A Survey on Proof of Retrievability for Cloud Data Integrity and Availability: Cloud Storage State-of-the-Art, Issues, Solutions and Future Trends

Tan Choon Beng[1], Mohd Hanafi Ahmad Hijazi[1], Yuto Lim[2], Abdullah Gani[3]

[1]Faculty of Computing and Informatics, Universiti Malaysia Sabah, Jalan UMS, 88400 Kota Kinabalu, Sabah, Malaysia

[2] WiSE Laboratory, School of Information Science, Japan Advanced Institute of Science and Technology, Japan

[3] Centre for Mobile Cloud Computing Research (C4MCCR), Faculty of Computer Science and Info Technology, University of Malaya, Malaysia

Abstract: Cloud storage has emerged as the latest trend for data storage over the traditional storage method which consume more storage spaces of data owner resources for backup and disaster recovery purposes. Due to the openness nature of cloud storage, trustworthy to the storage providers remains a critical issue amongst data owners. Hence, a huge number of businesses around the world remains choosing traditional storage method over cloud storage. This indicates a need for cloud storage providers to adopt cloud integrity schemes to ensure the outsourced data is secured to gain trustworthiness from clients. There are two main cloud integrity schemes available to ensure data integrity and availability: (i) Provable Data Possession (PDP) and (ii) Proof of Retrievability (PoR). PDP and PoR are protocols designed for cloud storage to proof to clients that the stored data is intact. Although PDP and PoR have similar functionality for providing cloud data integrity and availability, PoR is found to be much better than PDP with respect to full data retrievability as PoR provides recovery to faulty or corrupted outsourced data in which PDP does not cover. The objective of this paper is to examine the state-of-the-art of PoR and subsequently to identify the issues of employing PoR on cloud storage and suggest possible solutions. We analyse available PoR schemes. Then, the issues and challenges as a result of employing PoR specifically and cloud storage generally are described. Some possible countermeasures to address the identified issues are suggested. Finally, the potential future work of PoR schemes and future trends of cloud storage are presented.

Keywords: cloud computing, cloud storage integrity scheme, proof of retrievability, data integrity, data availability

1. INTRODUCTION

Cloud computing is a term we widely heard and used in our modern daily lives. According to definition of the term "cloud computing" given by National Institute of Standards and Technology (NIST), it is:

"*A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."* [1]

Generally, cloud computing is a distributed shared service provided by cloud service provider (CSP), where shared resources are available to its users, usually on a pay-as-you-go basis. As for cloud computing, it can be categorized into three types, namely Platform as a Service (PaaS), Software as a Service (SaaS), and Infrastructure as a Service (IaaS) [2]. Social media applications such Facebook, Twitter, YouTube, etc. are examples of cloud computing services we have been using since years ago. Besides, application such as Amazon Web Services, Google Apps, and Dropbox are also widely used in different sectors of society around the world in 24/7 for various purposes, not only for personal use, but also for business use as well as information sharing. These facts show that cloud computing is ubiquitous, where the services are available for everyone in anywhere at any time, provided Internet connection.

Statistics provided by Statista, one of the international online statistics databases, shown that the worldwide spending on public cloud increases from year to year without inflation [3]. This statistic in other mean has shown the fact that the global demand on cloud computing is increasing. The main reason lies behind the increasing in demand of cloud computing over traditional storage method is the benefits provided by cloud computing itself, including efficient telecommute, data storage and backup, as well as disaster recovery [4].

Although the adoption of cloud computing is increasing all the way, but not all corporates move to cloud. Indeed, there are obstacles that inhibit the adoption of cloud, for instances, vendor lock-in, reliability, privacy, pricing, interoperability, and the most important factor to mention, the security [5] [6]. But why security is so important in cloud? As thing goes open where accessibility is ubiquitous to everyone, like cloud, there is a high possibility that it will be taken advantages by some malicious adversaries such as hackers with no good means. If this huge information pool is targeted by pro-hackers, serious damages

could be inflicted to not only the data owners, but other stakeholders as well. Even those well-known large-scale cloud service providers such as Amazon, Google, Microsoft and Sony could not escape and suffered from cloud incidents, in fact, they contributed to more than half of overall [7]. When security is absent or weak in cloud storage, it could cause data leakage as someone else who is unauthorized can access the cloud data easily. For example, one of the infamous cloud data breach was the incident happened in 2010, in which data stored in Microsoft Business Productivity Online Suite (BPOS) was downloaded by unauthorized cloud users [98] [99].

Again, from the statistic provided by Statista, it is clearly shown that global spending on public cloud IaaS is always overwhelming the total of the other two (PaaS and SaaS) from year to year [2]. In other words, IaaS such as cloud storage is the main demand of the world for cloud computing. Therefore, by relating the increasing global demand to cloud [2], high number of cloud incidents occurred in top cloud storage providers [7], and cloud security as the major obstacle which inhabits the adoption of cloud in some corporates [5] [6], hence it is clear that cloud information security is playing a significant role in reducing or even solving most of the cloud incidents.

Information Systems Audit and Control Association (ISACA), had defined the term information security as:

"*Ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity), and non-access when required (availability).*" [8]

In short, information security is composite of three main elements as highlighted in ISACA Glossary of Terms [8], confidentially, integrity and availability. Usually, these three components are known as CIA triad, but to avoid confusion with the term Central Intelligence Agency (CIA), the information security's CIA triad model sometimes is termed as AIC triad instead.

Similarly, as far as cloud storage security is concerned, lots of cloud storage security schemes have introduced by researchers since years ago. Generally, cloud data security schemes can be categorized into three main categories, Proof of Ownership (PoW), Provable Data Possession (PDP), and Proof of Retrievability (PoR). For a brief understanding of differences between PoW, PDP and PoR, a general view of proofs in cloud storage (provided from prover and shown to auditor) is shown in Figure 1 below.

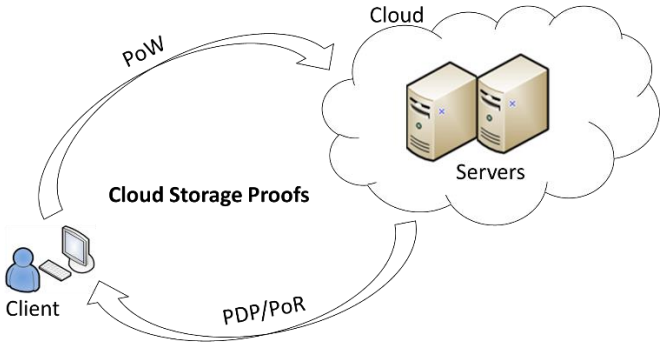

Figure 1: Difference Between PoW vs PDP / PoR

As a brief introduction, PoW was firstly introduced by [9] to allow a cloud user proof to a cloud in which the file is truly owned by the user to prevent malicious adversaries from downloading it even without legal access provided. Since then, there were more PoW schemes been introduced by other researchers for the same purpose but with improvement in algorithm, for example [10], [11], and [12].

Although PoW ensure only true data owner or legitimate shared data client is allowed to retrieve the stored data, cloud server is always labeled untrustworthy. With respect to this, PDP was introduced by [13] to allow the storage server to proof to its client that the stored data is actually possessed by the server with probabilistic possession guarantees. Since then, other PDP schemes such as [14], [15], and [16] were introduced to highlight cloud data integrity. Nevertheless, as PDP itself does not provide recovery on corruption, hence stored data will be irretrievable if corruption occurs, thus causing negative impacts to stakeholders respectively such as data loss, financial damage, as well as loss of trust from client.

PoR [17] that ensure cloud data integrity, similar to that of PDP, but with error-correcting codes (ECC) to allow recovery of data corruption was introduced to address the limitation of PDP. Later, another PoR scheme was introduced by [18], in which erasure coding was applied to allow recovery in case of data corruption. Meanwhile, limitations in [17] such as constrained number of challenges could be conducted by client to the server to verify the integrity of a stored file, were then overcome in [18], provided unbounded number of PoR challenges.

As more and more PoR schemes have been proposed in the recent years, there is a need to make a survey to summarize the latest trend of PoR schemes. Even though there are some cloud storage security related survey papers been published, such as [19], [20], and [21], but they did not sufficiently address the techniques, issues and trend on PoR schemes. Brief surveys on PoR specifically can be found in [22] and [23] with limited number of PoR schemes surveyed and insufficient examples and details. Therefore, the motivation of this paper is to provide a survey on work of recent PoR schemes published from 2013 to 2016. The objectives are (i) to identify the current state of PoR schemes, (ii) to identify issues of employing PoR on cloud storage and potential solutions and (iii) to identify future works of PoR schemes.

The key contributions of this survey paper, each of which addressed each of the identified objective, are listed as follow:

1. We provide a taxonomy on recent PoR schemes with details by adapting several relevant attributes from [69] while widen the categorization which fits for PoR schemes.
2. Discussion and summarization on current cloud storage security issues and countermeasure works correspond to the security issues.
3. Discussion and identification of future trends of cloud storage and future works of PoR schemes.

This paper is organized as follows. Section 2 described about methodology used in this survey. Section 3 discusses and

summarizes current cloud storage issues and vulnerabilities, as well as countermeasure works had done by cloud security teams corresponding to the security issues. In Section 4, latest existing PoR schemes are discussed and a taxonomy of recent PoR schemes is presented. Section 5 presents the discussion and identification on future trends of PoR schemes and cloud storage. Lastly, Section 6 concludes this paper.

2. METHODOLOGY

In this section, the methodology used to conduct the survey of recent PoR schemes is described.

Firstly, to identify the risks of cloud storage and issues of recent PoR schemes which related to data integrity and availability, several sources are referred which include online resources such as news, forums and articles, cloud vendors' sites, as well as published works such as survey and technical papers. Online sources are used to obtain the latest information about cloud storage such as associated risks and past cloud incidents. Meanwhile, survey and technical papers are used to identify the state-of-the-art of PoR related research, cloud storage risks, PoR related issues as well as future work for cloud and PoR.

To ensure that this survey covers the latest trend of cloud storage and PoR schemes, only articles of PoR schemes published in recent years (2013-2016), are considered. Two papers that first present PoRs, [17] and [18], are also considered. A total of 97 articles and references are included in this survey. Most of the articles present work on PoR (43 articles). The remaining are articles on PoW, PDP and cloud data integrity. All the articles referred in this survey can be found in Scopus database.

3. STATE-OF-THE-ART CLOUD STORAGE AND POR SCHEMES

In this section, discussions on current cloud storage issues, vulnerabilities and challenges as well as countermeasures are presented. Based on the work found in the literature, we identify the possible cloud storage issues, vulnerabilities and challenges, together with some suggestions about their countermeasures.

3.1 RISKS ASSOCIATED WITH CLOUD STORAGE

According to [70], there are several risks associated with cloud storage. First of all, using cloud storage, client data is outsourced to cloud storage servers, meaning that the data is at possession of someone else and has full control over it. Without any data integrity schemes, the outsourced data may be tampered, modified, re-outsourced, and even deleted without notice by malicious CSP. Therefore, it is more trustworthy from client view that CSP adopts a PoR scheme to ensure stored data integrity. Besides, as CSP is having full control over the stored data, the security of stored data lies within the responsibility of CSP as data client has no physical control and access to the stored data. Better safe than sorry, data should be encrypted at client side before being uploaded to cloud storage. Another thing is stored data deletion. Regarding to this, as the CSP has full control over the stored data, it may still possess by CSP as a duplicate copy even data client has permanently deleted the file, given reason for rollback deletion function. For this issue, there is no way data clients can confirm their data is still possessed by CSP after deletion. The reason is that, since at the moment this issue is happens, it indicates that the CSP is dishonest, and it is no way for a dishonest CSP notice its client about the fact that they are possessing the deleted copy. Anyway, the best prevention of this issue is to choose a trustable CSP for data outsourcing and apply privacy measures such as encryption to secure the outsourced data.

To ensure data privacy, encryption usually is the best hit. Many large CSP such as Dropbox, Microsoft OneDrive and Google Drive are offering their services with encryption on outsourced data. Regarding to this, [72] and [73] have provided some evidences on comparing Dropbox, OneDrive and Google Drive. Dropbox uses 128-bit Secure Sockets Layer / Transport Layer Security (SSL/TLS) to encrypt data in transit and 256-bit Advanced Encryption Standard (AES) encryption for data at rest [75]; Google Drive uses 256-bit SSL/TLS encryption for data in transit and 128-bit AES encryption for data at rest [76]; OneDrive uses 128-bit SSL/TSL encryption for data in transit, but 256-bit AES encryption for data at rest only available in OneDrive for Business [77], which means data stored in personal OneDrive accounts are vulnerable as having no encryption on data at rest [74]. By looking at these facts, it is clear that which CSP is more secure and otherwise. For encryption, it can be done on either client side or server side, as where the encryption keys are kept. For a stronger security means in term of privacy, it is better to go for client-side encryption rather than server-side encryption although computation and processing time are much a burden on client device. This is to allow client to possess the encryption key for data security. However, decryption on encrypted data would be impossible if client loss the encryption key. Nonetheless, for resource constraint devices like smart phones and tablets, client-side encryption is not recommended due to high computation cost needed.

The next major risk mentioned in [70] is government intrusion. This issue is closely related to confidentiality of stored data. Having information stored in cloud servers make ease for authorities to gain access to it without any knowledge of data client. It is possible for some authorities to claim that data is owned by CSP, thus making CSP to legally obligated to hands-out needed or targeted data stored under their respective storage servers. Although some CSP will not easily hands out data demanded by the authorities without a court order, but no entity can guarantee there will be no data leakage or confidential disclosure of outsourced sensitive information. Nevertheless, data privacy concern was significantly raised in 2013 when one of the contractor Edward Snowden from U.S. Department of Justice (DOJ), the National Security Agency (NSA), had exposed information indicating that NSA was using USA Patriot Act [79] to justify the bulk collection of data about millions of phone calls [78]. A suggestion of countermeasure is that performing encryption on client side [85] before outsourcing data to cloud storage servers. If confidential data has to be stored in cloud servers, it should be encrypted first before being uploaded, else it is not advisable to store confidential data online. Even though it is not impossible for pros to break the encryption, however as it is costly and time consuming to do so, unless the data is the truly targeted by some authorities, else there is very low possibility for them to do so [85].

Last but not least, outage of cloud storage servers is also a major risk that requires serious concern. This issue is closely

related to availability of stored data. When cloud storage is outage, all outsourced data is unavailable. Regarding to this, usually cloud storage servers' outage is less likely or very rarely to occurs, according to 99.99% guaranteed availability by CSP [71]. Nevertheless, it does not mean data outage won't happens. For examples, even those CSP titans like Microsoft [80], Amazon [81] and Dropbox [82] were having their storage service outage. Although there is nothing major has been lost on a wide scale during these outages, but these should have raise the concern and awareness of both data client and CSP for cloud storage outage risk. As a possible solution, synchronization of cloud data with local devices should be always allowed and turned on, so that the latest possible version of data can be used in case of cloud storage outage. Nonetheless, frequent synchronization of local devices with cloud data would cause a high consumption of bandwidth. Figure 2 summarizes about the issues and challenges of PoR schemes and cloud storage.

From what we have discussed in this sub-section, it can be summarized that cloud storage is having three main issues: data integrity, data confidentiality and data availability. Out of these three main issues, data integrity and availability are the most important factors as these are the pre-conditions of the existence of a cloud storage service [33]. Although data confidentiality is also important, but it is not as important as the other two factors, data availability and data integrity. In fact, not all CSPs provide cryptography protect against stored data, for example Microsoft OneDrive do not provide any encryption services on data at rest of personal accounts [77] to ensure data confidentiality. This is the reason why we need PoR schemes which ensure both integrity and availability of data stored in cloud storage.

3.2 ISSUES OF POR WITH RESPECT TO CLOUD STORAGE

From the previous sub-section, we have explained the reasons why PoR schemes are needed in cloud storage. In this, sub-section, issues associated with PoR schemes are discussed. Although PoR schemes ensure data availability and data integrity, but in exchange several issues arise, such as efficiency, supportability of devices, malicious threats, and data deduplication issues.

First of all, we would like to address the efficiency issues regarding to computational, storage and communication of cloud integrity schemes (e.g. PoR) for the stored data in cloud storage servers [69]. In general, data integrity schemes such as PoR, preprocess the data before outsourcing it to cloud storage servers. The data preprocessing is time and resource consuming. Thus, a cloud storage service which has implemented cloud integrity schemes suffers from slower data storing process than others which store data directly in storage servers without employ security measures. This is because additional data preprocessing such as employing erasure codes before storing the data in storage servers takes time. Therefore, it is crucial for a cloud integrity scheme to have a computational and communicational efficient construction to chase up the pace of lagging behind due to additional time spent on data preprocessing. At the same time, the storage efficiency is also as important as computational and communicational efficiency, as the cloud data growth rate is exponential [69]. This is a reason why replication of full data across distributed cloud servers [71] is no longer suitable and applicable in the near future, thus further emphasizing the importance of cloud integrity schemes and thus the reason why PoR schemes should be adopted. As a solution to ensure both storage, and communication efficiency, XOR based coding such as network coding which is widely adopted in communication network can be employed to replace full replication, while computational performance of PoR using XOR based coding can be enhanced by parallel processing.

With the emergence of Internet of Things (IoT), we have many electronic devices like smart phones and tablets integrated to the Internet, and so to cloud storage services. We may need our smart phones or tablets to have access to our cloud storage account, working on outsourced storing documents using these resource constraint devices. Thus, there exists a challenge to design a lightweight data auditing scheme for mobile devices which are resource limited [15] [19]. Although people is working on this, as we can see in the work of [49], the researchers have proposed a lightweight data auditing scheme for resource constraint devices like smart phones and tablets. However, according to researchers the scheme [49] needs more efficient constructions for less storage requirement and a lower communication cost. As mentioned in previous paragraph, XOR based coding like network coding can be used to save more information using similar or less storage spaces and better communication performance.

On the other hand, data integrity schemes such as PoR schemes are vulnerable to malicious threats and similarly cyber-attacks that cause data loss. Some malicious threats include tag forgery attack [69] [83] where malicious cloud storage servers attempt to hide stored data damage and bypass auditing process, data deletion attack [69] in situation where only tags are needed for proof generation rather than data itself, and replace attack [69] where corrupted or deleted stored data block and tag pairs are replaced with other valid pairs so to pass data auditing. For another thing, malicious storage servers may try to cache responses of precious passed auditing challenge to be replayed in future auditing [53] [57]. Not limited to these attacks, it is possible for a malicious storage server to act dishonest by pass the auditing process using valid data, but providing corrupted stored data blocks during repair phase to construct a faulty new data blocks instead of recovery. This is known as pollution attack [53] [69]. Besides, there is also a malicious threat known as data leakage attack [69], where malicious cloud storage servers attempt to extract stored data when verification is using wiretapping. Nevertheless, [69] also suggested that data blocks and metadata pairs should be constructed in such a way that they have strong binding with each other, while proof generation during data auditing should involves both data and metadata pairs as well as randomness factor in challenge-response mechanism. For example, [33] construct the coded block and metadata in such a way that coded block is the index of permutation list for recover back the original data for data retrieval using information stored in its metadata.

The last issue of PoR to address here is data deduplication. Data deduplication is a process of eliminates redundant data copies in the cloud to saves storage spaces [84], where data deduplication is commonly adopted in PoW. Meanwhile, PoR is making redundant copies at data blocks level to provide recovery and retrievability. In general, PoR schemes are contradicting the nature of cloud data deduplication as PoR tends to form data redundancy while data deduplication tends to

eliminates redundant data. Faulty deduplication on data stored using PoR can cause permanent data loss whether partly or fully. Although there are few PoR schemes have been proposed in recent years to integrate PoR schemes with data deduplication where PoR integrate with PoW, for example [30], [44], [47], and [59]. To the best of our knowledge, the work done on integrating PoR with deduplication is limited to static data only. Hence, future work is needed to allow dynamic operations in PoR while integrating with PoW as cloud data like documents stored in Google Docs can be edited online smoothly and safely.

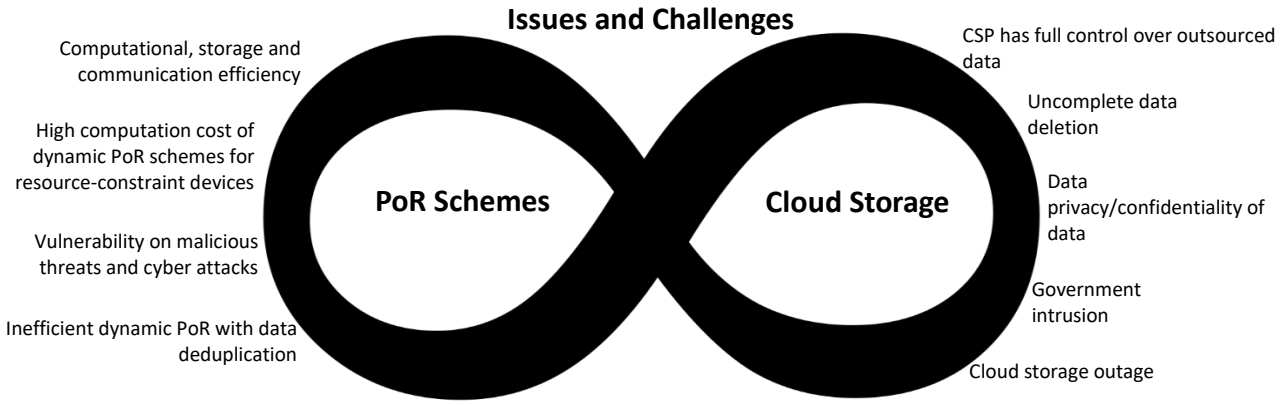

Figure 2: Summary of Issues and Challenges of PoR Schemes and Cloud Storage

4. POR SCHEMES FOR CLOUD STORAGE

This section firstly shows the time line of PoR schemes. Then, the details on PoR schemes proposed by researchers in recent years are reviewed based on several attributes in taxonomy. Lastly, the taxonomy about reviewed recent PoR schemes is tabulated in Table 1.

The first PoR scheme was introduced by [17] in 2007 and later, [18] was proposed in 2008 for unbounded number of times of PoR data integrity challenge (challenge client to provide a proof), which is a limitation in [17]. Since then, many PoR schemes have been proposed by researchers. Figure 3 shows the time line of PoR schemes. In this paper, we consider only articles indexed by Scopus corresponding to PoR schemes proposed in recent years (2013-2016). Since we are only interested with the recent PoR schemes, the schemes proposed before the year 2013 are not included in this paper except [17] and [18] as these two papers are widely referenced and contributed to the idea and construction of PoR schemes.

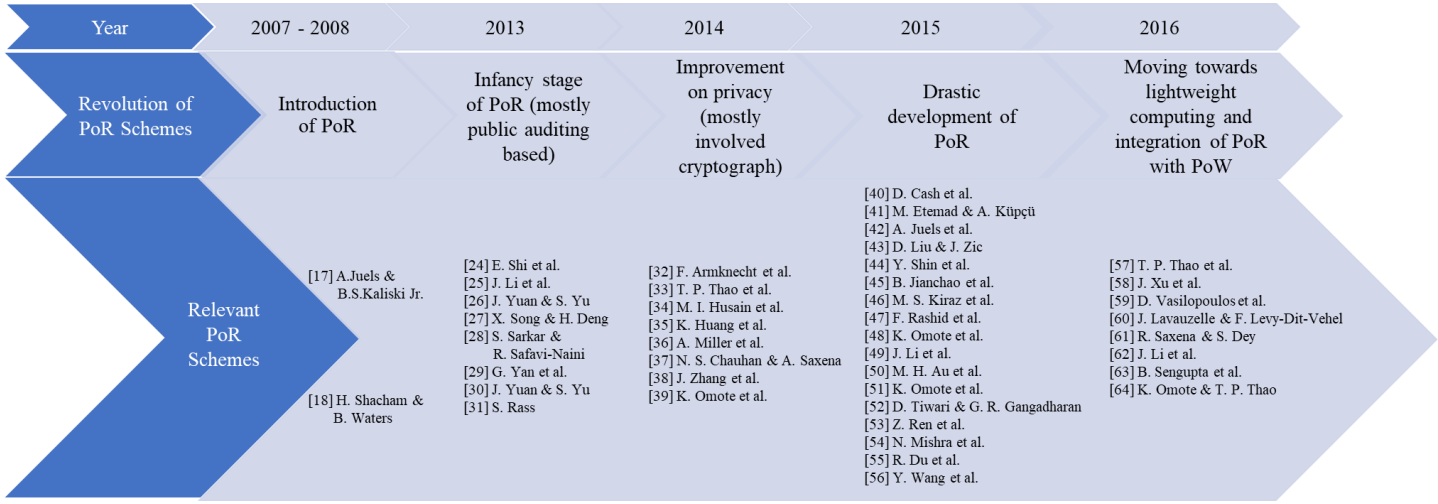

Figure 3: Time Line of PoR Schemes

4.1 PRELIMINARY

Before the first PoR scheme [17] is proposed, availability of outsourced data using replication throughout distributed servers in cloud is very resource extensive, especially in this exponential data growth era. Basically, [17] is a sentinel based PoR scheme, proposed not only to ensure availability of cloud data like PDP, but with error correcting codes employed, it enable cloud data to recover from corruption. Sentinel is a randomly-valued check block embedded in encrypted file for storage verification [17]. Meanwhile, Message Authentication Code (MAC) is employed to determine whether the corruption is correctly recovered, while its function is primitively to verify whether the stored file is subjected to tampering or not [17]. The function of the sentinel embedded in data is for storage auditing purpose (storage verification); to verify if the data is entirely stored or otherwise.

Besides, the security of this stored file is ensured by means of encryption; in addition to the way the sentinels are embedded into the encrypted file randomly [17], archive cannot distinguish between sentinels and portions of original file (which blocks are sentinels and which blocks are data), making the storage servers have no choice but to store the entrusted file properly.

Nevertheless, due to the limitation of bounded number of PoR challenge (number of times where client or auditor can challenge storage servers to provide proof where the entrusted file is stored properly via PoR) in [17], two auditing schemes proposed in [18] to overcome the limitations, on which are private audit by using pseudorandom functions (PRF), and public audit by using Boneh-Lynn-Shacham signature (BLS signature). Meanwhile, both schemes used homomorphic authenticators (BLS and PRFs) to reduce response length by combining blocks and a number of authenticators into a single aggregated block and authenticator. This is because homomorphic authenticators allow any entity to certify the output of a complex computation over a huge authenticated data with only a short tag. Nevertheless, the private audit scheme shown a shorter server response time compared to the public audit scheme [18]. In term of recovery and data corruption resiliency, [18] used erasure coding to recover corrupted data. As time passes, more and more PoR schemes have been proposed. In the next sub-section, we will review PoR schemes proposed in recent years, from 2013 to 2016.

4.2 POR SCHEMES PROPOSED IN RECENT YEARS

As we can see in the time line of PoR schemes shown in Figure 3, lots of PoR schemes have been proposed using different approaches and techniques of implementation. To adopt the PoR in real cloud environment, CSPs have to choose the one that best fits their business objectives. By this mean, we constructed a taxonomy of PoR schemes that describes the attributes of the surveyed papers; nature of data, cloud storage server setup, form of stored data, recovery, storage auditing, cryptography, as well as experimentation and analysis. The idea of taxonomy of this paper adapted and modified the structure and several relevant attributes from [69]. As researchers [69] made their taxonomy based on cloud storage integrity schemes in general (PDP, PoR, etc.), and since we focus specifically on PoR schemes only, hence not all attributes in [69] are relevant to be assimilated in our paper. The following sub-section describes the taxonomy in details by summarizing recent PoR schemes.

4.2.1 RELATED WORKS - RECENT POR SCHEMES

In recent years, a number of PoR schemes have been proposed by researchers to address cloud integrity issues. To gain a better understanding of related works in PoR schemes, this section provides a taxonomy of recent PoR schemes corresponding to attributes as follows: nature of data, cloud server setup, form of data stored, recovery, auditing, cryptography, and experimentation and analysis.

The first attribute included in the taxonomy of PoR schemes in this paper is nature of data. Data can be in mainly two forms, static data and dynamic data. Static data is the data that stay unchanged after created for examples YouTube videos, whereas dynamic data is the data that consistently changing due to updates such as word documents stored using Google Docs. Nature of data is an important attribute to look in as some CSPs provide storage of static data, while some others provide storage of dynamic data. Hence, adoption of which PoR scheme in their cloud depending on their needs and the compatibility of PoR schemes in term of dynamic operation supports such as update, delete and insert operations on stored data. The founder of PoR [17] as well as widely referenced model of PoR [18] are both exhibit static data nature in their schemes, which means they do not support dynamic operations. Similarly, PoR schemes such as [30], [32], [33], [37] and [39] are PoR schemes deal with static data. Meanwhile, PoR schemes which support for dynamic data operations include [24], [25], [31], [34], [35] and [36].

The second attribute included in the taxonomy is cloud server setup. There are mainly two ways of cloud storage server setup for PoR schemes; single server setup and multi-servers' setup or distributed servers' setup. Single server usually has a better specification and bigger compared to multiple servers which are comparably smaller. This is because single server has to be very powerful and all-in-one to cover all needed functionalities such as proxy and storage. PoR schemes which apply single server's setup require the full data to be stored in a single server, such as [40], [43], [44], [46] and [47]. On the other hand, multiple servers have different functionalities, but often comes with lower specification. In cloud storage, multiple servers' setup not only allow better performance on large amount of concurrent storage-retrieval requests, but also represent the resiliency of the cloud storage system against outages. PoR schemes which apply distributed servers' setup require the full data to be partitioned or split into parts or chunks, and then distributed to store in multiple servers, for example [41], [42], [45], [48] and [49]. Obviously, using distributed servers to store a single file is much more resilient compared to store full data in a single server in term of data availability. Although single server setup may yield considerably lower communication cost as this requires no communication between servers, but this setup requires the scheme to enable recovery of full data each time server corruption happens. They also have the risk of server downtime problem. In short, distributed servers' setup is better in term of data availability and corruption resiliency than that of single server setup for PoR schemes. As a matter of fact, PoR schemes proposed in recent years that employ distributed servers' setup have outnumber the single server's setup PoR schemes. Nevertheless, there exists PoR schemes which can be implemented in both server setup method, for example [34].

The third attribute of the taxonomy is the form of stored data in cloud storage servers. There are lots of forms a file can be stored in cloud storage servers, like data in their original form (not encrypted or coded) and distributed erasure coded data chunks. Nevertheless, it is very difficult to tell which data storage form is better as it depends on the techniques used in PoR schemes which work on them such as erasure coding and replication. Depends on different techniques and requirements, data can be stored as chunks across distributed servers, or even as forward error-correcting coded (FEC) data stored in just a single server. Note that FEC is a code to allow the server to have the ability to correct the error without needing for a retransmission of the data, for example Hamming code. For PoR schemes reviewed in this paper, we can categorize this attribute into (i) coded blocks with metadata or tags, (ii) data with signature or tags, and (iii) others. The first form (i) coded blocks and metadata or tags, can be seen as data that is broken into

pieces of chunks or parts, then these data chunks changed into coded form (eg. 1100 ⊕ 0011 = 1111) after undergo some operations such as XOR. Metadata or tags in this case served as a key or information for some purpose such as decoding, for example the number of bit '1' in the coded data. PoR schemes with data stored as form (i) such [24], [25] and [26] are mostly applied in distributed server's setup, although there are some exception cases like [40], [58], and [60]. The second form (ii) data with signature or tags, can be seen as data which its form un-change, but added with some codes (eg. parity bits), mostly to preserves their correctness (no corruption) known as metadata or tags. For PoR schemes which have the data to be stored in the form (ii), we found that it is more favorable with single server's setup PoR schemes compared to other form for data to be stored in cloud storage server mostly for the sake of saving communication time, for example [37], [43], [44], [46] and [47]. Lastly, some PoR schemes have their client's data to be stored in other forms (iii), not limited to [31], [34], and [41], but we can see that the two forms (i) and (ii) outnumber than other forms (iii). Nevertheless, it seems there is no problem in which form data is more favorable to be stored in cloud storage servers, for those PoR schemes apply distributed servers' setup.

The forth attribute of the taxonomy is recovery. A common technique used for data recovery is by adding error correcting codes (ECC) such as cyclic redundancy check codes (CRC) and parity check codes. Usually, computing ECC consume less computation time and resources like storage and memory compared to other recovery techniques. Due to simplicity and lower computation cost of ECC, we can see many PoR schemes are employing ECC, which including [17], [25], [31], [42], and [52]. However, ECC generally causes considerably great increase in data size. For example, in parity check codes, each data bit has to be assigned a parity bit for error checking. The second recovery technique is erasure coding. Erasure coding is a type of coding by which data is split into pieces, encoded with other data pieces, and stored across distributed storage servers. Not to mentioned, erasure coding contributes to lesser increase in data size, approximately 50% increase in data size, compared to ECC as well as replication. Due to this minimal increase in data size, currently many PoR schemes are designed using erasure coding, for example [18], [24], [32], [40], [55], and [63]. The third technique is network coding (NC), which is widely used in data transmission, is assimilated in PoR schemes [48], [57], and [64] due to its efficiency. The main idea of NC is conducting exclusive OR (XOR) operation among data blocks to form a coded block. Similar to erasure coding, NC only causes data to increase its size by around 50%. However, network coding is better than erasure coding in term of efficiency. This can be explain using a data corruption scenario, where erasure coded data required the retrieval of full data before recovery can be applied. In NC coded data on the other hand, only coded blocks which are constructed from the data blocks used to form the corrupted coded blocks are needed for recovery. Other recovery techniques (such as dispersal coding and Slepian-Wolf coding) not limited to techniques mentioned are adopted in PoR schemes, for example [54], [56], [60], and [61], while PoR schemes [27], [39], [51], and [53] have adopted more than one recovery techniques.

The fifth attribute of the taxonomy is storage auditing. In PoR schemes, storage auditing is a method of verification to check either the cloud storage servers are properly storing clients' data. Data auditing is initiated by client asking the storage servers to provide proofs via PoR challenges. There are two ways of storage auditing; (i) first is private auditing where data auditing is conducted by data owners or shared data users, (ii) second is public auditing conducted by third party auditor (TPA). For privacy concern, private auditing is preferred as data is not exposed to someone unknown or not trustable, whereas public auditing usually requires trust to TPA or implementation of cryptography schemes to the stored data. There are almost similar in number of PoR schemes adopting public auditing such as [24], [32], [44], and [48] whereas private auditing such as [17], [40], [45], and [59]. Only a few PoR schemes adopting both private and public auditing such as [18], [35], and [38].

The sixth attribute of the taxonomy is cryptography. Cryptography is applied on the stored data for privacy concern. Cryptographic techniques reviewed including encryption, hashing and others. Generally, encryption is one of the widely-used cryptography approach, where data is translated into secret codes, where key(s) is needed to read the encrypted data via decryption (reverse process of encryption). There are two main encryption techniques employed, (i) symmetric encryption that uses the same key for both encryption and decryption process, and (ii) asymmetric encryption that uses different key for encryption and decryption. Asymmetric encryption is stronger and more secure than symmetric encryption as it uses different keys for encryption and decryption, making brute-force cracking encrypted data a more difficult task. However, asymmetric encryption consumed more time to compute compared to symmetric encryption. As for application of encryption in PoR schemes, most of the work employed symmetric encryption which include [17], [24], [26], [39], [40], [56], and [63]. For another thing, although not as frequent as encryption, hashing is another cryptography approach used in PoR schemes. Generally, hashing is a one-way cryptographic function to transform data into a shorter fixed-length value or key such as digital fingerprint and checksum. Using a fine designed algorithm, reversing he hashing process to reveal the hashed data is nearly impossible. Examples of PoR schemes adopted hashing for the stored data are [25], [31], [34], [35], and [52]. Meanwhile, there are some PoR schemes without adopting any cryptography approaches, such as [33], [38], [41], and [55], most probably due to performance and efficiency concern.

The seventh attribute of the taxonomy is experimentation and analysis. For cloud storage integrity schemes like PoR schemes, there are a few methods can be used for showing, proving and comparing the effectiveness and performances of the proposed schemes. As regards the experimentation and analysis methods for PoR schemes, analytical solution, simulation, prototype, etc. are commonly used to show and compare performance of PoR schemes. Analytical solution is method of showing the performance of proposed or compared schemes, by giving a general description about the performance of the schemes for any value of parameters [65]. As for simulation, it is also a method of showing the performance of proposed or compared schemes, but different with analytical solution in which simulation is a process of imitation of the schemes in a real-world process over time with specified parameters [66], [67]. Meanwhile, prototype is a preliminary product of a scheme designed to collect more experimental or testing data before a better version of the schemes could be implemented [68]. Depending on many factors,

such as precision and accuracy of complexity analysis, compatibility and viability of simulation in real cloud environment, feasibility of prototype, judging which is the most trustworthy proving and comparing method for PoR schemes is very difficult. Indeed, it is a very subjective question or topic to discuss. However, performance comparison among the surveyed PoR schemes is less relevant and not very applicable, because the surveyed PoR schemes have different aspect of focus. Some PoR schemes are focusing on improving communication (transmission) performance [26], whereas some are focusing on error recovery computation performance [48]. Thus, comparing the surveyed PoR schemes in term of computation performance is less relevant and lack of fairness in comparison. Hence, performance comparison among the survey PoR schemes is not conducted in this paper. Nevertheless, it is possible to look for the trend of experimentation and analysis used in recent PoR schemes. As for PoR schemes' papers reviewed in this paper, obviously analytical and simulation approach are more or less similar in their use frequency, whereas prototype and other methods are less likely to go favorable, not to mentioned how infrequent researchers shown their proposed PoR schemes' performances using more than one method.

Table 1: Taxonomy of Recent PoR Schemes

	Attributes	**Sub-Attributes**	**References**
PoR Schemes	Nature of data	Static	[17] A.Juels & B.S.Kaliski Jr., [18] H. Shacham & B. Waters, [26] J. Yuan & S. Yu, [27] X. Song & H. Deng, [28] S. Sarkar & R. Safavi-Naini, [29] G. Yan et al., [30] J. Yuan & S. Yu, [32] F. Armknecht et al., [33] T. P. Thao et al., [37] N. S. Chauhan & A. Saxena, [38] J. Zhang et al., [39] K. Omote et al., [42] A. Juels et al., [43] D. Liu & J. Zic, [44] Y. Shin et al., [45] B. Jianchao et al., [47] F. Rashid et al., [48] K. Omote et al., [50] M. H. Au et al., [51] K. Omote et al., [55] R. Du et al., [57] T. P. Thao et al., [59] D. Vasilopoulos et al., [60] J. Lavauzelle & F. Levy-Dit-Vehel, [62] J. Li et al., [63] B. Sengupta et al.
		Dynamic	[24] E. Shi et al., [25] J. Li et al., [31] S. Rass, [34] M. I. Husain et al., [35] K. Huang et al., [40] D. Cash et al., [41] M. Etemad & A. Küpçü, [46] M. S. Kiraz et al., [49] J. Li et al., [52] D. Tiwari & G. R. Gangadharan, [53] Z. Ren et al., [54] N. Mishra et al., [56] Y. Wang et al., [58] J. Xu et al., [61] R. Saxena & S. Dey, [64] K. Omote & T. P. Thao
	Cloud storage server setup	Single server	[31] S. Rass, [37] N. S. Chauhan & A. Saxena, [40] D. Cash et al., [43] D. Liu & J. Zic, [44] Y. Shin et al., [46] M. S. Kiraz et al., [47] F. Rashid et al., [58] J. Xu et al., [60] J. Lavauzelle & F. Levy-Dit-Vehel,
		Distributed servers	[17] A.Juels & B.S.Kaliski Jr., [18] H. Shacham & B. Waters, [24] E. Shi et al., [25] J. Li et al., [26] J. Yuan & S. Yu, [27] X. Song & H. Deng, [28] S. Sarkar & R. Safavi-Naini, [29] G. Yan et al., [30] J. Yuan & S. Yu, [32] F. Armknecht et al., [33] T. P. Thao et al., [35] K. Huang et al., [36] A. Miller et al., [38] J. Zhang et al., [39] K. Omote et al. [41] M. Etemad & A. Küpçü, [42] A. Juels et al., [45] B. Jianchao et al., [48] K. Omote et al., [49] J. Li et al., [50] M. H. Au et al., [51] K. Omote et al., [52] D. Tiwari & G. R. Gangadharan, [53] Z. Ren et al., [54] N. Mishra et al., [55] R. Du et al., [56] Y. Wang et al., [57] T. P. Thao et al., [59] D. Vasilopoulos et al., [61] R. Saxena & S. Dey [62] J. Li et al., [63] B. Sengupta et al., [64] K. Omote & T. P. Thao
		Either setup methods	[34] M. I. Husain et al.
	Form of data stored	Coded blocks and metadata / tags	[17] A.Juels &.S.Kaliski Jr., [24] E. Shi et al. [25] J. Li et al., [26] J. Yuan & S. Yu, [33] T. P. Thao et al., [40] D. Cash et al., [45] B. Jianchao et al., [48] K. Omote et al., [49] J. Li et al., [51] K. Omote et al., [53] Z. Ren et al., [55] R. Du et al., [58] J. Xu et al. [60] J. Lavauzelle & F. Levy-Dit-Vehel, [64] K. Omote & T. P. Thao
		Data and signature / tags	[18] H. Shacham & B. Waters, [27] X. Song & H. Deng, [28] S. Sarkar & R. Safavi-Naini, [29] G. Yan et al., [30] J. Yuan & S. Yu, [32] F. Armknecht et al., [35] K. Huang et al., [36] A. Miller et al., [37] N. S. Chauhan & A. Saxena, [38] J. Zhang et al. [39] K. Omote et al., [42] A. Juels et al., [43] D. Liu & J. Zic, [44] Y. Shin et al., [46] M. S. Kiraz et al., [47] F. Rashid et al., [50] M. H. Au et al., [52] D. Tiwari & G. R. Gangadharan, [54] N. Mishra et al., [56] Y. Wang et al., [57] T. P. Thao et al., [61] R. Saxena & S. Dey, [62] J. Li et al.
		Others	[31] S. Rass, [34] M. I. Husain et al., [41] M. Etemad & A. Küpçü, [59] D. Vasilopoulos et al., [63] B. Sengupta et al.
	Recovery	Error correcting codes (ECC)	[17] A.Juels & B.S.Kaliski Jr., [25] J. Li et al., [31] S. Rass, [34] M. I. Husain et al., [37] N. S. Chauhan & A. Saxena, [42] A. Juels et al., [47] F. Rashid et al., [52] D. Tiwari & G. R. Gangadharan, [59] D. Vasilopoulos et al., [62] J. Li et al.
		Erasure coding	[18] H. Shacham & B. Waters, [24] E. Shi et al., [26] J. Yuan & S. Yu, [29] G. Yan et al. [30] J. Yuan & S. Yu, [32] F. Armknecht et al., [36] A. Miller et al., [38] J. Zhang et al. [40] D. Cash et al., [41] M. Etemad & A. Küpçü, [44] Y. Shin et al., [49] J. Li et al. [50] M. H. Au et al., [55] R. Du et al., [58] J. Xu et al., [63] B. Sengupta et al.
		Network coding (NC)	[48] K. Omote et al., [57] T. P. Thao et al., [64] K. Omote & T. P. Thao
		Others	[28] S. Sarkar & R. Safavi-Naini, [33] T. P. Thao et al., [35] K. Huang et al., [43] D. Liu & J. Zic, [45] B. Jianchao et al., [46] M. S. Kiraz et al., [54] N. Mishra et al., [56] Y. Wang et al, [60] J. Lavauzelle & F. Levy-Dit-Vehel, [61] R. Saxena & S. Dey
		More than one	[27] X. Song & H. Deng, [39] K. Omote et al., [51] K. Omote et al., [53] Z. Ren et al.

		technique	
	Storage auditing	Public	[24] E. Shi et al., [25] J. Li et al., [26] J. Yuan & S. Yu, [27] X. Song & H. Deng, [28] S. Sarkar & R. Safavi-Naini, [29] G. Yan et al., [30] J. Yuan & S. Yu, [32] F. Armknecht et al., [34] M. I. Husain et al., [44] Y. Shin et al., [46] M. S. Kiraz et al., [48] K. Omote et al., [49] J. Li et al., [50] M. H. Au et al., [52] D. Tiwari & G. R. Gangadharan, [53] Z. Ren et al., [54] N. Mishra et al., [56] Y. Wang et al., [57] T. P. Thao et al., [61] R. Saxena & S. Dey
		Private	[17] A.Juels & B.S.Kaliski Jr., [31] S. Rass, [33] T. P. Thao et al., [36] A. Miller et al., [37] N. S. Chauhan & A. Saxena, [39] K. Omote et al., [40] D. Cash et al., [41] M. Etemad & A. Küpçü, [42] A. Juels et al., [43] D. Liu & J. Zic, [45] B. Jianchao et al, [47] F. Rashid et al., [51] K. Omote et al., [55] R. Du et al., [58] J. Xu et al., [59] D. Vasilopoulos et al., [60] J. Lavauzelle & F. Levy-Dit-Vehel, [62] J. Li et al., [63] B. Sengupta et al., [64] K. Omote & T. P. Thao
		Both methods	[18] H. Shacham & B. Waters, [35] K. Huang et al., [38] J. Zhang et al.
	Cryptography	Asymmetric encryption	[18] H. Shacham & B. Waters, [32] F. Armknecht et al., [36] A. Miller et al. [46] M. S. Kiraz et al., [50] M. H. Au et al., [53] Z. Ren et al., [64] K. Omote & T. P. Thao
		Symmetric encryption	[17] A.Juels & B.S.Kaliski Jr., [24] E. Shi et al., [26] J. Yuan & S. Yu, [28] S. Sarkar & R. Safavi-Naini, [29] G. Yan et al., [30] J. Yuan & S. Yu, [37] N. S. Chauhan & A. Saxena, [39] K. Omote et al., 40] D. Cash et al., [42] A. Juels et al., [43] D. Liu & J. Zic, [45] B. Jianchao et al., [47] F. Rashid et al., [48] K. Omote et al., [51] K. Omote et al., [54] N. Mishra et al., [56] Y. Wang et al., [58] J. Xu et al., [59] D. Vasilopoulos et al., [60] J. Lavauzelle & F. Levy-Dit-Vehel, [61] R. Saxena & S. Dey, [62] J. Li et al., [63] B. Sengupta et al.
		Others (Hashing, etc.)	[25] J. Li et al., [27] X. Song & H. Deng [31] S. Rass, [34] M. I. Husain et al., [35] K. Huang et al., [49] J. Li et al., [52] D. Tiwari & G. R. Gangadharan
		None	[33] T. P. Thao et al., [38] J. Zhang et al., [41] M. Etemad & A. Küpçü, [44] Y. Shin et al., [55] R. Du et al., [57] T. P. Thao et al.
	Experimentation and analysis	Analytical	[17] A.Juels & B.S.Kaliski Jr., [18] H. Shacham & B. Waters, [25] J. Li et al., [26] J. Yuan & S. Yu, [28] S. Sarkar & R. Safavi-Naini, [31] S. Rass, [37] N. S. Chauhan & A. Saxena, [39] K. Omote et al., [40] D. Cash et al., [41] M. Etemad & A. Küpçü, [44] Y. Shin et al., [45] B. Jianchao et al., [46] M. S. Kiraz et al., [50] M. H. Au et al., [51] K. Omote et al., [56] Y. Wang et al., [58] J. Xu et al., [59] D. Vasilopoulos et al., [64] K. Omote & T. P. Thao
		Simulation	[24] E. Shi et al., [30] J. Yuan & S. Yu, [33] T. P. Thao et al., [34] M. I. Husain et al., [35] K. Huang et al., [36] A. Miller et al., [38] J. Zhang et al., [42] A. Juels et al., [47] F. Rashid et al., [48] K. Omote et al., [52] D. Tiwari & G. R. Gangadharan, [53] Z. Ren et al., [55] R. Du et al., [57] T. P. Thao et al., [60] J. Lavauzelle & F. Levy-Dit-Vehel, [61] R. Saxena & S. Dey, [62] J. Li et al., [63] B. Sengupta et al.
		Prototype	[32] F. Armknecht et al., [43] D. Liu & J. Zic, [54] N. Mishra et al.
		Others	[49] J. Li et al.
		More than one method	[27] X. Song & H. Deng, [29] G. Yan et al.

In summary, all PoR schemes are composing of all the seven attributes of the taxonomy discussed. From the taxonomy, we discovered that the construction of PoR is moving towards to dynamic data nature, as dynamic PoR suits not only dynamic data, but also compatible with static data which requires no update. On the other hand, distributed servers' setup is more prominent due to data corruption resiliency and backup compared to single server's setup. Meanwhile, all form of data stored seems work well in PoR schemes which employed distributed servers' setting, but coded blocks and metadata or tags form seems to be more secure, as data is not stored exactly the same form (for example, data such as 1100 is coded and stored as 1111) requires malicious adversary to work harder to retrieve the data. In term of recovery, although erasure coding is still leading the trend, but in future, network coding might be a good choice for PoR construction, as its resource and computation efficiency in data recovery process compared to erasure coding. For storage auditing, it is very difficult to tell which is more prominent, but it would be better if both public and private auditing are made selectable in a PoR scheme to fulfill the wide variety needs of different users worldwide (some users concerns privacy, whereas some busy users need TPA to help data auditing). For cryptography, it is a give and take or trade-off between efficiency and security, but our review had shown most PoR schemes do provide a minimum of security with symmetric encryption. Lastly, it is easier for other researchers to do comparison between theirs and those reviewed if analytical method is used for experimentation and analysis towards efficiency of PoR schemes.

5. FUTURE TRENDS OF POR SCHEMES AND CLOUD STORAGE

5.1 FUTURE TRENDS OF POR SCHEMES

New issues and challenges are emerging associated with the emergence of new technologies. Hence it is important to keep up the pace with evolution of information technologies.

Corresponding to several issues of PoR schemes identified in Section 3, there are research gaps left for future works need to be conducted to address those issues. Firstly, geo-location of outsourced data, which is the actual location of servers where the data is stored [69]. For example, Dropbox cloud storage are hosted in data centers across the United States.

As mentioned in previous section, some authorities may have access to the data hosted in their countries with the use of law enforcement. Therefore, it is important for CSP to provide data clients information about where the outsourced data is stored. At the same time, there is a need to ensure stored data is not migrated to data center hosted in other region or even re-outsourcing to other cheaper storage vendor [69] without providing notice to data client or agreement from data client. In future PoR schemes, geo-location of stored data should be considered one of the integrity factor to be checked during data auditing challenges.

Secondly, assured deletion [69] should be considered in future PoR schemes as well. Assured deletion of data means upon delete action done by data client, no roll-back can be done and the data is deleted entirely without any backup copies remain in cloud servers. The assured deletion mentioned should include permanent deletion of targeted data, at the same time other versions of data that shares common data should be remain unaffected. This means that after permanent deletion operation is performed on the targeted version of data, it should be made not only permanently inaccessible, but also permanently unrecovered after a period of agreed deletion unroll time, in order to ensure data integrity. It is important to prevent malicious CSP from secretly keeping a copy of deleted data for some reasons without agreement from data client.

Thirdly, deduplication [69] as mentioned in previous section as well, should be included in future PoR schemes, but the idea here is slightly different from [69]. The main idea here is to integrate PoR scheme with PoW schemes. In order to ensure only legitimate data clients are able to fully retrieve the outsourced data without the risk of data lost and data leakage due to eavesdropping, PoR scheme needs to properly integrate with PoW scheme which employed deduplication. As mentioned in previous section, there are some works done by researchers for PoR schemes that allow deduplication [30], [44], [47], [59], but computation and storage efficiency is still left a problem. In short, PoR and PoW are mutually contradict in nature, thus future work is still needed to efficiently integrated PoR with PoW schemes.

Another future work of PoR schemes is efficient and low resource cost in term of storage and memory usage for client-side encryption [85]. This has been mentioned in Section 2 that it is still a risk to have an untrusted storage provider to encrypt outsourced data and at the same time keeping the cryptographic keys. If malicious cloud servers intend to extract stored data secretly, with the keys hold in hand, information can be easily decrypted and extracted out the stored data without anyone notice. If this happens, data confidentially is loss, as there is no more privacy. This shows the importance of enabling client-side encryption for not letting CSP to hold the keys, but the main problem associated with this is computational and resources efficiency. There is no assurance that client device is very high end and with unlimited resources (storage and memory) that allow heavy computation of encryption at client-side. Hence, this left a future work for PoR schemes to allow efficient and low-cost resource consumption, so that even a resource-constraint device of client can afford client-side encryption in PoR schemes.

Finally, work on lightweight dynamic data auditing for resource constraint devices such as mobile phones [19] need to be conducted. Generally, dynamic operation such as edit, delete, and insert operation on online stored data is considerably resource extensive and timely [19], not to mentioned mobile devices like smart phones, but even for laptops as well. Looking from users' perspective, for editing documents on Google Docs using laptops, lagging is always a critic point. It shows a clear picture where dynamic operation is very resource extensive, and hence the case is applied in mobile device even worse situation. Therefore, it is crucial to involve efficient algorithm in PoR schemes for dynamic updates, hence benefiting mobile device users by affording lightweight mobile PoR schemes with dynamic operations enabled.

5.2 FUTURE TRENDS OF CLOUD STORAGE

With the emergence of Software Defined Networking (SDN), a network protocol that allows centralized control of network applications and devices [89], cloud services can be made more efficient by adopting SDN [90]. One of the benefits of integrating cloud services with SDN is cross-storage in various geo-located servers [88]. The general concept of cross-storage is applying software-defined storage [91], frankly speaking data center plus SDN. As regards to the nature of centralizing in SDN concept to applied in storage services, storage managing can be made increased efficiency and reduced complexity. Stick to the point of cross-storage, there are few examples including multi-clouds, hybrid clouds, meta-clouds and clouds federations provided in [87]. As regard to this, many CSP titans like Microsoft [90] and IBM [92] are working on cross-cloud, hence indicates the future direction of cloud storage.

Next, machine learning and artificial intelligence (AI) will be the future trend of cloud storage [94] [95]. Although thorough application of machine learning and AI, especially on cloud storage still at the stage of infancy, but the works have shown some preliminary results. One of the example is Google's AlphaGo, an AI for a board game called Go, developed using deep learning and other techniques [93]. Besides, systems like Cortana from Microsoft and Siri from Apple are also products from researches in the field of machine learning and AI. From the rise of machine learning and AI, the way of storing and managing big data in cloud may change in near future, and thus the future trend of cloud storage. For example, deep learning can be integrated in dynamic storage system for gaining more storage capacity at a lower cost. Enhanced security and reliability of cloud storage can be expected by employing AI and machine learning to prevent data loss and smart security features to detect data loss during transit in hybrid storage clouds or within cloud [100].

Besides, cloud-to-cloud backup will become the norm in near future [96]. Cloud-to-cloud backup is a process where data stored in a cloud is backup by copying it to another cloud [97]. Even with many recovery technologies invented, but the stored data is still exposed to the risk of data loss due to hardware failure. Imagine if only a copy of data is stored in the data center without backup, when the data center is struck by disaster such as fire or flood, the stored data will never be recovered as storage hardware is destroyed. Nevertheless, as cloud-to-cloud backup which creates more duplicates that is contradict with

deduplication technologies including PoW, further research is needed to allow a secured cloud-to-cloud backup.

Last but not least, cloud security will be considerably improved in the future [95]. As the emergence as many new technologies to integrate with cloud, the openness nature of cloud which should be the benefits but also become threats to its users. In general, anything that is open is insecure as anyone also have access to it, including malicious users like hackers. By integrating other new technologies into cloud, more cloud services can be delivered to cloud users, but weakness or security holes of those technologies may be taken advantage by malicious users to gain benefits, for example patent stealing or credential information leaking. Encryption could be the choice for data privacy protection. Nevertheless, efficiency of intrusion detection systems for guarding a large-scale system like cloud storage and cloud services have to be greatly improved for security concern. One way to do this is to adapt AI and machine learning [100] in the field of cloud security for better intrusion detection and prevention. Real-time encryption technology [86] and real-time efficient defensive system can be the solutions for cloud based malicious threats in the future. Figure 4 below summarizes about the future work of PoR schemes and future trends of cloud storage.

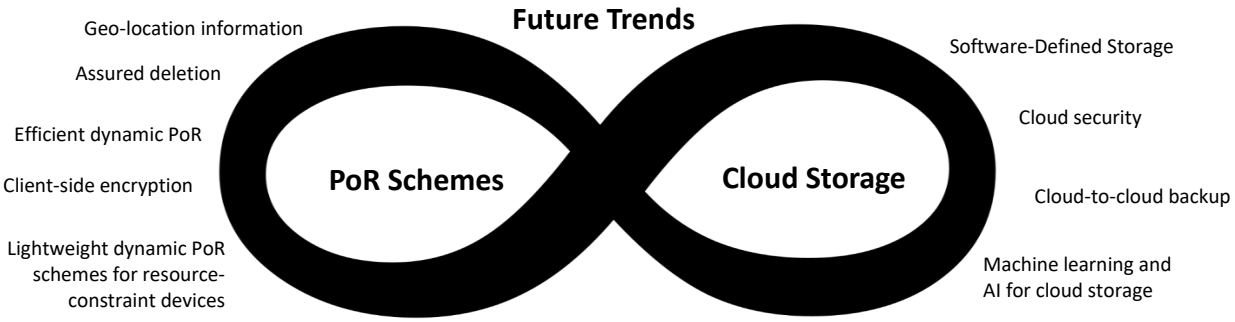

Figure 4: Summary of Future Work of PoR Schemes and Future Trends of Cloud Storage

6. CONCLUSION

In conclusion, cloud storage has been introduced to lessen the burden of local storage including management and maintenance cost, but the existence of cloud storage itself required specific concern about integrity of outsourced data. Regrading to this, many data integrity schemes especially PoR schemes, have been proposed by researchers, to ensure data availability and data integrity. This paper presents the survey on state-of-the-art of PoR schemes, published in 2013-2016. the issues of applying PoR has also been identified. Some possible future work to address the identified issues are also presented. In addition, current cloud storage issues and vulnerabilities together with countermeasures are also discussed.

REFERENCES

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," *NIST Spec. Publ.*, vol. 145, p. 7, 2011.

[2] J. Srinivas, K. Reddy, and A. Qyser, "Cloud Computing Basics," *Build. Infrastruct. Cloud Secur.*, vol. 1, pp. 3–22, 2014.

[3] "Public cloud infrastructure spending worldwide 2015-2026 | Statistic", *Statista*, 2017. [Online]. Available: https://www.statista.com/statistics/507952/worldwide-public-cloud-infrastructure-hardware-and-software-spending-by-segment/. [Accessed: 15- Nov- 2016].

[4] I. Baciu, "Advantages and disadvantages of cloud computing services, from the employee's point of view," no. 13, pp. 95–101, 2015.

[5] Quest Technology Management for Business, "The Benefits and Challenges of Cloud Computing," vol. 32, no. 7, p. 2015, 2015.

[6] B. Nedelcu, S. Madalina-Elena, T. Ioan-Florentin, T. Smaranda-Elena, and V. Alin, "Cloud Computing and its Challenges and Benefits in the Bank System," *Database Syst. J.*, vol. VI, no. 1, pp. 44–58, 2015.

[7] R. Ko, S. Lee, and V. Rajan, "Cloud Computing Vulnerability Incidents: A Statistical Overview," *Cloud Secur. Alliance*, p. 21, 2013.

[8] ISACA, "Isaca," *Glossary*, pp. 1–103, 2015.

[9] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg, "Proofs of Ownership in Remote Storage Systems," *Proc. 18th ACM Conf. Comput. Commun. Secur.*, pp. 491–500, 2011.

[10] C. M. Yu, C. Y. Chen, and H. C. Chao, "Proof of ownership in deduplicated cloud storage with mobile device efficiency," *IEEE Netw.*, vol. 29, no. 2, pp. 51–55, 2015.

[11] J. Hur, D. Koo, Y. Shin, and K. Kang, "Secure Data Deduplication with Dynamic Ownership Management in Cloud Storage," *IEEE Trans. Knowl. Data Eng.*, vol. 28, no. 11, pp. 3113–3125, 2016.

[12] L. González-Manzano and A. Orfila, "An efficient confidentiality-preserving Proof of Ownership for deduplication," *J. Netw. Comput. Appl.*, vol. 50, pp. 49–59, 2015.

[13] G. Ateniese, R. Burns, and J. Herring, "Provable Data Possession at Untrusted Stores," *Proc. 14th ...*, no. 1, pp. 598–610, 2007.

[14] R. Mukundan, S. Madria, and M. Linderman, "Efficient integrity verification of replicated data in cloud using homomorphic encryption," *Distrib. Parallel Databases*, vol. 32, no. 4, pp. 507–534, 2014.

[15] C. Lin, Z. Shen, Q. Chen, and F. T. Sheldon, "A Data Integrity Verification Scheme in Mobile Cloud Computing," *J. Netw. Comput. Appl.*, vol. 77, pp. 146–151, 2017.

[16] Y. Wang, Q. Wu, B. Qin, S. Tang, W. Susilo, and S.

Member, “Online / Offline Provable Data Possession,” *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 5, pp. 1182–1194, 2017.

[17] A. Juels and B. S. Kaliski Jr., “Pors: Proofs of retrievability for large files,” *Proc. ACM Conf. Comput. Commun. Secur.*, pp. 584–597, 2007.

[18] H. Shacham and B. Waters, “Compact proofs of retrievability,” *J. Cryptol.*, vol. 26, no. 3, pp. 442–483, 2008.

[19] M. Sookhak, H. Talebian, E. Ahmed, A. Gani, and M. K. Khan, “A review on remote data auditing in single cloud server: Taxonomy and open issues,” *J. Netw. Comput. Appl.*, vol. 43, pp. 121–141, 2014.

[20] S. G. Worku, T. Zhong, and Z. G. Qin, “Survey on cloud data integrity proof techniques,” *Proc. 2012 7th Asia Jt. Conf. Inf. Secur. AsiaJCIS 2012*, pp. 85–91, 2012.

[21] A. Singh and K. Chatterjee, “Cloud security issues and challenges: a survey Cloud security issues and challenges: a survey,” *J. Netw. Comput. Appl.*, vol. 79, no. November 2016, pp. 88–115, 2016.

[22] A. M. Jadhav and D. P. Gadekar, “A Survey on Proof of Retrievability and its Techniques,” *Int. J. Eng. Tech.*, vol. 4, no. Iii, pp. 269–272, 2016.

[23] M. T. Student, “A Survey on Public Auditing With a Proof of Retrievability in Secure Cloud Storage,” *Int. J. Mag. Eng. Technol. Manag. Res.*, vol. 2, no. March, pp. 118–125, 2015.

[24] E. Shi, E. Stefanov, and C. Papamanthou, “Practical Dynamic Proofs of Retrievability,” *CCS ’13 Proc. 2013 ACM SIGSAC Conf. Comput. Commun. Secur.*, pp. 325–336, 2013.

[25] J. Li, X. Tan, X. Chen, and D. S. Wong, “An efficient proof of retrievability with public auditing in cloud computing,” *Proc. - 5th Int. Conf. Intell. Netw. Collab. Syst. INCoS 2013*, pp. 93–98, 2013.

[26] J. Yuan and S. Yu, “Proofs of retrievability with public verifiability and constant communication cost in cloud,” *Cloud Comput. ’13 Proc. 2013 Int. Work. Secur. cloud Comput.*, pp. 19–26, 2013.

[27] X. Song and H. Deng, “Lightweight proofs of retrievability for electronic evidence in cloud,” *Inf.*, vol. 4, no. 3, pp. 262–282, 2013.

[28] S. Sarkar and R. Safavi-Naini, “Proofs of retrievability via fountain code,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7743 LNCS, pp. 18–32, 2013.

[29] G. Yan, Y. F. Zhu, C. X. Gu, Y. H. Zheng, and J. L. Fei, “An efficient proof of retrievability scheme for fully homomorphic encrypted data,” *J. Networks*, vol. 8, no. 2, pp. 339–344, 2013.

[30] J. Yuan and S. Yu, “Secure and constant cost public cloud storage auditing with deduplication,” *2013 IEEE Conf. Commun. Netw. Secur. CNS 2013*, pp. 145–153, 2013.

[31] S. Rass, “Dynamic Proofs of Retrievability from Chameleon-Hashes,” *Secur. Cryptogr. (SECRYPT), 2013 Int. Conf.*, 2013.

[32] F. Armknecht, J.-M. Bohli, G. O. Karame, Z. Liu, and C. A. Reuter, “Outsourced Proofs of Retrievability,” *CCS ’14 Proc. 2014 ACM SIGSAC Conf. Comput. Commun. Secur.*, pp. 831–843, 2014.

[33] T. P. Thao, L. C. Kho, and A. O. Lim, “SW-POR: A Novel POR Scheme Using Slepian-Wolf Coding for Cloud Storage,” *2014 IEEE 11th Intl Conf Ubiquitous Intell. Comput. 2014 IEEE 11th Intl Conf Auton. Trust. Comput. 2014 IEEE 14th Intl Conf Scalable Comput. Commun. Its Assoc. Work.*, pp. 464–472, 2014.

[34] M. I. Husain, S. Y. Ko, S. Uurtamo, A. Rudra, and R. Sridhar, “Bidirectional data verification for cloud storage,” *J. Netw. Comput. Appl.*, vol. 45, pp. 96–107, 2014.

[35] K. Huang, J. Liu, M. Xian, H. Wang, and S. Fu, “Enabling dynamic proof of retrievability in regenerating-coding-based cloud storage,” *2014 IEEE Int. Conf. Commun. Work. ICC 2014*, pp. 712–717, 2014.

[36] A. Miller, A. Juels, E. Shi, B. Parno, and J. Katz, “Permacoin: Repurposing bitcoin work for data preservation,” *Proc. - IEEE Symp. Secur. Priv.*, pp. 475–490, 2014.

[37] N. S. Chauhan and A. Saxena, “A robust scheme on proof of data retrievability in cloud,” *Proc. 2014 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2014*, pp. 665–671, 2014.

[38] J. Zhang, W. Tang, and J. Mao, “Efficient public verification proof of retrievability scheme in cloud,” *Cluster Comput.*, vol. 17, no. 4, pp. 1401–1411, 2014.

[39] K. Omote and T. P. Thao, “A New Efficient and Secure POR Scheme Based on Network Coding,” *2014 IEEE 28th Int. Conf. Adv. Inf. Netw. Appl.*, 2014.

[40] D. Cash, A. Küpçü, and D. Wichs, *Dynamic Proofs of Retrievability via Oblivious RAM*. Journal of Cryptology, 2015.

[41] M. Etemad and A. Küpçü, “Generic Efficient Dynamic Proofs of Retrievability,” *Cryptol. ePrint Arch.*, pp. 85–96, 2015.

[42] A. Juels, J. Kelley, R. Tamassia, and N. Triandopoulos, “Falcon Codes: Fast, Authenticated LT Codes (Or : Making Rapid Tornadoes Unstoppable),” *Ccs ’15*, pp. 1032–1047, 2015.

[43] D. Liu and J. Zic, “Proofs of encrypted data retrievability with probabilistic and homomorphic message authenticators,” *Proc. - 14th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2015*, vol. 1, pp. 897–904, 2015.

[44] Y. Shin, D. Koo, J. Hur, and J. Yun, “Secure proof of storage with deduplication for cloud storage systems,” *Multimed. Tools Appl.*, 2015.

[45] B. Jianchao, L. Huixia, L. Shoushan, Z. Yaxing, and L. Wei, “Proof of retrievability based on LDPC codes,” *J. China Univ. Posts Telecommun.*, vol. 22, no. 4, pp. 17–25, 2015.

[46] M. S. Kiraz, I. Sertkaya, and O. Uzunkol, “An efficient ID-based message recoverable privacy-preserving auditing

scheme," *2015 13th Annu. Conf. Privacy, Secur. Trust. PST 2015*, pp. 117–124, 2015.

[47] F. Rashid, A. Miri, and I. Woungang, "Proof of Storage for Video Deduplication in the Cloud," *Proc. - 2015 IEEE Int. Congr. Big Data, BigData Congr. 2015*, pp. 499–505, 2015.

[48] K. Omote and T. P. Thao, "MD-POR: Multisource and Direct Repair for Network Coding-Based Proof of Retrievability.," *Int. J. Distrib. Sens. Networks*, vol. 2015, pp. 1–14, 2015.

[49] J. Li, X. Tan, X. Chen, D. S. Wong, and F. Xhafa, "OPoR: Enabling proof of retrievability in cloud computing with resource-constrained devices," *IEEE Trans. Cloud Comput.*, vol. 3, no. 2, pp. 195–205, 2015.

[50] M. H. Au, Y. Mu, and H. Cui, "Proof of retrievability with public verifiability resilient against related-key attacks," *IET Inf. Secur.*, vol. 9, no. 1, pp. 43–49, 2015.

[51] K. Omote and P. T. Tran, "ND-POR: A POR based on network coding and dispersal coding," *IEICE Trans. Inf. Syst.*, vol. E98D, no. 8, pp. 1465–1476, 2015.

[52] D. Tiwari and G. R. Gangadharan, "A novel secure cloud storage architecture combining proof of retrievability and revocation," *2015 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2015*, pp. 438–445, 2015.

[53] Z. Ren, L. Wang, Q. Wang, and M. Xu, "Dynamic proofs of retrievability for coded cloud storage systems," *IEEE Trans. Serv. Comput.*, vol. PP, no. 99, pp. 1–13, 2015.

[54] N. Mishra, R. Bhardwaj, and R. Kumar, "Data traceability in cloud environment," *Int. Conf. Comput. Commun. Autom. ICCCA 2015*, pp. 674–677, 2015.

[55] R. Du, L. Deng, J. Chen, K. He, and M. Zheng, "Proofs of ownership and retrievability in cloud storage," *Proc. - 2014 IEEE 13th Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2014*, pp. 328–335, 2015.

[56] Y. Wang, Q. Wu, B. Qin, X. Chen, X. Huang, and Y. Zhou, "Group-oriented Proofs of Storage," *Asiaccs*, no. 1, pp. 73–84, 2015.

[57] T. P. Thao and K. Omote, "ELAR: Extremely Lightweight Auditing and Repairing for Cloud Security," *ACM Int. Conf. Proceeding Ser.*, vol. 5, pp. 40–51, 2016.

[58] J. Xu, F. Zhou, Z. Jiang, and R. Xue, "Dynamic proofs of retrievability with square-root oblivious RAM," *J. Ambient Intell. Humaniz. Comput.*, vol. 7, no. 5, pp. 611–621, 2016.

[59] D. Vasilopoulos, S. Antipolis, M. Önen, S. Antipolis, S. Antipolis, and S. Antipolis, "Message-Locked Proofs of Retrievability with Secure Deduplication," *CCSW 2016 - Proc. 2016 ACM Cloud Comput. Secur. Work.*, pp. 73–83, 2016.

[60] J. Lavauzelle and F. Levy-Dit-Vehel, "New proofs of retrievability using locally decodable codes," *IEEE Int. Symp. Inf. Theory - Proc.*, vol. 2016–Augus, pp. 1809–1813, 2016.

[61] R. Saxena and S. Dey, "Cloud Audit: A Data Integrity Verification Approach for Cloud Computing," *Procedia Comput. Sci.*, vol. 89, pp. 142–151, 2016.

[62] J. Li, J. Li, D. Xie, and Z. Cai, "Secure Auditing and Deduplicating Data in Cloud," *IEEE Trans. Comput.*, vol. 65, no. 8, pp. 2386–2396, 2016.

[63] B. Sengupta, S. Bag, S. Ruj, and K. Sakurai, "Retricoin: Bitcoin Based on Compact Proofs of Retrievability," *Proc. 17th Int. Conf. Distrib. Comput. Netw.*, p. 14:1--14:10, 2016.

[64] K. Omote and T. P. Thao, "D2-POR : Direct Repair and Dynamic Operations in Network Coding-Based Proof of Retrievability," *IEICE Trans. Inf. Syst.*, no. 4, pp. 816–829, 2016.

[65] P. Impact, T. Changes, W. Paper, and R. S. Company, "Simulation versus Analytic Modeling in Large Computing Environments."

[66] S. Sahin, "Computer simulations in science education: Implications for distance education," *Turkish Online J. Distance Educ.*, vol. 7, no. 4, pp. 132–146, 2006.

[67] A. Maria, "Introduction to modelling and simulation," *Winter Simul. Conf.*, pp. 7–13, 1997.

[68] E. J. Christie *et al.*, "Prototyping Strategies: Literature Review and Identification of Critical Variables," *Am. Soc. Eng. Educ. pp. 01154-22. 2012.*, pp. 1154–1122, 2012.

[69] F. Zafar *et al.*, "A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends," *Comput. Secur.*, vol. 65, 2017.

[70] D. Sullivan, "Top Ten Major Risks Associated With Cloud Storage", *Cloudwards*, 2017. [Online]. Available: https://www.cloudwards.net/top-ten-major-risks-associated-with-cloud-storage/. [Accessed: 05- Apr- 2017].

[71] "Amazon Simple Storage Service (S3) — Cloud Storage — AWS", *Amazon Web Services, Inc.*, 2017. [Online]. Available: https://aws.amazon.com/s3/faqs/. [Accessed: 06- Apr- 2017].

[72] "How secure are Dropbox, Microsoft OneDrive, Google Drive and Apple iCloud cloud storage services?", *Alphr*, 2017. [Online]. Available: http://www.alphr.com/apple/1000326/how-secure-are-dropbox-microsoft-onedrive-google-drive-and-apple-icloud-cloud-storage. [Accessed: 06- Apr- 2017].

[73] "Dropbox Encryption vs. Google Drive Encryption", *Virtru*, 2017. [Online]. Available: https://www.virtru.com/blog/dropbox-encryption/. [Accessed: 06- Apr- 2017].

[74] "OneDrive Security: An Overview", *Sookasa*, 2017. [Online]. Available: https://www.sookasa.com/resources/onedrive-security/. [Accessed: 06- Apr- 2017].

[75] "Security Architecture - Security - Trust guide - Dropbox Business", *Dropbox*, 2017. [Online]. Available: https://www.dropbox.com/business/trust/security/architecture. [Accessed: 06- Apr- 2017].

[76] "Security - Google Cloud Help", *Support.google.com*, 2017. [Online]. Available: https://support.google.com/work/answer/6056693?hl=en. [Accessed: 06- Apr- 2017].

[77] "Microsoft Trust Center | Encryption", *Microsoft.com*, 2017. [Online]. Available: https://www.microsoft.com/en-

us/trustcenter/security/encryption. [Accessed: 06- Apr- 2017].
[78] "What is USA Patriot Act? - Definition from WhatIs.com", *SearchDataManagement*, 2017. [Online]. Available: http://searchdatamanagement.techtarget.com/definition/Patriot-Act. [Accessed: 06- Apr- 2017].
[79] J. Gilbert, "USA Patriot Act Effect on Cloud Computing Services", *ITLG*, 2017. [Online]. Available: https://www.itlawgroup.com/resources/articles/113-usa-patriot-act-effect-on-cloud-computing-services. [Accessed: 06- Apr- 2017].
[80] M. Mozart, "Human Error Caused Microsoft Azure Outage - Cloudwards", *Cloudwards*, 2017. [Online]. Available: https://www.cloudwards.net/news/human-error-caused-microsoft-azure-outage-5776/. [Accessed: 06- Apr- 2017].
[81] M. Balneario and Bjelleklang, "Time to Get Real: Amazon's AWS is Terrifying", *Cloudwards*, 2017. [Online]. Available: https://www.cloudwards.net/time-to-get-real-amazons-aws-is-terrifying/. [Accessed: 06- Apr- 2017].
[82] "Dropbox Explains Reason Behind 2014 Outage", *Cloudwards*, 2017. [Online]. Available: https://www.cloudwards.net/news/dropbox-explains-reason-behind-2014-outage-2534/. [Accessed: 06- Apr- 2017].
[83] J. M, C. A, and K. S, "Survey On Verification Of Storage Correctness In Cloud Computing," *Int. J. Eng. Comput. Sci.*, vol. 4, no. 9, pp. 14336–14340, 2015.
[84] "Data Deduplication - EMC Glossary", *Emc.com*, 2017. [Online]. Available: https://www.emc.com/corporate/glossary/data-deduplication.htm. [Accessed: 07- Apr- 2017].
[85] "Cloud encryption - client-side vs server-side", *Stackfield.com*, 2017. [Online]. Available: https://www.stackfield.com/blog/cloud-encryption---client-side-vs-server-side-1. [Accessed: 07- Apr- 2017].
[86]]D. Quick, B. Martini and K. Choo, *Cloud Storage Forensics*, 1st ed. Syngress, 2013, p. 143.
[87] Y. Elkhatib, "Defining Cross-Cloud Systems," pp. 1–4, 2016.
[88] W. Dou, X. Zhang, J. Liu and J. Chen, "HireSome-II: Towards Privacy-Aware Cross-Cloud Service Composition for Big Data Applications", *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 2, pp. 455-466, 2015.
[89] "What is software-defined networking (SDN)? - Definition from WhatIs.com", *SearchSDN*, 2017. [Online]. Available: http://searchsdn.techtarget.com/definition/software-defined-networking-SDN. [Accessed: 08- Apr- 2017].
[90] A. Greenberg, *SDN for the Cloud*, 1st ed. Microsoft, 2015, pp. 1-47.
[91] D. Raffo, "Hot data storage technology trends for 2017", *SearchStorage*, 2017. [Online]. Available: http://searchstorage.techtarget.com/feature/Hot-data-storage-technology-trends-for-2017. [Accessed: 08- Apr- 2017].
[92] R. Kennedy, "Hybrid cloud storage: Past, present and future", *Cloud computing news*, 2017. [Online]. Available: https://www.ibm.com/blogs/cloud-computing/2016/08/hybrid-cloud-storage-past-present-future/. [Accessed: 08- Apr- 2017].
[93] J. Chen, "The Evolution of Computing: AlphaGo", *Computing in Science & Engineering*, vol. 18, no. 4, pp. 4-7, 2016.
[94] D. Basile, "5 huge trends in big data and storage", *The Next Web*, 2017. [Online]. Available: https://thenextweb.com/insider/2016/04/01/5-big-data-storage-trends-watch/#.tnw_FA3yw6Rq. [Accessed: 08- Apr- 2017].
[95] P. Dholakiya, "Five key cloud trends to look forward to in 2017: Containers, AI, and more", *Cloud Tech News*, 2017. [Online]. Available: https://www.cloudcomputing-news.net/news/2017/feb/03/five-key-cloud-trends-look-forward-2017-containers-ai-and-more/. [Accessed: 08- Apr- 2017].
[96] D. Raffo, "Hot data storage technology trends for 2017", *SearchStorage*, 2017. [Online]. Available: http://searchstorage.techtarget.com/feature/Hot-data-storage-technology-trends-for-2017. [Accessed: 08- Apr- 2017].
[97] "What is cloud-to-cloud backup? - Definition from WhatIs.com", *WhatIs.com*, 2017. [Online]. Available: http://whatis.techtarget.com/definition/cloud-to-cloud-backup. [Accessed: 08- Apr- 2017].
[98] I. Orton, A. Alva, and B. Endicott-Popovsky, *Legal Process and Requirements for Cloud Forensic Investigations*. 2013.
[99] K. Thomas, "Microsoft Cloud Data Breach Heralds Things to Come," *PCWorld*, 2010. [Online]. Available: https://www.pcworld.com/article/214775/microsoft_cloud_data_breach_sign_of_future.html. [Accessed: 20-Dec-2017].
[100] D. Robb, "Top 10 AI and Machine Learning Data Storage Trends," Enteprise Storage Focum.com, 2017. [Online]. Available: http://www.enterprisestorageforum.com/storage-management/top-10-ai-and-machine-learning-data-storage-trends.html. [Accessed: 21-Dec-2017].