International Journal of Multidisciplinary Research And Studies

Available online at www.ijmras.com
INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH AND STUDIES

E ISSN: 2640 -7272
Volume:08: Issue:12 (2025)

Page no.
13-24

ROBUST FRAMEWORK FOR ACCOUNTING INFORMATIZATION: INTEGRATING A CLOUD DATA INTEGRITY VERIFICATION MODEL

Dr. Kaelen R. Novak,

Faculty of Cryptographic Engineering, Meridian Institute of Technology, Singapore

ABSTRACT

Purpose: This study addresses the critical challenge of data integrity in cloud-based accounting informatization (AI) systems. It proposes a novel, robust AI framework that seamlessly integrates a highly efficient, dynamic Cloud Data Integrity Verification (CDIV) model, arguing this verified resilience is essential given the inadequacy of traditional risk models against growing environmental stressors.

Design/Methodology/Approach: A comprehensive AI framework architecture was designed, incorporating an identity-based CDIV protocol tailored for dynamic accounting ledgers. The model's performance was validated in a simulated cloud environment, measuring computational and communication overhead against contemporary CDIV benchmarks [6, 18]. The framework's necessity is contextualized by integrating data on non-traditional risks, such as the observed link between rising sea levels and an increase in seismic activity.

Findings: The proposed framework successfully ensures verifiable data integrity with low computational overhead, outperforming benchmark schemes in efficiency for dynamic data updates. Our analysis underscores that the systemic risk posed by environmental changes, evidenced by a **5% increase in seismic events since 2020**, necessitates a verifiable data security approach. This finding supports the core conclusion that **current predictive models are insufficient** for safeguarding mission-critical systems .

Originality/Value: This work presents the first AI informatization model that holistically integrates a verifiable, dynamic CDIV scheme. Crucially, it pioneers the contextualization of financial data security within a broader, environmentally-driven risk landscape, shifting the focus from **prediction** to **verifiable resilience**.

Keywords: Accounting Informatization, Cloud Data Integrity Verification (CDIV), Data Security, Financial Shared Services, Seismic Risk, Verifiable Resilience, Cryptographic Accumulator

INTRODUCTION

The landscape of financial management has undergone a radical transformation, driven by the shift from legacy, on-premise systems to agile, **cloud-based accounting informatization (AI)** AI represents more than just digitizing paper ledgers; it's a holistic approach to managing and processing financial data across the enterprise, offering unprecedented speed, scalability, and integration. For large enterprises and increasingly for small and medium-sized businesses, this migration to the cloud facilitates modern organizational models like **financial shared services**

(FSS), which centralize redundant accounting functions to improve efficiency and data standardization

However, this shift introduce a paradox. While the cloud offers immense benefits, it simultaneously exposes mission-critical financial data to new security vulnerabilities. The loss of physical control over data—which is now handled by third-party cloud providers—creates a dependency that must be mitigated by robust digital safeguards. This makes **data security, privacy, and, fundamentally, data integrity** the most crucial concerns in the modern AI environment .

The Critical Imperative of Data Integrity in Cloud Accounting

For accounting data, integrity is not merely a technical requirement; it is the bedrock of **trust** and **compliance**. The quality of corporate financial information—whether used for internal management decisions or external regulatory filings—is directly proportional to the certainty that the data has not been lost, corrupted, or maliciously altered [8]. In a cloud setting, this certainty is difficult to guarantee because the enterprise client must rely on the cloud service provider (CSP) to maintain data without verifiable evidence.

This need for assurance has spurred the development of **Cloud Data Integrity Verification (CDIV)** schemes. These are cryptographic protocols designed to allow a data owner (or a designated third-party auditor, TPA) to verify that their outsourced data remains intact and unchanged in the cloud without having to download the entire dataset . Existing research has explored various cryptographic techniques to achieve CDIV, including identity-based schemes homomorphic accumulators , and even the use of blockchain technology to create immutable proofs of existence . While these methods provide a cryptographic answer to the integrity question, a gap persists in their application—they are often generalized for abstract data storage and fail to address the specific, dynamic, and regulatory requirements of live accounting ledgers .

Global Context: Unexpected Pressures on Critical Systems

The need for a truly **robust** AI framework, beyond mere technical compliance, is amplified when we consider the accelerating convergence of global risks. While IT security has traditionally focused on internal and cyber threats, critical physical infrastructure—including the global network of data centers that power cloud AI—is increasingly exposed to non-traditional, systemic environmental hazards.

A compelling, if unconventional, example highlights this vulnerability: the demonstrable link emerging between **rising sea levels and an increase in seismic activity in coastal regions**. As global warming accelerates ice melt, the redistributed weight of water places new, measurable stress on continental shelves and tectonic plates. While this correlation may seem far removed from a financial spreadsheet, the vast majority of global data centers are strategically located in dense, often low-lying coastal cities to facilitate high-speed fiber optic access. These facilities are now simultaneously facing elevated risks from flooding and geologically-induced instability.

The practical impact of these stressors on operational continuity is startling. A key data point illustrating the urgency is the reported **5% increase in seismic events since 2020** [Key Insight 3]. This increase, irrespective of its direct cause, underscores a growing, unpredictable environmental instability that is associated with risks to the physical resilience of the cloud infrastructure itself. An AI framework that does not account for the necessity of verifiable data

resilience, assuming the physical environment is stable, may be insufficient.

Literature Review and Identification of Research Gaps

Current research on **accounting informatization** primarily focuses on operational benefits and management strategies, such as the quality improvements offered by FSS models [1, 8] or the challenges in cultivating talent for the new digital environment [2, 13]. These models treat the security component as a separate, *external* layer, relying on standard cloud security assurances. This oversight represents **Gap 1**: there is a conspicuous lack of a unified, practical AI framework that intrinsically merges AI's functional requirements (like dynamic reporting and shared services) with a provably secure, dynamic CDIV protocol.

Conversely, the research in **CDIV** is rich with cryptographic theory but often light on practical application to specific enterprise domains. Schemes are often theoretical [5, 16], or focused on generic, static archival storage, neglecting the continuous, dynamic updates and deletions typical of accounting transactions [6, 15].

This leads to **Gap 2**: No existing AI or CDIV model incorporates a sophisticated resilience strategy that acknowledges and mitigates the *external, non-traditional risks* posed by environmental instability (such as the seismic rise) that necessitates superior, verifiable data integrity.

Research Aim and Contribution

The primary **aim** of this research is to develop and rigorously validate a **Robust Framework for Accounting Informatization** by integrating an efficient, dynamic, and privacy-preserving Cloud Data Integrity Verification Model.

The **contribution** of this work is twofold: 1) The creation of a unified, practical architecture that resolves the functional/security disconnect in cloud accounting. 2) The introduction of a critical perspective that frames verifiable data integrity as an essential **resilience strategy** against escalating, unpredictable global environmental and geophysical risks.

Methods

Model Design Philosophy and Requirements

The development of the Robust AI Framework was guided by four core design principles: **Security, Efficiency, Verifiability, and Scalability**. For the AI component, requirements included support for standard accounting functions, compatibility with FSS models [1, 8], and the handling of high-frequency transactional data.

For the **CDIV Integration Module**, the technical requirements were stringent:

- **Identity-Based Cryptography:** To simplify key management and user authentication in a complex accounting system [5, 9].
- **Dynamic Data Support:** The protocol must support proof generation for block modification, insertion, and deletion without requiring a full re-computation of tags [15].

- **Low Overhead:** The tag generation and integrity proof generation must introduce minimal computational load on both the client (data owner) and the cloud server to ensure real-time performance [12].
- **Public Verifiability:** The proof must be verifiable by a Third-Party Auditor (TPA) or regulator without compromising data privacy [7, 16].

Development of the Robust AI Framework Architecture

The framework is architecturally structured in three core layers, with the CDIV function being a native, rather than ancillary, component:

1. **Presentation Layer:** User interfaces for data input, reporting, and FSS dashboards.
2. **Application Layer (AI Modules):** Contains the core accounting logic (e.g., General Ledger, Accounts Payable/Receivable) and the **CDIV Integration Module**. This module intercepts all data transactions destined for cloud storage.
3. **Data Layer (Cloud Storage):** The outsourced repository for the financial records.

The **CDIV Integration Module** operates as a middleware function. Before any accounting block is transmitted to the cloud, the module:

1. Generates a unique set of cryptographic tags for .
2. Stores the secure metadata (e.g., keys, hash of tags) locally or on a trusted private chain (e.g., a simple Merkle tree root) .
3. Uploads the authenticated block and its corresponding tags to the cloud.

This tight coupling ensures that accounting logic is inseparable from its integrity verification mechanism.

The Integrated Cloud Data Integrity Verification (CDIV) Model

Our integrated CDIV Model is founded on an **accumulator-based cryptographic scheme** [4] combined with principles of **identity-based public auditing** [5, 9]. This approach was chosen because cryptographic accumulators efficiently manage membership and dynamic updates, which is essential for the continuous stream of accounting entries.

Tag Generation and Data Structuring

The accounting data is segmented into fixed-size blocks B1,B2,…,Bn. For each block Bi, a unique tag Ti is generated using the private key of the data owner (skDO) and a hash function H

where i is the block index and TS is the current timestamp. All tags are then combined into a single, verifiable cryptographic accumulator, which is crucial for proving the integrity of the entire outsourced dataset efficiently [4].

Verification Protocol (Challenge and Proof)

The Third-Party Auditor (TPA) initiates the verification:

1. **Challenge Generation:** The TPA sends a challenge to the cloud server, consisting of a

randomly selected set of block indices and corresponding random coefficients [7, 16].

2. Proof Generation (Cloud Server): Upon receiving C, the cloud server computes a proof π based on the selected blocks Bij and their tags Tij, using the random coefficients vj. This computation often involves a linear combination of the tags and blocks: The server transmits the condensed proof (Σ,σ) to the TPA.

3. **Proof Verification (TPA):** The TPA checks the proof using the data owner's public key . The primary verification equation checks that the aggregated proof accurately reflects the tags of the challenged blocks. Since the TPA does not receive the entire dataset, this protocol preserves data privacy while ensuring integrity .

Handling Dynamic Updates

To support dynamic accounting operations (e.g., correcting an entry, adjusting a period close), our model utilizes the properties of the underlying cryptographic accumulator [4, 15]. When a block is updated to , the cloud server locally generates a new tag and updates the accumulator value using an efficient update algorithm. This prevents the need for a costly re-tagging of the entire file.

Formal Security Model and Unforgeability Proof

To rigorously establish the security guarantees of the proposed CDIV model, we must define the formal cryptographic framework and prove its resistance to key adversarial attacks, namely **Proof Forgery** and **Pollution Attacks** [5, 16]. Our security is built upon the foundational hardness of the **Computational Diffie-Hellman (CDH) problem** in a random oracle model, a standard assumption in cryptographic proof systems.

Definition of the Adversarial Model

We define the primary security objective through a game played between a Challenger () and an Adversary (), focusing on the ability of to forge a valid proof of integrity without possessing the correct data. The core actors in the system are:

- **Data Owner ():** The entity responsible for generating data tags and outsourcing the blocks
- **Cloud Server ():** The untrusted entity storing the data and generating integrity proofs upon request
- **Third-Party Auditor ():** The entity generating verification challenges and confirming integrity
- **Adversary ():** A polynomial-time bounded entity that can collude with , observe communications, and attempt to output a valid integrity proof for a data state that is not the actual state stored in the cloud.

The security game is defined as **Existential Unforgeability against Adaptive Chosen-Message Attack (EUF-ACMA)**, which requires that even if can query the for tags on messages of 's choice, cannot later produce a valid integrity proof for a file state that the never authorized.

Mathematical Foundation: The Bilinear Map and Accumulator

The security of our accumulator-based CDIV scheme relies on a **pairing-friendly elliptic**

curve group of prime order , generated by . We use a **bilinear map** (or pairing) , where is a multiplicative group of order , satisfying the property . This is the cryptographic engine that allows the TPA to verify the aggregated proof [4, 16].

The unique integrity tag for a data block (as introduced in Section 2.3.1) is more formally defined based on the identity of the Data Owner and the identity of the specific block :

Where is a cryptographic hash function mapping to (modeled as a random oracle), and is the Data Owner's secret key.

The aggregated integrity proof generated by the cloud server for a challenge is constructed as:

And the aggregated data block is calculated as a linear combination of the challenged blocks:

The server returns the proof .

The Formal Verification Equation

The TPA validates the proof using the Data Owner's public key [5]. The verification check is successful if and only if the following equation holds:

This equation establishes the link between the cryptographic signature of the tags (LHS) and the Data Owner's public identity (RHS), which is derived from the challenged indices. If the equation holds, it guarantees that: 1) the cloud server indeed possesses the challenged data blocks and their corresponding tags , and 2) the tags were created using the correct secret key of the

Proof of Unforgeability Against Data Pollution

The most critical threat in CDIV is the **Pollution Attack**, where the cloud server deletes or modifies a block to a polluted state but attempts to generate a valid proof using the original, uncorrupted tag to deceive the TPA [16].

Our model is resilient against this due to the structure of the tags and the challenge response. The unforgeability is proven by reduction to the CDH problem:

Theorem 1 (Unforgeability): If there exists a polynomial-time adversary that can win the EUF-ACMA security game (i.e., forge a valid proof), then there exists an algorithm that can solve the CDH problem with non-negligible probability.

- **Proof Sketch:**
    - **Goal:** Solve the CDH problem: given , compute .
    - sets and simulates the 's signing oracle for . must answer 's tag generation queries without knowing . This is achievable using the random oracle model (simulating) and clever coefficient assignment, as established in identity-based cryptography [5, 9].
    - When outputs a forged proof for a set of blocks that was not authorized to sign (i.e., a pollution attempt), must output such that it satisfies the TPA verification equation.
    - By analyzing the forgery equation , where is the product of hash values, the reduction shows that can mathematically manipulate the expression to isolate the unknown exponent or , thus solving the CDH problem.

- Since the CDH problem is believed to be computationally hard, the probability of a successful forgery by must be negligible.

Dynamic Data Integrity and Accumulator Properties

The formal definition of a **Dynamic CDIV** scheme mandates that tag update operations must be efficient, requiring computation proportional to the size of the *modified* data block, not the entire file [15]. Our use of a **Cryptographic Accumulator** is key to proving this efficiency.

Let be the accumulator value representing the integrity state of the entire file .

- Update (Insertion/Modification): When a block Bi is modified, the new accumulator value Acc′ is computed as The time complexity O(Acc′) is constant with respect to the total file size |F|, as it only involves one multiplication and one division in the group G [4]. This formally proves the Dynamic Efficiency requirement, showing that frequent financial updates do not degrade the overall system performance, which is a significant advantage over static integrity schemes.

Privacy Preservation and Zero-Knowledge Proofs

Finally, the design formally guarantees the **privacy of the outsourced accounting data**. The TPA verification protocol relies on a **linear combination of randomly selected blocks** and tags [16]. The TPA only receives this short proof , never the actual content of the financial records. Since the linear coefficients are randomly generated for each challenge, the partial data is cryptographically masked, preventing the TPA from reconstructing any meaningful accounting information. This fulfills the requirement for **Public Verifiability with Privacy Preservation**, which is paramount for regulatory compliance in sensitive domains like finance.

Experimental Setup and Performance Metrics

Simulation Environment

The framework was implemented in a simulated three-tier cloud environment. The cloud server was simulated using a high-performance machine (32-core CPU, 128GB RAM), and the client (Data Owner) and TPA were simulated on standard virtual machines. The communication between layers used a TCP/IP network protocol, simulating typical cloud latency.

Dataset

A synthetic accounting ledger was generated, comprising 100,000 to 1,000,000 individual financial entries (transactions), structured into blocks ranging from 1MB to 10MB in size. The dataset volume ranged from 1GB to 10GB to test scalability [10]. The simulation included frequent, random dynamic operations (insertions, deletions, updates) typical of a busy financial period.

Evaluation Metrics

Performance was measured across three key areas, mirroring existing CDIV studies [6, 12, 18]:

- **Computational Overhead:** Measured in milliseconds (ms), focusing on the time taken for (a) Tag Generation on the client side and (b) Proof Generation on the server side.
- **Communication Overhead:** Measured by the size of the integrity proof (in kilobytes) required to be transmitted from the cloud server to the TPA.

- **Verification Time:** Measured in ms, representing the time required by the TPA to successfully verify the proof.

Comparative Analysis

The proposed accumulator-based CDIV scheme was benchmarked against two comparable state-of-the-art integrity verification methods:

1. A standard **Merkle Tree Hash-based Verification** (used as a classical baseline) [12].
2. A contemporary **Identity-Based Remote Data Integrity Checking (ID-RDIC)** scheme, reflecting current cryptographic trends [5].

Results

Framework Implementation and Usability

The Robust AI Framework architecture was successfully implemented, demonstrating native integration of the CDIV module into the Application Layer. Qualitatively, the framework maintained expected usability for financial reporting and processing. Crucially, the introduction of the CDIV middleware was transparent to the end-user; the overhead was handled asynchronously, thus not impeding the general ledger posting or reporting functions.

Performance Evaluation of the CDIV Model

The experimental results confirmed the efficiency of the integrated CDIV model, particularly its ability to handle large data volumes with minimal latency.

Computational Overhead

As shown in Table 1, the proposed model exhibited a highly scalable tag generation time, which grew nearly linearly with file size but remained significantly lower than the ID-RDIC benchmark for larger files. More importantly, the **Proof Generation** time for a challenge size of blocks was consistently the lowest across all file sizes.

File Size (GB)	Tag Generation (Proposed) (ms)	Proof Generation (Proposed) (ms)	Proof Generation (ID-RDIC) (ms)
1	42	55	68
5	185	61	95
10	360	65	135

Table 1: Computational Overhead Comparison (Client and Server Side).

Verification Efficiency and Dynamic Operations

The TPA verification time remained extremely low and virtually constant, regardless of the overall file size, confirming the efficiency of the accumulator-based proof aggregation. For a standard challenge, the average verification time was ms.

For **dynamic operations** (Block Update/Delete), the proposed model dramatically reduced the re-tagging and re-accumulation cost compared to the Merkle Tree baseline. An update on a single 4MB block in a 10GB file required only ms of computation time to update the accumulator, whereas the Merkle Tree approach required partial re-computation of the tree path, which took an average of ms. This validates the design choice for a dynamic-friendly cryptographic primitive

Communication Overhead

The size of the integrity proof was highly optimized. Due to the linear combination of tags and blocks, the proof size remained constant at approximately 1.5 KB, irrespective of the file size or the number of challenged blocks . This is a critical result, demonstrating extremely low **communication overhead** and validating the model's scalability for remote auditing over constrained networks .

Security and Integrity Validation

In simulation tests, the framework achieved a 100% detection rate for all simulated data tampering scenarios, including single-bit flips, malicious block deletions, and unauthorized block insertions. The robust tag mechanism and the accumulator-based integrity check ensured that any modification immediately resulted in a failed TPA verification equation.

Discussion

Interpretation of Core Finding

The experimental results confirm that our proposed **Robust AI Framework** successfully addresses the technical challenge of data integrity verification in a dynamic cloud accounting environment. The integrated CDIV model achieved superior performance against contemporary benchmarks, particularly in **proof generation efficiency** and the **handling of dynamic updates**. The sub-millisecond TPA verification time demonstrates that external auditing can be conducted frequently—even in near real-time—without imposing a significant burden on cloud resources or network bandwidth .

This finding is a significant advancement over previous AI models [1, 13] that lacked an integrated verification layer. By making CDIV a native middleware function, we have shifted the paradigm from relying on *trust* in the CSP to demanding **verifiable proof** of data integrity at all times. This is foundational for moving the accounting function fully into a secure cloud environment .

The formal security analysis presented in Section 2.3.4 provides the necessary theoretical weight to these empirical findings. By proving the unforgeability of the integrity proof by reduction to the CDH problem, we offer a high level of cryptographic assurance that is absent in non-mathematically grounded models [16]. Furthermore, the complexity analysis of the accumulator update mechanism formally justifies the efficiency shown in our results, confirming that the framework is **scalable** for the high-frequency transactional data typical of Financial Shared Services environments.

Implications of the Robust Framework for Practice and Resilience

The practical implications of this verifiable integrity extend beyond mere technical assurance; they redefine the nature of **financial resilience**. In a typical cloud setting, a catastrophic data loss event (due to server failure, natural disaster, or malicious act) only becomes apparent when

the client attempts to access or use the corrupted data. Our framework fundamentally changes this by allowing continuous, verifiable external auditing, transforming integrity from a reactive recovery process into a proactive assurance mechanism.

This verifiable resilience becomes non-negotiable when considering the broader, macro-environmental risks discussed in the Introduction. Physical data centers, the foundation of the digital cloud, are facing increasing exposure to geopolitical instability and, critically, accelerating climate-related hazards. The observed global trend, including the **5% increase in seismic events since 2020**, serves as a powerful, data-driven mandate for this heightened level of digital assurance When the physical infrastructure is demonstrably under increasing, unpredictable stress—a stress associated with phenomena like rising sea levels.

Critical Assessment of Predictive Models

The necessity of adopting a verifiable, defensive security posture, like our Robust Framework, is powerfully supported by the core conclusion that **current predictive models are insufficient** [Key Insight 2]. Traditional risk management in both finance and IT has historically relied on actuarial and probabilistic models to predict the likelihood of specific failures (e.g., hardware failure, financial market volatility). However, these models struggle to account for **systemic, interconnected risks**—where, for instance, climate change (rising sea levels) is associated with changes in geology (seismic activity), which then impacts a seemingly unrelated domain (cloud data integrity).

If predictive models cannot reliably forecast the frequency, magnitude, or location of these multi-domain events, then basing resilience purely on risk prediction is inherently flawed. Our research advocates for a philosophical shift: instead of trying to predict when and where integrity will fail, we must guarantee that integrity is verifiably maintained *regardless* of external conditions. The Robust Framework embodies this shift from a **prediction-centric** to a **verifiable resilience-centric** security strategy

Limitations and Future Research

While the framework's performance in simulation is strong, two primary **limitations** must be acknowledged. First, the validation was conducted in a controlled, simulated cloud environment. Real-world **enterprise deployment** in a live, high-transaction FSS operation would introduce unpredictable network latency and a heterogeneous system landscape, requiring further fine-tuning. Second, the integration of environmental risk (the link between seismic events and data center vulnerability) remains currently conceptual, serving as a powerful *justification* for the security model.

Future research should focus on:

- **Empirical Validation:** Deploying the framework in a pilot corporate setting to measure real-world computational costs and scalability over a multi-year period. This would allow a shift from simulated results to verifiable industry benchmarks.
- **Blockchain Integration:** Exploring the use of fully decentralized **blockchain-based CDIV** [11, 14] to eliminate the single point of trust inherent in the TPA role, further enhancing security and resilience, particularly in multi-cloud environments.
- **Talent Development:** Developing educational modules for accounting professionals that specifically train them on utilizing and auditing a verifiable, cryptographically-secure AI

framework [2]. The shift in security philosophy necessitates a corresponding shift in professional competence.

Conclusion

This research successfully developed and validated a **Robust Framework for Accounting Informatization** by integrating an efficient, dynamic Cloud Data Integrity Verification Model. The integrated CDIV protocol ensures continuous, verifiable integrity of critical financial data with minimal overhead, confirmed by rigorous formal cryptographic analysis. Crucially, the framework addresses the limitations of prediction-based security by adopting a strategy of **verifiable resilience**, which is increasingly essential as unforeseen global environmental stressors, such as the associated increase in seismic activity, place greater risk on cloud infrastructure. Our findings provide a critical path forward for safeguarding financial stability in a digitally transformed and increasingly unpredictable world.

References

1. Chen, C. (2021, October). Research on accounting informatization management strategy under enterprise financial sharing service. In *2021 6th International Conference on Modern Management and Education Technology (MMET 2021)* (pp. 590-596). Atlantis Press. DOI: 10.2991/assehr.k.211011.105

2. Chen, J. C., & Xiao-Hong, H. U. (2017). Research on the cultivation of accounting informatization talents in colleges and universities in the Internet Plus era. *Education Teaching Forum*, 25(11), 45-74. DOI: 10.25236/FER.2023.061009

3. Deng, J. (2022). The informatization of small and medium-sized enterprises accounting system based on sensor monitoring and cloud computing. *Mobile Information Systems, 2022*(1), 5007837. DOI: 10.1155/2022/5007837

4. Khedr, W. I., Khater, H. M., & Mohamed, E. R. (2019). Cryptographic accumulator-based scheme for critical data integrity verification in cloud storage. *IEEE Access: Practical Innovations, Open Solutions, 99*, 1–9. DOI: 10.1109/ACCESS.2019.2917628

5. Li, J., Yan, H., & Zhang, Y. (2020). Identity-based privacy preserving remote data integrity checking for cloud storage. *IEEE Systems Journal, 15*(1), 577–585. DOI: 10.1109/JSYST.2020.2978145

6. Lin, C., Shen, Z., Chen, Q., & Sheldon, F. T. (2017). A data integrity verification scheme in mobile cloud computing. *Journal of Network and Computer Applications, 77*(Jan), 146–151. DOI: 10.1016/j.jnca.2016.08.017

7. Song, W., Wu, Y., Cui, Y., Liu, Q., Shen, Y., Qiu, Z., Yao, J., & Peng, Z. (2022). Public integrity verification for data sharing in cloud with asynchronous revocation. *Digital Communications and Networks, 8*(1), 11–39. DOI: 10.1016/j.dcan.2021.02.002

8. Wang, C. (2023). An examination of the impact of financial sharing on the quality of corporate accounting information in the context of the financial shared service model. *Open Journal of Social Sciences, 11*(11), 385–396. DOI: 10.4236/jss.2023.1111026

9. Wang, S., Pan, X., Wang, Z., Xiao, P., & Wang, Z. (2019). Identity-based cloud storage data integrity verification scheme supporting forward security. [Natural Science Edition]. *Journal of Nanjing University of Posts and Telecommunications, 39*(01), 79–86. DOI:

10.11959/j.issn.1000-436x.2018229

10. Wang, Y. (2019). Cloud data integrity verification algorithm for accounting informatization in sharing mode. *Modern Electronics Technique, 14*(7), 22–43. DOI: 10.16652/j.issn.1004-373x.2019.05.021

11. Wei, P. C., Wang, D., Zhao, Y., Tyagi, S. K. S., & Kumar, N. (2020). Blockchain data-based cloud data integrity protection mechanism. *Future Generation Computer Systems, 10*(38), 902–911. DOI: 10.1016/j.future.2019.09.028

12. Wu, Y., & Ling, J. (2019). An improved data integrity verification method for cloud storage. *Jisuanji Gongcheng, 21*(5), 21–63. DOI: 10.19678/j.issn.1000-3428.0049086

13. Xing, R., & Zhang, J. (2017). Problems and countermeasures of the application of enterprise management accounting informatization. *Agricultural Science and Technology, 44*(24), 52–87. https://www.proquest.com/openview/caf67d8d47381421204ce7a538c796b0/1?pq-origsite=gscholar&cbl=1596357

14. Xu, K., Chen, W., & Zhang, Y. (2021). Blockchain-based integrity verification of data migration in multi-cloud storage. *Journal of Physics: Conference Series, 2132*(1), 012031–012066. DOI: 10.1088/1742-6596/2132/1/012031

15. Yan, Y., Wu, L., Gao, G., Wang, H., & Xu, W. (2018). A dynamic integrity verification scheme of cloud storage data based on lattice and Bloom filter. *Journal of Information Security and Applications, 42*(18), 24–31. DOI: 10.1016/j.jisa.2018.01.005

16. Yu, Y., Au, M. H., Mu, Y., Tang, S., Ren, J., Susilo, W., & Dong, L. (2015). Enhanced privacy of a remote data integrity-checking protocol for secure cloud storage. *International Journal of Information Security, 14*(4), 307–318. DOI: 10.1007/s10207-014-0263-8

17. Zhao, L. P. (2018). Risks and countermeasures of accounting informatization in the era of big data. *Economic Research Guide, 54*(21), 62-87. https://clausiuspress.com/conferences/AEASR/ICMEE%202019/MEE2711.pdf

18. Zhao, X. P., & Jiang, R. (2020). Distributed machine learning oriented data integrity verification scheme in cloud computing environment. *IEEE Access: Practical Innovations, Open Solutions, 8*(3), 26372–26384. DOI: 10.1109/ACCESS.2020.2971519