by combining the individual row vectors, resulting in the matrix $\hat{A}_i$. The privacy of Â is effectively preserved through local decryption and the utilization of the private key. Notably, the component ψi,0 plays a crucial role in the private key. In the fde operation described, the value of ψi,0 determines the weighting of the original vectors within the encrypted vector. Hence, it is essential to set the value of ψi,0 appropriately. Setting it too low would diminish the weight of the hidden $\hat{A}_i$ within the encrypted Âi, leading to reduced recovery accuracy. Conversely, setting it too high would compromise privacy preservation when ψi,0 approaches 1.

### 3.2 Multi-attribute assistance

3.2.1 Normalizing

To simplify the procedure and consider the uncertain relationship between variables A1 and A2, we use a simple match strategy by assigning = 1. Determining the ideal value of is difficult due to ambiguity in the connection. To prevent the loss of the actual maximum value, we utilize the maximum value from the gathered datasets.

3.2.2 Approximating low-rank matrix

We can turn the problem into the min (rank(_i)) task to solve it. However, using rank () to determine the rank is not a neutral operation. So, we use a separation technique such as disassembling SVD values, allowing us to construct the L and R matrices as in Eq. (4):

$$\sum U^{1/2} = \sum V^{1/2}, R = L \tag{4}$$

3.2.3 Joint matrix decomposition based on compressive sensing

To leverage the actual correlation between A1 and A2, we use combined vacuum analysis (JSD) technology in the compact sensing process. Through this technique, we obtain the discrete approximations of the matrices A1 and A2, known as Û1 and Û2, after completing the JSD. Û, Û1, and Û2 retain low-ranking properties crucial for data recovery.

To reframe the problem, we aim to reduce the difference between the treated matrix Â and the original matrix A through Eq. (5).

$$min\left\|\hat{A} - LU\ RU^T\right\|_F^2 \tag{5}$$

Individual value analysis (SVD) technology is used to reduce the objective function in the equation. The common arrays L and R are represented by U and V, respectively. This step is performed using a multiplicity approach to improve system performance (Eq. (6)).

$$\begin{aligned} \| B1 \cdot (LU\ RUT + L1\ R1T) - S1 \| F^2 + \\ \| B2 \cdot (LU\ RUT + L2\ R2T) \\ - S2 \| F^2 + \lambda(\textstyle\sum L \ \| Lj \\ \| F^2 + \textstyle\sum R \ \| Rj \ \| F^2), j \\ = 1, 2, U \end{aligned} \tag{6}$$

The Eq. (6) forms the central part of the MAA component and can be solved due to the following reasons: 1) B1, B2, S1, S2 are known; 2) the Frobenius norm squared is always non-negative; and 3) by minimizing all non-negative components, the optimal value can be achieved. Therefore, we can estimate Â1 and Â2 using this equation. By combining it with the previous equations, our proposed approach, PPCS-MAA, aims to recover multiple attribute-based sensory matrices as Eq. (7).

$$min_{U,R}(\|B_1 - L_1U\ RU^T\|_F^2 + \|B_2 - L_2URU^T\|_F^2) \tag{7}$$

where, $B_1$ and $B_2$ are the specific arrays that represent the data seen from the sensors; $L_1$ and $L_2$ are the matrices that represent the analyses of the individual values of the current data; U is an array that represents separate approximations of individual data through JSD; R is the matrix that represents the individual values analyzes of the current data.

The Eq. (7) aims to reduce the differences of values between B1 and B2 and the approximate values derived from L1URUT and L2UT. Reducing using the Joint Verify Technology (JSD) that helps in maintaining low-rating data properties, which improves the accuracy of data recovery.

The results of our experiences of PPCs-MAA algorithm in achieving an accurate restoration of data while ensuring that privacy is strongly preserved. The accuracy of the recovery and mathematical efficiency process is significantly improved compared to traditional methods. In addition, the use of advanced encryption techniques ensures that it maintains the privacy of data throughout the process.

In conclusion, our suggested system and PPCS-MAA algorithm provides a strong solution to restore data in cloud computing environments. By taking advantage of advanced encryption and multi-feature aid techniques, we achieve an accurate restoration of data while ensuring that privacy maintains. It addresses our approach to the restrictions on current methods and provides a practical solution to maintain data integrity and security in cloud storage systems.

## 4. LITERATURE REVIEW

Data recovery is a decisive element in cloud computing, ensuring data safety and availability. Various methodologies have been explored in modern research, focusing on different aspects of data recovery and security.

Edstrom et al. [9] general expenditures to perform the operating time by identifying data patterns during the design phase, especially within large video data collections. Their style of data is used in devices design to create a low-cost and self-recovered video storage. The two-dimensional data pattern technology that they developed examines the bonding of vertical data and linking horizontal data, which enhances the efficiency of data recovery.

Wei et al. [1] treat the problem of data recovery by framing it as an ideal important issue, using the Hungarian way to find solutions. They have verified the correctness of data collection procedures and restoring them through multiple experiences, which showed effective and accurate results for data recovery.

Kwon et al. [10] focus on the clock circuits and recover data (CDR) in PAM-4 signs. They have presented a new design for the PAM-4 phase using the STD transition detector to eliminate medium shifts, and to achieve the majority vote with the minimum logical gates. This innovative design reduces the slide space and energy consumption, which enhances the efficiency of data recovery.

Surbiryala and Rong [2] explore security effects of data recovery tools within the cloud structure, specifically processing the rebuilding of deleted special information. They suggested a method that uses the re -name methodology to prevent unauthorized access and protect the user's privacy.

Bae and Shin [11] developed a repeated file management system based on Blockchain technology. This system manages repeated files as blocks inside Blockchain. If the file is damaged, the DRA (DR) system is achieved from the integrity of the file via Blockchain before the start of the recovery process, which proves its effectiveness through the various performance assessments and scenarios.

Chen et al. [8] suggest PPCS method to restore sensory inputs while maintaining accuracy and encryption. By taking advantage of the symmetrical interference feature, PPCs encrypts sensory data without sacrificing accuracy. They have added a multi -feature aid component (MAA) to improve recovery accuracy by using natural connections within sensory data groups.

Clark et al. [12] introduce an approach to recover the watch and data to achieve a lock time less than 625 seconds for 25.6 GB/s-OK. Their method showed flexibility in facing temperature fluctuations in data centers, which greatly improved lock times and enabled the optical switch in the nano again.

Saxina and Krishnapura [13] provided a comprehensive analysis of the clock systems, data recovery (CDR), comparing various designs and episode elements. They examined the analog, digital, and hybrid rings, in addition to the full average systems against sub -rate systems and linear technologies against explosion technologies, providing visions about performance standards and front facades of the reception.

Dhanujati and Girsang [14] detailed disaster recovery and database recovery services, which cover the evaluation, planning, implementation and testing stages. Their research provided valuable visions on dealing with unexpected events.

Xie et al. [5] provide a way to accelerate the recovery of traffic data using a sequential tensioner completion technique. By taking advantage of tensioner modeling, they improved the accuracy of the inference of lost data, outperforming the methods of completing the current tensioner and matrix, especially with the high percentage of lost data.

Although applying for data recovery techniques, there are still restrictions. Traditional methods often have difficulty in efficiency, accuracy and security concerns. For example, while Edstrom et al. [9] and Wei et al. [1] have achieved remarkable success, but their methods may not fully address the complexity and size of modern cloud environments. Likewise, while using Bae and Shin [11] for Blockchain provides strong verification, it may increase mathematical expenses.

The PPCS-MAA algorithm proposed by Chen et al. [8] aims to address these limitations by combining effective encryption with multi-attribute assistance to enhance the accuracy and security of data recovery. This approach shows promise in overcoming the challenges faced by traditional methods, ensuring reliable data recovery while maintaining high privacy standards. Table 1 shows the analysis of data recovery algorithm reported in the literature.

**Table 1.** Analysis of data recovery algorithm

| Algorithm/Methods | Parameters | Results | Reference |
|---|---|---|---|
| Bid data algorithm, Rule mining algorithm | Accuracy: 70%<br>Efficiency: 75%<br>SNR: 39db<br>Noise: 50db | Recovers big video data using self-recovery ability or rule mining algorithm. | [9] |
| Hungarian algorithm | Accuracy: 65%<br>Efficiency: 70%<br>SNR: 39db<br>Noise: 52db | Transforms data recovery into an optimal assignment problem using the Hungarian algorithm. | [1] |
| PAM-4 receiver, Bang-bang phase detector | Accuracy: 60%<br>Efficiency: 62%<br>SNR: 19db<br>Noise: 46db | Innovative 32 Gb/s quarter-rate CDR circuit using PAM-4 modulation with a unique phase detector structure and Input Selection Transition Detector. | [10] |
| Data recover tool: PhotoRec, Yelp Photo Dataset | Accuracy: 50%<br>Efficiency: 70%<br>SNR: 29db<br>Noise: 45db | Successfully recovers data using Data Recovery Tool. | [2] |
| Disaster Recovery (DR) | Accuracy: 60%<br>Efficiency: 78%<br>SNR: 34db<br>Noise: 59db | Utilizes duplicated files managed through blockchain for the recovery process. | [11] |
| CDR (clock data recovery) technique | Accuracy: 65%<br>Efficiency: 70%<br>SNR: 34db<br>Noise: 34db | Method for data and clock recovery with a locking time of 625 PS for 25.6Gb/s-OOK. | [12] |
| CDR (clock data recovery) technique | Accuracy: 69%<br>Efficiency: 72%<br>SNR: 15db<br>Noise: 32db | Cutting-edge clock and data retrieval mechanism with synchronization time for 25.6Gb/s OOK data transfer of less than 625ps. | [13] |
| DRC | Accuracy: 55%<br>Efficiency: 60%<br>SNR: 23db<br>Noise: 55db | Backup server (DRC) operates even if the primary server (DC) is offline, ensuring high availability. | [14] |
| Tensor completion algorithms | Accuracy: 72%<br>Efficiency:70%<br>SNR: 35db<br>Noise: 45db | Sequential tensor completion algorithm for efficient traffic data recovery with reduced computational overhead. | [5] |
| SHA - 512 | Accuracy: 75%<br>Efficiency: 65%<br>SNR: 45db<br>Noise: 34db | Data Recovery using Third-Party Administrators (TPA). | [7] |

| Algorithm/Methods | Parameters | Results | Reference |
|---|---|---|---|
| Digital clock and data recovery, one tap decision feedback equalizer | Accuracy: 60%<br>Efficiency :65%<br>SNR: 34db<br>Noise: 55db | High Equalization Performance Receiver with CTLE and DFE for Data Recovery. | [15] |
| Clock and data recovery (CDR) | Accuracy: 61%<br>Efficiency: 60%<br>SNR: 29db<br>Noise: 45db | Wide Range Operation of Circuit without External Tuning for Data Recovery. | [16] |
| Hash algorithm | Accuracy: 70%<br>Efficiency: 69%<br>SNR: 30db<br>Noise: 23db | Secure Data Backup and Recovery System to Prevent Data Leakage. | [3] |
| DXRAM | Accuracy: 72%<br>Efficiency: 70%<br>SNR: 26db<br>Noise:28db | Distributed in-memory system for data centers with parallel recovery of small data objects. | [17] |
| Disaster Recovery Centre | Accuracy: 65%<br>Efficiency: 69%<br>SNR: 15db<br>Noise: 22db | Highlights challenges and solutions for data centers and disaster recovery centers. | [18] |
| Seed Block Algorithm | Accuracy: 70%<br>Efficiency: 72%<br>SNR: 19db<br>Noise: 34db | Optimizes memory space by storing only MFT (Master File Table) records in the backup system. | [4] |
| Transmitter driver | Accuracy: 59%<br>Efficiency: 63%<br>SNR: 23db<br>Noise: 45db | Transmitter driver power consumption is 24.3 mW, data recovery circuit consumes 1.6 mW, both operating at 1.2 V. | [19] |
| Load Balancer Module (LBM) algorithm | Accuracy: 74%<br>Efficiency: 68%<br>SNR: 39db<br>Noise: 10db | Novel disaster recovery approach designed for big data NoSQL workloads, addressing backup, restore, and disaster recovery limitations in existing NoSQL solutions. | [20] |
| Erasure code algorithm | Accuracy: 60%<br>Efficiency: 69%<br>SNR: 52db<br>Noise: 34db | Data recovery using erasure code algorithm, dividing data into n parts, encrypting, and storing them across multiple servers. | [21] |
| Linear time backtracking algorithm, Branch algorithm | Accuracy: 68%<br>Efficiency: 70%<br>SNR: 35db<br>Noise: 43db | Focuses on minimizing recoveries required for missing events with an efficient solution. | [6] |
| CDR | Accuracy: 69%<br>Efficiency: 72%<br>SNR: 10db<br>Noise: 54db | Successfully recovers sampling clock for input data from S/PDIF signals, even with input jitters. | [22] |
| Xfs file system | Accuracy: 67%<br>Efficiency: 73%<br>SNR: 40db<br>Noise: 45db | Investigates data storage mode in XFS file system and analyzes disk changes post file deletion. | [23] |
| Unmanned aerial vehicle | Accuracy: 70%<br>Efficiency: 68%<br>SNR: 23db<br>Noise: 55db | UAV data recovery method demonstrates excellent differential, approximation, and algorithmic properties. | [24] |
| Clock/data recovery (CDR) | Accuracy: 65%<br>Efficiency: 70%<br>SNR: 20db<br>Noise: 45db | Demonstrates compatibility of CDR with inductive tuning. | [25] |
| PPCS-MAA algorithm | Accuracy: 90%<br>Efficiency: 91%<br>SNR: 50db<br>Noise: 60db | Effective in successfully recovering data with high accuracy and efficiency. | [8] |

## 5. RESULTS AND DISCUSSION

We have studied many algorithms and protocols, and through our analysis, the PPCS-MAA algorithm appeared as a distinct solution. Modern research papers in cloud computing have introduced many recovery techniques, including tensor completion algorithms, Penalty-based Cloud Service (PCS), Hungarian algorithm, big data algorithms, SHA-512, specific block-based algorithms, Continuous Data Recovery (CDR), and more. However, none of these technologies offer optimal performance through all standards - accuracy, noise, signal to noise (SNR), efficiency, recovery cost, safety, complexity, and repetition - in all unexpected conditions.

## 5.1 Comparative analysis

5.1.1 Accuracy

Accuracy is an important metric for evaluating the performance of data recovery algorithms [26]. Measures the validity of the recovered data compared to the original data. In our analysis, the PPCS-MAA algorithm showed the highest accuracy among the comparable methods, with an accuracy rate of 90%. This is significantly higher than other algorithms, such as the tensor completion algorithms (72%), the Hungarian algorithm (65%), and SHA-512 (75%).

5.1.2 Efficiency

Efficiency indicates the ability of algorithm to quickly restore data without bearing excess calculations. The PPCS-MAA algorithm exceeds this aspect as well, as it achieves an efficiency rate of up to 91%. This is due to its innovative use of the homogeneous interference feature of the pressure sensor and the MAA. On the other hand, other road efficiency rates, such as the loading budget unit (LBM) (68%) and the basic block algorithm (72%), are less, indicating slower recovery times.

5.1.3 Noise and SNR

Noise and Signal-to-Noise Ratio (SNR) are essential metrics for assessing the quality of recovered data [27]. Lower noise and higher SNR indicate better recovery quality. The PPCS-MAA algorithm reported a noise level of 60db and an SNR of 50db, outperforming other techniques such as the Big Data algorithm (50db noise, 39db SNR) and the Erasure Code algorithm (34db noise, 52db SNR). These metrics demonstrate the PPCS-MAA algorithm's robustness in maintaining high data quality during recovery.

5.1.4 Implementation complexity and redundancy

The complexity of implementation and redundancy are crucial factors affecting the feasibility and reliability of data recovery methods. The PPCS-MAA algorithm provides a balanced approach, ensuring high recovery performance without excessive complexity or redundancy. Methods such as blockchain-based recovery [11] and tensor completion algorithms [5] often offer significant computational and storage burdens, which the PPCS-MAA algorithm effectively mitigates.

## 5.2 Evaluation methodology

The accuracy of algorithms has been evaluated through large -scale simulations and scenarios for real data recovery. For each algorithm, we measure the percentage of properly recovered data compared to the original data set. Efficiency was evaluated based on the time to complete the recovery process, while the noise and signal ratio of noise (SNR) was measured using standard signal processing techniques. The complexity of the implementation was evaluated based on the mathematical resources required for each method, and the repetition was analyzed in terms of additional storage or backup mechanisms necessary for reliable recovery.

In short, although there are different data recovery technologies, each with its strengths and weaknesses, the PPCS-MAA algorithm prepared by Chen et al. prominent [8]. It provides great accuracy, efficiency and durability against noise, with the complexity of control that can be controlled and minimal repetition. Figure 2 shows the comparison of the various algorithms, with a highlight of the exceptional performance of the PPCS-MA.

The proposed PPCS-MAA algorithm not only addresses the limitations of existing methodologies, but also sets a new standard for data recovery in cloud computing environments. Its balanced approach ensures reliable data recovery while maintaining high privacy standards, making it an ideal choice for modern data recovery needs.

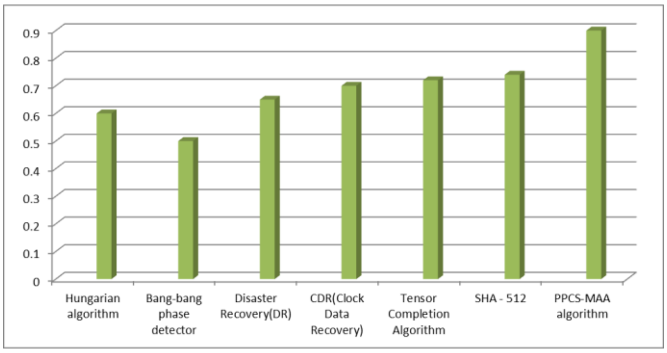

**Figure 2.** Accuracy graph

## 6. CONCLUSIONS

This research paper deals with the processing of privacy concerns related to multi -feature data in the context of data recovery. We have developed an algorithm that regains lost or damaged files automatically without the need for user intervention. By simulating the approved data, we showed the wide application of our approach to realistic scenarios, ensuring restoration, integration, availability and privacy protection. PPCs-MAA algorithm provides an effective solution to recover lost data while maintaining data privacy. Using sensory pressure and multi -feature aid techniques, the algorithm ensures accurate restoration of data and privacy protection. The system also supports dynamic data and general auditing with the help of a third external auditor, ensuring transparency and trust. The algorithm provides additional benefits such as cost efficiency and data management, which makes it a practical solution to multiple applications.

However, there are some challenges and restrictions, such as the arithmetic burden resulting from the application of pressure and sensory assistance technologies, especially with large data groups. Future research needs to focus on improving the algorithm to reduce this burden. The system's ability to deal with tremendous data sizes and different types of files must be studied. The algorithm depends on a third external auditor for general audit, which raises some concerns related to performance and safety. Ways should be explored to reduce this accreditation.

Future research is expected to expand the system capabilities to support the types of audio and video files and various PDF files, which will enhance their applications in various fields. The system can be improved using new algorithms based on user reactions and realistic requirements. Additional safety measures can also be combined to enhance data protection, especially in sensitive environments. You should also search for ways to achieve data in actual time, which enhances the system response and benefit in vital applications.

In short, the PPCS-MA algorithm provides a strong and effective solution to recover data, processing accuracy and privacy fears. Using sensory pressure and multi -feature aid techniques, the algorithm determines a new standard for data recovery systems. Although there are some challenges, future research trends provide a clear path to improve and expand the capabilities of the system. This paper greatly contributes to the field of data recovery, providing practical solutions to realistic applications and paving the most developments.

## ACKNOWLEDGMENT

The author would like to thank Department of Computer Science, College of Medicine, University of Baghdad for supporting this work.

## REFERENCES

[1] Wei, T.H., Dutta, S., Shen, H.W. (2018). Information guided data sampling and recovery using bitmap indexing. In 2018 IEEE Pacific Visualization Symposium (PacificVis), Kobe, Japan, pp. 56-65. https://doi.org/10.1109/PacificVis.2018.00016

[2] Surbiryala, J., Rong, C. (2018). Data recovery and security in cloud. In 2018 9th International Conference on Information, Intelligence, Systems and Applications (IISA), Zakynthos, Greece, pp. 1-5. https://doi.org/10.1109/IISA.2018.8633640

[3] Zhang, J., Li, H. (2017). Research and implementation of a data backup and recovery system for important business areas. In 2017 9th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC), Hangzhou, China, 2: 432-437. https://doi.org/10.1109/IHMSC.2017.209

[4] Pandurang, G.H., Bhimrao, C.S., Chothe, P. (2016). Data recovery through indexing in cloud computing. In 2016 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, pp. 1-5. https://doi.org/10.1109/CESYS.2016.7889921

[5] Xie, K., Wang, L., Wang, X., Xie, G.G., Wen, J.G., Zhang, G.X., Cao, J.N., Zhang, D.F. (2018). Accurate recovery of internet traffic data: A sequential tensor completion approach. IEEE/ACM Transactions on Networking, 26(2): 793-806. https://doi.org/10.1109/TNET.2018.2797094

[6] Wang, J., Song, S., Zhu, X., Lin, X., Sun, J. (2016). Efficient recovery of missing events. IEEE Transactions on Knowledge and Data Engineering, 28(11): 2943-2957. https://doi.org/10.1109/TKDE.2016.2594785

[7] Patil, S., Rai, N. (2017). An efficient data integrity & data recovery with two TPAs in cloud data storage. In 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), Chennai, India, pp. 1301-1304. https://doi.org/10.1109/ICECDS.2017.8389654

[8] Chen, C., Zhang, M., Zhang, H., Huang, Z., Li, Y. (2018). Privacy-preserving sensory data recovery. In 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, pp. 1646-1650. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00243

[9] Edstrom, J., Chen, D., Gong, Y., Wang, J., Gong, N. (2019). Data-pattern enabled self-recovery low-power storage system for big video data. IEEE Transactions on Big Data, 5(1): 95-105. https://doi.org/10.1109/TBDATA.2017.2750699

[10] Kwon, D.H., Kim, M., Kim, S.G., Choi, W.Y. (2019). A 32-Gb/s PAM-4 quarter-rate clock and data recovery circuit with an input slew-rate tolerant selective transition detector. IEEE Transactions on Circuits and Systems II: Express Briefs, 66(3): 362-366. https://doi.org/10.1109/TCSII.2018.2855692

[11] Bae, S., Shin, Y. (2018). An automated system recovery using blockchain. In 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), Prague, Czech Republic, pp. 897-901. https://doi.org/10.1109/ICUFN.2018.8437040

[12] Clark, K., Ballani, H., Bayvel, P., Cletheroe, D., Gerard, T., Haller, I., Jozwik, K., Shi, K., Thomsen, B., Watts, P., Williams, H., Zervas, G., Costa, P., Liu, Z. (2018). Sub-nanosecond clock and data recovery in an optically-switched data centre network. In 2018 European Conference on Optical Communication (ECOC), Rome, Italy, pp. 1-3. https://doi.org/10.1109/ECOC.2018.8535333

[13] Saxena, S., Krishnapura, N. (2018). Tutorial T1C: High-speed serial links: Architectures and circuits for clock and data recovery (CDR). In 2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID), Pune, India, pp. xxxv-xxxvi. https://doi.org/10.1109/VLSID.2018.19

[14] Dhanujati, N., Girsang, A.S. (2018). Data center-disaster recovery center (DC-DRC) for high availability IT service. 2018 International Conference on Information Management and Technology (ICIMTech), Jakarta, Indonesia, pp. 55-60. https://doi.org/10.1109/ICIMTech.2018.8528170

[15] Tang, L., Gai, W., Shi, L., Xiang, X. (2017). A 40 Gb/s 74.9 mW PAM4 receiver with novel clock and data recovery. In 2017 IEEE International Symposium on Circuits and Systems (ISCAS), Baltimore, MD, USA, pp. 1-4. https://doi.org/10.1109/ISCAS.2017.8050226

[16] Guerrero, E., Sánchez-Azqueta, C., Gimeno, C., Aguirre, J., Celma, S. (2017). An adaptive bitrate clock and data recovery circuit for communication signal analyzers. IEEE Transactions on Instrumentation and Measurement, 66(1): 191-193. https://doi.org/10.1109/TIM.2016.2614745

[17] Beineke, K., Nothaas, S., Schoettner, M. (2017). Parallelized recovery of hundreds of millions small data objects. In 2017 IEEE International Conference on Cluster Computing (CLUSTER), Honolulu, HI, USA, pp. 621-622. https://doi.org/10.1109/CLUSTER.2017.48

[18] Bhattacharya, S., Roy, A., Sen, S., Debnath, N.C. (2017). Distributed data recovery architecture based on schema segregation. In 2017 IEEE International Conference on Industrial Technology (ICIT), Toronto, ON, Canada, pp. 1238-1243. https://doi.org/10.1109/ICIT.2017.7915540

[19] Seong, K., Lee, W.C., Kim, B., Sim, J.Y., Park, H.J. (2016). All-synthesizable transmitter driver and data recovery circuit for USB2.0 interface. In 2016 International SoC Design Conference (ISOCC), Jeju, Korea (South), pp. 63-64. https://doi.org/10.1109/ISOCC.2016.7799709

[20] Abadi, A., Haib, A., Melamed, R., Nassar, A., Shribman,

A., Yasin, H. (2016). Holistic disaster recovery approach for big data NoSQL workloads. In 2016 IEEE International Conference on Big Data (Big Data), Washington, DC, USA, pp. 2075-2080. https://doi.org/10.1109/BigData.2016.7840833

[21] Carolin, S.P., Somasundaram, M. (2016). Data loss protection and data security using agents for cloud environment. In 2016 International Conference on Computing Technologies and Intelligent Data Engineering (ICCTIDE'16), Kovilpatti, India, pp. 1-5. https://doi.org/10.1109/ICCTIDE.2016.7725349

[22] Kang, J., Lee, C. (2016). Digital clock data recovery circuit fot S/PDIF. 2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), Jeju, Korea (South), pp. 325-326. https://doi.org/10.1109/APCCAS.2016.7803965

[23] Zheng, W. (2016). Research of data storage mode and recovery method based on XFS file system. In 2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS), Beijing, pp. 369-372. https://doi.org/10.1109/ICSESS.2016.7883088

[24] Kharchenko, V.P., Kuzmenko, N.S., Kukush, A.G., Ostroumov, I.V. (2016). Multi-parametric data recovery for unmanned aerial vehicle navigation system. In 2016 4th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC), Kiev, Ukraine, pp. 295-299. https://doi.org/10.1109/MSNMC.2016.7783165

[25] Samavaty, B., Green, M.M. (2016). A half-rate 100 Gb/s injection-locked clock/data recovery circuit. 2016 14th IEEE International New Circuits and Systems Conference (NEWCAS), Vancouver, BC, Canada, pp. 1-4. https://doi.org/10.1109/NEWCAS.2016.7604811

[26] Kasmi, M., Aman, A., Asriany, A., Angriawan, R., Karma, K., Radi, A., Ilham, I., Yuliastuti, H., Sulkifli, S. (2023). Predictive analysis of the ornamental angelfish export market demand: An application of the least square method. Ingénierie des Systèmes d'Information, 28(3): 621-631. https://doi.org/10.18280/isi.280310

[27] Nizamuddin, M.K., Mohammad, A.A.K., Hashmi, S.S., HariKrishna, D., Anusha, M. (2024). Efficient routing in MANETs by optimizing packet loss. Ingénierie des Systèmes d'Information, 29(3): 961-968. https://doi.org/10.18280/isi.290316