Survey on Data Integrity and Verification for Cloud Storage

Suchetha R Pujar
Computer Science Engineering
M S Ramaiah Institute of Technology
Bangalore, India
suchethap2@gmail.com

Shilpa S Chaudhari
Computer Science Engineering
M S Ramaiah Institute of Technology
Bangalore, India
shilpasc29@msrit.edu

Aparna R
Computer Science Engineering
M S Ramaiah Institute of Technology
Bangalore, India
aparna@msrit.edu

***Abstract*— Nowadays people store much of their information in Cloud, which is a vast network of remote servers, each with a unique function. Cloud storage provides reliable storage space for the users where the data can be stored in pay-as-you-go pricing model. Cloud storage data is monitored, backed up and remotely maintained. The Cloud Storage provides the benefits of low-cost storage, easy accessibility of data and disaster recovery of the data but faces challenges on confidentiality, data security and integrity of the data. Data integrity and verification checks whether the data stored in the cloud is unaltered as the data may be altered by cloud service providers or by malicious attackers. This paper gives a brief introduction about different techniques used for data integrity and verification for cloud storage and classification of them based on the security level provisioning used in the techniques.**

Keywords*— *Data Integrity, Data verification, Cloud storage, Cloud computing.

I. INTRODUCTION

Cloud based infrastructure provides resources, services, platforms to the user device on demand from anywhere irrespective of the location, anytime through internet from various servers. Main characteristics of cloud model includes on demand automatic provisioning of computing capabilities over the network through standard mechanism, dynamic resource grant using multi-tenant model for monitored, controlled and reported resource provisioning.

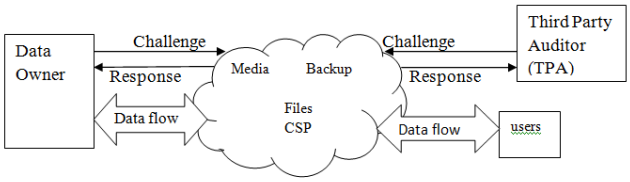
Cloud model consists of three types of service models as follows. (1) Software as a Service (SaaS) model: No prior installation of the software is required. We can easily use the web service to fulfill our requirements. (2) Platform as a Service (PaaS) model: This service model provides a Platform to develop, test and organize the different applications. (3) Infrastructure as a Service (IaaS) model: An IaaS cloud service model provides entire computing infrastructure such as storage, servers, networking and support like Amazon Web Service (AWS), Microsoft Azure etc.

Cloud model also composed of deployment models that provides infrastructure for exclusive uses by single organization or specific community, open use by general public or a combination of two or more distinct cloud infrastructure.

This paper focuses on the various techniques proposed in literature for Infrastructure as a Service Platform to store the data in the cloud. The data can be in any form like files, images, audio, video etc. Data Integrity technique provides the assurance that the data is safe and unaltered when stored in the cloud. The Data Integrity and verification is done remotely as depicted in Figure 1, which consist of following entities.

1. The Data owner stores the data into the cloud
2. Users access the data from the cloud
3. Third Party Auditor who checks the integrity of the data stored in the cloud
4. Cloud Service Provider (CSP) who provides the necessary storage and manages the resources stored in the cloud.

Figure 1 Schematic representation of remote data integrity and verification



In Figure 1, the Data owner wants to check the integrity of data stored in the cloud, so he undergoes following phases.

1. Key generation: Generating the private key and the public key for securing the data.
2. Integrity phase: In this phase different algorithms of cryptography like AES, RSA etc. are used to encode the data.
3. Challenge phase: It is run by the data owner or the Third-party Auditor.
4. Proof generation: Proof generation is executed by the Cloud Service Provider (CSP).
5. Action phase: Based on the verification report the data owner re-signatures or re upload the data

Apart from data Owner the Third-party Auditor can also check the Integrity of data stored in the cloud by providing a Challenge to the Cloud Service Provider. The Data owner can insert, update or delete the data stored in the cloud but the users can access the data and can also modify the publicly available data.

To this end, a few groups of researchers have started advocating the utilization of various security provisioning approaches to provide data integrity. This paper surveys the existing data integrity and verification techniques designed for cloud storage highlighting the comparison of the proposed techniques in terms of data integrity check, techniques used, performance metrics, security attacks, and update modes. The taxonomy developed for data integrity and verification techniques provides global view of the problem and solution.

The rest of this paper is organized as follows. Section II provides some of the related work exists on survey of data

integrity and verification techniques. Section III explains the classification of the current state of research in terms of taxonomy. Section IV explains the existing data integrity and verification techniques. Section V compares the discussed data integrity and verification techniques in various comparison parameters. We conclude on the survey done in Section VI.

II. Related Works

The paper "A review on remote data auditing in single cloud server: Taxonomy and open issues" [26] presents a survey on the remote data storage auditing in single cloud server domain and presents taxonomy of RDA approaches. The paper highlighted the challenges and issues related to current RDA protocols in the cloud. It also describes the thematic taxonomy of RDA. The survey paper mainly deals with proof of retrievability, provable data possession and proof of ownership.

The paper "Review of remote data integrity auditing schemes in cloud computing: taxonomy, analysis, and open issues" [27] also presents a survey on remote data storage auditing in cloud server. The objective of the paper is to highlight the challenges and issues present in the survey of different papers considered. The survey paper mainly deals with the provable data possession and proof of retrievability.

The survey paper on "A review on remote data auditing in single cloud server: Taxonomy and open issues"[26] deals with the survey of papers till the year 2013 and the paper "Review of remote data integrity auditing schemes in cloud computing: taxonomy, analysis, and open issues"[27] deals with the survey of papers till 2017. In this work, we surveyed papers till 2019 and form the comparison based on the data integrity check, techniques used, performance metrics, security attacks, and update modes as shown in Table 1.

Table 1
Different parameters used for comparison In Data integrity and verification for cloud storage

SN	Parameters	Definition
1	Technique Used	It describes about the different methods used to perform the Data Integrity and verification for cloud storage.
2	Static Update Mode	In Static Update Mode Data Owner cannot modify the files stored in the cloud.
3	Dynamic Update Mode	In Dynamic Update Mode Data Owner can update the files without retrieving the whole file.
4	Data Integrity & Verification (DIV) Check	It checks the integrity of data stored in the cloud which is either done by Data Owner or Third-Party Auditor (TPA).
5	Security against attacks	It describes which paper is resistant to which attack.
6	Performance Metrics	It consists of storage overhead and computational cost.

Our contribution

In order to tackle the situation, there are total twenty-six research article that proposes data integrity and verification techniques to provide security in cloud storage. Assessment of the research articles in this area motivates us to review data integrity and verification techniques as the existing survey does not include the recent papers on the topic. The main goal of this survey is to understand the subject of this article clearly in depth, status, and their comparison with the required security parameters. Our specific contributions are as follows. (1) Covering the survey of all possible existing data integrity and verification techniques used for cloud storage in last five years. (2) Design of taxonomy to classify the different possible data integrity and verification techniques. This paper outlines systematic review focusing on classification and identification of existing literature on data integrity and verification techniques. (3) Comparison of the discussed data integrity and verification techniques.

III. Taxonomy of Data Integrity And Verification For Cloud Storage

This section discusses the desinged taxonomy for the existing data integrity and verification techniques. We collected recent twenty-six papers from last five years as the survey exists in on the topic in details in reputed journal and covered most of the existing proposal discussion. These selected twenty-six papers proposed data integrity and verification techniques are divided into two main categories based on security services used. We observe that few techniques use confidentiality in addition to integrity provisioning where Confidentiality deals with encrypting the data before it is outsourced to the cloud and Integrity deals with whether the stored data is corrupted or altered or not. One category provides confidentiality using encryption algorithm while other category only provides integrity service as shown in Figure 2. We further classify confidentiality+Integrity category based on the usage of cryptographic algorithm such as RSA, ABE, AES and bulk copy encryption. The data integrity provisioning category is classified based on the technique used for signature/authentication such as Merkle Hash tree function, proxy/bilinear, homomorphic and identity based. The corresponding method is given in the Figure 2. The categories are defined as follows. (1) Merkle Hash tree: every leaf node is labeled with a hash value of the data and every non-leaf node contains cryptographic hash of the leaf node. If the data to be processed is very large, then the tree grows and the storage overhead occurs. (2) Proxy re-signature: the data owner encrypts the data and provides an original signature to the proxy. The proxy using pre-sign key re encrypts the encrypted data and provides the encrypted signature to be stored in the cloud. (3) Homomorphic tag: the block of data to be encrypted forms the verified metadata and all the verified metadata are aggregated to form the Aggregated Verified Metadata. The Homomorphic tag contains the Block id, Signature, Block identifier, Signature identifier. (4) Identity based: for each file a tag is generated, and the file is not encrypted. (5) Rivest-Shamir-Adleman (RSA): we select two prime numbers 'p' and 'q' and perform the multiplication because multiplication is very time consuming it causes computational overhead. (6) Advanced Encryption Standard (AES): the encrypted data is generated by following Rounds where each round contains the operation like add round key, mix columns, shift rows and substitute bytes. (7) Attribute based encryption (ABE): user provides private key which

consist of a list of "attributes" and Files are encrypted using attributed-based policy. (8) Bulk Copy: uses polynomial to provide encrypted data that is secure, but the computation cost is more.

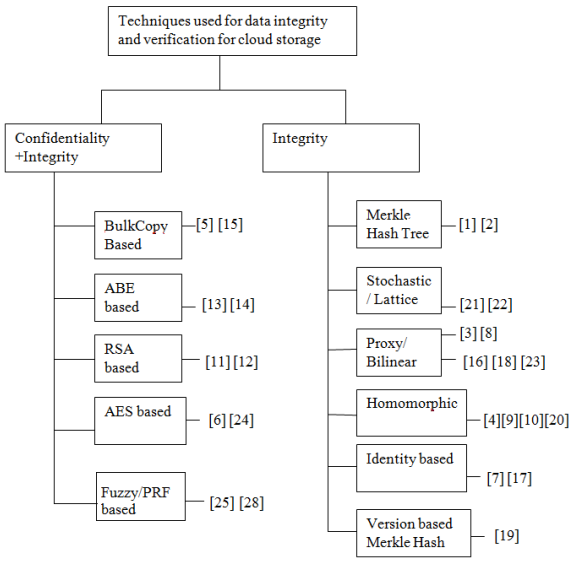


Figure 2: Taxonomy of data integrity and verification techniques

Diffie Hellman Key exchange scheme used in few techniques that helps for key exchange between data owner and cloud service provider and uses public key algorithm and Reversible water marking embeds watermark in the images to encrypt the image and Version based Merkle Hash Tree Stores both hash value and version number of the data blocks. The lattice method includes the Setup, extracting partial private key, setting the secret value, private key, public key and Challenge, response. Stochastic is probabilistic in nature. Fuzzy signature uses biometric data and PRF uses Pseudo random function to encrypt data.

IV. Data Integrity And Verification Techniques

Liu et al [1] in the year 2014 used BLS signature and Merkle Hash tree where BLS signature uses Bilinear pairing like pairing (hashed key, plaintext) to verify a group of data and Merkle Hash tree for generating hash values for the data. In Merkle Hash tree every leaf node is labeled with a hash value of the data and every non-leaf node contains cryptographic hash of the leaf node. If the data to be processed is very large, then the tree grows in size and the storage overhead occurs. It works better for single user but lacks the support for multiuser. It also suffers from storage overhead when processing huge files. This Technique prevents from DDOS (Distributed Denial of Service) attack by allowing a single Third-Party Auditor (TPA) to challenge the cloud for data integrity and verification check. If all or multi TPA challenge the cloud for data integrity and verification check then it causes collision and DDOS attack can occur.

Huang et al [2] in the year 2014 used Regenerating codes method to minimize bandwidth and the storage overhead and Merkle Hash tree method. In Merkle Hash tree every leaf node is labeled with a hash value of the data and every non-leaf node contains cryptographic hash of the leaf node. If the data to be processed is very large, then the tree grows and the storage overhead occurs. They developed regenerating codes using the product matrix framework and stored the Hash value on multiple servers. It supports multiuser but lacks batch and public auditing. Here the data integrity and verification check are performed by the Data Owner and this technique prevents from Byzantine attack.

Wang et al[3]in the year 2015 used Bilinear pairing, Proxy re-signature where the data owner generates a signature and send it to proxy and proxy perform re-signature of the block of data and Homomorphic authenticators who aggregate the block and forms an aggregated block which consist of block, signature, block identifier and signer identification. It supports multiuser and batch auditing, but Third-Party Auditor is able to retrieve the values, so privacy of data is not supported in this scheme. This scheme prevents from internal attack which is either caused by the Cloud Service Provider or Third-Party Auditor.

Shen et al [4] in the year 2015 implemented an efficient integrity check using Bilinear codes, Erasure codes where 'k' blocks of data are converted into 'n' blocks of data which is longer than 'k' blocks of data and also used Homomorphic integrity tags. It suffers from data redundancy and storage overhead.

Jianbing Ni et al [5] in the year 2016 used BCP (Bulk copy) encryption scheme, polynomial-based authenticators and proxy re-encryption technique to secure outsourced data in cloud storage. The Communication overhead between the users and cloud is constant but in integrity check phase the length of proof linearly varies with number of sectors processed. The scheme prevents from internal and external attack which is caused by the cloud service providers, Third party Auditor or the Malicious attackers.

In the year 2017 Shivarajkumar et al [6] introduced A novel data auditing approach using AES algorithm for Encryption and SHA-2(Secure Hash Algorithm) and the integrity check is carried out by the Third-Party Auditor. In this proposed method the user encrypt data using AES algorithm and uses SHA-2 to get Message Digest of the encrypted data. The Encrypted data is sent to cloud server and message digest is sent to Third Party Auditor (TPA) who performs the integrity check of the data. It prevents from the malicious attack. The scheme consumes more computation time because AES performs the following Rounds to encrypt the data where each round contains the operation like the add round key, mix columns, shift rows and substitute bytes.

Jinxia Wei et al [7] in 2017 used Identity-based integrity auditing protocol where each file to be processed are associated with a tag and the scheme supports batch auditing for multi users. This method has constant computation cost, but the issue is the file is stored in the form of plaintext and is not encrypted. It prevents from forgery attack, replace attack and replay attack caused by the Cloud Service Provider.

Laicheng Cao et al[8] in 2017 proposed an integrity verification scheme of completeness and zero-knowledge for

multi cloud storage using Bilinear pairing maps and Index hash tables where in Index Hash Tables encrypts the data using a hash function and computes the index and stores it into the index hash table. The scheme also supports dynamic update of data and the integrity check is performed by Trusted Third Party. It prevents from forgery attack.

Krithikashree et al [9] in the year 2018 used the third-party auditors, PHC (Paillier Homomorphic Cryptography) which uses Euler function and Homomorphic tags for data integrity verification. The drawback of this scheme is there is a nefarious use of cloud resources, sharing of technologies and related issues and also there is misuse of administrator rights or malicious insiders. But the scheme prevents from the internal attack caused by the Cloud Service Provider or the Third-party Auditor.

Filipe et al [10] in 2018 proposed S-Audit: Efficient Data Integrity Verification for Cloud Storage, which uses Homomorphic authentication with digital signatures to avoid retrieving of data from the cloud. It is targeted to provide integrity proofs without retrieving data. The scheme prevents from the Spoofing attack and here the data integrity and verification check are performed by the Data Owner.

B.Mahalakshmi et al[11] in 2019 proposed a method using RSA algorithm and MD5 to achieve data integrity in cloud storage where the Third party auditor does integrity check and data owner uses cryptography algorithm but communication cost is more. In this proposed method the user encrypt data using RSA algorithm and uses MD5 to get Message Digest of the encrypted data. The Encrypted data is sent to cloud server and message digest is sent to Third Party Auditor (TPA) who performs the integrity check of the data. The scheme prevents from the Malicious attack.

Walid et al [12] in the year 2019 proposed Cryptographic Accumulator Based Scheme for Data integrity verification for cloud storage which uses RSA based cryptographic accumulator. The proposed model prevents tag forgery which is performed by Cloud Service Provider(CSP), data deletion, replacement, data leakage attacks and detect replay attacks where Cloud Service Provider might use an old challenge response to respond to a challenge which is new that matches it, and shown to be efficient, feasible and practical in real-life applications and also minimizes computational and storage overhead.

Jin Sun et al [13] in 2019 used Combining Ciphertext Policy Attribute-Based Encryption (CP-ABE) and auditing methods. The TPA verify the correctness of the search results and realize the function of user attribute revocation. The scheme has proven to be secure against selectively chosen keyword attack in the general bilinear group model and be resistant to selective plaintext attacks.

Anyi Liu et al [14] in 2019 proposed LiveForen to ensure integrity of forensic data, the proposed scheme uses Trusted Platform Module (TPM) and Attribute Based Encryption (ABE). The scheme verifies the data integrity, as well as detects and localizes malicious modification at run time. The scheme also prevents from Man-in-the-middle attack, Denial attack and also from malicious attack.

Xin Tang et al [15] in 2019 preserved the integrity and privacy for Images in cloud storage using adaptive reversible watermarking algorithm which provides a fixed embedding capacity for images to embed authentication data. It also uses Diffie Hellman key exchange scheme to check integrity of data. It eliminates communication and storage overhead for the authentication data. The data integrity checks are performed by the Third-Party Auditor. The scheme prevents from replay attack which is caused by the Cloud Service Provider.

Balasubramanian et al [16] in 2018 proposed a method using Bilinear pairing and Network Coding. It was a Novel approach to check integrity of data and provides facilities for data recovery. For data integrity check he used spot checking technique in Remote data auditing framework, which is probabilistic in nature, here the data integrity check is done by the third-party auditor. The proposed method also prevents from security breach and recovers data through Functional Minimum Storage Generating code (FMSR) used in Network Coding technique. The Computational and storage overhead is also Minimized.

Jiang Hong et al [17] in the year 2018 proposed a protocol which is based on ID and public auditing for Data integrity check for Cloud Storage. Here the Third-Party Auditor does the integrity check of data and this technique provides security against forgery attack and minimizes the computational cost. The proposed technique also performs the verification of file tag, block tag and preserves privacy of data. The data update mode in this proposed technique is Dynamic in nature.

Aiping Li et al [18] in the year 2016 used the technique of bilinear maps, Computational Diffie-Hellman (CDH) and Compact proofs of retrievability (CPOR). The data update mode is Dynamic in nature. It supports dynamic update mode and Third-Party Auditor performs the integrity check of data and it prevents from forgery attack. The proposed method supports public and batch auditing, Storage correctness where the Third-Party Auditor verifies the data stored in the Cloud.

Xiuqing Lu et al [19] in the year 2019 proposed a technique of Version Based Merkle Hash Tree (VBMHT) where Third Party Auditor performs the integrity check of data and provides security against Denial of Service (DOS) attack on Cloud Service Provider. It also minimizes computational cost due to version based when compared to other techniques which uses Merkle Hash Tree. Each Node or Data block has Hash value and version number associated with it. The data update mode in the proposed scheme is dynamic in nature.

Rajat Saxena et al [20] in the year 2018 proposed a technique of Paillier Cryptography along with homomorphic tags where Data Owner (DO) performs the integrity check and provides security against Man in the middle(MITM) attack. The proposed method also minimizes computational cost. It also supports data operations like update, append and delete once the data is stored in the cloud.

M Ramanan et al [21] in the year 2018 proposed a technique of Stochastic Diffusion where the update mode of data is dynamic and the Data Owner performs the integrity check. The proposed technique also prevents from malicious attack and minimizes storage overhead, if the data is corrupted in the cloud it also recovers the data and also the

recovery time is low.

C.Sasikala et al [22] in the year 2018 proposed a technique based on Lattice in the Cloud storage where the update mode of the data is static and the Third Party Auditor performs the integrity check of the data. The proposed technique prevents from quantum computer attacks and also Minimizes the computational overhead The main drawback of the proposed method is it supports single cloud and single user environment but not supports multi cloud and multi user environment that is the proposed scheme do not support batch auditing.

Imad El Ghoubachet al [23] in the year 2019 used the technique of bilinear maps and also uses Computational Diffie-hellman method where the update mode of the data is Dynamic in nature and Third Party Auditor performs the data integrity check. The proposed method prevents from replay and forgery attack and also minimizes the computational and communication overhead. The drawback of the scheme is it does not provide support against the data corruption for the data stored in the cloud. This scheme consist of entities like Cloud Service provider (CSP), Data Owner (DO), Third Party Auditor (TPA) and Private Key Generator (PKG).

Mai Rady et al [24] in the year 2019 used the technique of Advanced Encryption Standard(AES), MD5 and BGLS(an aggregate signature scheme by Boneh et al.) where the update mode of the data is Dynamic in nature and the Trusted third party auditor performs the integrity check of the data. The proposed method prevents from Distributed Denial of Service(DDoS) attack but the computational overhead is more. It provides both confidentiality and integrity of the data stored in the cloud.

Lixue Sun et al [25] in the year 2019 proposed a technique of Obfuscated Program and punctured pseudorandom function(PRF), where punctured PRF uses hash value of user data as input and Obfuscated program contains signing key and key for PRF. The update mode is Dynamic in nature and the proposed method prevents from malicious attacks and also reduces the storage and computational overhead. The Third Party Auditor does the integrity check of the data and also the proposed scheme prevents from potential breaches of data from Third Party Auditor by providing privacy to the data.

Wenting Shen et al [28]s al in the year 2018 used the technique of Fuzzy signature and Modified BLS short signature (MBLSS) where Fuzzy signature uses biometric data such as iris scan and fingerprints as private key and MBLSS is the modified form of BLS signature where the order of the prime ‘p’ is a smallest prime but BLS uses the order of the ‘p’ as the largest prime number. The update mode is dynamic and the data integrity check is performed by the Third-party auditor. The proposed method reduces the storage overhead and also prevents from malicious attacks.

V. Comparison Of Data Integrity And Verification Techniques

This section compares the existing data integrity and verification techniques in terms of the techniques used, data integrity check, update mode as shown in Table 2 and performance metrics, security against attacks as shown in Table 3. The Figure 3 depicts the different parameters used for comparing different data integrity and verification techniques.

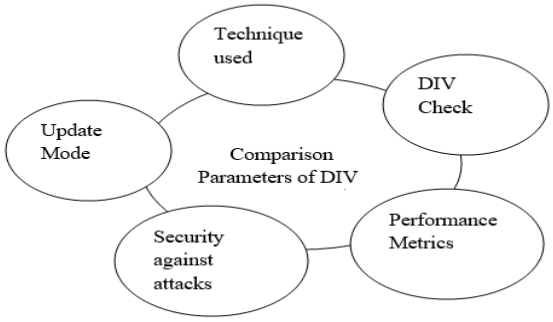


Figure 3: Parameters used for comparison of different data integrity and verification techniques

TABLE 2
COMPARISON OF DIFFERENT PAPERS BASED ON TECHNIQUE USED, UPDATE MODE AND DATA INTEGRITY AND VERIFICATION(DIV) CHECK

Author	Techniques used	Update Mode	DIV Check
[1]	BLS signature and Merkle Hash tree	Dynamic	Third Party Auditor
[2]	Regenerating codes and Merkle Hash tree	Dynamic	Data Owner
[3]	Homomorphic authenticators, Proxy re-signatures and Bilinear pairing	Dynamic	Third Party Auditor
[4]	Bilinear maps, Erasure codes and Homomorphic integrity tags	Dynamic	Data Owner
[5]	BCP encryption scheme, proxy re-encryption and polynomial based authentication.	Dynamic	Data Owner
[6]	AES algorithm for encryption and Secure Hash Algorithm(SHA-2).	Dynamic	Third Party Auditor
[7]	Identity-based integrity auditing protocol	Dynamic	Data Owner and Third party Auditor
[8]	Bilinear pairing maps and Index hash tables	Dynamic	Trusted Third Party
[9]	The third party auditors, PHC and Homomorphic tags for data integrity verification.	Static	Third Party
[10]	Digital signature and Homomorphic authentication	Dynamic	Data owner
[11]	RSA and MD5	Static	Third Party Auditor
[12]	RSA based cryptographic accumulator	Static	Third Party Auditor
[13]	ciphertext policy attribute-based encryption (CP-ABE)	Dynamic	Third Party Auditor
[14]	Attribute based encryption(ABE) and trusted platform module (TPM)	Dynamic	Third Party Auditor
[15]	adaptive reversible watermarking algorithm and Diffie Hellman key exchange scheme.	Dynamic	Third Party Auditor

Author	Techniques used	Update Mode	DIV Check
[16]	Bilinear pairing and Network Coding	Dynamic	Third Party Auditor
[17]	Protocol based on ID and public auditing	Dynamic	Third Party Auditor
[18]	Bilinear maps, CDH, CPOR	Dynamic	Third Party Auditor
[19]	Version Based Merkle Hash Tree(VB_MHT)	Dynamic	Third Party Auditor
[20]	Paillier Cryptography along with homomorphic tags	Dynamic	Data Owner
[21]	Stochastic Diffusion Methods	Dynamic	Data Owner
[22]	Lattice in Cloud Storage	Static	Third Party Auditor
[23]	Bilinear maps, CDH	Dynamic	Third Party Auditor
[24]	AES, MD5 and BGLS	Dynamic	Trusted Third Party Auditor
[25]	Obfuscated program and puncturable PRF	Dynamic	Third Party Auditor
[28]	Fuzzy Signature and Modified BLS short signature	Dynamic	Third Party Auditor

TABLE 3
COMPARISON OF DIFFERENT PAPERS BASED ON SECURITY AGAINST ATTACK, PERFORMANCE METRICS

Author	Security against attack	Performance Metrics
[1]	DDOS attack	Less communication overhead but suffers from storage overhead
[2]	Byzantine attack	It suffers from storage overhead
[3]	Internal attack	Computation overhead is more
[4]	Storage failure	Computation overhead is more
[5]	Prevents from internal and external attack	Constant communication overhead
[6]	Prevents from malicious attackers	Less storage overhead
[7]	Prevents from forgery, replace and replay attack	Constant Computation Time
[8]	Forgery attack	Less Computation time
[9]	Internal attack	Storage overhead
[10]	Spoofing attack	Minimizes storage overhead
[11]	Malicious Attack	Suffers from Storage overhead
[12]	prevent from forgery tag, data deletion, replacement, data leakage attacks and detect replay attack	Minimize computational and storage overhead
[13]	Resistant to selectively chosen keyword attack, plaintext attack.	Low storage overhead but high computational cost
[14]	Prevents from Man-in-the-middle attack, Denial attack, Malicious attack.	Lower Computational cost
[15]	Prevents from replay attack	Minimize computation and storage overhead
[16]	Prevents from security breach by using Bilinear Pairing	Minimizes Computational cost and storage overhead
[17]	Prevents from forgery attack	Lower computational cost
[18]	Prevents from forgery attack	Computational time of server and TPA is low
[19]	Prevents DoS (Denial of Service) attack on Cloud Service Provider	Lower Computational cost
[20]	Prevents from Man in the Middle (MITM) attack	Lower Computational cost
[21]	Prevents from malicious attack	Minimizes storage overhead
[22]	Prevents from quantum computer attacks	Lower computational overhead
[23]	Prevents from replay and forgery attack	Low Computational and communication overhead
[24]	Prevents from DDOS attack	Computational overhead is more
[25]	Prevents from malicious attack	Reduces Computational and Storage overhead
[28]	Prevents from malicious attack	Reduces storage overhead

VI. CONCLUSION

The paper provides a comparative survey on different techniques used to provide data integrity and verification for data stored in the cloud. It also provides the different techniques used, Security and Performance Metrics to achieve Data Integrity and Verification for cloud storage. The papers are also classified into the papers that provide confidentiality and integrity and some papers which only provide the integrity of the data which is stored in the cloud. As future work, we think it is worth exploring further different optimization techniques in order to achieve less storage overhead and reduce computational time to encrypt data.

REFERENCES

[1] Liu, C., Chen, J. and Yang, L. "Authorized public auditing of dynamic big data storage. On cloud with efficient verifiable fine-grained updates", IEEE Transactions on Parallel and Distributed Systems, Vol.25, No. 9, pp. 2234–2244, Sep 2014.

[2] Huang, K., Liu, J., Xian, M., Wang, H. and Fu, S. "Enabling dynamic proof of retrievability in regenerating-coding-based cloud storage", ICC'14, pp. 712–717, 2014.

[3] Wang, B., Li, B. and Li, H. 'Panda: public auditing for shared data with efficient user revocation in the cloud', IEEE Trans. Serv. Comput., Vol. 8, No. 1, pp. 92–106, 2015.

[4] Shen, S.T., Lin, H.Y. and Tzeng, W.G. 'An effective integrity check scheme for secure erasure code-based storage systems', IEEE Transactions on Reliability, Vol. 64, No. 3, pp. 840–851, 2015.

[5] Jianbing Ni, Xiaodong Lin, Kuan Zhang, Yong Yu and Xuemin Shen "Secure Outsourced Data Transfer with Integrity Verification in Cloud Storage", IEEE Conference, 2016.

[6] Shivarajkumar Hiremath, Sanjeev Kunte "A Novel Data Auditing Approach to Achieve Data Privacy and Data Integrity in Cloud Computing", IEEE Conference, pp. 306-310, 2017.

[7] Jinxia Wei, Ru Zhang, Jianyi Liu, Jing Li, XinxinNiu, Yuangang Yao "Dynamic data integrity auditing for secure outsourcing in the cloud" International Journal, pp. 1-15, 2017.

[8] Laicheng Cao, Wenwen He, Yufei Liu, Xian Guo, Tao Feng "An integrity verification scheme of completeness and zero-knowledge for multi-Cloud storage", International Journal on Communication System, pp. 1-10, 2017.

[9] Krithikashree.L, S.Manisha, Dr.Sujithra M "Audit Cloud: Ensuring Data Integrity for Mobile Devices in Cloud Storage", IEEE Conference, 2018.

[10] Filipe Apolinario, Miguel L. Pardal, Miguel Correia "S-Audit: Efficient Data Integrity Verification for Cloud Storage", IEEE International Conference on Trust, Security and Privacy in Computing and Communications, pp. 465-474, 2018.

[11] B.Mahalakshmi and G.Suseendran "An Analysis of Cloud Computing Issues on Data Integrity, Privacy and its Current solutions", Research Article, pp. 467-482, 2019.

[12] Walid I.Khedr, Heba M. Khater, Ehab R. Mohamed "Cryptographic Accumulator-Based Scheme for Critical Data Integrity Verification in Cloud Storage", IEEE Journal, Vol. 7, pp.65635-65651, 2019.

[13] Jin Sun, Lili Ren, Shagping Wang and Xiaominyao "Multi-Keyword Searchable and Data Verifiable Attribute-Based Encryption Scheme for Cloud Storage", IEEE Journal, Vol. 7, pp. 66655-66667, 2019.

[14] Anyi Liu, Huirong Fu, Yuan Hong, Jigangliu, Yingjiu Li "LiveForen: Ensuring Live Forensic Integrity in the Cloud", IEEE Trans on Information Forensics and security, Vol. 14, No. 10, pp. 2749-2764, 2019.

[15] Xin Tang, Yongfeng Huang, Chin-Chen Chang and Linna Zhou "Efficient Real-Time Integrity Auditing with Privacy-Preserving Arbitration for Images in Cloud Storage System", IEEE Journal, Vol 7, pp. 33009-33023, 2019.

[16] V.Balasubramanian, T.Mala "Cloud data integrity checking using bilinear pairing and network coding", Springer Science Conference on Cluster Computing, pp. 6927-6935, 2018.

[17] Jiang Hong, Xie Mingming, Kang Baoyuan, Li Chunquing, Si Lin "ID-Based Public Auditing Protocol for Cloud Storage Data Integrity Checking with Strengthened Authentication and Security", Wuhan University Journal of Natural Science Vol 23, No. 4, pp. 362-388, 2018.

[18] Aiping Li, Shuang Tan, Yan Jia "A method for achieving provable data integrity in cloud computing", Springer Science on Supercomputing, pp. 92-108, 2016.

[19] Xiuqing Lu, Zhenkuan Pan, Hequn Xian "An Integrity Verification Scheme of Cloud Storage for Internet-of-Things Mobile Terminal Devices", Journal on Computers and Security, Vol. 92, pp. 1-17, 2019.

[20] Rajat Saxena and Somnath Dey "Data integrity verification: a novel approach for cloud computing", Springer Science copyright of Indian Academy of Science, pp. 1-12, 2018.

[21] M. Ramanan, P Vivekanandan "Efficient data integrity and data replication in cloud using stochastic diffusion method", Springer Science on Cluster Computing, pp. 14999-15006, 2018.

[22] C.Sasikala, C.Shoba Bindu "Certificateless remote data integrity checking using lattices in cloud storage", Springer Science on Neural Computing and Applications , pp. 1513-1519, 2018.

[23] Imad El Ghoubach, Rachid Ben Abbou. Fatiha Mrabti "A secure and efficient remote data auditing scheme for cloud storage", Journal of King Saud University Computer and Information Sciences, pp. 1-7, 2019.

[24] Mai Rady, Tamer Abdelkader, Rasha Ismail "Integrity and Confidentiality in Cloud Outsourced Data", Ain Shams Engineering Journal Science Direct, pp. 275-285, 2019.

[25] Lixue Sun, Chunxiang Xu, Yuan Zhang and Kefei Chen "An efficient iO-based data integrity verification scheme for cloud storage", Science China Inf Sci, Vol 62, 2019

[26] Mehdi Sookhak, Hamid Talebian, Ejaz Ahmed, Abdullah Gani, Muhammad Kurram Khan "A review on remote data auditing in single cloud server: Taxonomy and open issues", Journal of Network and Computer Applications, Vol. 43, pp. 121-141, 2014.

[27] Jaya Rao Gudeme, Syam Kumar Pasupuleti, Ramesh Kandukuri "Review of remote data integrity auditing schemes in cloud computing: taxonomy, analysis and open issues", Int. J. Cloud Computing, Vol 8, No.1, 2019.

[28] Wenting Shen, Jing Qin, Jia Yu, Rong Hao, Jiankun Hu and Jixin Ma "Data Integrity Auditing without Private key Storage for Secure Cloud Storage", IEEE Trans on Cloud Computing, pp.1-15, 2018.