

# Advancing integrity and privacy in cloud storage: challenges, current solutions, and future directions

Shrinivasa<sup>1</sup>, Chandrakala Beturpalya Muddaraju<sup>2</sup>, Annapurna Prashanth Patil<sup>2</sup>

<sup>1</sup>Department of Computer and Communication Engineering, NMAM Institute of Technology, NITTE (Deemed to be University), Nitte, India

<sup>2</sup>Department of Information Science and Engineering, Dayananda Sagar College of Engineering, Bangalore, India

## Article Info

### Article history:

Received Jan 29, 2024

Revised Jun 27, 2024

Accepted Jul 26, 2024

### Keywords:

Cloud computing

Cloud environments

Data integrity auditing

Homomorphic linear

authentication

Privacy preservation

## ABSTRACT

The rapid expansion of cloud computing has steered in an era where cloud storage is increasingly prevalent, offering significant advantages in terms of reducing local storage burden. However, this technological shift has also introduced complex security challenges, including data integrity and privacy concerns. In response to these challenges, various data integrity auditing (DIA) protocols have been developed, aiming to enable efficient and secure verification of data stored in cloud environments. This survey paper provides a comprehensive analysis of existing DIA mechanisms, focusing on methods like homomorphic linear authentication, dynamic hash tables, and watermarking techniques for integrity and privacy preservation. It critically evaluates these methods in terms of their advantages, limitations, and the unique challenges they face in practical applications, such as scalability, efficiency in multi-owner contexts, and real-time auditing. Furthermore, the paper identifies key research gaps, including the need for optimizing large-scale data handling, balancing watermarking imperceptibility with embedding capacity, and developing comprehensive solutions for decentralized public auditing. The survey serves as a critical resource for researchers to understand the current background of cloud data integrity auditing and the future directions in this evolving field.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



## Corresponding Author:

Shrinivasa

Department of Computer and Communication Engineering, NMAM Institute of Technology

NITTE (Deemed to be University)

Karkala Taluk, Udipi-574110, Karnataka, India

Email: shrinivasanaik2024@rediffmail.com

## 1. INTRODUCTION

Alongside the growth of cloud computing comes the popularity of cloud storage, large data sets may be moved to the cloud by data owners, which significantly lowers the demand for local storage. However, there are a number of security risks associated with cloud storage, including malware, human mistake, and hardware/software malfunctions. Even with the best efforts made by cloud service provider (CSP) to address security issues, data loss is an unavoidable event [1]. It is possible for CSPs to participate in dishonest tactics in data loss situations for their own financial goals. Owners of data must periodically confirm that the information they have outsourced is accurate. It makes sense for data owners to get their complete dataset back from the cloud in these conditions. But in reality, this strategy is impractical because of its inefficiency.

A data integrity auditing (DIA) protocol developed by [2] in order to solve the current issue, using condensed evidence from the cloud, this approach enables data owners to confirm the accuracy of their data. Because of their simplicity and effectiveness, many DIA techniques were put out after this finding. Enhancing

data integrity auditing's operational effectiveness is one goal, this idea may be shown using several instances, one such instance, which is based on the ideas of Fermat's little theorem, based on the discrete logarithm problem (DLP), is another example. A different strategy is to improve the features of DIA protocols, including third-party public auditing, data dynamics enablement, batch auditing, and key-exposure resilience [3].

Further, published the first privacy-preserving data publishing (PDP) [4] model for group data sharing, utilizing the ring signature technique to generate tags that allowed for both public auditing and user privacy preservation. The PDP technique was presented as a unique way to protect user privacy in shared data. In addition, the added feature of dynamic groups, allowing participants to easily join and exit the group as needed. A PDP approach provides dynamic group functioning, the foundation of this method is broadcast encryption. The PDP approach uses the proxy re-signature technique to assign the user revocation job to the CSP. A PDP protocol was formed to handle group data management while maintaining user identity privacy and traceability. A PDP technique was put up to make data sharing across several uploaders easier [5]. Identity-based cryptography was utilized to develop PDP protocol that protects user privacy in dynamic groups. It's crucial to remember, though, that this method is most likely to be beneficial just for devices with little processing power.

Thereafter, PDP system that manages shared data across groups by using certificate less cryptography [6]. Traditional key escrow and certificate management systems can be replaced with this approach, nevertheless, the design did not include the privacy protection component. A certificate less cryptography shared data system has been described that the trusted third-party auditor (TPA) is able to gain the connection between the data and the public keys at the verification step, even though the method is supposed to guarantee user identity. As a result, it lacked the understanding required to properly protect user privacy [7].

It is crucial to remember that different files are encrypted with different public keys. Rather, these data are frequently encrypted with various public keys and shared among numerous users. One interesting aspect of the application is that it lets users share data with other users only the data they choose to share. In this case, Alice could need to share confidential photos of her pals with her family and also need to send work-related documents to her co-workers. As a consequence, consumers of data can view some files partially provided that the appropriate data owner has granted access. One method that data owners frequently use is encryption, which uses different keys to safeguard different files. This allows various users, according to their own key assignments, to access particular files. Each user must have the secret keys that the data owner has issued [8].

A lack of confidence in the data is caused by the lack of control data owners have over their data kept in cloud storage systems. The main cause of this mistrust is the CSP dishonesty [9]. For instance, malicious CSPs can try to remove material that is rarely accessed without permission in order to free up storage space. As an alternative, they can act as though storing incorrect data, it is possible to manipulate particular data in order to fool owners and make more money. There is now a compromise with the security and dependability of cloud data. A team of researchers created the remote data auditing (RDA) method so that data owners may assess the reliability of CSPs without having to pay more money. Put another way, even after erasing the local copy, a data owner can use the RDA to verify the integrity and correctness of distantly stored data [10]. One typical strategy used by the data owner and CSP to help with RDA implementation is to use a "challenge-proof verify" mechanism while conducting private audits. Under this technique, the CSP verifies the accompanying proofs, while the data owner starts the process of creating data challenges, the tracking of distant data status is made possible by this procedure [11]. The data owner is the only one who conducts the verification process in the context of private auditing. It is possible that the auditing result was tampered with on purpose in an attempt to damage the CSP. It may become increasingly difficult and difficult for the data owner to rely only on private methods as the amount of data grows and the number of auditing requests rises. In order to streamline the public auditing process, a new organization called the TPA was established. It is the duty of TPAs to accept auditing delegations from data owners and carry them out as directed [12]. This procedure helps to remove any doubt regarding auditing findings and improves the energy efficiency of the data owners' verification process. However, these techniques rely on the fundamental supposition that the trusted TPA would behave in a trustworthy manner, which is impractical in real-world situations. Under some circumstances, a trusted TPA could conspire with the data owner to engage in dishonest activities in an effort to avoid fines. In a similar manner, the TPA and the CSP could work together to conceal data corruption incidents. Furthermore, a single centralized TPA is significantly vulnerable when it has a single point of failure [13].

The rapid growth of cloud computing and the increasing reliance on cloud storage have significantly reduced the local storage burdens for data owners but have introduced several complex security challenges. Key among these are vulnerabilities to hardware/software faults, operational errors, and malicious attacks, often leading to data loss incidents. Despite CSPs efforts to secure data, the risk of data loss persists, exacerbated by CSPs' potential lack of transparency due to economic motivation. This situation necessitates robust data integrity verification methods by data owners. Current DIA mechanisms, although efficient compared to traditional methods, are enhanced with issues like the unreliability of auditors, inadequate privacy protection in public auditing, susceptibility to manipulations by malicious CSPs in decentralized systems, limitations in real-time auditing and dispute resolution, and inefficiencies in precise tampering localization.

Therefore, there arises a need for a comprehensive, efficient, and secure cloud storage auditing framework that ensures data integrity and privacy while addressing these critical challenges.

## 2. LITERATURE REVIEW

### 2.1. Related work

In recent years, there has been a significant amount of research conducted to explore the subjects of cloud data integrity and privacy protection. Multiple open verification initiatives have been implemented with the aim of enhancing the integrity of cloud data [14]. Data integrity can be verified by employing public verification, which can be performed by either a user or a designated TPA. The auditor performs a comprehensive examination of the data within the designated time frame and promptly notifies the user of any discrepancies identified during the verification procedure. Additionally, in order to maintain user privacy, it is crucial for the auditor to abstain from acquiring any additional information about user data while functioning as a third party. Several privacy-preserving public auditing techniques have been developed [15]. The advancement of blockchain technology has led to the emergence of several benefits, including trustless consensus, tamper-proofing, traceability, and decentralization. Presently, a considerable number of scholars are actively involved in the investigation of decentralized public auditing techniques. The primary objective of this research is to tackle the problem of malicious auditors and mitigate their adverse effects.

The auditor is widely acknowledged as a dependable and trustworthy authority in the majority of public verification programs. It is imperative to take into account that the reliability of the auditor cannot be assured. In certain circumstances, there is a possibility of collusion between the auditor and the computer system (CS) in order to hide instances of data tampering. The current research lacks contemporary studies that specifically examine the existence of an adversarial auditor. Furthermore, it is imperative to acknowledge that a significant portion of current security protocols designed to minimize the effects of malicious auditors rely heavily on a dependable and centralized third party [16]. The integration of blockchain technology into public auditing methodologies provides a strong and efficient solution for addressing adversarial resistance faced by auditors. However, the consensus technique does present a number of challenges. Before commencing challenge messages, it is crucial for the auditor to acknowledge that a malicious cloud server can exploit public messages to retrieve auditing information.

The objective of this study is to examine a problem that has been identified in decentralized public auditing systems, specifically focusing on the cloud server's ability to predict challenge messages beforehand. In order to ensure the protection of user privacy, we have implemented various measures to prevent any unauthorized access by TPAs to additional user information. The execution of this process occurs concurrently with the execution of other processes. Bian *et al.* [17] conducted a study where they documented the effective deployment of integrity testing for files stored on remote servers using challenge-response protocols. In addition, the verifier is tasked with the responsibility of storing the precomputed checksum for each file that necessitates verification. The current methodology functions as an initial investigation into the problem of integrity verification. Nevertheless, this particular solution is suboptimal when it comes to effectively managing large amounts of data that are stored in cloud storage. The absence of proper consideration for the storage overhead of the verifier is the primary cause for this issue.

Yan and Gui [18] introduced the concept of privacy-preserving public auditing for secure cloud storage. The proposed approach utilizes a hybrid methodology that incorporates both a random masking technique and a homomorphic linear authentication method. The design of the server includes a mechanism that leverages randomness to obscure the linear combination of sampled blocks in its response. The TPA is unable to determine the data payload of the client. Numerous supplementary systems have been devised to augment the integrity audit capabilities within cloud storage. Shen *et al.* [19] introduced a rank-based authenticated dictionary in their research, which utilizes a skip list as its fundamental data structure. The present dictionary enhances the current framework of PDP by integrating the capability to authenticate any modifications made to the stored data. Liu *et al.* [20] focused on the implementation of modifications to the conventional structure of the merkle hash tree (MHT) used for block tag verification. The objective of these modifications was to optimize the efficiency of the MHT. The dynamic hash table, a two-dimensional data structure. The data property information related to dynamic auditing is stored at the TPA location. The data dynamic verification technique was extended to include scenarios involving multiple owners.

The approach proposed by [20] presents a method for conducting shared data integrity auditing, which incorporates the integration of identity-based concealment of sensitive information. The auditing techniques mentioned above rely on epochs, which means that the verifier conducts regular verifications of the outsourced data. The detection of corruption or manipulation can only be performed at the conclusion of each epoch. Furthermore, within these works, the responsibility of verifying is fulfilled by either the client itself or a third-party auditor specifically appointed by the client, rather than a universally acknowledged third-party authority. It is crucial to note that the methods outlined in these works do not provide a conclusive guarantee that the CSP

will acknowledge the client's accusation in the event of inaccurate audit results. The existing challenges have necessitated the advancement of fair arbitration protocols and real-time integrity audits in cloud storage.

The real-time audit scheme for file-oriented cloud storage systems was developed in their study [21], [22]. The implemented scheme allows for the simultaneous execution of auditing procedures alongside each file activity. The full binary hash tree (FBHTree), is a data structure that has been recently introduced. The CSP enables the facilitation of storing file hash values for authentication purposes. According to the proposed plan, the client will initiate a request for a designated segment of the FBHTree. The hash value of the file will be included in the request whenever a file action is executed. The following method provides the client with the ability to verify the accuracy of the file. Nevertheless, there are significant concerns regarding the efficacy of this scheme. The user must store the most recent root hash value of the FBHTree each time a file is downloaded. In order to maintain the integrity of the downloaded file, it is crucial for the client to verify the root hash of the received slice. The verification process involves the comparison of hash values. The approach employed by [23] utilizes the modulation technique known as difference expansion (DE). The process entails the computation of discrepancies between adjacent pixel values, followed by the selection of specific discrepancy values to facilitate the integration of a watermark using the DE technique. In order to address the issues of overflow and underflow, it is crucial to limit the difference value to a predetermined range. The technique of histogram shifting (HS) modulation-based was proposed as an alternative solution. The technique of HS is utilized to create a "gap" next to the peaks of the image histograms. The integration of the watermark component necessitates the displacement of pixels that correspond to the maximum histogram. The pixels have the option to be relocated to the designated gap or remain unaltered.

In a previous study, a method utilizing prediction error expansion (PEE) for data embedding method aims to enhance data integration by amplifying the disparity between a pixel and its projected value. The performance of the system surpasses that of DE and HS because of its improved distribution of the prediction error histogram (PEH) it generates. Zhou *et al.* [24] employed a partitioning technique to deliberately generate an elevation in prediction errors. This technique involves dividing the difference between the current pixel and its expected context. The study conducted by [25] involved the analysis of consecutive prediction errors. The errors mentioned earlier were combined to create a sequence comprising pairs of prediction errors. A novel scheme, known as pairwise PEE, has been devised with the aim of improving imperceptibility. The scheme utilizes both the sequence and the programmable execution hierarchy to achieve its goals.

In this comprehensive review, the authors introduce several innovative schemes and protocols addressing various challenges in the domains of cloud storage, internet of things (IoT), fog-cloud computing, mobile crowd-sensing, edge computing, and data privacy protection. They propose a ciphertext-policy attribute-based encryption (CP-ABE) scheme for cloud storage with efficient user revocation through user groups [26]–[30]. Additionally, a new resisting on-off attack data forwarding mechanism (OADM) for mobile sensor networks (MSNs) is presented, utilizing hidden markov models (HMM) for node behavior evaluation and effective relay node selection [30]. Another contribution is the dynamic trust relationships aware data privacy protection (DTRPP) mechanism for mobile crowd-sensing, integrating key distribution and trust management [31]. The authors also investigate content caching (CC) and user association (UA) optimization for edge computing, addressing the NP-hard nature of the problem with a proposed algorithm [32]. Furthermore, they explore the integration of big data and artificial intelligence (AI) and its implications in social networks, healthcare, and finance [33], [34]. In the context of cloud storage, various identity-based provable data possession schemes are introduced, such as identity-based privacy-preserving provable data possession scheme (ID-P3DP), ID-based PDP with compressed cloud storage, and an identity-based remote data possession checking scheme with dynamic update capability [35]–[39]. The authors improve upon existing work, presenting a more expressive access control policy based on attributes and relying on standard assumptions. They also propose a capability-based privacy protection handover authentication mechanism in software defined network (SDN)-based 5G HetNets [40]. The study introduces Polisma, a framework for learning attribute-based access control (ABAC) policies from data, combining data mining and machine learning techniques. An improved UCSA (iUCSA) protocol is provided, addressing weaknesses in a previous scheme [41]–[45]. Furthermore, the novel concept of provable data possession with outsourced data transfer (DT-PDP) is introduced, satisfying security requirements for data integrity, privacy, and transferability, with computation outsourced to public cloud servers [46], [47]. The authors re-consider the notion of proof of retrievability (PoR) protocol and propose the concept of admissible PoR protocol, imposing additional conditions [48]. The paper presents the first constructions of identity-based encryption and hierarchical identity-based encryption based on the hardness of the Diffie-Hellman problem [49]. Finally, a new remote data possession checking (RDPC) scheme with a designated verifier is introduced, ensuring data integrity based on the computational Diffie-Hellman assumption [50]. Table 1 shows the survey table.

## 2.2. Discussion

Current methods like homomorphic linear authentication are not fully optimized for large-scale data handling. Improvements are needed in scalability and dynamics, reducing the computational burden on time-based auditing (TPAs), efficient management in multi-owner contexts, streamlining the arbitration process,

developing real-time auditing solutions, balancing imperceptibility and embedding capacity in watermarking, optimizing watermarking techniques with minimal overhead, and enhancing the PEE method for data embedding. Additionally, comprehensive solutions for decentralized public auditing are needed to address challenges in resisting malicious auditors and ensuring privacy protection. Reducing computational overhead is crucial for the effectiveness of dynamic auditing scenarios.

Table 1. Survey table

Ref.	Method	Advantages	Disadvantages	Research gap
[2]	Homomorphic linear authentication with random masking	Preserves data content privacy during audits	Complex computations for large datasets	Needs optimization for handling large-scale data
[3]	Classic MHT construction for block tag verification	Improved efficiency for integrity audit	Limited scalability for dynamic data	Scalability and dynamics of data not fully addressed
[4]	Rank-based authenticated dictionary over a skip list	Supports provable updates to stored data	Increased complexity for data structure maintenance	Optimal data structure design for dynamic data
[5]	Dynamic hash table located at TPA for auditing	Efficient dynamic auditing	Increased overhead at TPA	Reducing TPA's computational burden
[6]	Data dynamic verification for multiple owners	Extends auditing to multi-owner scenarios	Complexity increases with more owners	Efficient management in multi-owner contexts
[10]	Signature exchange for fair arbitration	Ensures fair dispute resolution between parties	Inefficiency due to signature verification	Streamlining arbitration process
[12]	FBHTree for real-time audit	Immediate tampering detection	High overhead for verification	Reducing verification overhead
[15]	HS in watermarking	Reduces distortion, adaptable	Extra overhead due to additional data embedding	Balancing imperceptibility and embedding capacity
[20]	Identity-based shared data integrity auditing	Hides sensitive information during audit	Epoch-based, not real-time	Developing real-time auditing solutions
[14]	DE modulation in watermarking	Prevents overflow and underflow in watermarking	Additional overhead for auxiliary information	Optimizing watermarking with minimal overhead
[17]	Image classification process for watermarking	Identifies best areas in an image for watermarking	Complex classification process	Streamlining watermarking in diverse image types
[18]	PEE for data embedding	Superior performance in data embedding	Requires careful selection of prediction errors	Enhancing PEE method for broader applications
[26]	CP-ABE with user groups	Efficient user revocation for cloud storage	Not that much efficient	Further exploration of user group dynamics and scalability

### 3. CONCLUSION

The exploration of cloud storage integrity and privacy in this survey highlights significant advancements and underscores persisting challenges in the field. As cloud computing continues to evolve, it becomes imperative to focus on developing more scalable, efficient, and real-time data integrity auditing mechanisms. Future research should prioritize optimizing methods for handling large-scale data, enhancing real-time auditing capabilities, and furthering watermarking techniques for balanced imperceptibility and embedding capacity. Additionally, there is an essential need to address the complexities of multi-owner data environments and to refine decentralized public auditing systems to combat the risks posed by malicious auditors. Innovations in these areas could significantly enhance the security, privacy, and efficiency of cloud storage systems, thereby fostering greater trust and reliability in cloud-based services. This progression will not only benefit the cloud computing industry but also offer a more secure and efficient experience for end-users across various sectors. In charting the course for future advancements, the following areas present ripe opportunities for research and development, addressing current limitations and steering the field towards enhanced efficiency and innovation. Focusing on these aspects will contribute to the evolution of robust solutions in cloud storage integrity and privacy: i) watermarking techniques, such as HS, face challenges in achieving a balanced trade-off between imperceptibility and embedding capacity; ii) future work should focus on methods that can optimize this trade-off, ensuring watermarking effectiveness in various applications; and iii) further enhancement of the PEE method for data embedding is needed to broaden its applications and ensure careful selection of prediction errors.

### REFERENCES





- [1] Y. Miao, J. Ma, X. Liu, J. Weng, H. Li, and H. Li, "Lightweight fine-grained search over encrypted data in fog computing," *IEEE Transactions on Services Computing*, vol. 12, no. 5, pp. 772–785, Sep. 2019, doi: 10.1109/TSC.2018.2823309.
- [2] M. Jia, Z. Yin, D. Li, Q. Guo, and X. Gu, "Toward improved offloading efficiency of data transmission in the iot-cloud by leveraging secure truncating OFDM," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4252–4261, Jun. 2019, doi:

- 10.1109/JIOT.2018.2875743.
- [3] J. Sun, S. Hu, X. Nie, and J. Walker, "Efficient ranked multi-keyword retrieval with privacy protection for multiple data owners in cloud computing," *IEEE Systems Journal*, vol. 14, no. 2, pp. 1728–1739, Jun. 2020, doi: 10.1109/JSYST.2019.2933346.
  - [4] X. Gao *et al.*, "Achieving low-entropy secure cloud data auditing with file and authenticator deduplication," *Information Sciences*, vol. 546, pp. 177–191, Feb. 2021, doi: 10.1016/j.ins.2020.08.021.
  - [5] C. Hahn, H. Kwon, D. Kim, and J. Hur, "Enabling fast public auditing and data dynamics in cloud services," *IEEE Transactions on Services Computing*, vol. 15, no. 4, pp. 2047–2059, Jul. 2022, doi: 10.1109/TSC.2020.3030947.
  - [6] M. Suguna and S. M. Shalinie, "Privacy preserving data auditing protocol for secure storage in mobile cloud computing," in *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Mar. 2017, pp. 2725–2729, doi: 10.1109/WiSPNET.2017.8300258.
  - [7] X. Liu, W. Sun, W. Lou, Q. Pei, and Y. Zhang, "One-tag checker: Message-locked integrity auditing on encrypted cloud deduplication storage," in *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, pp. 1–9, May 2017, doi: 10.1109/INFOCOM.2017.8056999.
  - [8] X. Yang, R. Lu, J. Shao, X. Tang, and A. A. Ghorbani, "Achieving efficient secure deduplication with user-defined access control in cloud," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 1, pp. 591–606, Jan. 2022, doi: 10.1109/TDSC.2020.2987793.
  - [9] L. Liu, Y. Zhang, and X. Li, "KeyD: secure key-deduplication with identity-based broadcast encryption," *IEEE Transactions on Cloud Computing*, vol. 9, no. 2, pp. 670–681, Apr. 2021, doi: 10.1109/TCC.2018.2869333.
  - [10] Y. Shin, D. Koo, J. Yun, and J. Hur, "Decentralized server-aided encryption for secure deduplication in cloud storage," *IEEE Transactions on Services Computing*, vol. 13, no. 6, pp. 1–1, 2019, doi: 10.1109/TSC.2017.2748594.
  - [11] H. Zhao and Y. Wang, "A big data-driven financial auditing method using convolution neural network," *IEEE Access*, vol. 11, pp. 41492–41502, 2023, doi: 10.1109/ACCESS.2023.3269438.
  - [12] X. Yang, X. Pei, M. Wang, T. Li, and C. Wang, "Multi-replica and multi-cloud data public audit scheme based on blockchain," *IEEE Access*, vol. 8, pp. 144809–144822, 2020, doi: 10.1109/ACCESS.2020.3014510.
  - [13] T. Subha and S. Jayashri, "Efficient privacy preserving integrity checking model for cloud data storage security," in *2016 Eighth International Conference on Advanced Computing (ICoAC)*, pp. 55–60, Jan. 2017, doi: 10.1109/ICoAC.2017.7951745.
  - [14] L. Deng, B. Yang, and X. Wang, "A lightweight identity-based remote data auditing scheme for cloud storage," *IEEE Access*, vol. 8, pp. 206396–206405, 2020, doi: 10.1109/ACCESS.2020.3037696.
  - [15] Z. Liu, L. Ren, Y. Feng, S. Wang, and J. Wei, "Data integrity audit scheme based on quad merkle tree and blockchain," *IEEE Access*, vol. 11, pp. 59263–59273, 2023, doi: 10.1109/ACCESS.2023.3240066.
  - [16] P. Huang, K. Fan, H. Yang, K. Zhang, H. Li, and Y. Yang, "A collaborative auditing blockchain for trustworthy data integrity in cloud storage system," *IEEE Access*, vol. 8, pp. 94780–94794, 2020, doi: 10.1109/ACCESS.2020.2993606.
  - [17] G. Bian, Y. Fu, B. Shao, and F. Zhang, "Data integrity audit based on data blinding for cloud and fog environment," *IEEE Access*, vol. 10, pp. 39743–39751, 2022, doi: 10.1109/ACCESS.2022.3166536.
  - [18] H. Yan and W. Gui, "Efficient identity-based public integrity auditing of shared data in cloud storage with user privacy preserving," *IEEE Access*, vol. 9, pp. 45822–45831, 2021, doi: 10.1109/ACCESS.2021.3066497.
  - [19] W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, "Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 2, pp. 331–346, Feb. 2019, doi: 10.1109/TIFS.2018.2850312.
  - [20] J. Liu, X. A. Wang, Z. Liu, H. Wang, and X. Yang, "Privacy-preserving public cloud audit scheme supporting dynamic data for unmanned aerial vehicles," *IEEE Access*, vol. 8, pp. 79428–79439, 2020, doi: 10.1109/ACCESS.2020.2991033.
  - [21] M. Imran, S. Hamid, and M. A. Ismail, "Advancing process audits with process mining: a systematic review of trends, challenges, and opportunities," *IEEE Access*, vol. 11, pp. 68340–68357, 2023, doi: 10.1109/ACCESS.2023.3292117.
  - [22] D. He, S. Zeadally, and L. Wu, "Certificateless public auditing scheme for cloud-assisted wireless body area networks," *IEEE Systems Journal*, vol. 12, no. 1, pp. 64–73, Mar. 2018, doi: 10.1109/JSYST.2015.2428620.
  - [23] X. Tang, Y. Huang, C.-C. Chang, and L. Zhou, "Efficient real-time integrity auditing with privacy-preserving arbitration for images in cloud storage system," *IEEE Access*, vol. 7, pp. 33009–33023, 2019, doi: 10.1109/ACCESS.2019.2904040.
  - [24] X. Zhou, D. He, J. Ning, M. Luo, and X. Huang, "AADEC: Anonymous and auditable distributed access control for edge computing services," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 290–303, 2023, doi: 10.1109/TIFS.2022.3220030.
  - [25] Y. S. Abdulsalam and M. Hedabou, "Decentralized data integrity scheme for preserving privacy in cloud computing," in *2021 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC)*, pp. 607–612, Jun. 2021, doi: 10.1109/SPAC53836.2021.9539946.
  - [26] J. Li, W. Yao, Y. Zhang, H. Qian, and J. Han, "Flexible and fine-grained attribute-based data storage in cloud computing," *IEEE Transactions on Services Computing*, vol. 10, no. 5, pp. 785–796, Sep. 2017, doi: 10.1109/TSC.2016.2520932.
  - [27] H. Yan, J. Li, J. Han, and Y. Zhang, "A novel efficient remote data possession checking protocol in cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 78–88, Jan. 2017, doi: 10.1109/TIFS.2016.2601070.
  - [28] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, "Secure integration of IoT and cloud computing," *Future Generation Computer Systems*, vol. 78, pp. 964–975, Jan. 2018, doi: 10.1016/j.future.2016.11.031.
  - [29] P. Sirohi and A. Agarwal, "Cloud computing data storage security framework relating to data integrity, privacy and trust," in *2015 1st International Conference on Next Generation Computing Technologies (NGCT)*, pp. 115–118, 2015, doi: 10.1109/NGCT.2015.7375094.
  - [30] D. Wu, F. Zhang, H. Wang, and R. Wang, "Security-oriented opportunistic data forwarding in mobile social networks," *Future Generation Computer Systems*, vol. 87, pp. 803–815, Oct. 2018, doi: 10.1016/j.future.2017.07.028.
  - [31] D. Wu, S. Si, S. Wu, and R. Wang, "Dynamic trust relationships aware data privacy protection in mobile crowd-sensing," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2958–2970, Aug. 2018, doi: 10.1109/JIOT.2017.2768073.
  - [32] Y. Li, H. Ma, L. Wang, S. Mao, and G. Wang, "Optimized content caching and user association for edge computing in densely deployed heterogeneous networks," *IEEE Transactions on Mobile Computing*, vol. 21, no. 6, pp. 2130–2142, 2022, doi: 10.1109/TMC.2020.3033563.
  - [33] Q. Yi, M. Xu, S. Yi, and S. Xiong, "Identifying untrusted interactive behaviour in enterprise resource planning systems based on a big data pattern recognition method using behavioural analytics," *Behaviour & Information Technology*, vol. 41, no. 5, pp. 1019–1034, Apr. 2022, doi: 10.1080/0144929X.2020.1851767.
  - [34] J. Li, Z. Ye, and C. Zhang, "Study on the interaction between big data and artificial intelligence," *Systems Research and Behavioral Science*, vol. 39, no. 3, pp. 641–648, May 2022, doi: 10.1002/sres.2878.
  - [35] M. Yildirim, A. Çınar, and E. Cengil, "Investigation of cloud computing based big data on machine learning algorithms," *Bitlis Eren Üniversitesi Fen Bilimleri Dergisi*, vol. 10, no. 2, pp. 670–682, Jun. 2021, doi: 10.17798/bitlisfen.897573.
  - [36] K. Valaskova, P. Ward, and L. Svabova, "Deep learning-assisted smart process planning, cognitive automation, and industrial big data analytics in sustainable cyber-physical production systems," *Journal of Self-Governance and Management Economics*, vol. 9, no. 2, 2021, doi: 10.22381/jsme9220211.





- [37] J. Ni, K. Zhang, Y. Yu, and T. Yang, "Identity-based provable data possession from RSA assumption for secure cloud storage," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 3, pp. 1753–1769, May 2022, doi: 10.1109/TDSC.2020.3036641.
- [38] Y. Yang, Y. Chen, F. Chen, and J. Chen, "An efficient identity-based provable data possession protocol with compressed cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 1359–1371, 2022, doi: 10.1109/TIFS.2022.3159152.
- [39] G. Bian, R. Zhang, and B. Shao, "Identity-based privacy preserving remote data integrity checking with a designated verifier," *IEEE Access*, vol. 10, pp. 40556–40570, 2022, doi: 10.1109/ACCESS.2022.3166920.
- [40] Y. Ji, B. Shao, J. Chang, and G. Bian, "Flexible identity-based remote data integrity checking for cloud storage with privacy preserving property," *Cluster Computing*, vol. 25, no. 1, pp. 337–349, Feb. 2022, doi: 10.1007/s10586-021-03408-y.
- [41] Y. Yuan, J. Zhang, W. Xu, and Z. Li, "Identity-based public data integrity verification scheme in cloud storage system via blockchain," *The Journal of Supercomputing*, vol. 78, no. 6, pp. 8509–8530, Apr. 2022, doi: 10.1007/s11227-021-04193-6.
- [42] X. Zhou, M. Luo, P. Vijayakumar, C. Peng, and D. He, "Efficient certificateless conditional privacy-preserving authentication for VANETs," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 7, pp. 7863–7875, Jul. 2022, doi: 10.1109/TVT.2022.3169948.
- [43] M. Sedaghat and B. Preneel, "Cross-domain attribute-based access control encryption," *International Conference on Cryptology and Network Security*, pp. 3–23, 2021, doi: 10.1007/978-3-030-92548-2\_1.
- [44] J. Cao, M. Ma, Y. Fu, H. Li, and Y. Zhang, "CPPHA: Capability-based privacy-protection handover authentication mechanism for SDN-based 5G HetNets," *IEEE Transactions on Dependable and Secure Computing*, 2019, doi: 10.1109/TDSC.2019.2916593.
- [45] A. A. Jabal *et al.*, "Polisma - A framework for learning attribute-based access control policies," *Computer Security – ESORICS 2020*, pp. 523–544, 2020, doi: 10.1007/978-3-030-58951-6\_26.
- [46] H. Wang, L. Feng, Y. Ji, B. Shao, and R. Xue, "Toward usable cloud storage auditing, revisited," *IEEE Systems Journal*, vol. 16, no. 1, pp. 693–700, Mar. 2022, doi: 10.1109/JSYST.2021.3055021.
- [47] H. Wang, D. He, A. Fu, Q. Li, and Q. Wang, "Provable data possession with outsourced data transfer," *IEEE Transactions on Services Computing*, vol. 14, no. 6, pp. 1929–1939, Nov. 2021, doi: 10.1109/TSC.2019.2892095.
- [48] J. Chang, B. Shao, Y. Ji, M. Xu, and R. Xue, "Secure network coding from secure proof of retrievability," *Science China Information Sciences*, vol. 64, no. 12, p. 229301, Dec. 2021, doi: 10.1007/s11432-020-2997-0.
- [49] N. Döttling and S. Garg, "Identity-based encryption from the diffie-hellman assumption," *Advances in Cryptology – CRYPTO 2017*, pp. 537–569, 2017, doi: 10.1007/978-3-319-63688-7\_18.
- [50] H. Yan, J. Li, and Y. Zhang, "Remote data checking with a designated verifier in cloud storage," *IEEE Systems Journal*, vol. 14, no. 2, pp. 1788–1797, Jun. 2020, doi: 10.1109/JSYST.2019.2918022.

## BIOGRAPHIES OF AUTHORS







**Shrinivasa**     is working as an Assistant Professor Gd.-III in the Department of Computer and Communication Engineering, NMAM Institute of Technology, Nitte, Karkala. He has about 16 years of teaching and two years of industrial experience. He received his Bachelor of Engineering degree in Computer Science and Engineering and an M.Tech. degree in Computer Science and Engineering with Distinction from Visvesvaraya Technological University, Belagavi. He is pursuing his Ph.D. at Visvesvaraya Technological University, Belagavi. He has published eight papers in reputed journals and also has a patent. His areas of research include cloud computing and security. He is an active member of ISTE. He can be contacted at email: shrinivasanaik2024@rediffmail.com.



**Chandrakala Beturpalya Muddaraju**     working as an Associate Professor, Department of Information Science & Engineering, Dayananda Sagar College of Engineering, Bengaluru, Karnataka, India. She received her Ph.D. Degree in Computer and Information Science and Engineering, Visvesvaraya Technological University, Belagavi, Karnataka. She had been working as an Associate Professor for the past 20 years. Her research interests are in cloud computing, network security, cyber security, artificial intelligence, and machine learning. Published 44 papers in journals and conference. Published 5 patents. Guiding Research Scholars in various domains. She can be contacted at email: chandrakalabm-ise@dayanandsagar.edu.



**Annapurna Prashanth Patil**     is currently working as Dean in Dayananda Sagar College of Engineering. Her areas of interest are mobile ad hoc network (MANET) and wireless sensor networks (WSN). She has 27 years of teaching experience. She can be contacted at email: annapurnaap2@yahoo.com.