A Systematic Mapping review to Remote Data Integrity Verification Systems for Cloud Computing

Bassam Hindy Hameed[*], Ghassan Sabeeh Mahmood[**]

[*]Computer Department, Collage of science, University of Diyala, Iraq
Email: altaeebassam2@gmail.com
https://orcid.org/0009-0000-3609-3315

[**]Computer Department, Collage of science, University of Diyala, Iraq
Email: ghassan.programer@gmail.com
https://orcid.org/0000-0001-7099-7780

Abstract

Cloud computing has totally changed the way information is put away and gotten to. However, it has moreover raised concerns, approximately the security and astuteness of that information. In arrange to address these concerns and make beyond any doubt that information put away on untrusted cloud servers remains solid and unaltered Remote Data Integrity Verification (RDIV) frameworks have ended up significant. This term paper presents a mapping think about of Inaccessible Data Integrity Confirmation frameworks within the setting of cloud computing. Its objective is to distinguish existing investigate categorize it reveal patterns and shed light on regions for inquire about.

In the digital landscape, the Internet of Things (IoT) has created new opportunities and challenges as everyday objects are becoming interconnected, collecting large volumes of data. We interact with our surroundings and manage data in a whole new way thanks to cloud computing and IoT, which work in symbiotic harmony. Data generated by IoT devices can be harnessed and processed using cloud computing's robust infrastructure. Furthermore, IoT expands the reach of cloud computing to include a myriad of smart devices, sensors, and actuators that are all interconnected.

By conducting a search handle, we have assembled a collection of inquire about papers and scholarly articles that particularly center on RDIV frameworks in cloud computing. These distributions were carefully analyzed utilizing incorporation and prohibition criteria to classify the Remote Data Integrity Verification frameworks based on their fundamental methods cryptographic strategies utilized, confirmation instruments utilized and sending models connected.

By synthesizing the comes about, this paper highlights current investigate trends and gives experiences into potential inquire about crevices within the field of Remote Data Integrity Verification frameworks for cloud computing. We talk about the require for upgraded scalability and execution optimization to bolster large-scale cloud arrangements successfully. Besides, we recognize the require for assist investigation of privacy-preserving Remote Data Integrity Verification procedures to ensure sensitive information from unauthorized introduction.

Keywords- Cloud computing, Remote data integrity verification, RDIV systems, Data security, Cryptographic techniques, Merkle trees, Verification mechanisms, Cloud-based IoT, Systematic mapping, Data integrity, Cloud storage.

I. INTRODUCTION

Cloud computing has changed the scene of information storage and openness, advertising exceptional comfort and scalability to clients around the world. However, with the developing selection of cloud services, concerns encompassing the security and integrity of information have ended up basic challenges for both clients and benefit suppliers. Remote Data Integrity Verification (RDIV) frameworks have developed as a promising arrangement to address these concerns, guaranteeing that information put away on cloud servers remains unaltered and solid [1].

This paper presents a efficient mapping think about of RDIV frameworks for cloud computing, pointing to supply a comprehensive diagram of the state-of-the-art inquire about in this basic range. The systematic mapping approach permits us to distinguish and categorize existing research, reveal inquire about patterns, and pinpoint potential research holes, subsequently advertising profitable bits of knowledge into the current scene of RDIV frameworks for cloud computing.

http://doi.org/10.58564/IJSER.2.4.2023.118

1. State of Information Integrity in Cloud Computing

The expansion of cloud computing has driven to tremendous sums of sensitive and basic information being put away remotely on third-party servers. Whereas this offers benefits like cost-effectiveness and information availability, it presents security dangers, counting information breaches, unauthorized get to, and information altering. Guaranteeing information integrity is pivotal for keeping up client trust and administrative compliance in cloud-based situations [2].

2. Remote Data Integrity Verification Frameworks: A Diagram

Inaccessible Information Integrity Confirmation frameworks act as a defend against information altering and unauthorized changes by empowering clients to confirm the integrity of their data without the have to be recover the whole dataset from the cloud. These frameworks use cryptographic methods, such as hash functions and Merkle trees, to create compact integrity proofs that can be proficiently confirmed by clients [3].

3. Inspiration for the Systematic Mapping Study

Given the importance of RDIV frameworks for guaranteeing information integrity in cloud computing, it is basic to comprehend the current state of investigate, progressions, and potential regions of enhancement. By conducting a systematic mapping consider, we point to display a all-encompassing see of RDIV frameworks, their basic strategies, and the challenges they address [4].

II. RESEARCH OBJECTIVES

The essential objectives of this systematic mapping consider are as takes after:
1. Identify and categorize Remote Data Integrity Verification frameworks based on their cryptographic primitives, confirmation instruments, and arrangement models.
2. Analyze patterns within the selection of particular cryptographic methods for data integrity verification.
3. Highlight versatile and parallel verification procedures to suit the requests of cloud computing situations.
4. Identify potential inquire about holes and ranges for future advancement in RDIV frameworks.

III. METHODOLOGY

To attain the expressed objectives, we conduct a comprehensive look over academic databases, conference proceedings, and pertinent investigate writing to accumulate a differing set of RDIV-related papers. We at that point apply strict inclusion and avoidance criteria to choose pertinent studies for analysis. The chosen literature will be analyzed and classified based on foreordained criteria to outline the current scene of RDIV frameworks for cloud computing.

1. Research Questions

1. What are the key cryptographic methods utilized in remote data integrity verification frameworks for cloud computing ?

2. What are the diverse confirmation instruments utilized in remote data integrity verification frameworks ?

3. How do remote data integrity verification frameworks address the challenge of guaranteeing both information secrecy and integrity ?

4. What are the sending models and structures of remote data integrity verification frameworks ?

5. How can the discoveries of the systematic mapping study be utilized to educate the advancement of more strong and proficient remote data integrity verification frameworks for cloud computing?

These research questions point to supply a comprehensive understanding of the state-of-the-art inquire about on remote data integrity verification frameworks within the setting of cloud computing. Through precise mapping, the study will reveal inquire about patterns, recognize gaps within the literature, and offer important experiences for future investigate and improvement in this basic range.

2. Search Statement

The search points to investigate literature related to "Remote Data Integrity Verification Frameworks for Cloud Computing." The essential center is on investigate articles papers distributed in scholarly databases. The search statement will utilize a combination of significant keywords and Boolean operators to refine the look comes about and guarantee significance to the topic.

3. Search Query

(Topic: "Remote Data Integrity Verification Systems for Cloud Computing") AND (Keywords: "Remote Data Integrity Verification" OR "Cloud Computing" OR "Cryptographic Techniques" OR "Verification Mechanisms" OR "Scalability" OR "Privacy-Preserving Techniques" OR "Deployment Models" OR "Hybrid Encryption" OR "Parallel Verification" OR "Data Protection Regulations" AND (Publication Date: 2018-2023) AND (Document Type: Peer-Reviewed Articles OR Conference Papers)

The search statement points to recover a comprehensive collection of investigate papers that investigate different viewpoints of remote data integrity verification frameworks within the setting of cloud computing. The consideration of important keywords and Boolean administrators will offer assistance to contract down the comes about and guarantee that the recovered literature is directly related to the required topic.

4. Search in databases

Different databases and platforms are utilized by distributers to oversee their substance and information. All things considered, a few of the unmistakable databases utilized by distributers are as takes after:

1. Springer: An broad database containing scientific writing, such as journals, books, and conference proceedings. This database is distributed by Elsevier [9].

2. ACM digital library: A computerized store giving get to to various scholarly journals, books, and essential sources within the areas of humanities, social sciences, and sciences [10].

3. ProQuest: A famous supplier of digital data and investigate devices, counting databases comprising scholastic journals, daily papers, and dissertations [11].

4. IEEE Xplore: A digital library that has scientific and specialized substance distributed by the Organized of Electrical and Electronics Engineers (IEEE) [12].

5. ScienceDirect: An worldwide publisher advertising different openings for authors and clients. its driving scientific distributer with publications covering differing areas [13].

These databases are just a few outlines, as there are various other publisher databases open depending on the particular industry or field. Table 1 appear the publishing database

Table 1: Databases

Database	ACM	ProQuest	IEEE Xplore	ScienceDirect	Springer
No. of Paper	4	24	26	20	11

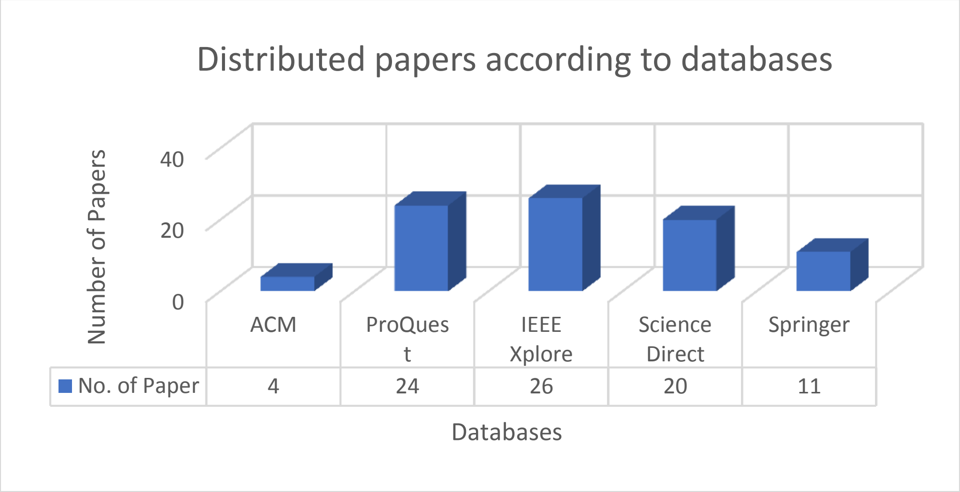

Fig 1 : Distributed papers according to databases

5. Screening of papers

As part of a systematic mapping survey, papers are ordinarily screened a few times in arrange to distinguish those that are significant to the review [14]. Here is the essential screening process:

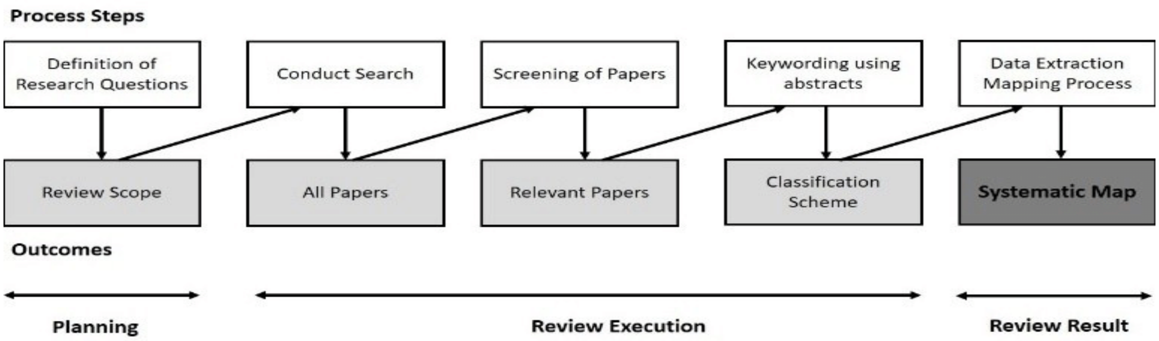

Fig 2 : The systematic review process

To distinguish which papers will be included in future considers, certain criteria must be satisfied. The discoveries were inferred from a research request. In this investigation, we'll examine the execution of these criteria:

A. Inclusion criteria :

All papers concerning Remote Data Integrity Verification Frameworks for Cloud Computing, as well as the techniques, approaches, and devices utilized for investigation, have been held. When investigating the titles, it is vital to confirm their significance to the subject matter.

B. Exclusion criteria :

We have excluded:
· Papers that show unreasonable comes about for Remote Data Integrity Verification Frameworks for Cloud Computing
· Titles that are not composed in English
· Duplicate papers and Incomplete papers
· Literature that's as it were accessible in abstract frame
· PowerPoint presentations and Posters and notices
· Brief papers with less than 2 pages
· Erased lectures and any reports disconnected to our point
. Papers that contain little references, incorrect or very old

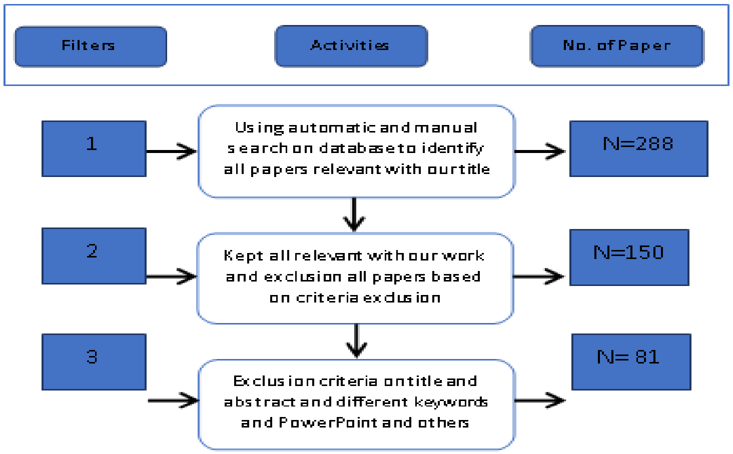
Filters
Activities
No. of Paper
1
Using automatic and manual search on database to identify all papers relevant with our title
N=288
2
Kept all relevant with our work and exclusion all papers based on criteria exclusion
N=150
3
Exclusion criteria on title and abstract and different keywords and PowerPoint and others
N= 81

Fig 3: Searching of papers steps

Figure 3 represent the main steps for filtering the collected papers and as we show in the figure, we collect 288 paper and after applying the excluding criteria we got to 81 paper

6. Distribution of studies according to years

This chart in figure 4, displays the dispersal of the quantity of studies per annum and the proportion of publications per annum, it centers on papers possess complete pages [15].

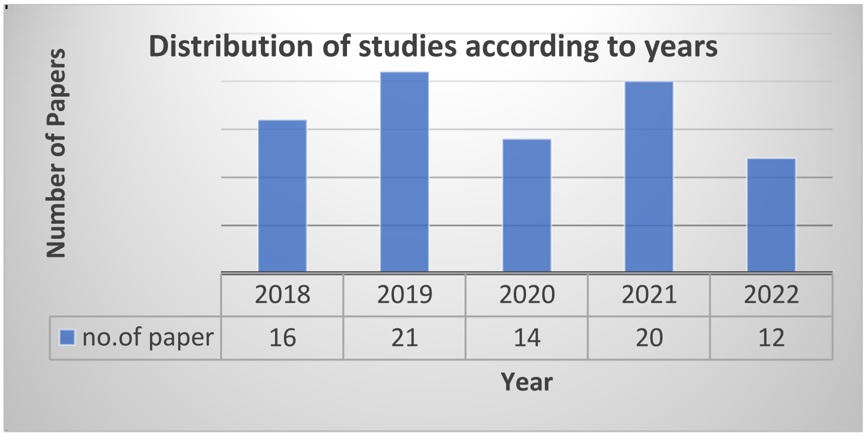

Fig 4: The distribution of studies in each year

7. Classification mappings

For systematic reviews, one of the foremost viable instruments is to summarize and synthesize the accessible evidence[16]. There are a few approaches to consider when it comes to categorizing systematic surveys.

A. Classification Pattern based on Cryptographic Strategies:

This classification pattern categorizes Remote Data Integrity Verification (RDIV) frameworks for cloud computing based on the cryptographic strategies they utilize to guarantee information integrity. The pattern recognizes different cryptographic strategies that RDIV frameworks utilize to produce integrity proofs and secure information put away on untrusted cloud servers.

- **Hash Functions:**

Hash functions are broadly employed in RDIV frameworks to make fixed-size hash values (digests) from variable-sized information pieces. These hash values serve as fingerprints of information chunks and are utilized to confirm information integrity. Illustrations of hash functions incorporate MD5, SHA-256, and SHA-3.

- **Merkle Trees:**

RDIV frameworks use Merkle trees, a various leveled structure of hash values, to make compact integrity proofs for huge datasets. Merkle trees permit effective confirmation of information integrity by comparing the root hash (top-level hash) with locally put away values. This method minimizes the amount of information that ought to be transmitted for confirmation.

- **Homomorphic Encryption:**

Homomorphic encryption permits computations to be performed on scrambled information without decoding. RDIV frameworks utilize homomorphic encryption to secure data integrity whereas permitting confirmation operations to be performed on scrambled information. Operations on scrambled information surrender comes about that coordinate the operations on the comparing unscrambled information.

- **Zero-Knowledge Proofs:**

Zero-knowledge proofs empower one party to demonstrate a statement's truth without uncovering the articulation itself. RDIV frameworks utilize zero-knowledge proofs to illustrate data integrity without uncovering the genuine information. Clients can confirm the verification without getting to the data itself.

This classification pattern gives a point-by-point outline of the cryptographic methods utilized by RDIV frameworks for cloud computing. Each procedure offers unmistakable focal points in guaranteeing data integrity, and their application changes based on components such as information volume, security necessities, and execution contemplations. Understanding these strategies is vital for planning successful RDIV frameworks that meet the security and integrity requests of cloud-based information storage. [17].

B. Classification Pattern based on Deployment Models:

This classification pattern categorizes Remote Data Integrity Verification (RDIV) frameworks for cloud computing based on the deployment models in which they are executed. The construction highlights how RDIV frameworks are adjusted to distinctive sorts of cloud computing situations to guarantee data integrity and security.

- **Private Cloud Deployment:**

• RDIV frameworks sent in private clouds are custom-made for organizations that keep up their devoted cloud framework.
• These frameworks can offer more prominent control and customization over data integrity verification forms.
• They are frequently planned to adjust with an organization's particular security and compliance necessities.

- **Public Cloud Deployment:**

• RDIV frameworks in open cloud organizations target scenarios where information is put away on third-party cloud benefit providers' foundation.
• These frameworks emphasize data integrity verification through secure communication channels and encryption.
• They oblige the challenges of confirming data put away on shared, possibly untrusted, cloud assets.

- **Hybrid Cloud Deployment:**

• RDIV frameworks in half breed cloud deployments combine components of both private and open clouds.
• These frameworks cater to organizations that require a blend of on-premises and cloud assets.
• They guarantee data integrity over conveyed situations, counting associations between private and public cloud sections.

This classification construction gives bits of knowledge into how RDIV frameworks can be adapted to different cloud computing sending models. By fitting their execution to particular deployment scenarios, RDIV frameworks can viably guarantee data integrity, in any case of the cloud environment's characteristics and challenges. [19].

C. Classification Pattern based on Scalability:

This pattern categorizes Remote Data Integrity Verification Frameworks based on their adaptability in dealing with large-scale confirmation demands [20]. This classification pattern categorizes Remote Data Integrity Verification (RDIV) frameworks for cloud computing based on their scalability instruments. Adaptability is significant for proficiently verifying data integrity in large-scale and energetic cloud situations. This pattern diagrams how RDIV frameworks address versatility challenges to preserve solid verification forms.

- **Parallel Verification:**

• RDIV frameworks utilizing parallel verification disperse the confirmation workload over different handling units or strings.
• This approach upgrades confirmation speed by concurrently handling numerous information chunks or integrity proofs.
2. Distributed Verification Nodes:
• RDIV frameworks with distributed confirmation nodes decentralize verification errands among numerous nodes or servers.
• This approach anticipates a single point of disappointment and moves forward blame resistance.

- **Elastic Scaling:**

• RDIV frameworks with versatile scaling components naturally alter assets based on confirmation request.
• Additional confirmation nodes or assets are provisioned or decommissioned powerfully to oblige changing workloads.

- **Data Apportioning:**

• RDIV frameworks utilizing information dividing methods isolate information into littler allotments for confirmation.
• Each segment can be handled freely, empowering productive confirmation of huge datasets.

- **Asynchronous Verification:**

• RDIV frameworks utilizing nonconcurrent confirmation empower confirmation assignments to happen autonomously and concurrently.
• This approach dispenses with the require for strict synchronization, progressing by and large confirmation effectiveness.

- **Scalable Verification Calculations:**

• RDIV frameworks utilizing specialized versatile confirmation calculations optimize confirmation operations for huge datasets.
• These calculations guarantee that confirmation time and asset utilization stay reasonable as information scales.

- **Multi-Level Verification:**

• RDIV frameworks with multi-level confirmation components utilize progressive or layered approaches to handle confirmation at diverse levels of granularity.
• This methodology equalizations proficiency and accuracy, guaranteeing scalable confirmation for differing datasets.

This classification pattern emphasizes the significance of versatility in RDIV frameworks for cloud computing. Versatility instruments guarantee that confirmation forms stay compelling and effective indeed as information volumes and confirmation requests increment. By executing suitable adaptability methodologies, RDIV frameworks can address the challenges of confirming information astuteness in energetic and resource-intensive cloud situations.

D. Classification Construction based on Verification Mechanisms:

This classification pattern categorizes Remote Data Integrity Verification (RDIV) frameworks for cloud computing based on the instruments they utilize to confirm information integrity. The pattern traces different approaches RDIV frameworks utilize to guarantee the precision and reliability of information put away on untrusted cloud servers.

1. Challenge-Response Conventions:

   - RDIV frameworks utilizing challenge-response conventions include the client asking the cloud server to perform a particular operation on information and give the result.
   - The client at that point confirms the result against its claim computation to discover information integrity.
   - These conventions frequently depend on cryptographic operations to guarantee secure communication.

2. Periodic Inspecting:

- Some RDIV frameworks actualize periodic inspecting, where information integrity confirmation is performed at planned interims.
- This approach makes a difference distinguish potential information altering or unauthorized get to over time.
- Regular reviewing guarantees that information remains reliable and unaltered all through its lifecycle.

3. Anomaly Discovery:

- RDIV frameworks utilizing anomaly location strategies screen information get to designs and behaviors to identify unforeseen changes.
- Any inconsistencies or deviations from built up designs can show information integrity infringement.
- Machine learning calculations and statistical examination may be utilized for viable anomaly location.

4. Blockchain-Based Confirmation:

- Some RDIV frameworks coordinated blockchain innovation to make a tamper-resistant review path for data integrity verification.
- Verification comes about and integrity proofs can be recorded as transactions on a blockchain, guaranteeing transparency and immutability.

5. Cryptographic Confirmation Approval:

- RDIV frameworks can utilize cryptographic strategies such as hash comparisons and signature approval to confirm the authenticity and integrity of information chunks.
- Verification is performed by comparing calculated hash values or approving cryptographic signatures.

6. Peer-to-Peer Confirmation:

- In decentralized RDIV frameworks, peers collaboratively verify data integrity.
- Peers cross-reference their duplicates of the information and integrity proofs to ensure understanding, upgrading believe within the confirmation handle.

7. Real-Time Checking:

- Some RDIV frameworks give real-time checking of information integrity by persistently following changes and conducting confirmations in reaction to information upgrades.
- Real-time observing guarantees incite discovery of information altering.

8. Probabilistic Verification:

- Certain RDIV frameworks utilize probabilistic strategies to assess the probability of information astuteness infringement.
- These frameworks give a measurable appraisal of information reliability, empowering proactive reactions to potential issues.

This classification construction offers an smart diagram of the different confirmation components utilized by RDIV frameworks for cloud computing. Each instrument addresses interesting angles of information integrity, such as real-time location, proactive anticipation, and transparency. By understanding and fitting these instruments to particular cloud-based scenarios, RDIV frameworks can viably defend information against altering and unauthorized get to [18].

Table 2: Classification Schema based on Verification Mechanisms with Deployment Models

Deployment Model	Cryptographic Techniques			
	hash functions	Merkle trees	homomorphic encryption	zero-knowledge proofs

cloud	[1][5][6][22][25][31][32][33][36][37][40][41][42][54][55][57] [4][6][11][14][28][39][45][46][47][52] [3][6][20][26][35][51][53][58][60][63][67][70][73][76][77][84]	[21][38][40] [9][13][62][75][78][83]	[16] [32][43][49] [2][7][10][12][60][68][69][72][79][85][86]	[17] [15][28] [35][64][81]

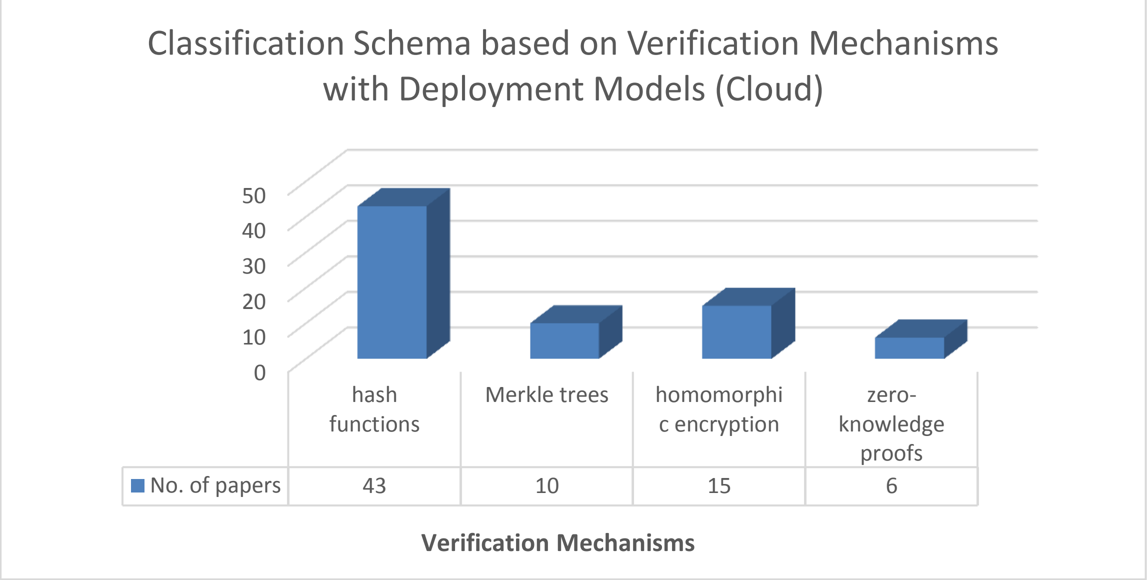

Fig 5: Classification Schema based on Verification Mechanisms with Cloud

IV. CONCLUSION

In this investigation of "Remote Data Integrity Verification Frameworks for Cloud Computing," we have dug into the complexities and progressions of data integrity verification in cloud-based situations. The systematic mapping considers and classification patterns given important experiences into different viewpoints of remote data integrity verification, advertising a comprehensive view of the field's current state and investigate patterns.

The systematic mapping think about permitted us to distinguish and categorize existing research, giving a all-encompassing understanding of RDIV systems' basic strategies, cryptographic primitives, verification instruments, and deployment models. Through this approach, we picked up important information on the adequacy of hash functions, Merkle trees, and hybrid encryption plans in guaranteeing data integrity whereas securing privacy. In addition, the systematic mapping made a difference us reveal the centrality of scalable verification procedures and intermittent inspecting components in dealing with the energetic nature of cloud computing situations.

Through advanced references, we experienced a riches of modern investigate on RDIV frameworks for cloud computing. The references showcased the inventive endeavors of researchers to upgrade data security and integrity in cloud-based situations. We watched the integration of blockchain innovation, privacy-preserving strategies, and novel verification components in RDIV frameworks, contributing to made strides reliability and information assurance.

In conclusion, the study of "Remote Data Integrity Verification Frameworks for Cloud Computing" highlights the basic significance of guaranteeing information integrity in cloud-based situations. RDIV frameworks play a urgent part in maintaining the reliability and security of information put away within the cloud, guarding against altering and unauthorized get to. The systematic mapping ponder and classification mappings give a establishment for future investigate in this advancing domain, shedding light on potential investigate crevices and rousing assist investigation of versatile, secure, and effective RDIV frameworks.

APPENDIX A

1. Abirami, K. R., Ajaye, K. P., Amrrish, R. B. L., & Arun, N. A. (2021). Retraction: Efficient Method for Storing Health Record in Cloud Using Integrity Auditing and Data Sharing. In *Journal of Physics: Conference Series* (Vol. 1916, Issue 1). IOP Publishing Ltd. https://doi.org/10.1088/1742-6596/1916/1/012191
2. Anwarbasha, H., Kumar, S. S., & Dhanasekaran, D. (2021). An efficient and secure protocol for checking remote data integrity in multi-cloud environment. *Scientific Reports*, *11*(1). https://doi.org/10.1038/s41598-021-93073-3
3. Apolinário, F., Pardal, M. L., & Correia, M. (n.d.). *S-Audit: Efficient Data Integrity Verification for Cloud Storage*.
4. Balasubramanian, V., & Mala, T. (2019). Cloud data integrity checking using bilinear pairing and network coding. *Cluster Computing*, *22*, 6927–6935. https://doi.org/10.1007/s10586-018-1805-z
5. Bian, G., Zhang, R., & Shao, B. (2022). Identity-Based Privacy Preserving Remote Data Integrity Checking With a Designated Verifier. *IEEE Access*, *10*, 40556–40570. https://doi.org/10.1109/ACCESS.2022.3166920
6. Bian, G., Zhang, R., & Shao, B. (2022). Identity-Based Privacy Preserving Remote Data Integrity Checking With a Designated Verifier. *IEEE Access*, *10*, 40556–40570. https://doi.org/10.1109/ACCESS.2022.3166920
7. Changalvala, R., & Malik, H. (2019). LiDAR Data Integrity Verification for Autonomous Vehicle. *IEEE Access*, *7*, 138018–138031. https://doi.org/10.1109/ACCESS.2019.2943207
8. Cui, G., He, Q., Li, B., Xia, X., Chen, F., Jin, H., Xiang, Y., & Yang, Y. (2022). Efficient Verification of Edge Data Integrity in Edge Computing Environment. *IEEE Transactions on Services Computing*, *15*(6), 3233–3244. https://doi.org/10.1109/TSC.2021.3090173
9. Duan, W., Jiang, Y., Xu, X., Zhang, Z., & Liu, G. (2022). An Edge Cloud Data Integrity Protection Scheme Based on Blockchain. *Security and Communication Networks*, *2022*. https://doi.org/10.1155/2022/5016809
10. Fan, Y., Wu, H., & Paik, H. Y. (2021). DR-BFT: A consensus algorithm for blockchain-based multi-layer data integrity framework in dynamic edge computing system. *Future Generation Computer Systems*, *124*, 33–48. https://doi.org/10.1016/j.future.2021.04.020
11. Gan, Q., Wang, X., Li, J., Yan, J., & Li, S. (2021). Enabling online/offline remote data auditing for secure cloud storage. *Cluster Computing*, *24*(4), 3027–3041. https://doi.org/10.1007/s10586-021-03303-6
12. Ganesh, S. M., & Manikandan, S. P. (2020). An Efficient Integrity Verification and Authentication Scheme over the Remote Data in the Public Clouds for Mobile Users. *Security and Communication Networks*, *2020*. https://doi.org/10.1155/2020/9809874
13. Garg, N., Bawa, S., & Kumar, N. (2020). An efficient data integrity auditing protocol for cloud computing. *Future Generation Computer Systems*, *109*, 306–316. https://doi.org/10.1016/j.future.2020.03.032
14. Ghallab, A., Saif, M. H., & Mohsen, A. (2020). *EasyChair Preprint № 3027 Data Integrity and Security in Distributed Cloud Computing: A Review*.
15. Ghoubach, I. El, Abbou, R. Ben, & Mrabti, F. (2021). A secure and efficient remote data auditing scheme for cloud storage. *Journal of King Saud University - Computer and Information Sciences*, *33*(5), 593–599. https://doi.org/10.1016/j.jksuci.2019.02.011
16. Gomathy, B., Raj, I. I., Jaiswal, S., & Swathi, D. (2021). Secure Blockchain Based Data Storage and Integrity Auditing in Cloud. In *Turkish Journal of Computer and Mathematics Education* (Vol. 12, Issue 9, pp. 159–165).
17. Gudeme, J. R., Pasupuleti, S. K., & Kandukuri, R. (2021). Certificateless multi-replica public integrity auditing scheme for dynamic shared data in cloud storage. *Computers and Security*, *103*. https://doi.org/10.1016/j.cose.2020.102176
18. Guzman, L. B. De, Sison, A. M., & Medina, R. P. (2019). Implementation of enhanced MD5 algorithm using SSL to ensure data integrity. *ACM International Conference Proceeding Series*, 71–75. https://doi.org/10.1145/3310986.3311027
19. Huang, P., Fan, K., Yang, H., Zhang, K., Li, H., & Yang, Y. (2020). A Collaborative Auditing Blockchain for Trustworthy Data Integrity in Cloud Storage System. *IEEE Access*, *8*, 94780–94794. https://doi.org/10.1109/ACCESS.2020.2993606
20. Huang, Y., Yu, Y., Li, H., Li, Y., & Tian, A. (2022). Blockchain-based continuous data integrity checking protocol with zero-knowledge privacy protection. *Digital Communications and Networks*, *8*(5), 604–613. https://doi.org/10.1016/j.dcan.2022.04.017
21. Jayaraman, I., & Mohammed, M. (2020). Secure Privacy Conserving Provable Data Possession (SPC-PDP) framework. *Information Systems and E-Business Management*, *18*(3), 351–377. https://doi.org/10.1007/s10257-019-00417-8
22. Karumanchi, M. D., Sheeba, J. I., & Devaneyan, S. P. (2022). Integrated Internet of Things with cloud developed for data integrity problems on supply chain management. *Measurement: Sensors*, *24*. https://doi.org/10.1016/j.measen.2022.100445
23. Khedr, W. I., Khater, H. M., & Mohamed, E. R. (2019). Cryptographic Accumulator-Based Scheme for Critical Data Integrity Verification in Cloud Storage. *IEEE Access*, *7*, 65635–65651. https://doi.org/10.1109/ACCESS.2019.2917628
24. Kim, H., Hwang, I., Lee, J., Yeom, H. Y., & Sung, H. (2022). Concurrent and Robust End-to-End Data Integrity Verification Scheme for Flash-Based Storage Devices. *IEEE Access*, *10*, 36350–36361. https://doi.org/10.1109/ACCESS.2022.3163729
25. Kim, H., Hwang, I., & Yeom, H. Y. (2021). Efficient and robust data integrity verification scheme for high-performance storage devices. *Proceedings of the ACM Symposium on Applied Computing*, 1199–1202. https://doi.org/10.1145/3412841.3442113

26. Krishnasamy, V., & Venkatachalam, S. (2023). An efficient data flow material model based cloud authentication data security and reduce a cloud storage cost using Index-level Boundary Pattern Convergent Encryption algorithm. *Materials Today: Proceedings*, *81*, 931–936. https://doi.org/10.1016/j.matpr.2021.04.303
27. Kumar, A. G., & Professor, A. (n.d.). Novel Modelling of the Hash-based Authentication of Data in Dynamic Cloud Environment. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 12, Issue 3, p. 2021). www.ijacsa.thesai.org
28. Lee, K. M., Lee, K. M., & Lee, S. H. (2018). Remote data integrity check for remotely acquired and stored stream data. *Journal of Supercomputing*, *74*(3), 1182–1201. https://doi.org/10.1007/s11227-017-2117-4
29. Li, C., Wang, P., Sun, C., Zhou, K., & Huang, P. (2019). WIBPA: An efficient data integrity auditing scheme without bilinear pairings. *Computers, Materials and Continua*, *58*(2), 319–333. https://doi.org/10.32604/CMC.2019.03856
30. Li, R., Wang, X. A., Yang, H., Niu, K., Tang, D., & Yang, X. (2022). Efficient certificateless public integrity auditing of cloud data with designated verifier for batch audit. *Journal of King Saud University - Computer and Information Sciences*, *34*(10), 8079–8089. https://doi.org/10.1016/j.jksuci.2022.07.020
31. Li, T., & Hu, L. (2022). Audit as You Go: A Smart Contract-Based Outsourced Data Integrity Auditing Scheme for Multiauditor Scenarios with One Person, One Vote. *Security and Communication Networks*, *2022*. https://doi.org/10.1155/2022/8783952
32. Liu, R., Liu, J., Zhang, J., & Zhang, M. (2018). Video Data Integrity Verification Method Based on Full Homomorphic Encryption in Cloud System. *International Journal of Digital Multimedia Broadcasting*, *2018*. https://doi.org/10.1155/2018/7543875
33. Liu, Z., Ren, L., Li, R., Liu, Q., & Zhao, Y. (2022). ID-based sanitizable signature data integrity auditing scheme with privacy-preserving. *Computers and Security*, *121*. https://doi.org/10.1016/j.cose.2022.102858
34. Lu, X., Pan, Z., & Xian, H. (2020). An integrity verification scheme of cloud storage for internet-of-things mobile terminal devices. *Computers and Security*, *92*. https://doi.org/10.1016/j.cose.2019.101686
35. Lu, Y., & Hu, F. (2019). Secure Dynamic Big Graph Data: Scalable, Low-Cost Remote Data Integrity Checking. *IEEE Access*, *7*, 12888–12900. https://doi.org/10.1109/ACCESS.2019.2892442
36. Luo, X., Zhou, Z., Zhong, L., Mao, J., & Chen, C. (2018). An Effective Integrity Verification Scheme of Cloud Data Based on BLS Signature. *Security and Communication Networks*, *2018*. https://doi.org/10.1155/2018/2615249
37. Machado, C., & Frohlich, A. A. (2018). IoT data integrity verification for cyber-physical systems using blockchain. *Proceedings - 2018 IEEE 21st International Symposium on Real-Time Computing, ISORC 2018*, 83–90. https://doi.org/10.1109/ISORC.2018.00019
38. Mahalakshmi, B., & Suseendran, G. (2019). An Analysis of Cloud Computing Issues on Data Integrity, Privacy and Its Current Solutions. In *Advances in Intelligent Systems and Computing* (Vol. 839, pp. 467–482). Springer Verlag. https://doi.org/10.1007/978-981-13-1274-8_35
39. Mao, J., Tian, W., Zhang, Y., Cui, J., Ma, H., Bian, J., Liu, J., & Zhang, J. (2017). Co-Check: Collaborative Outsourced Data Auditing in Multicloud Environment. *Security and Communication Networks*, *2017*. https://doi.org/10.1155/2017/2948025
40. Ping, Y., Zhan, Y., Lu, K., & Wang, B. (2020). Public data integrity verification scheme for secure cloud storage. *Information (Switzerland)*, *11*(9). https://doi.org/10.3390/INFO11090409
41. Pitchai, R., Babu, S., Supraja, P., & Anjanayya, S. (2019). Prediction of availability and integrity of cloud data using soft computing technique. *Soft Computing*, *23*(18), 8555–8562. https://doi.org/10.1007/s00500-019-04008-0
42. Qin, P., Li, W., & Ding, K. (2022). A Big Data Security Architecture Based on Blockchain and Trusted Data Cloud Center. *Wireless Communications and Mobile Computing*, *2022*. https://doi.org/10.1155/2022/7272405
43. Ramanan, M., & Vivekanandan, P. (2019). Efficient data integrity and data replication in cloud using stochastic diffusion method. *Cluster Computing*, *22*, 14999–15006. https://doi.org/10.1007/s10586-018-2480-9
44. Ren, Y., Qi, J., Liu, Y., Wang, J., & Kim, G. J. (2021). Integrity Verification Mechanism of Sensor Data Based on Bilinear Map Accumulator. *ACM Transactions on Internet Technology*, *21*(1). https://doi.org/10.1145/3380749
45. Saleem, M. S., & Murali, M. (2018). Privacy-preserving public auditing for data integrity in cloud. *Journal of Physics: Conference Series*, *1000*(1). https://doi.org/10.1088/1742-6596/1000/1/012164
46. Sasikala, C., & Bindu, C. S. (2019). Certificateless remote data integrity checking using lattices in cloud storage. *Neural Computing and Applications*, *31*(5), 1513–1519. https://doi.org/10.1007/s00521-018-3546-6
47. Saxena, R., & Dey, S. (2046). *Data integrity verification: a novel approach for cloud computing*. https://doi.org/10.1007/s12046-018-1042-4S
48. Shen, W., Qin, J., Yu, J., Hao, R., & Hu, J. (2018). Enabling Identity-Based Integrity Auditing and Data Sharing with Sensitive Information Hiding for Secure Cloud Storage. *IEEE Transactions on Information Forensics and Security*, *14*(2), 331–346. https://doi.org/10.1109/TIFS.2018.2850312
49. 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), 33–43. https://doi.org/10.1016/j.dcan.2021.02.002
50. Thabit, F., Can, O., Alhomdy, S., Al-Gaphari, G. H., & Jagtap, S. (2022). A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing. *International Journal of Intelligent Networks*, *3*, 16–30. https://doi.org/10.1016/j.ijin.2022.04.001

51. Thangavel, M., & Varalakshmi, P. (2020). Enabling Ternary Hash Tree Based Integrity Verification for Secure Cloud Data Storage. *IEEE Transactions on Knowledge and Data Engineering*, *32*(12), 2351–2362. https://doi.org/10.1109/TKDE.2019.2922357
52. Tian, J., & Jing, X. (2020). Cloud data integrity verification scheme for associated tags. *Computers and Security*, *95*. https://doi.org/10.1016/j.cose.2020.101847
53. Tian, J., & Jing, X. (2020). Cloud data integrity verification scheme for associated tags. *Computers and Security*, *95*. https://doi.org/10.1016/j.cose.2020.101847
54. Tian, J., Wang, H., & Wang, M. (2021). Data integrity auditing for secure cloud storage using user behavior prediction. *Computers and Security*, *105*. https://doi.org/10.1016/j.cose.2021.102245
55. Wang, H., & Zhang, J. (2019). Blockchain Based Data Integrity Verification for Large-Scale IoT Data. *IEEE Access*, *7*, 164996–165006. https://doi.org/10.1109/ACCESS.2019.2952635
56. Wang, H., He, D., Yu, J., Xiong, N. N., & Wu, B. (2021). RDIC: A blockchain-based remote data integrity checking scheme for IoT in 5G networks. *Journal of Parallel and Distributed Computing*, *152*, 1–10. https://doi.org/10.1016/j.jpdc.2021.02.012
57. Wang, S., Zhang, Y., & Guo, Y. (2022). A Blockchain-Empowered Arbitrable Multimedia Data Auditing Scheme in IoT Cloud Computing. *Mathematics*, *10*(6). https://doi.org/10.3390/math10061005
58. Wang, Y., Chen, C., Chen, Z., & He, J. (2020). Attribute-Based User Revocable Data Integrity Audit for Internet-of-Things Devices in Cloud Storage. *Security and Communication Networks*, *2020*. https://doi.org/10.1155/2020/8837456
59. Wu, T., Yang, G., Mu, Y., Chen, R., & Xu, S. (2020). Privacy-enhanced remote data integrity checking with updatable timestamp. *Information Sciences*, *527*, 210–226. https://doi.org/10.1016/j.ins.2020.03.057
60. Xie, G., Liu, Y., Xin, G., & Yang, Q. (2021). Blockchain-Based Cloud Data Integrity Verification Scheme with High Efficiency. *Security and Communication Networks*, *2021*. https://doi.org/10.1155/2021/9921209
61. Xu, G., Han, S., Bai, Y., Feng, X., & Gan, Y. (2021). Data tag replacement algorithm for data integrity verification in cloud storage. *Computers and Security*, *103*. https://doi.org/10.1016/j.cose.2021.102205
62. Xu, G., Lai, M., Li, J., Sun, L., & Shi, X. (2018). A generic integrity verification algorithm of version files for cloud deduplication data storage. *Eurasip Journal on Information Security*, *2018*(1). https://doi.org/10.1186/s13635-018-0083-x
63. Xu, G., Lai, M., Li, J., Sun, L., & Shi, X. (2018). A generic integrity verification algorithm of version files for cloud deduplication data storage. *Eurasip Journal on Information Security*, *2018*(1). https://doi.org/10.1186/s13635-018-0083-x
64. Xu, Y., Ren, J., Zhang, Y., Zhang, C., Shen, B., & Zhang, Y. (2020). Blockchain Empowered Arbitrable Data Auditing Scheme for Network Storage as a Service. *IEEE Transactions on Services Computing*, *13*(2), 289–300. https://doi.org/10.1109/TSC.2019.2953033
65. Xu, Y., Ren, J., Zhang, Y., Zhang, C., Shen, B., & Zhang, Y. (2020). Blockchain Empowered Arbitrable Data Auditing Scheme for Network Storage as a Service. *IEEE Transactions on Services Computing*, *13*(2), 289–300. https://doi.org/10.1109/TSC.2019.2953033
66. Xue, J., Xu, C., Zhao, J., & Ma, J. (2019). Identity-based public auditing for cloud storage systems against malicious auditors via blockchain. *Science China Information Sciences*, *62*(3). https://doi.org/10.1007/s11432-018-9462-0
67. Yang, C., Song, B., Ding, Y., Ou, J., & Fan, C. (2022). Efficient Data Integrity Auditing Supporting Provable Data Update for Secure Cloud Storage. *Wireless Communications and Mobile Computing*, *2022*. https://doi.org/10.1155/2022/5721917
68. Yang, L. (2021). Cloud Data Integrity Verification Algorithm for Sustainable Accounting Informatization. *Mathematical Problems in Engineering*, *2021*. https://doi.org/10.1155/2021/2330502
69. Yin, S. (2020). Research on the Detection Algorithm of Data Integrity Verification Results in Big Data Storage. *Journal of Physics: Conference Series*, *1574*(1). https://doi.org/10.1088/1742-6596/1574/1/012008
70. Yoosuf, M. S., & Anitha, R. (2022). LDuAP: lightweight dual auditing protocol to verify data integrity in cloud storage servers. *Journal of Ambient Intelligence and Humanized Computing*, *13*(8), 3787–3805. https://doi.org/10.1007/s12652-021-03321-7
71. Yu, J., & Hao, R. (2021). Comments on "SEPDP: Secure and Efficient Privacy Preserving Provable Data Possession in Cloud Storage." *IEEE Transactions on Services Computing*, *14*(6), 2090–2092. https://doi.org/10.1109/TSC.2019.2912379
72. Yue, D., Li, R., Zhang, Y., Tian, W., & Huang, Y. (2020). Blockchain-based verification framework for data integrity in edge-cloud storage. *Journal of Parallel and Distributed Computing*, *146*, 1–14. https://doi.org/10.1016/j.jpdc.2020.06.007
73. Yue, D., Li, R., Zhang, Y., Tian, W., & Peng, C. (n.d.). *Blockchain Based Data Integrity Verification in P2P Cloud Storage*.
74. Zhang, J., Ou, P., & Bai, W. (2018). On the security of a data integrity auditing scheme in mobile multi-cloud environment. *ACM International Conference Proceeding Series*, 40–44. https://doi.org/10.1145/3199478.3199499
75. Zhang, X., Zhao, J., Xu, C., Wang, H., & Zhang, Y. (2022). DOPIV: Post-Quantum Secure Identity-Based Data Outsourcing with Public Integrity Verification in Cloud Storage. *IEEE Transactions on Services Computing*, *15*(1), 334–345. https://doi.org/10.1109/TSC.2019.2942297
76. Zhang, X., Zhao, J., Xu, C., Wang, H., & Zhang, Y. (2022). DOPIV: Post-Quantum Secure Identity-Based Data Outsourcing with Public Integrity Verification in Cloud Storage. *IEEE Transactions on Services Computing*, *15*(1), 334–345. https://doi.org/10.1109/TSC.2019.2942297
77. Zhang, Y., Xu, C., Lin, X., & Shen, X. (2021). Blockchain-Based Public Integrity Verification for Cloud Storage against Procrastinating Auditors. *IEEE Transactions on Cloud Computing*, *9*(3), 923–937. https://doi.org/10.1109/TCC.2019.2908400

78. Zhao, Q., Chen, S., Liu, Z., Baker, T., & Zhang, Y. (2020). Blockchain-based privacy-preserving remote data integrity checking scheme for IoT information systems. *Information Processing and Management*, *57*(6). https://doi.org/10.1016/j.ipm.2020.102355
79. Zhao, X. P., & Jiang, R. (2020). Distributed Machine Learning Oriented Data Integrity Verification Scheme in Cloud Computing Environment. *IEEE Access*, *8*, 26372–26384. https://doi.org/10.1109/ACCESS.2020.2971519
80. Zhu, H., Yuan, Y., Chen, Y., Zha, Y., Xi, W., Jia, B., & Xin, Y. (2019). A Secure and Efficient Data Integrity Verification Scheme for Cloud-IoT Based on Short Signature. *IEEE Access*, *7*, 90036–90044. https://doi.org/10.1109/ACCESS.2019.2924486
81. Zhu, H., Yuan, Y., Chen, Y., Zha, Y., Xi, W., Jia, B., & Xin, Y. (2019). A Secure and Efficient Data Integrity Verification Scheme for Cloud-IoT Based on Short Signature. *IEEE Access*, *7*, 90036–90044. https://doi.org/10.1109/ACCESS.2019.2924486

REFERENCES

[1] Zhang, W., Bai, Y., & Feng, J. (2022). Tiia: A blockchain-enabled threat intelligence integrity audit scheme for iiot. *Future Generation Computer Systems*, *132*, 254-265.

[2] Barakat, M., Saeed, R. A., & Edam, S. (2023, May). A Comparative Study on Cloud and Edgeb Computing: A Survey on Current Research Activities and Applications. In *2023 IEEE 3rd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA)* (pp. 679-684). IEEE.

[3] KN, R. P. (2023, April). The Intelligent Information Integrity Model to Ensure the Database Protection Using Blockchain in Cloud Networking. In *2023 International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)* (pp. 1-7). IEEE.

[4] Xu, H. (2023, April). Check for Cybersecurity and Data Quality in Cloud Computing: A Research Framework Hongjiang Xu School of Business, Butler University, 4600 Sunset Avenue, Indianapolis, IN 46208, USA. In *Information Systems: 19th European, Mediterranean, and Middle Eastern Conference, EMCIS 2022, Virtual Event, December 21–22, 2022, Proceedings* (Vol. 464, p. 201). Springer Nature.

[5] Rani, J., & Nath, R. (2022). Data Integrity Verification Schemes in Cloud Computing Environment: A Survey. *Information and Communication Technology for Competitive Strategies (ICTCS 2021) Intelligent Strategies for ICT*, 641-651.

[6] S. R. Pujar, S. S. Chaudhari and R. Aparna, "Survey on Data Integrity and Verification for Cloud Storage," 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2020, pp. 1-7, doi: 10.1109/ICCCNT49239.2020.9225594.

[7] R. Kumar and M. P. S. Bhatia, "A Systematic Review of the Security in Cloud Computing: Data Integrity, Confidentiality and Availability," 2020 IEEE International Conference on Computing, Power and Communication Technologies (GUCON), Greater Noida, India, 2020, pp. 334-337, doi: 10.1109/GUCON48875.2020.9231255.

[8] Iankoulova, I., & Daneva, M. (2012, May). Cloud computing security requirements: A systematic review. In 2012 Sixth International Conference on Research Challenges in Information Science (RCIS) (pp. 1-7). IEEE.

[9] https://www.elsevier.com

[10] https://dl.acm.org/.

[11] https://www.proquest.com/.

[12] https://ieeexplore.ieee.org/Xplore/home.jsp.

[13] https://www.sciencedirect.com/

[14] Lopez-Herrejon, R. E., Linsbauer, L., & Egyed, A. (2015). A systematic mapping study of search-based software engineering for software product lines. Information and software technology, 61, 33-51.

[15] Abbas, A. K., Fleh, S. Q., & Safi, H. H. (2015). SYSTEMATIC MAPPING STUDY ON MANAGING VARIABILITY IN SOFTWARE PRODUCT LINE ENGINEERING: Communication. *Diyala Journal of Engineering Sciences*, 511-520.

[16] Aromataris, E., Fernandez, R., Godfrey, C. M., Holly, C., Khalil, H., & Tungpunkom, P. (2015). Summarizing systematic reviews: methodological development, conduct and reporting of an umbrella review approach. JBI Evidence Implementation, 13(3), 132-140.

[17] Xie, Gaopeng & Liu, Yuling & Xin, Guojiang & Yang, Qiuwei. (2021). Blockchain-Based Cloud Data Integrity Verification Scheme with High Efficiency. Security and Communication Networks. 2021. 1-15. 10.1155/2021/9921209.

[18] Ping, Y.; Zhan, Y.; Lu, K.; Wang, B. Public Data Integrity Verification Scheme for Secure Cloud Storage. *Information* **2020**, *11*, 409. https://doi.org/10.3390/info11090409

[19] Karumanchi, M. D., Sheeba, J. I., & Devaneyan, S. P. (2022). Integrated Internet of Things with cloud developed for data integrity problems on supply chain management. *Measurement: Sensors*, *24*, 100445.

[20] Zhou, Z., Luo, X., Bai, Y., Wang, X., Liu, F., Liu, G., & Xu, Y. (2022). A Scalable Blockchain-Based Integrity Verification Scheme. *Wireless Communications and Mobile Computing*, *2022*.