INTERNATIONAL MULTI DISCIPLINARY JOURNAL FOR RESEARCH & DEVELOPMENT
eISSN 2394-6334 Impact factor: 7,854 Volume 13, issue 07 (2026)

# Reliable Information Preservation Strategy for Trusted Multi-Node Computing Repositories

**Dr. Valentina Rojas Méndez**
Department of Computer Science, Secure Cloud Database Systems, Andean Research Digital University

**Abstract:** The rapid expansion of distributed computing environments, cloud repositories, and multi-node data infrastructures has increased the importance of reliable information preservation strategies capable of ensuring data integrity, availability, security, and trust. Modern computing repositories increasingly manage heterogeneous and high-volume information generated from scientific applications, healthcare systems, financial platforms, remote sensing environments, and enterprise services. However, the distributed nature of these repositories introduces significant challenges related to unauthorized modification, data inconsistency, node failures, anomaly detection, and protection against malicious activities. This research examines reliable information preservation strategies for trusted multi-node computing repositories by analysing intelligent monitoring mechanisms, secure replication approaches, anomaly detection frameworks, and distributed data protection techniques.

The study adopts a conceptual analytical methodology based on the synthesis of existing research related to anomaly detection, cloud-based data processing, distributed repositories, artificial intelligence-based monitoring, and secure database protection. The research develops a framework that integrates information replication, intelligent anomaly identification, adaptive verification, and trusted repository management to improve reliability in multi-node computing environments.

The analysis demonstrates that effective information preservation requires a combination of computational intelligence and robust distributed storage mechanisms. Traditional preservation approaches based primarily on static backup and replication methods may not adequately address dynamic threats and complex operational failures. Intelligent anomaly detection techniques provide enhanced capabilities by identifying abnormal patterns and potential security risks before they affect repository reliability. Deep learning-based anomaly detection approaches demonstrate the potential of automated models in identifying complex deviations within large-scale datasets (Chalapathy & Chawla, 2019).

Furthermore, secure replication and protection mechanisms play a critical role in maintaining data consistency and availability across distributed cloud databases. Recent research on data replication and protection emphasizes the importance of structured mechanisms for improving reliability and security in distributed environments (Jatav & Avula, 2026). The proposed strategy integrates these principles with intelligent monitoring approaches to establish a trusted multi-node computing repository framework.

**Keywords:** Reliable Information Preservation, Multi-Node Computing, Distributed Repository, Data Replication, Anomaly Detection, Cloud Database Security, Artificial Intelligence, Trusted Computing, Information Integrity.

## 1. Introduction

### 1.1 Background

The growth of digital transformation has resulted in an unprecedented increase in the generation, storage, and processing of information. Modern organizations increasingly depend on distributed computing infrastructures where data is stored and processed across multiple interconnected nodes rather than centralized systems. Multi-node computing repositories have become essential components of cloud platforms, scientific data systems, healthcare information networks, and large-scale enterprise applications because they provide scalability, flexibility, and computational efficiency.

However, the transition from centralized storage models to distributed repositories has introduced new challenges regarding information preservation. In centralized environments, data management and protection mechanisms are

controlled through a limited number of systems, making monitoring and security management comparatively straightforward. In contrast, multi-node repositories involve numerous computing components operating simultaneously, creating complex relationships between storage reliability, communication efficiency, security mechanisms, and data consistency.

Reliable information preservation refers to the ability of a computing repository to maintain data accuracy, availability, confidentiality, and recoverability throughout its operational lifecycle. This concept extends beyond conventional backup strategies because modern repositories must protect information against multiple forms of disruption, including hardware failures, software errors, cyber threats, accidental modifications, and inconsistent synchronization among nodes.

The importance of intelligent preservation mechanisms has increased because modern repositories handle increasingly diverse and complex information sources. For example, remote sensing platforms generate large volumes of scientific data requiring efficient processing and reliable storage mechanisms. Research on remote sensing big data computing highlights the challenges associated with managing massive datasets, including computational scalability and efficient information processing (Ma et al., 2015). Similarly, cloud-enabled web processing services demonstrate the need for reliable infrastructure capable of supporting large-scale data operations (Chen et al., 2012).

Traditional preservation methods based mainly on periodic backups and simple replication strategies may not provide sufficient protection in dynamic computing environments. These approaches often lack the ability to detect abnormal behaviour, predict potential failures, or adapt to changing operational conditions. As a result, intelligent computing techniques such as artificial intelligence-based monitoring and anomaly detection have become increasingly important for improving repository reliability.

Anomaly detection represents a significant component of trusted information preservation because many security incidents and operational failures are preceded by unusual patterns. Machine learning and deep learning approaches can analyse large-scale data streams and identify deviations that may indicate threats or system failures. Chalapathy and Chawla (2019) highlighted the importance of deep learning approaches for anomaly detection, demonstrating how advanced computational models can improve identification of complex abnormal patterns.

## 1.2 Problem Statement

Although multi-node computing repositories provide significant advantages in scalability and availability, maintaining trust and reliability remains a critical challenge. Distributed architectures introduce multiple points of failure, where problems in individual nodes can affect overall system performance and information integrity.

One major challenge is maintaining consistent information across multiple nodes. Data replication is commonly used to improve availability, but improper synchronization mechanisms may result in conflicting versions, incomplete updates, or inconsistent information states. Therefore, reliable preservation requires intelligent coordination between replication strategies and verification mechanisms.

Another challenge involves detecting abnormal activities within large-scale repositories. Traditional security monitoring approaches often depend on predefined rules, which may fail to identify new or evolving threats. Intelligent anomaly detection models provide improved adaptability by learning patterns from existing data and identifying unexpected behaviour.

Security and privacy concerns further complicate information preservation. Distributed repositories may contain sensitive information requiring strong protection mechanisms. Without effective security frameworks, unauthorized access, data manipulation, and system compromise can reduce trust in computing infrastructures.

Recent research on secure distributed cloud databases emphasizes the importance of combining replication and protection mechanisms to maintain data reliability and security in distributed environments (Jatav & Avula, 2026). However, achieving complete trust requires integrating security, intelligence, and preservation techniques into a unified framework.

## 1.3 Research Relevance

Reliable information preservation has become a fundamental requirement for modern computing infrastructures because organizations increasingly depend on digital repositories for critical operations. The ability to maintain trustworthy

information directly affects operational continuity, decision accuracy, and system resilience.

The relevance of this research is strengthened by the increasing complexity of multi-node environments. As data volume and computational requirements continue to expand, conventional preservation approaches require enhancement through intelligent technologies. AI-based monitoring, adaptive replication, and automated anomaly detection provide opportunities to create more reliable computing repositories.

Research on unsupervised anomaly detection demonstrates the potential of intelligent models for identifying abnormal behaviour without requiring extensive labelled datasets (Ye et al., 2023). Such approaches are particularly valuable in distributed repositories where unknown threats and operational variations frequently occur.

## 2. Literature Review

### 2.1 Distributed Computing Repositories and Information Management Challenges

The development of distributed computing environments has transformed the way organizations store, process, and manage information. Multi-node repositories enable large-scale data management by distributing computational and storage responsibilities across interconnected systems. However, this distributed structure creates challenges related to data consistency, accessibility, security, and reliability.

Research on cloud-enabled processing systems highlights the importance of efficient information management mechanisms in large-scale computing environments. Chen et al. (2012) examined cloud computing-enabled web processing services for earth observation data processing and demonstrated the importance of scalable infrastructure for handling complex information workloads. Their work indicates that distributed repositories require efficient computational frameworks capable of maintaining performance while processing large volumes of data.

Similarly, remote sensing applications demonstrate the increasing complexity of modern information repositories. Ma et al. (2015) discussed challenges and opportunities associated with remote sensing big data computing, emphasizing issues related to data volume, computational requirements, and efficient processing methods. These challenges are applicable to various distributed repositories where large-scale information must be preserved while maintaining reliability and accessibility.

### 2.2 Data Replication and Protection Mechanisms in Trusted Repositories

Data replication represents one of the fundamental approaches for improving reliability in distributed computing environments. By maintaining multiple copies of information across different nodes, organizations can reduce the risk of data loss caused by hardware failure, network disruption, or system errors. However, effective replication requires appropriate synchronization, consistency management, and security protection.

Jatav and Avula (2026) examined data replication and protection mechanisms for secure distributed cloud databases, emphasizing the importance of structured approaches for maintaining information security and reliability. Their research highlights that replication alone is insufficient because replicated data must also be protected against unauthorized access, corruption, and inconsistency.

The integration of replication with intelligent monitoring creates stronger preservation strategies. While replication ensures availability, intelligent systems can evaluate repository conditions and identify situations where additional protection measures are required. This combination improves resilience by enabling proactive responses rather than relying only on recovery after failures occur.

### 2.3 Artificial Intelligence-Based Anomaly Detection

Anomaly detection has become an essential component of trusted computing environments because abnormal patterns often indicate security threats, system failures, or data integrity issues. Traditional detection approaches frequently depend on predefined rules and known patterns, limiting their ability to identify new and evolving risks.

Ahmed et al. (2016) surveyed anomaly detection techniques in the financial domain and demonstrated the importance of identifying unusual behaviours within complex information systems. Although their research focuses on financial applications, the underlying principles of detecting abnormal patterns are highly relevant to distributed repositories where unexpected activities may indicate security or operational problems.

Deep learning approaches have further improved anomaly detection capabilities by enabling systems to identify complex patterns from large datasets. Chalapathy and Chawla (2019) reviewed deep learning methods for anomaly detection and highlighted their ability to address challenges associated with high-dimensional data environments. These approaches provide significant potential for multi-node repositories because distributed systems generate continuous streams of operational information.

Unsupervised anomaly detection is particularly valuable in distributed environments because many emerging threats do not have previously identified examples. Ye et al. (2023) introduced an unsupervised anomaly detection approach, demonstrating the importance of adaptive models capable of identifying abnormal patterns without extensive labelled datasets. Such techniques can strengthen repository monitoring by detecting unknown risks.

2.4 Digital Repository Management and Scientific Data Preservation

Scientific and technological applications require specialized repositories capable of managing complex information types. Hyperspectral imagery and remote sensing data represent examples of large-scale scientific information requiring reliable preservation mechanisms.

Plaza (2011) explored content-based hyperspectral image retrieval using spectral unmixing techniques, demonstrating the importance of efficient information organization and retrieval within scientific repositories. The study highlights that preservation is not limited to storage but also includes accessibility and intelligent information management.

Similarly, Sevilla and Plaza (2014) developed a digital repository approach for hyperspectral imagery with retrieval functionality implemented through GPU-based processing. Their work illustrates how advanced computational methods can improve repository performance and usability. These approaches demonstrate that trusted repositories require both reliable storage mechanisms and intelligent processing capabilities.

The lessons from scientific repositories can be applied to broader multi-node computing environments. As organizations increasingly manage complex datasets, preservation strategies must support not only data survival but also efficient retrieval, analysis, and utilization.

2.5 Integrated Security and Trust Management

Trust in distributed computing repositories depends on multiple factors, including data integrity, availability, authentication, and system transparency. A repository cannot be considered reliable if information remains available but lacks protection against unauthorized modification.

The integration of artificial intelligence, replication mechanisms, and security controls creates opportunities for developing more comprehensive trust frameworks. Intelligent monitoring systems can continuously evaluate repository behaviour, while replication strategies ensure recovery capabilities during failures.

Jatav and Avula (2026) emphasized the importance of protection mechanisms in distributed cloud databases, supporting the need for combined approaches that address both availability and security. This perspective indicates that future repository architectures must move beyond isolated security solutions toward integrated preservation ecosystems.

Recent advancements in Semantic Artificial Intelligence have further improved trusted computing environments by enabling knowledge-driven decision intelligence and explainable reasoning. Goyal (2025) proposed a Semantic AI Infrastructure for Sustainable Decision Intelligence that integrates semantic knowledge representation with intelligent reasoning to improve transparency, contextual understanding, and reliable decision-making. Such semantic frameworks can strengthen trusted multi-node repositories by supporting intelligent monitoring, adaptive security policies, and interpretable repository management decisions.

2.6 Research Gap and Theoretical Positioning

Existing research provides valuable insights into cloud computing, anomaly detection, scientific repositories, and database protection. However, limited research has examined an integrated strategy specifically focused on reliable information preservation within trusted multi-node computing repositories.

Previous studies often address individual challenges separately. For example, anomaly detection research focuses on identifying abnormal patterns, while replication research emphasizes availability and recovery. However, real-world

distributed repositories require simultaneous management of security, reliability, and intelligent monitoring.

This research addresses this gap by proposing a conceptual framework that combines replication, protection mechanisms, and AI-based anomaly detection into a unified preservation strategy. The theoretical positioning of this study is based on the assumption that trust in multi-node repositories emerges from the interaction between data reliability, intelligent monitoring, and adaptive security mechanisms.

## 3. Methodology

3.1 Research Approach

This study adopts a conceptual analytical methodology based exclusively on the analysis of the provided literature. The objective is to develop a theoretical framework explaining how reliable information preservation can be achieved in trusted multi-node computing repositories.

The methodology synthesizes concepts from distributed computing, anomaly detection, cloud data management, artificial intelligence, and security protection. The selected studies provide technological foundations for understanding how different preservation mechanisms contribute to repository reliability.

3.2 Proposed Preservation Framework

The proposed framework consists of four integrated layers:

Data Management Layer:

This layer manages information storage, distribution, and replication across multiple computing nodes. Replication mechanisms ensure availability and reduce risks associated with node failure.

Protection and Verification Layer:

This component focuses on maintaining data integrity through authentication, consistency verification, and security mechanisms. It ensures that replicated information remains accurate and protected.

Intelligent Monitoring Layer:

Artificial intelligence-based anomaly detection techniques continuously analyse repository behaviour. Machine learning models identify unusual patterns that may indicate failures, security breaches, or abnormal operations.

Recovery and Adaptation Layer:

This layer enables repositories to respond to detected problems through automated recovery, synchronization, and optimization processes.

The proposed preservation framework can be further enhanced through Semantic AI techniques that organize repository knowledge using semantic relationships and intelligent reasoning. According to Goyal (2025), semantic decision infrastructures improve adaptive decision support by enabling contextual interpretation of repository events, thereby supporting more transparent and trustworthy information preservation.

3.3 Analytical Model

The conceptual model assumes that repository trust depends on three major factors: reliability, security, and intelligence.

Reliability is achieved through replication and fault tolerance mechanisms.

Security is maintained through protection strategies and integrity verification.

Intelligence is provided through adaptive monitoring and anomaly detection models.

The interaction among these components creates a resilient information preservation environment capable of responding

to dynamic operational challenges.

3.4 Methodological Limitations

The study is conceptual and does not include experimental validation using real-world datasets. Future research should evaluate the proposed framework through practical implementation in cloud platforms and distributed computing environments.

Additionally, intelligent preservation systems depend on data quality, computational resources, and algorithm transparency. These factors must be considered during implementation to ensure effective and trustworthy repository management.

## 4. Results

The analysis identifies that reliable information preservation in trusted multi-node computing repositories requires an integrated combination of distributed storage mechanisms, intelligent monitoring, and adaptive security strategies. The findings indicate that traditional preservation methods based only on replication or backup mechanisms are insufficient for modern computing environments where repositories face dynamic operational and security challenges.

The first major finding is that data replication remains a fundamental component of information reliability. Distributed repositories require multiple information copies to maintain availability during node failures, communication disruptions, or hardware problems. However, the analysis shows that replication effectiveness depends on synchronization accuracy, consistency management, and protection mechanisms. Replication without adequate verification may create multiple versions of inaccurate or compromised information. Research on secure distributed cloud databases emphasizes that replication and protection must operate together to ensure reliable information management (Jatav & Avula, 2026).

The second finding demonstrates the importance of artificial intelligence-based anomaly detection for maintaining repository trust. Multi-node computing environments continuously generate operational data, making manual monitoring inefficient. Intelligent anomaly detection models can analyse system behaviour, identify unusual patterns, and provide early warnings regarding potential failures or security threats. Deep learning approaches improve this capability by recognizing complex relationships within high-dimensional datasets (Chalapathy & Chawla, 2019).

The third finding indicates that unsupervised learning approaches provide significant advantages for trusted repository management. Distributed computing environments frequently encounter unknown threats and unexpected operational conditions for which predefined detection rules may be ineffective. Unsupervised anomaly detection methods allow systems to identify deviations without requiring extensive labelled datasets. This capability strengthens repository resilience by enabling detection of previously unidentified risks (Ye et al., 2023).

The analysis also reveals that information preservation extends beyond storage reliability. Modern repositories require intelligent retrieval, processing, and accessibility mechanisms. Studies involving scientific repositories demonstrate that effective information management requires computational approaches capable of organizing and processing complex datasets. Research on hyperspectral image repositories highlights the importance of combining storage capabilities with intelligent retrieval functionality to improve usability and efficiency (Plaza, 2011; Sevilla & Plaza, 2014).

Another important finding concerns scalability challenges. As information volumes continue to increase, distributed repositories must maintain performance while managing growing computational requirements. Research on remote sensing big data computing demonstrates that large-scale information environments require advanced processing frameworks capable of addressing data complexity and computational demands (Ma et al., 2015).

The findings further indicate that cloud-based computing environments require flexible preservation architectures. Cloud-enabled processing services demonstrate the importance of scalable infrastructure for supporting complex data operations. Effective preservation strategies must therefore combine computational efficiency with reliability and security mechanisms (Chen et al., 2012).

However, the analysis identifies several limitations. Intelligent preservation systems require significant computational resources and high-quality operational data. Complex machine learning models may also create transparency challenges because system administrators may find it difficult to interpret automated decisions. Additionally, implementing comprehensive preservation frameworks can increase infrastructure complexity and operational costs.

Overall, the results demonstrate that trusted multi-node computing repositories require a holistic preservation approach. The combination of secure replication, intelligent anomaly detection, adaptive monitoring, and recovery mechanisms provides stronger protection against data loss, system failures, and emerging threats. The findings support the development of future repository architectures where intelligence and security are integrated into fundamental information preservation processes.

## 5. Discussion

The findings highlight that reliable information preservation in multi-node computing repositories is becoming an increasingly complex challenge requiring integration between distributed computing principles and intelligent technologies. The traditional view of preservation as a simple storage and backup problem is insufficient for modern environments where data reliability depends on security, adaptability, and continuous monitoring.

A significant theoretical implication of this research is the expansion of the concept of repository trust. In distributed computing environments, trust is not created only through availability of information but through the combination of integrity, consistency, security, and intelligent management. A repository that can store large volumes of data but cannot detect unauthorized changes or operational anomalies cannot provide complete reliability.

The findings support previous research on anomaly detection, which demonstrates that intelligent models improve the identification of abnormal patterns within complex datasets. Ahmed et al. (2016) emphasized the importance of anomaly detection techniques in identifying irregular behaviours, while Chalapathy and Chawla (2019) demonstrated the effectiveness of deep learning approaches for complex anomaly identification. These concepts are particularly relevant to multi-node repositories where operational behaviour continuously changes.

The research also confirms the importance of combining replication with protection mechanisms. Replication improves availability, but without security controls it may reproduce damaged or unauthorized information across multiple nodes. Therefore, preservation strategies must ensure that data copies are not only available but also trustworthy. Jatav and Avula (2026) emphasized the importance of secure replication and protection mechanisms for distributed cloud databases, supporting the need for integrated approaches.

Another limitation involves algorithmic transparency. Automated anomaly detection systems may identify potential risks but may not always provide clear explanations for their decisions. In critical computing environments, administrators require understandable information to verify system recommendations and take appropriate actions.

Semantic AI-based decision infrastructures provide an additional layer of transparency by combining knowledge representation with explainable reasoning. Goyal (2025) demonstrated that semantic intelligence enables AI systems to generate interpretable and context-aware decisions, which can improve administrator trust and support reliable management of distributed computing repositories.

The discussion also highlights the importance of adaptive security approaches. Distributed repositories face evolving threats that cannot always be addressed through fixed security mechanisms. Intelligent systems provide opportunities for continuous learning and adaptation, allowing repositories to respond more effectively to changing conditions.

The role of human oversight remains essential despite technological advancements. Intelligent preservation systems should support administrators rather than completely replace human decision-making. Effective repository management requires combining computational intelligence with organizational policies, security practices, and expert evaluation.

Overall, the research demonstrates that reliable information preservation requires a multidimensional strategy integrating replication, security, anomaly detection, and adaptive intelligence. Future computing repositories will increasingly depend on such integrated frameworks to maintain trust, resilience, and operational continuity.

## 6. Conclusion

The rapid growth of distributed computing environments has created a critical need for reliable information preservation strategies capable of maintaining trust across multi-node repositories. This research examined how intelligent monitoring, secure replication, anomaly detection, and adaptive protection mechanisms can contribute to the development of trustworthy computing infrastructures.

The study demonstrates that information preservation in modern repositories requires a comprehensive approach that

extends beyond traditional storage and backup methods. Multi-node environments introduce complex challenges involving data consistency, security threats, operational failures, and increasing information volumes. Addressing these challenges requires integration between distributed computing technologies and intelligent analytical methods.

The proposed conceptual framework emphasizes four essential components: reliable data management, protection and verification mechanisms, intelligent anomaly detection, and adaptive recovery processes. Together, these components create a resilient preservation architecture capable of maintaining information integrity and availability under changing operational conditions.

The findings indicate that artificial intelligence-based anomaly detection provides significant benefits by identifying abnormal patterns and potential risks before they negatively affect repository performance. Deep learning and unsupervised detection approaches offer improved capabilities for handling complex and previously unknown threats. At the same time, secure replication mechanisms remain essential for ensuring information availability and recovery.

The research also highlights that trustworthy repositories require a balance between automation and human oversight. While intelligent systems improve monitoring and decision support, effective governance, security policies, and expert evaluation remain necessary for responsible implementation.

Future repository preservation frameworks may incorporate Semantic AI infrastructures to improve intelligent knowledge management, explainable decision support, and sustainable trust in distributed computing environments (Goyal, 2025).

The contribution of this research lies in presenting an integrated perspective on reliable information preservation for trusted multi-node computing repositories. It connects concepts from distributed computing, artificial intelligence, cloud security, and data management to explain how future repositories can achieve greater resilience.

Future research should focus on empirical evaluation of intelligent preservation frameworks using real-world distributed computing environments. Additional studies may explore explainable anomaly detection, autonomous recovery systems, and energy-efficient preservation strategies. As digital infrastructures continue to expand, reliable information preservation will remain a fundamental requirement for secure and trustworthy computing ecosystems.

## References


**1.** Ahmed, M., A. N. Mahmood, and M. R. Islam, “A survey of anomaly detection techniques in financial domain,” Future Generation Computer Systems, vol. 55, pp. 278–288, 2016.

**2.** Ajitha, P., “Artificial intelligence based anomaly detection in patient health monitoring using ensemble learning methods,” in Proceedings of the 1st International Conference on Artificial Intelligence, Communication, IoT, Data Engineering and Security, IACIDS 2023, 23–25 November 2023, Lavasa, Pune, India, 2024.

**3.** Chalapathy, R. and S. Chawla, “Deep learning for anomaly detection: A survey,” arXiv preprint arXiv: 1901.03407, 2019.

**4.** Chen Z, Chen N, Yang C, Cloud Computing Enabled Web Processing Service for Earth Observation Data Processing. IEEE Journal of Selected Topics in Applied Earth Observations & Remote Sensing, pp. 1637–1649, 2012.

**5.** D. S. Jatav and C. S. Reddy Avula, "Data Replication and Protection Mechanism for Secure Distributed Cloud Databases," 2026 2nd International Conference on Big Data & Machine Learning (ICBDML), Bhopal, India, 2026, pp. 1-6, doi: 10.1109/ICBDML68582.2026.11544812.

**6.** Ma Y, Wu H, Wang L, Remote sensing big data computing: Challenges and opportunities. Future Generation Computer Systems, pp. 47–60, 2015.

**7.** Plaza, A. J., Content-based hyperspectral image retrieval using spectral unmixing. Proceedings of SPIE-The International Society for Optical Engineering, pp. 17, 2011.

**8.** Sevilla, J. and Plaza, A., A New Digital Repository for Hyperspectral Imagery With Unmixing-Based Retrieval Functionality Implemented on GPUs. IEEE Journal of Selected Topics in Applied Earth Observations &

Remote Sensing, pp. 2267–2280, 2014.

**9.** K. K. Goyal, "Semantic AI Infrastructure for Sustainable Decision Intelligence," 2025 8th International Conference on Informatics and Computational Sciences (ICICoS), Semarang, Indonesia, 2025, pp. 434-439, doi: 10.1109/ICICoS68590.2025.11329920.

**10.** Ye, H., Liu, Z., Shen, X., Cao, W., Zheng, S., Gui, X., Zhang, H., Chang, Y., and Bian, J., "Uadb: Unsupervised anomaly detection booster," arXiv preprint arXiv: 2306.01997, 2023.