SURVEY ON SECURITY AND INTEGRITY OF DATA IN CLOUD COMPUTING

1*Gonavath Manthru Naik, 2Dr.K.Gangadhara Rao

1Research Scholar, Department of CSE, Acharya Nagarjuna University, Guntur, AP.
2Professor & Head, Department of CSE, Acharya Nagarjuna University, Guntur, AP.
*Associate Professors, Deparment of CSE, Kallam Haranadha Reddy Institute of Technology, Guntur, AP.

ABSTRACT: Cloud computing changed the world of Internet. Cloud computing has emerged as a significant paradigm for delivering computing resources and services over the internetWith the help of cloud computing user can easily share, store and retrieve their data from anywhere. Cloud computing is scalable, fast, flexible, and cost-effective technology platform for IT (Information Technology) enabled services over the internet. Cloud computing provides hardware, software and infrastructural storage to many users at a time Most of the times cloud users don't know the exact location of their data or the sources of data stored with their data.Despite the rapid development of cloud computing for many years, data security and trusted computing are still the main challenges in current cloud computing applications. In order to solve this problem, many scholars have carried out a lot of research on this, and proposed many models including data integrity test and secure multi-party calculation. However, most of these solutions face problems such as excessive computational complexity or lack of scalability. In this work, a survey on Security and Integrity of Data in Cloud Computing is presented. Data security and integrity concerns like access control, searchable encryption techniques, key management, ownership proofs and remote integrity check arise are discussed here. This analysis discusses and review the security and integrity of data in cloud computing.

KEYWORDS: Cloud Computing, Data Security, Integrity.

I. INTRODUCTION

Cloud computing is a distributed computing model based on a large shared virtualized computing resource pool, it helps users use powerful computing and storage resources. And it can greatly reduce the burden of data storage on hardware and software for users, which encourages many enterprises and individuals to store their data on cloud servers [1].Cloud computing is defined as the management and release of resources, software, applications, and information as services over the internet on demand. Numerous organizations are utilizing the cloud services because of the economy and technology changes [2]. Over the past several years, cloud computing has made life easier for many people or organizations by allowing people to have access to information from anywhere in the world through the internet.

Cloud computing is a new technology that has recently drawn a lot of interest from both business and academia. By using cloud computing, users can access many types of software's internet services without having to purchase or install them on their computers. According to the National Institute of Standards and Technology, cloud computing (NIST). access across a network to a common pool of adaptable computer resources is a paradigm for delivering useful, on-demand information.

Cloud computing facilitates fast and efficient parallel processing of terabyte-scale data in the virtual environment. In cloud computing, there are three entities (stakeholders) namely Data Owner (DO), Cloud Service Provider (CSP) and user. The DO shares their own data or file on the cloud server. The CSP provides the cloud services for both DO and user. The users access data or file from the cloud server. The users cannot access data randomly by their wishes. Each CSP has its own access policy or right. So, when the users want to access any data or file from the cloud server, they must satisfy the access right to access the requested data from the cloud environment [3].

In the current scenario, the data that needs to be stored is passed on to the remote service provider and the owner himself is not aware of the location of the data which raises a security concern. Thus data security, proof of ownership and recovery period and data protection becomes a prime issue to be addressed in the cloud data migration process. When it comes to cloud data security, no specific new methods are required. Protecting data in the cloud environment is same as protecting it within a traditional data center. Encryption, access control, authentication and identity, data masking, secure deletion, and integrity checking are all data protection methods that are applied in cloud computing [4].

The rapid growth of cloud computing has brought numerous benefits and opportunities, but it has raised concerns about data security. To protect sensitive data stored in the cloud is crucial and to ensure data privacy, confidentiality, and integrity for cloud users [5]. Despite the great success of cloud storage, it also faces various challenges, and its security, reliability and privacy have always been serious issues. After the user stores the data on the cloud server, the server provider may damage or delete the user data due to various factors, verifying the integrity of outsourced data becomes a crucial issue in cloud storage. Remote data integrity audit technology is very convenient and safe to help users check the integrity of data stored in outsourced environment.

While cloud computing offers several benefits to consumers, its rapid development also presents considerable risks. Ensuring the integrity and privacy of data stored in cloud environments poses a significant challenge of utmost importance. The Cloud Service Provider (CSP) is a prime target for malicious actors due to its role in the cloud storage architecture, wherein it maintains a substantial volume of client data in a centralized manner, resulting in considerable financial gains. Despite the existence of several cloud data auditing tools, instances of cloud data leakage and manipulation continue to occur sporadically. This is because when users transfer data to cloud storage, they relinquish physical custody and control of the data. Cloud service providers try to protect their reputation by hiding any data-related problems. Guaranteeing the confidentiality and integrity of data in cloud environments substantially influences the evolution of cloud computing and cloud storage technologies [6]. Data Privacy and Integrity in cloud is discussed as follows:

Data Privacy: Continuous data expansion leads to several security issues where data privacy is one of the security challenges associated with cloud computing. Cloud computing 's privacy challenges include the uncertainty associated with risk management, increasing market demands the advent of timely deployment of innovative business models and their effect onspecific regulatory compliance, customer privacy, data protection concerns in design leading to lack of clarity and poor data quality. Data privacy protocols apply to data and software communication protocols, data processing protocols impact data privacy mostly in cloud [7].
Data Integrity: Data integrity is useful for data authenticity, and guarantees data consistency and reliability as well. Lack of credibility is a big challenge in the cloud world, because of data privacy problems, there are many security threats and attacks. Data integrity ensures that the data is not modified or altered without the knowledge of the user. When the intruder or unauthorized person has control to the stored data, data privacy is at stake. The user data can be attacked by data modification, Tag forgery attack and data leakage attack. Monitoring data integrity is important to prevent data manipulation and data crashing in cloud providers. Various mechanisms are adopted to prevent cloud environment data integrity attacks such as cooperative provable data possession (CPDP), which combines hash indexing hierarchy and homomorphic verifiable response [8].

Data security is a top concern for consumers interested in cloud computing. This technology needs the right security concepts and practises to soothe users' concerns. Most users of cloud services are concerned that their personal information might be moved to other cloud service providers or utilised for unrelated purposes. To solve these issues and present an effective technique we reviewed the data security and integrity techniques in cloud. In this work, a survey on data security and integrity of data in cloud computing is presented. The rest of the work is arranged as follows: The section II describes the literature survey. The section III discusses the few of the data security and integrity techniques in cloud computing. The section IV analyzes the result analysis of various data security and integrity in cloud computing. The section V ends with Conclusion.

II. LITERATURE SURVEY

There are many security mechanisms that have been put forth by various researchers. In this section, the authors have presented a review of the literature on the subject.

X. Pei, Y. Wang, W. Yao, J. Lin and R. Peng et. al., [9] describes Security Enhanced Attribute Based Signcryption for Private Data Sharing in Cloud. This paper proposes the identity and attribute based signcryption algorithm to enhance the security of storage and sharing of remote data. The proxy re-encryption and multi- attribute authority based signcryption techniques are used to achieve fault-tolerant attributes management and collusion resistant system. In the Healthcare system, the attribute-based signature, encryption and signcryption methods are separately applied to scenarios of different data security levels in order to keep data access efficiency. Accordingly, the security properties and the access efficiencies of proposed algorithm are compared with known methods.

F. Fatemi Moghaddam, A. Majd, M. Ahmadi, T. Khodadadi and K. Madadipouya et. al., [10] describes A dynamic classification index to enhance data protection procedures in cloud-based environments. dynamic index classification model has been presented in this paper to ensure data security in cloud computing environments based on their attributes. Index Classification (IC) value has been defined based on three parameters (i.e. data confidentiality, data integrity, and data availability) and various sub-parameters to classify data into 4 main groups. The evaluation procedure of the suggested model involves two main parameters: functionality, and security. Each parameter was examined by simulation processes to investigate strengths and weaknesses of this model in comparison with other models. In overall, the results show that this model has met defined demands of this research to enhance the reliability and efficiency of data protection in cloud computing environments.

Sumathi M, Rajkamal M, Dr B Gomathy, I Infant Raj, Dr. Sushma Jaiswal and D. Swathi et. al., [11] presents Secure Blockchain Based Data Storage and Integrity Auditing in Cloud. Implemented secure data storage with the help of blockchain based data storage. Provides the strongest security guarantee compared with existing schemes. Double SHA (Secure Hash Algorithm) provides collision free secure storage compared to other techniques. In this system, public owners and data owner integrity is verified for providing highest accuracy. The obtained results indicate that presented SHA technique provides better security and results to user data in an effective manner. Future work is focused on TPA (Third Party Auditor) that may concurrently handle multiple audit sessions from different users for their outsourced data files. Further the privacy-preserving public auditing protocol is extended into a multi-user setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency.

Parin Patel, Hiren Patel et. al., [12] presents LCHAIN: A Secure Log Storage Mechanism using IPFS and Blockchain Technology. We recommend the usage of Blockchain technology due to its inherent feature of immutability to address the issue of log tempering. We present LChain which provides immutable storage of logs with tracing. Blockchain technology helps yp create immutable logs but also offers non-repudiation and scalability. Smart contracts are used for efficient searching. This system has less validation and storage overhead. The proposed system creates trust between Cloud users and Cloud storage servers using IPFS and Blockchain technology.

H. Anwarbasha, S. Sasi Kumar & D. Dhanasekaran et. al., [13] presents An efficient and secure protocolfor checking remote data integrityin multi-cloud environment This paper presents a Dynamic Level Based Integrity Checking Protocol (DA-ICP) for storing data in multicloud environment. The proposed method introduces Provable Data Possession (PDP) approach which enables a user who outsources the data at an untrusted multi-cloud for ensuring that the server possesses the original data without downloading it. This model creates a probabilistic proof of possession by sampling an arbitrary collection of blocks from server that considerably minimizes the cost. The effective and secured outsourced data has been resolved using public key cryptography and undergo encryption using Efficient-PDP (EPDP). During experimentation, the presented DA-ICP shows a maximum accuracy of 96.78%. The proposed method uses Multi-cloud in DA-ICP which produces an efficient output than other existing techniques.

S. Gokulakrishnan and J. M. Gnanasekar et. al., [14] describes Data Integrity and Recovery Management in Cloud Systems. A new methodology is focused and proposed data recovery and data management to assure high-level scalability and high order reliability to provide fault recognition and fault tolerance cloud-based systems. We propose a methodology of segmenting data and generating tokens for the data split-up by adding the address of the cloud or locations of the cloud storage using the tailing method. Thus the missing segment of any faulty node is easily recognized within a short range of limits and will get the data backup from the neighboring nodes.

T. Li, J. Chu and L. Hu et. al., [15] describes CIA: A Collaborative Integrity Auditing Scheme for Cloud Data With Multi-Replica on Multi-Cloud Storage Providers. A new model for remote data integrity auditing: CIA (Collaborative Integrity Auditing) is presented. In addition to the reduction in computational overhead, the proposed scheme provides unprecedented support for free data blocking. The proposed scheme employs only hash functions in the calculation, which has a negligible computational overhead compared to the traditional bilinear pairing-based schemes. Theoretical analysis and experimental results show that the proposed scheme provides high efficiency and flexibility with security assurance, and can be used as a lightweight alternative to traditional remote data integrity auditing schemes in multi-replica multi-CSP scenarios.

Y. Hou, S. Garg, L. Hui, D. N. K. Jayakody, R. Jin and M. S. Hossain et. al., [16] describes A Data Security Enhanced Access Control Mechanism in Mobile Edge Computing In this paper, a data security enhanced Fine-Grained Access Control mechanism (FGAC) is proposed to ensure data security during data access in mobile edge computing. In FGAC, a dynamic fine-grained trusted user grouping scheme based on attributes and metagraphs theory was first designed. Secondly, the scheme was combined with the traditional role-based access control mechanism to assign roles to users based on user group credibility. And then, based on attribute matching the user authentication further verifies whether the user is

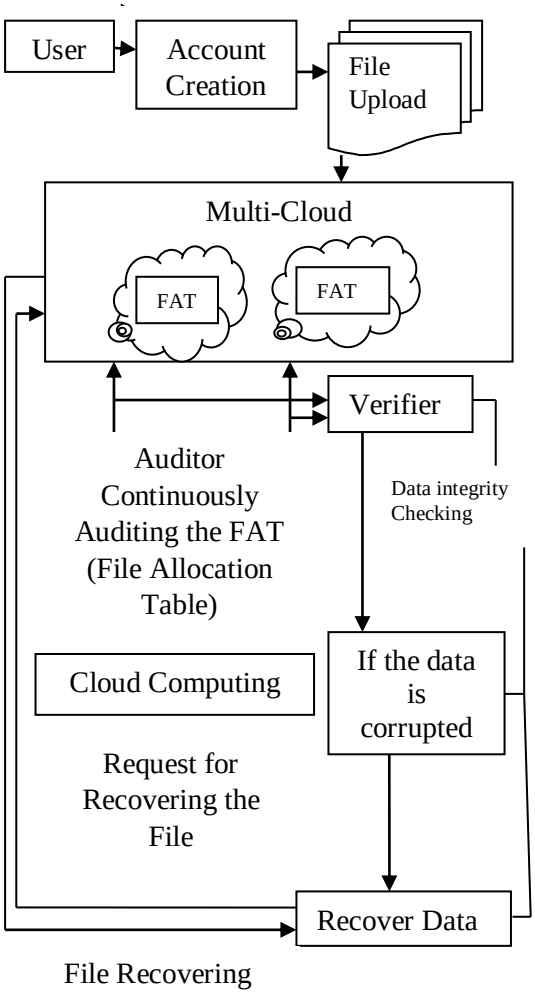
allowed to perform the access operations to achieve fine-grained data protection. Experimental results show that FGAC can effectively identify malicious users and make group adjustments, while achieving fine-grained access control and assure the data security during the data access process in mobile edge computing.

R. Awadallah and A. Samsudin et. al., [17] discusses Using Blockchain in Cloud Computing to Enhance Relational Database Security. We proposed two systems to improve cloud-RDB namely, agile BC-based RDB and secure BC-based RDB. Both are distributed among several cloud service providers based on the Byzantine Fault Tolerance consensus. Additionally, both rely on linking records to each other using the SHA-256. At the same time, secure BC-based RDB uses a proof-of-work consensus to make data offensive operation impossible. On the basis of performance of both systems' and security analysis, the agile BC-based RDB is highly suggested for the high throughput database. On the other hand, the secure BC-based RDB is recommended for RDB that contains sensitive data and low throughput performance. The improved RDB is flexible and can be operated according to the data owner's specifications. However, it is a financially stressful and arduous system.

III. CLOUD INTEGRITY MECHANISM

In the modern day, maintaining enormous volumes of data for huge companies that operate abroad has proven difficult. Because cloud storage provides better archiving, distribution, and upload capabilities, many firms have switched to it. Maintaining data confidentiality and integrity while, also assisting with data security are the main concerns that cloud computing needs to cope with. Encryption, access control, authentication and identity, data masking, secure deletion, and integrity checking are all data protection methods that are applied in cloud computing. Few of the cloud security and integrity techniques are discussed in this section.

S. Suganya and P. M. D. R. Vincent et. al., [18] describes Improving cloud security by enhancing remote data integrity checking algorithm a unused successive cloud auditing technique is presented and it provides uninterrupted certificates to the user and as well auditing the data which is verified with help of fresh data integrity checking protocol. The data integrity technique will address the issues like if attacker corrupts the data in Multi-Cloud, the proposed continuous auditing method will help the verifier to perform block level and file level checking to ensure this process. The objective of this work is to provide the secure cloud service and this process to be efficient in all cases which will be illustrated in this paper. The Fig. 1 shows the detailed architecture. In this paper, we analyze many issues in the cloud server; in that we have taken data integrity with auditing is one of the main issues to check whether the data has been stored in a correct location and monitoring those data frequently. That file has been stored in the Multi-cloud storage in an encrypted format.



over Cloud service

In that multi-cloud, file allocation table has been maintained for storing the data. The file allocation table should be segmented into many blocks also for each and every block signature must be maintained that signature should be matched with auditor's signature only then we came to know that the file is not corrupted, and the file is not modified it maintains the only original file. The proposed continuous auditing technique audits the data which is verified with the help of data integrity protocol based on MD5 (Message Digest Algorithm. Furthermore, we are using dynamic block generation method for chunking the data which is stored in FAT (file allocation table). This proposed system is efficient, provides more security to the cloud service provider and heavy confidential against cloud auditing. However more concentrate is need for managing the continuous auditing that is future technology helps us to audit the data without checking the data integrity.

Shipra Yadava, Keshao D. Kalaskarb and Pankaj Dhumane et. al., [20] describes Design And Implementation Technique For Cloud Computing Security Improvement. The proposed data security model utilized three-level guard framework structure, in which each floor plays out its own obligation to guarantee that the information security of cloud as shown in Fig. 2. The first phase: strong authentication is achieved by using OTP.

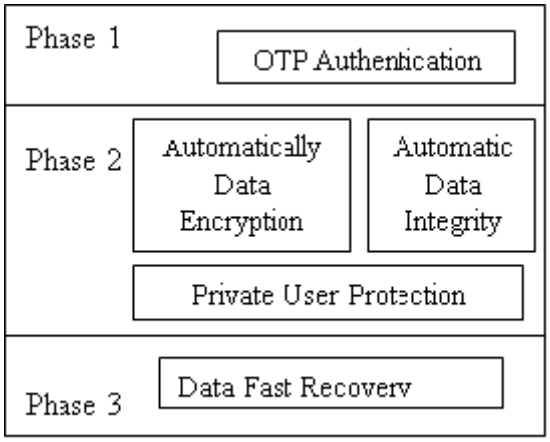


Fig. 2: Proposed data security model

According to the simulation results, in the authentication phase in the proposed data security model, OTP is used as two-factor authentication software. OTP archived more password strength security than other authentication systems (BIN and static password). This appears by comparing between OTP, BIN, and static password authentication systems based on the space time size and entropy bits. From the simulation results of the second phase in the proposed data security model, test the proposed system in Ubunto Amazon Micro Instance EC2, and from randomness and performance evaluation to eight modern encryption algorithms AES is the best encryption algorithm in Ubunto Amazon Micro Instance EC2. In addition to the randomness and performance evaluation, data integrity must be ensured. Moreover, the proposed data security model encourages users to use true-crypt to encrypt his/her sensitive data. From the comparison and performance evaluation, fast recovery of data achieved to the user. These appear in the proposed data security model third phase. From the comparison and performance evaluation, cloud computing depend on some condition, however it has advanced security technologies rather than traditional desktop.
Yuan Ping, Yu Zhan, Ke Lu and Baocang Wang et. al., [21] describes Public Data Integrity Verification Scheme for Secure Cloud Storage. In this paper, we first propose a public data integrity verification scheme based on the algebraic signature and elliptic curve cryptography. This scheme not only allows the third party authority deputize for users to verify the outsourced data integrity, but also resists malicious attacks such as replay attacks, replacing attack and forgery attacks. Data privacy is guaranteed by symmetric encryption. Furthermore, we construct a novel data structure named divide and conquer hash list, which can efficiently perform data updating operations, such as deletion, insertion, and modification. Unlike traditional solutions, the proposed scheme introduces symmetric encryptions to protect data privacy that is critical and suitable for practical use. Meanwhile, a novel data structure named DCHL is designed to support dynamic updating with low communication and computational costs. Theoretical analysis shows that the TPA can detect the corrupted data blocks with a high probability, Even though the CSP conducts the misbehavior. Furthermore, real experimental results make the proposed scheme substantially more convincing.Moreover, no single method can achieve perfect data integrity verification for various scenarios.Due to the query, the complexities of the operations on a linked list are not constant in differentscenarios. Frequent data changes on a massive number of data blocks put forward higher requirementsfor the query performance. Therefore, how to improve the efficiency with specially designed datastructures is expected to be tackled in the future.

B. Sowmiya, E. Poovammal, K. Ramana, S. Singh and B. Yoon et. al., [22] describes Linear Elliptical Curve Digital Signature (LECDS) With Blockchain Approach for Enhanced

Security on Cloud Server. Linear Elliptical Curve Digital Signature (LECDS) is adopted with Hyperledger blockchain, to prevent private data loss. The elliptic curve digital signatures algorithms (ECDSA) are used as the basis for bitcoin security. The Fig. 3 shows the block diagram of presented approach.

The key feature of ECDSA is shorter key length with high degree of security similar to RSA. The proposed Linear Elliptical Curve Digital Signature (LECDS) with hyperledger blockchain framework provides security for sensitive and non-sensitive information from a cloud database using shorter key length.

The proposed Linear Elliptical Curve Digital Signature (LEADS) with hyperledger blockchain framework provides security for sensitive and non-sensitive information from a cloud database. The cloud security method first classifies the user information before cloud storage. Data classification is determined based on the availability, integrity, and confidentiality of the security target and the data classification's sensitivity. Data owners must monitor the data throughout its life cycle and carefully analyze each piece of data to determine the potential impact of unauthorized leakage or destruction of these data.

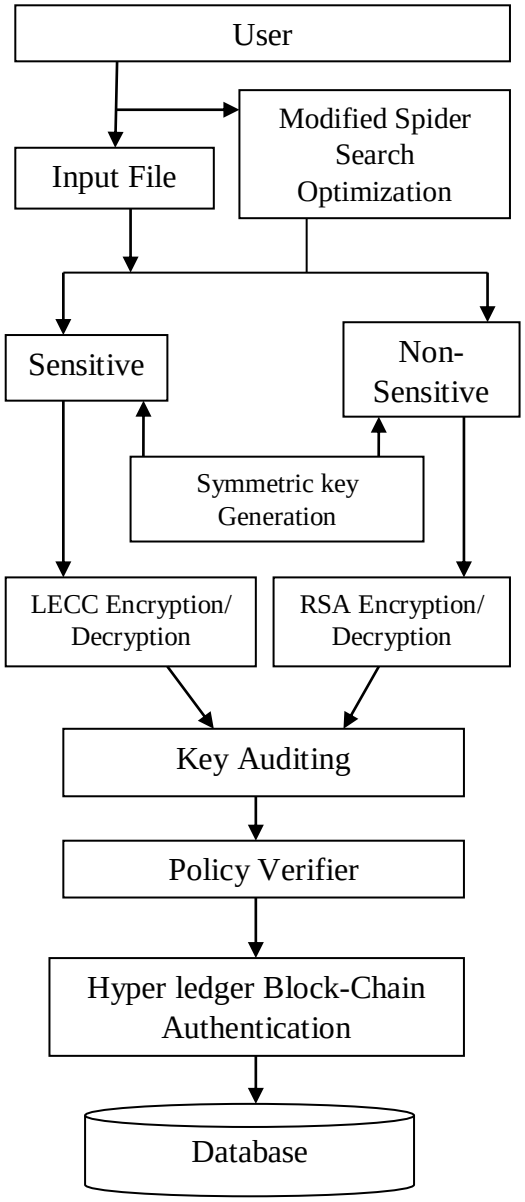


Fig. 3: Proposed Method Block Diagram

Symmetric key generation is used to provide a public key for each data for service verification. The Linear regression method is used to classify the user information into two classes namely sensitive and non-sensitive.

The non-sensitive data is encrypted using RSA and sensitive data is encrypted using LECC method. Modified Spider optimization search Algorithm (MSOA) is used to verify the integrity of outsourced data and search user query information in a cloud server. The hyper ledger blockchain verifies the user policy to create a private network through which the user communicates the cloud. In the analysis of the proposed method, the results are evaluated using various performance metrics such as security, throughput, classification accuracy and error rate. This overall proposed method LECC method, provides better performance compared to another existing method. Although this work has addressed security, privacy and usefulness, the limitations are cost and time taken to split anrd encrypt the sensitive and non-sensitive data in Hyperledger platform.

W. Susilo, P. Jiang, F. Guo, G. Yang, Y. Yu and Y. Mu et. al., [23] describes EACSIP: Extendable Access Control System With Integrity Protection for Enhancing Collaboration in the Cloud. In this system, a user encrypts and uploads his/her data to the cloud with an access policy, such that only people who satisfy that access policy can decrypt the data. When a recipient would like to enable another person who is originally unauthorized by the original access policy, this recipient will need to extend the access policy by adding a new policy that includes the new person - hence, the notion of Extendable Access Control System. Admitting new users to access the uploaded data is an important requirement in enhancing collaborations. The main issue is with regards to the integrity protection during the process of extending the access policy. When a new access policy is added, the cloud has to be sure that the extended access policy remains guarding the same encrypted data as the original access policy, even though the cloud cannot decrypt this ciphertext, which is a challenging problem to solve. The construction of EACSIP is built on top of a novel cryptographic primitive, namely Functional Key Encapsulation with Equality Testing (FKE-ET). The security proof and the performance evaluation of EACSIP are provided in this work.Compared with the relevant schemes in the literature, security analysis and performance evaluations show that the proposed scheme gains some advantages in integrity verification and dynamic updating. We conducted the performance evaluations of EACSIP from terms of transfer bandwidth and computation overhead. We demonstrated EACSIP is suitable for the access control applications in collaborative environment.

IV. DISCUSSION

In this section, different research works on data integrity and security techniques in cloud computing is discussed. The Table 1 represents different data integrity and security techniques in Cloud computing.

Table 1: Different data integrity and security techniques in Cloud computing

Citation	Proposed System	Methods Used	Description	Results
H. Wang, D. He and S. Tang et. al., [24]	Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity Checking in Public Cloud	ID-PUIC (Identity-based Proxy-oriented data Uploading and remote data Integrity checking in	Concrete ID-PUIC protocol is designed by using the bilinear pairings. The concrete ID-	ID-PUIC protocol can realize private remote data integrity checking, delegated

		public Cloud)	PUIC protocol is provably secure and efficient by using the formal security proof and efficiency analysis.	remote data integrity checking and public remote data integrity checking.
T. Li, J. Chu and L. Hu et. al., [25]	CIA: A Collaborative Integrity Auditing Scheme for Cloud Data With Multi-Replica on Multi-Cloud Storage Providers	CIA (Collaborative Integrity Auditing	The proposed scheme provides unprecedented support for free data blocking. The proposed scheme employs only hash functions in the calculation, which has a negligible computational overhead compared to the traditional bilinear pairing-based schemes.	Theoretical analysis and experimental results show that the proposed scheme provides high efficiency and flexibility with security assurance.
P. Sirohi and A. Agarwal et. al., [26]	Cloud computing data storage security framework relating to data integrity, privacy and trust	-	The proposed framework focuses on the encryption and decryption approach facilitating the cloud user with data security assurance. The model is proposed talks about three level authentication mechanisms for improving security to the data as compared to the old traditional system.	Proposed solution only talks about the increased security but does not talk about the performance

Q. Hu et. al., [27]	A Data Integrity Verification Scheme of Deduplication for Cloud Ciphertexts	block signatures and proxy re-signature methods is used to verify the users and data integrity.	This paper proposes a data integrity verification scheme of deduplication for cloud ciphertexts, including cloud ciphertext deduplication and cloud data integrity verification. In the data integrity verification, the proxy re-signature method is adopted. In addition, our scheme realizes user revocation, ensures the privacy of cloud data, and satisfies unforgeability of tags	This scheme has higher efficiency in data deduplication and integrity verification.
S. Tan, L. Tan, X. Li and Y. Jia et. al., [28]	An efficient method for checking the integrity of data in the Cloud	-	In this paper, we propose a simple but effi cient auditing scheme for checking the integrity of data stored in the cloud. We try to reduce the cost of the initialization phase for executing an auditing protocol by exploiting some good attributes of the bilinear group.	Extensive security and performance analysis shows that the proposed scheme is highly efficient and provably secure
H. Yan, Z. Zhang, S. Qiu, H. Qian, Z.	Public Data Integrity Checking for Cloud Storage	An efficient Remote Data Integrity Checking	Data masking technique is used to randomize the original data	Computation cost for proof generation and verification is 2.7

Bian and Y. Liu et. al., [29]	with Privacy Preserving	(RDIC) is used	before generating the final proof which makes the verifier can not get any knowledge about the stored data.	seconds.
Mahalakshmi, J. ., Reddy, A. M. ., T., S. ., Chowdary, B. V. ., & Raju, P. R. et. al., [30]	Enhancing Cloud Security with AuthPrivacyChain: A Blockchain-based Approach for Access Control and Privacy Protection	AuthPrivacyChain	It uses a zero-knowledge proof mechanism to enable users to prove their identity without revealing any sensitive information. The authors evaluate the AuthPrivacyChain approach using a prototype implementation and show that it can provide effective access control and privacy protection for cloud-based resources	AuthPrivacyChain approach delivers superior speeds and effectiveness in accessing resources when compared with alternative methods.However Future exploration could concentrate on finding ways to improve overall security and robustness in access control systems.
Shravan S Kamath, Deepak Sai V, Sharath S V et. al., [31]	An Efficient and Secure Protocol for Ensuring Data Integrity in Multi Cloud Environment	AES(Advanced Encryption Standard) is used	a framework that would provide integrity of data of multiple users through Third Party Auditor (TPA) and proposes different set of algorithms based on the sensitivity of the data. In the proposed framework concept of multi cloud platform has been used to provide best cost	The proposed framework is easy to implement and provides better performance by using the traditional algorithms of network security over the various issues of cloud computing.

			optimization for various requirements of user.	
Amr M. Sauber, Passent M. El-Kafrawy, Amr F. Shawish , Mohamed A. Amin and Ismail M. Hagag et. al., [32]	A New Secure Model for Data Protection over Cloud Computing	One Time Password	We develop the one-time password (OTP) as a logging technique and uploading technique to protect users and data owners from any fake unauthorized access to the cloud. We implement our model using a simulation of the model called Next Generation Secure Cloud Server (NG-Cloud).)ese results increase the security protection techniques for end user and data owner from fake user and fake data owner in the cloud.	It provides security and scalability of data sharing for users on the cloud computing. Our model achieves the security functions over cloud computing such as identification and authentication, authorization, and encryption. However, The performance and efficiency of the cloud-computing environment need to be improved.

Data Confidentiality and data integrity is the major concern of cloud computing. Few mechanisms were discussed for the mitigating the risks to prevent data loss. However, the cloud computing need to be designed very sensitively and should think in all aspects of security to make data secure. Data integrity is the wide-open issue in cloud computing and a good opportunity for the research work.

V. CONCLUSION

In this work, a survey on data security and integrity of data in cloud computing is presented. Data security and integrity problems are the barrier and obstacles to the rapid growth of cloud computing. The purpose of this survey is to highlight the security problems associated with cloud computing and to present some solutions suggested or implemented by researchers to improve security and integrity. Various research works on cloud computing, data security, data integrity using different techniques are reviewed and analyzed. This work also discussed and various research works of secured cloud data and integrity of cloud. However, there are

still many gaps to be filled. More research in the field of cloud computing is needed to make it appropriate for users of the cloud service. An effort will the mark in the done course of research to address the problems Cloud Security, Privacy and Integrity.

VI. REFERENCES

[1] Zhenpeng Liu, Yongjiang Feng, Lele Re, And Weihua Zheng, "Data Integrity Audit Scheme Based on Blockchain Expansion Technology," IEEE Access, vol. 10, 2022, doi: 10.1109/ACCESS.2022.3176754
[2] Nawaf Alharbe, Abeer Aljohani, Mohamed Ali Rakrouki and Mashael Khayyat, "An Access Control Model Based on System Security Risk for Dynamic Sensitive Data Storage in the Cloud," Appl. Sci, vol. 13, pp. 1-17, 2023, doi:10.3390/app13053187
[3] Suyel Namasudra, "Data Access Control in the Cloud Computing Environment for Bioinformatics," International Journal of Applied Research in Bioinformatics, vol. 11, no. 1, January-June 2021, doi: 10.4018/IJARB.2021010105
[4]N. Tutubala and T. E. Mathonsi, "A Hybrid Framework to Improve Data Security in Cloud Computing," 2021 Big Data, Knowledge and Control Systems Engineering (BdKCSE), Sofia, Bulgaria, 2021, pp. 1-5, doi: 10.1109/BdKCSE53180.2021.9627294.
[5]M. M. R and A. T.P, "Novel Weight-Improved Particle Swarm Optimization to Enhance Data Security in Cloud," 2023 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Kirtipur, Nepal, 2023, pp. 195-200, doi: 10.1109/I-SMAC58438.2023.10290704.
[6] Jianming Du, Guofang Dong, Juangui Ning, Zhengnan Xu, And Ruicheng Yang, "A Blockchain-Assisted Certificateless Public Cloud Data Integrity Auditing Scheme," IEEE Access, vol. 11, pp.123018- 123029, 2023, doi: 10.1109/ACCESS.2023.3329558
[7]F. Wang, H. Wang and L. Xue, "Research on Data Security in Big Data Cloud Computing Environment," 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China, 2021, pp. 1446-1450, doi: 10.1109/IAEAC50856.2021.9391025.
[8] Weihua Duan, Yu Jiang, Xiaolong Xu, Ziming Zhang, and Guanpei Liu, "An Edge Cloud Data Integrity Protection Scheme Based on Blockchain," Security and Communication Networks, vol. 2022, pp. 1-15 pages, doi:10.1155/2022/5016809
[9]X. Pei, Y. Wang, W. Yao, J. Lin and R. Peng, "Security Enhanced Attribute Based Signcryption for Private Data Sharing in Cloud," 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, China, 2016, pp. 737-743, doi: 10.1109/TrustCom.2016.0133.
[10]F. Fatemi Moghaddam, A. Majd, M. Ahmadi, T. Khodadadi and K. Madadipouya, "A dynamic classification index to enhance data protection procedures in cloud-based environments," 2015 IEEE 6th Control and System Graduate Research Colloquium (ICSGRC), Shah Alam, Malaysia, 2015, pp. 17-22, doi: 10.1109/ICSGRC.2015.7412457.
[11] Sumathi M, Rajkamal M, Dr B Gomathy, I Infant Raj, Dr. Sushma Jaiswal and D. Swathi, "Secure Blockchain Based Data Storage and Integrity Auditing in Cloud,"Turkish Journal of Computer and Mathematics Education,vol.12, no.9, pp. 159-165, 2021
[12]Parin Patel, Hiren Patel, "LCHAIN: A Secure Log Storage Mechanism using IPFS and Blockchain Technology," International Journal on Recent and Innovation Trends in Computing and Communication, vol. 11, no. 5, ISSN: 2321-8169, 2023, doi:10.17762/ijritcc.v11i5s.6592
[13] H. Anwarbasha, S. Sasi Kumar & D. Dhanasekaran, "An efficient and secure protocolfor checking remote data integrity
in multi-cloud environment,"Scientific Reports, vol. 11, 2021, doi:10.1038/s41598-021-93073-3

[14] S. Gokulakrishnan and J. M. Gnanasekar, "Data Integrity and Recovery Management in Cloud Systems," 2020 Fourth International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 2020, pp. 645-648, doi: 10.1109/ICISC47916.2020.9171066.
[15]T. Li, J. Chu and L. Hu, "CIA: A Collaborative Integrity Auditing Scheme for Cloud Data With Multi-Replica on Multi-Cloud Storage Providers," in IEEE Transactions on Parallel and Distributed Systems, vol. 34, no. 1, pp. 154-162, 1 Jan. 2023, doi: 10.1109/TPDS.2022.3216614.
[16]Y. Hou, S. Garg, L. Hui, D. N. K. Jayakody, R. Jin and M. S. Hossain, "A Data Security Enhanced Access Control Mechanism in Mobile Edge Computing," in IEEE Access, vol. 8, pp. 136119-136130, 2020, doi: 10.1109/ACCESS.2020.3011477.
[17]R. Awadallah and A. Samsudin, "Using Blockchain in Cloud Computing to Enhance Relational Database Security," in IEEE Access, vol. 9, pp. 137353-137366, 2021, doi: 10.1109/ACCESS.2021.3117733.
[18]S. Suganya and P. M. D. R. Vincent, "Improving cloud security by enhancing remote data integrity checking algorithm," 2017 Innovations in Power and Advanced Computing Technologies (i-PACT), Vellore, India, 2017, pp. 1-6, doi: 10.1109/IPACT.2017.8245194.
[19] Yogita and N. Kumar Gupta, "Integrity Auditing with Attribute based ECMRSA Algorithm for Cloud Data Outsourcing," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, 2020, pp. 1284-1289, doi: 10.1109/ICISS49785.2020.9315948.
[20] Shipra Yadava, Keshao D. Kalaskarb and Pankaj Dhumane, “Design And Implementation Technique For Cloud Computing Security Improvement,”Contemporary Issues in Computing (CIC),
vol. 2, no. 1, pp. 25-32, 2020, doi: 10.26480/cic.01.2020.25.32
[21]Yuan Ping, Yu Zhan, Ke Lu and Baocang Wang, “Public Data Integrity Verification Scheme for Secure Cloud Storage,”Information, vol. 11, pp. 1-16, 2020, doi:10.3390/info11090409
[22] B. Sowmiya, E. Poovammal, K. Ramana, S. Singh and B. Yoon, "Linear Elliptical Curve Digital Signature (LECDS) With Blockchain Approach for Enhanced Security on Cloud Server," in IEEE Access, vol. 9, pp. 138245-138253, 2021, doi: 10.1109/ACCESS.2021.3115238.
[23] W. Susilo, P. Jiang, F. Guo, G. Yang, Y. Yu and Y. Mu, "EACSIP: Extendable Access Control System With Integrity Protection for Enhancing Collaboration in the Cloud," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 12, pp. 3110-3122, Dec. 2017, doi: 10.1109/TIFS.2017.2737960.
[24]H. Wang, D. He and S. Tang, "Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity Checking in Public Cloud," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1165-1176, June 2016, doi: 10.1109/TIFS.2016.2520886.
[25]T. Li, J. Chu and L. Hu, "CIA: A Collaborative Integrity Auditing Scheme for Cloud Data With Multi-Replica on Multi-Cloud Storage Providers," in IEEE Transactions on Parallel and Distributed Systems, vol. 34, no. 1, pp. 154-162, 1 Jan. 2023, doi: 10.1109/TPDS.2022.3216614.
[26]P. Sirohi and A. Agarwal, "Cloud computing data storage security framework relating to data integrity, privacy and trust," 2015 1st International Conference on Next Generation Computing Technologies (NGCT), Dehradun, India, 2015, pp. 115-118, doi: 10.1109/NGCT.2015.7375094.
[27]Q. Hu, "A Data Integrity Verification Scheme of Deduplication for Cloud Ciphertexts," 2020 IEEE 9th Joint International Information Technology and Artificial Intelligence

Conference (ITAIC), Chongqing, China, 2020, pp. 865-869, doi: 10.1109/ITAIC49862.2020.9339001.
[28]S. Tan, L. Tan, X. Li and Y. Jia, "An efficient method for checking the integrity of data in the Cloud," in China Communications, vol. 11, no. 9, pp. 68-81, Sept. 2014, doi: 10.1109/CC.2014.6969712.
[29]H. Yan, Z. Zhang, S. Qiu, H. Qian, Z. Bian and Y. Liu, "Public Data Integrity Checking for Cloud Storage with Privacy Preserving," 2019 IEEE 19th International Conference on Communication Technology (ICCT), Xi'an, China, 2019, pp. 1408-1412, doi: 10.1109/ICCT46805.2019.8947275.
[30] Mahalakshmi, J. ., Reddy, A. M. ., T., S. ., Chowdary, B. V. ., & Raju, P. R. . (2023). Enhancing Cloud Security with AuthPrivacyChain: A Blockchain-based Approach for Access Control and Privacy Protection", International Journal of Intelligent Systems and Applications in Engineering, vol. 11, no. 6, pp. 370–384. Doi:https://ijisae.org/index.php/IJISAE/article/view/2863
[31] Shravan S Kamath, Deepak Sai V, Sharath S V, "An Efficient and Secure Protocol for Ensuring Data Integrity in Multi Cloud Environment,"International Journal Of Engineering Research & Technology (Ijert) Icret – 2016 (Volume 4 – Issue 21), pp. 1-5, 2016, doi: 10.17577/IJERTCONV4IS21024
[32] Amr M. Sauber, Passent M. El-Kafrawy, Amr F. Shawish , Mohamed A. Amin and Ismail M. Hagag, "A New Secure Model for Data Protection over Cloud Computing," Computational Intelligence and Neuroscience, vol. 2021, pp. 1-11, 2021, doi:10.1155/2021/8113253