Comparison of Privacy-Preserving Models based on a Third-Party Auditor in Cloud Computing

[1]Mohamed Ben Haj Frej
Computer Science and Engineering Department
University of Bridgeport,CT, US
[1]mbenhaj@bridgeport.edu

[2]Julius Dichter[2]
Computer Science and Engineering Department
University of Bridgeport,CT, US
[2]dicher@bridgeport.edu

[3]Navarun Gupta
Electrical Engineering Department
University of Bridgeport,CT, US
[3]navarung@bridgeport.edu

Abstract: Cloud computing is emerging as a significant utility service with a focus on outsourcing the data for individual consumers as well as for organizations. It has drastically transformed the way consumers store and organize their private and confidential data. Despite significant advancements in the cloud computing technology, concerns about security and other cloud adoption issues, are holding consumers from fully trusting this promising technology. We discuss the involvement of a TPA, the security requirements, as well as the vulnerabilities that lead to security threats. We extensively analyze and classify the TPA's privacy preserving models into different categories with a focus on their dynamicity. Furthermore, we discuss the characteristics of each TPA model from the privacy-preserving perspective. Finally, we compared our proposed LAPP (Light-weight Accountable Privacy Preserving) with existing known privacy preserving model.

Keywords: Cloud Client (CC); Cloud computing; Cloud Service Provider (CSP); Security; Service Level Agreement (SLA); Privacy Preserving Model (PPM); Third-party auditor (TPA).

I. INTRODUCTION

Cloud computing is a utility-driven, based on "pay as you use," technology for remotely sharing the information technology resources rather than having local servers or personal devices handle applications [1-6]. Cloud computing is developing as a paradigm that aims to deliver dependable, personalized, with guaranteed quality of service, computation environment for the cloud clients. In cloud computing, and from the end user perspective, IT-related skills are provided as services, accessible without requiring in-depth knowledge of the underlying technologies, and with a nominal management effort. The term cloud refers to the storing of data anywhere and accessing it anytime. The stored data can be obtained by users who have adequate and required permissions. There are many characteristics associated with the cloud, as defined in [7]. Cloud computing supports four delivery models: public cloud, private cloud, community cloud, and hybrid cloud [8-12].

- The public cloud can be used for data that is not extremely sensitive and where the integrity of the data is subject to frequent changes.
- The private cloud can be used for data that is highly confidential and is made available only to a small number of users.
- A community cloud is a form of the public cloud where several customers share the same infrastructure with a community formed from other entities that share the same interest.
- The hybrid cloud is a combination of two or more clouds; they also apply to clients who want to keep their most critical data on-premise and deploy their essential data on the cloud. It can be private, community, or public but are bound together by standardized technology. The hybrid cloud offers enhanced security at a lower price but could end up with high management complexity [13].

Cloud computing integrates different technologies and strategies to protect clients' data. The cloud service providers compete on using the latest security schemes. Nonetheless, there are still many ambiguities, security-wise, that are making many companies skeptical from fully embracing the cloud realm [14]. In cloud computing safety, security and privacy of data are essential metrics which build the trust level of the clients. Cloud computing is vastly used in different domains (e.g., social, economic, industries, financial institutions, government offices, educational institutions). Thus, individuals store their confidential data through cloud computing. Hence, before adopting the design and development of cloud computing, security requirements and privacy should be thoroughly investigated. Many companies, as well as individuals, are still skeptical about cloud computing when considering the security vulnerabilities associated with it. There are still no specified privacy and security protection laws explicitly created for cloud computing [15-16]. Many researchers are focusing on identifying the security and privacy issues which can be faced by cloud computing clients. Another area of research explores how to select trustable and suitable cloud providers to minimize security and privacy risks. To handle security issues, particularly privacy issues, the concept of TPA is introduced. The TPA has the expertise and the capabilities that the CC's and CSP's do not possess. The TPA is trusted to assess the CSP's storage security upon request from both the CC and the CSP, so the data is immune from Byzantine failures, malicious data, data modification attack, and even server colluding attacks.

The main contributions of this comparison analysis paper could be summarized as follows:

- The state-of-the-art on privacy-preserving paradigms for cloud computing based on a TPA is discussed.

978-1-7281-3101-6/19/$31.00 ©2019 IEEE
DOI 10.1109/CloudSummit47114.2019.00020

- The CSP's vulnerabilities that provide a platform for a malicious TPA to use and generate the threats for data privacy are discussed.
- Simulations experiment on the four most eminent PPM compared to our previously introduced LAPP.

The remainder of the paper is summarized as follows: Section II discusses the cloud vulnerabilities. Section III presents TPA's comparison of security factors. Section IV discusses the simulation parameters and results. And Section V concludes the entire paper.

II. CLOUD VULNERABILITIES

The data on the cloud should be encrypted without leading to major processing overhead. Considering the benefits of cloud computing, various organizations leaning towards cloud-based IT solutions. However, before starting the journey to the cloud, adopters must consider the possible vulnerabilities depicted in Figure-1that may convert their dreams of enhancing scalability and saving management cost into a nightmare of either data loss and misuse [17]. Hence, users must consider the risks involved with cloud adoption. The cloud experiences the vulnerabilities (e.g., lack of trust, loss of control). As, these vulnerabilities greatly affect several security requirements such as privacy, authentication, authorization, accountability, privacy, confidentiality, integrity, non-repudiation, access control, and availability. Based on these vulnerabilities, different types of threats are possible such as re-entry, intoxication, Byzantine, colluding, discrimination threats.

A. Possible Threats to Cloud Computing

The threats on cloud result from various vulnerabilities in the security requirements depicted in Figure 1.

a) Collusion threat

Consists of a threat from malicious cloud users who use feedbacks to manipulate trust model results. It is called a Collusive malicious feedback attack [18]. It consists of three types:

- Self-Promoting: consists of promoting a Cloud service provider. Malicious cloud users enter significant positive feedback.
- Slandering: to defame a cloud service provider. Malicious cloud users enter Significant negative feedback.
- Occasional Collusion Feedback attack: in this case, the user occasionally enters significant positive or negative feedback.

b) Intoxication Attack

Malicious users behave alternatively in ethical or bad fashions [19]. In other words, the user first acts normal, but as time progresses, the user starts to misbehave after earning trust. These types of users are difficult to identify. This vulnerability is also called the dynamic personality of peers in the p2p network system. Uses a Forgetting factor technique to resolve this problem.

c) Discrimination Attacks

When a CSP delivers different qualities of services provided to CSU's, it could result in different ratings to these providers and impact their trust. Then the group who offered contradictory results might be labeled as dishonest. To date, there is no practical solution to mitigate such an attack.

d) Reentry threat

It consists of the case when the user who previously produced bad behavior reenters with a new identity to attack again [19]. It is called newcomer or reentry Attack. By comparing credential recodes using location, unique id, we can reduce reentry Attacks.

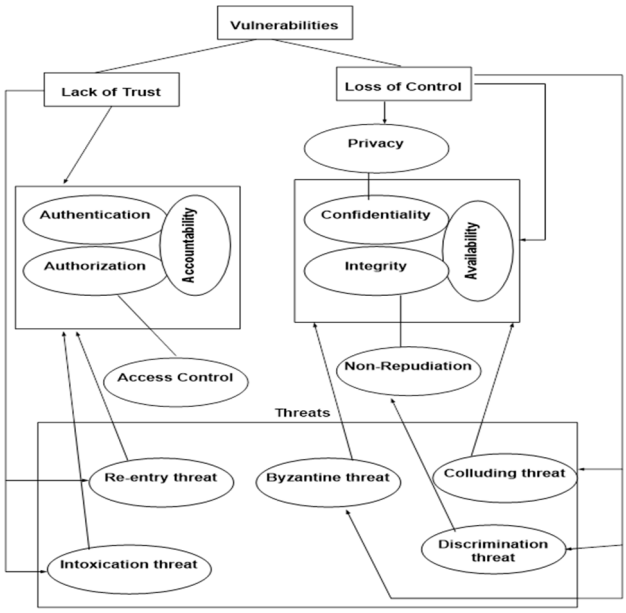

Figure 1: Security Requirements, Vulnerabilities, and Threats

III. TPA COMPARISON'S SECURITY FACTORS

Our study elaborated on the below factors in comparing the studied schemes depicted in Figure 2.

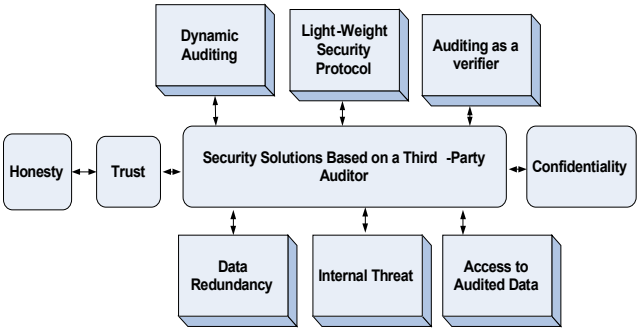

Figure 2: Security solutions based on TPA

a) Dynamic Auditing

Based on our study, dynamic auditing factors are given as

- RSA based storage security supports dynamic operation and identifies misbehaving servers in the cloud. However, TPA has control of the private keys (which is deemed unsafe).
- Privacy Negotiation Mechanism protects against Byzantine failures by dynamic auditing and server colluding attacks. However, it does not guarantee the privacy of the user's data.
- Privacy-preserving public auditing is highly efficient for dynamic groups, but it consumes more time and bandwidth to achieve high error detection probability.
- Third party storage audit service protects the privacy of the data, and it has less communication cost. In some cases, due to dynamic operations, which tend to make the auditing protocol insecure.

b) *Lightweight security*

- The novel third-party auditor scheme ensures data confidentiality using encryption techniques leading to secure authentication.
- Data Privacy by authenticating and secret sharing achieve mutual authentication between the client and the server. This method reduces the information cost in secret sharing.
- In the SCLPV technique, the malicious auditor cannot have much impact on security. Also, safety is guaranteed by the large verification overhead.

c) TPA acting as a verifier

- While protecting data privacy in the public cloud, the verifier is not trusted.
- In the Knox and Oruta approach, during the verification phase adversary may corrupt the data.
- A designated public verifier can significantly improve reliability, which leads to a reduction of the computational burden.

d) Adopting a TPA as Trust Party

- Public auditing mechanism reduces computation and communication overhead. Sometimes there can be a problem of internal attacks.
- While managing trust in TPA, security strength is effective. However, feedback from the cloud user is not supported.
- Data confidentiality is enhanced by utilizing the encryption scheme, also reducing the computational burden.
- Centralized trust model approach establishes a high-level of trust for cloud users, and updating changes are made easy. However, cloud user feedback cannot always be trusted.

e) Access to audited data

- TPA achieves better efficiency while performing multiple auditing tasks using a homomorphic non-linear authenticator and random masking technique. However, a local copy of the data can be present in the TPA.
- To maintain strong anonymity in a cloud environment, a data possession scheme can be used.
- During auditing, recovering the singleton losses is efficient by using the layered interleaving technique. However, the TPA should not get hold of the user's data content.

f) Data Redundancy

- In the PoOR scheme, the traffic cost is optimized. However, there is a problem with data duplication, which could lead to data redundancy.
- Centralized trust model approach significantly establishes the trust for cloud users and made updating changes easy. However, we cannot always trust cloud users' feedback cannot in this scheme.

IV. SIMULATIONS SETUP AND RESULTS

As detailed in our previous publication introducing LAPP [20], below is a recapitulation of the main simulation parameters given in table 1.

TABLE I: SIMULATION SETUP AND PARAMETER

Parameters	**Description**
Number of chassis switches at L4	1920
Line cards at L4	1630
Ports at L4	72
Number of racks at L4	16
Number of chassis switches at L3	432
Line cards at L3	164
Ports at L3	48
Number of racks at L3	128
Used virtual machines	1800
Number of Servers	64
Maximum number of Cloud Service Users	18000
Hosts in each rack	132
Each Host supports	16 processors
Memory with each processor	256 GB
Storage Memory	512 GB
Virtual Disk Memory	430 GB
Bandwidth for L4	256 GB/Sec
Bandwidth for L3	128 GB/Sec
Bandwidth for L2	64 GB/Sec
Bandwidth for L1	16 GB/Sec
Queue delay	0.005 Seconds
Burst time	0.0056 Seconds
Idle time	0.0032 Seconds
Packet Size	1260 KB

In this round of simulation experiments, we compared our introduced method LAPP to the below methods:

- Security and Privacy for Storage (SPS) [21].
- Panda Public Auditing (PPA)[22]
- Privacy-Preserving Public Auditing (PPPAS) [23]
- Secure and Efficient Privacy-Preserving Public Auditing (SEPPPA) Protocol [24].

Our experiments were conducted using Greencloud platform. The experiments have been obtained based on the malicious attempts at the following rates: 0%, 1%, 2%, and 5%, and for the sake of simplicity we are only presenting the graphs with 0% and 2% malicious activities. We have conducted the following experiments:

- The processing time versus the volume of data
- The average auditing time of each service user versus the number of clients in the system.

A. The processing time versus the volume of data

Figures 3 and 4 illustrate the change in the needed processing time versus the volume of data that has been processed with no malicious attempts in figure 3 and 2% in figure 4; adding 5 MB of data at a time. The simulation results show that LAPP requires less processing time than the method it has been compared against, as we progress in time.

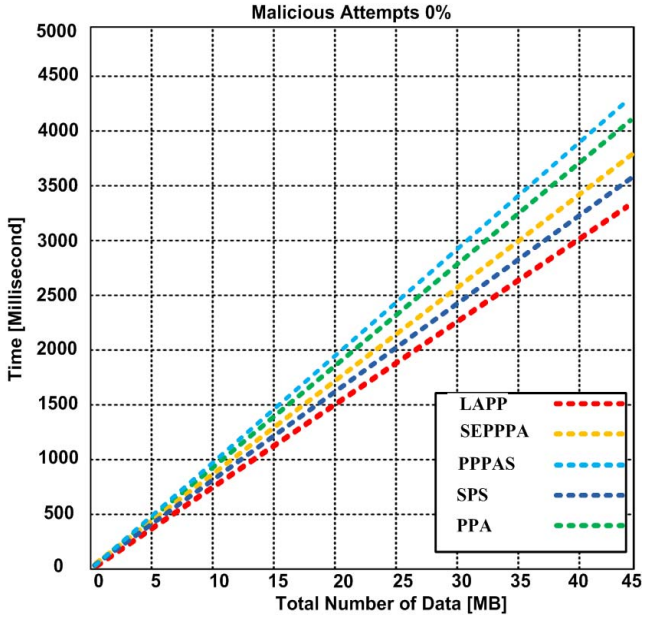

Figure 3: Time versus Total Number of Data (0% Attempts)

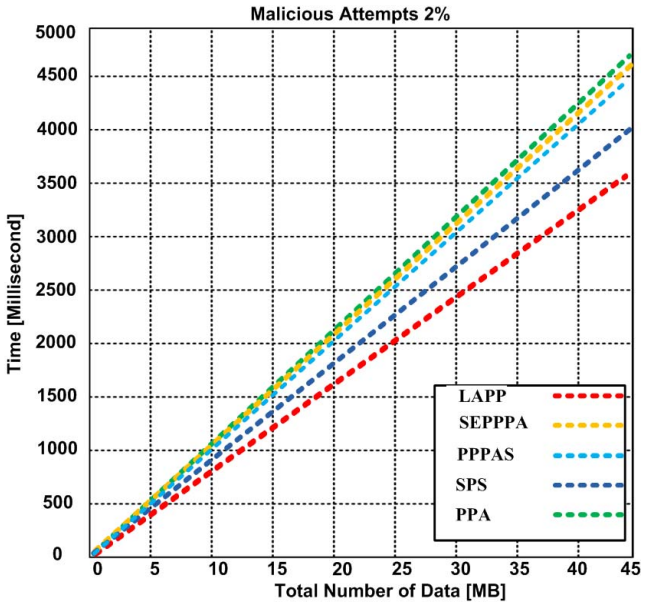

Figure 4: Time versus Total Number of Data (2% Attempts)

B. *The average auditing time versus the number of clients*

Figures 5 and 6 illustrate the advancement in the average auditing time for each CC versus the number of the CCs in the system, with no malicious attempts in figure 5, and 2% in figure6; adding 2000 CCs at a time. The simulation results show that a drop in the average auditing time when we have 8000 users then kept around the same average while increasing the number of users up to18000 showing superiority to the other methods it has been compared to.

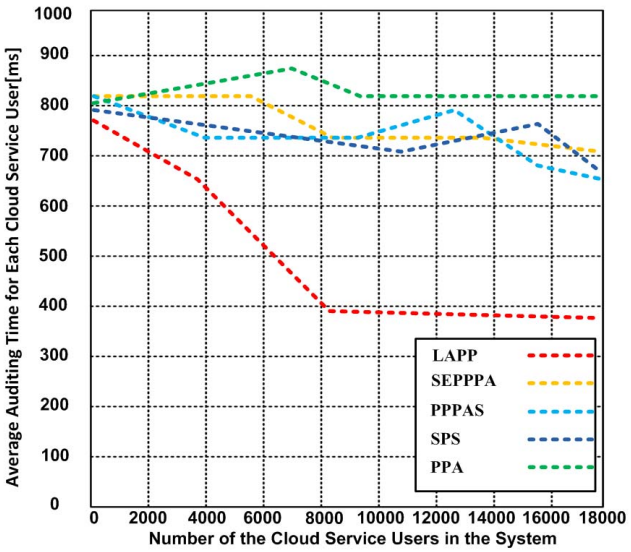

Figure 5: Average Auditing Time V. the Number of CCs (0% Attempts)

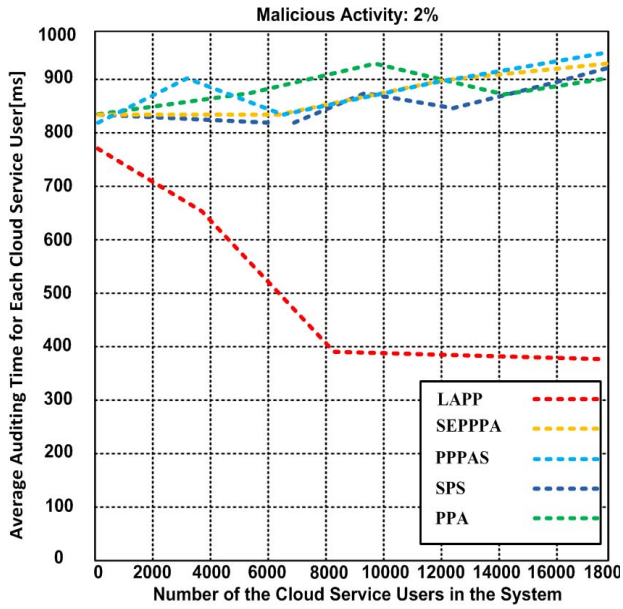

Figure 6: Average Auditing Time Vs. the Number of CCs (2% Attempts)

VI. CONCLUSION

In this paper, we have recapitulated and compared the state of the art of the existing PPM methods and studied cloud security when having to benefit from the services of a Third-Party Auditor (TPA). The TPA's role in cloud computing is to assure the auditing function on behalf of the client and to establish a secure connection for the sake of achieving the integrity of the data. Nonetheless, there are some issues mainly related to trust that could emerge from involving a TPA. Many research approaches addressing security using a TPA and proposing solutions have been elaborated.

To pursue this goal, we have studied the most recent TPA-based approaches, classified them based on their adopted security methods using mind-map; and recapitulated these methods based the security requirements. The comparison analysis starts with the vulnerabilities of the CC that are discussed and provide the different scenarios for the TPA to use and generate threats on the CC's data privacy. The study reveals the major impact brought in by the TPA's adoption in securing cloud computing. This option comes with its concerns, as adopting a solution with a TPA can come with trust concerns, extra overhead, security, and data manipulation breaches. The privacy-preserving models are classified and categorized, focusing only on the dynamicity of the TPA. Furthermore, the limitations of each privacy preserving model are extensively discussed, concluding with suggested recommendations for future improvement. Based on the comparison analysis, we recommend to researchers to plan and orient their efforts towards developing a more simplistic lightweight, and secure solution compared to our proposed method LAPP that should help alleviate the gap in the cloud users' decision compromise and to increase the trust in adopting a solution based on a TPA.

REFERENCES

[1] Razaque, A. and S.S. Rizvi, Privacy preserving model: a new scheme for auditing cloud stakeholders. Journal of Cloud Computing, 2017. 6(1): p. 7.

[2] Zhang, Qi, Lu Cheng, and Raouf Boutaba. "Cloud computing: state-of-the-art and research challenges." Journal of internet services and applications 1, no. 1 (2010): 7-18.

[3] Marston, Sean, Zhi Li, Subhajyoti Bandyopadhyay, Juheng Zhang, and Anand Ghalsasi. "Cloud computing—The business perspective." Decision support systems 51, no. 1 (2011): 176-189.

[4] Krutz, Ronald L., and Russell Dean Vines. Cloud security: A comprehensive guide to secure cloud computing. Wiley Publishing, 2010.

[5] Feng, Deng-Guo, Min Zhang, Yan Zhang, and Zhen Xu. "Study on cloud computing security." Journal of software 22, no. 1 (2011): 71-83.

[6] Jadeja, Yashpalsinh, and Kirit Modi. "Cloud computing-concepts, architecture, and challenges." In Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on, pp. 877-880. IEEE, 2012.

[7] Akbari, Elham, Francis Cung, Hardik Patel, Abdul Razaque, and Hemin Nilesh Dalal. "Incorporation of weighted linear prediction technique and M/M/1 Queuing Theory for improving energy efficiency of Cloud computing datacenters." In 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT), pp. 1-5. IEEE, 2016.

[8] Mell, P. and T. Grance, The NIST definition of cloud computing. 2011.

[9] Wang, Q., et al., Enabling public auditability and data dynamics for storage security in cloud computing. Parallel and Distributed Systems, IEEE Transactions on, 2011. 22(5): p. 847-859.

[10] Xiao, Z. and Y. Xiao, Security and privacy in cloud computing. Communications Surveys & Tutorials, IEEE, 2013. 15(2): p. 843-859.

[11] Razaque, Abdul, Nikhileshwara Reddy Vennapusa, Nisargkumar Soni, and Guna Sree Janapati. "Task scheduling in cloud computing." In 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT), pp. 1-5. IEEE, 2016.

[12] Rizvi, S., A. Razaque, and K. Cover. Cloud Data Integrity Using a Designated Public Verifier. in High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), 2015 IEEE 12th International Conferen on Embedded Software and Systems (ICESS), 2015 IEEE 17th International Conference on. 2015. IEEE.

[13] Subashini, S. and V. Kavitha, A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 2011. 34(1): p. 1-11.

[14] Das, P., H. Classen, and R. Davé, Cyber-Security threats and privacy controls for cloud computing, emphasizing software as a service. The Computer & Internet Lawyer, 2013. 30: p. 20-24.

[15] Razaque, Abdul, Saty Siva Varma Nadimpalli, Suharsha Vommina, Dinesh Kumar Atukuri, Dammannagari Nayani Reddy, Poojitha Anne, Divya Vegi, and Vamsee Sai Malllapu. "Secure data sharing in multi-clouds." In 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pp. 1909-1913. IEEE, 2016.

[16] Martucci, L.A., et al. Privacy, security and trust in cloud computing: the perspective of the telecommunication industry. in Ubiquitous Intelligence & Computing and 9th International Conference on Autonomic & Trusted Computing (UIC/ATC), 2012 9th International Conference on. 2012. IEEE.

[17] Popović, K. and Ž. Hocenski. Cloud computing security issues and challenges. in Proceedings of the 33rd International Convention. IEEExplore, Opatija. 2010.

[18]Noor, T.H., et al., CloudArmor: Supporting reputation-based trust management for cloud services. IEEE transactions on parallel and distributed systems, 2016. 27(2): p. 367-380.
[19]Sun, Y.L., et al. A Trust Evaluation Framework in Distributed Networks: Vulnerability Analysis and Defense Against Attacks. in INFOCOM. 2006.
[20]Frej, Mohamed Ben Haj, Julius Dichter, and Navarun Gupta. "Light-weight accountable privacy preserving (LAPP) protocol to determine dishonest role of third party auditor in cloud auditing." In 2018 IEEE International Conference on Consumer Electronics (ICCE), pp. 1-6. IEEE, 2018.
[21] Wei, L., et al., Security and privacy for storage and computation in cloud computing. Information Sciences, 2014. 258: p. 371-386.
[22]Wang, Boyang, Baochun Li, and Hui Li. "Panda: Public auditing for shared data with efficient user revocation in the cloud." IEEE Transactions on services computing 8, no. 1 (2013): 92-106.
[23]Wang Cong, Sherman SM Chow, Qian Wang, Kui Ren, Wenjing Lou, "Privacy-preserving public auditing for secure cloud storage", IEEE transactions on computers, vol. 62, no. 2, pp. 362-375, 2013.
[24]Worku, S.G., et al., Secure and efficient privacy-preserving public auditing scheme for cloud storage. Computers & Electrical Engineering, 2014. 40(5): p. 1703-1713.