Cloud Data Security using Auditing Scheme

Anuj Kumar Yadav
DIT University
Dehradun, Uttarakhand

M. L. Garg, PhD
DIT UNIVERSITY
Dehradun Uttarakhand

Ritika, PhD
DIT UNIVERSITY
Dehradun , Uttarakhand

ABSTRACT
Cloud computing has emerged as one of the latest computing paradigm and is a growing technology for upcoming years. According to NIST Cloud computing is a model for convenient, on-demand network access to a large pool of computing resources. Resource can be hardware or software resource and this pool of resources can be rapidly provisioned and released with minimum management effort or cloud service provider interaction [1].

In Cloud computing, different types of data and program can be stored at different locations, the cloud data centers and can be accessed whenever required, from anywhere, via different type of devices having internet connection. Due to this method of storing user's data at cloud provider's end, users gets numerous benefits such as, access flexibility, large storage capability, and resilience. In Cloud computing vendor supplies the hardware infrastructure, and the software interacts with the user through a front-end portal [2][3].

One of the service provided by the Cloud computing is Cloud storage, in which user information and data is stored, managed, backed up on multiple locations as a replica and made available to users via interconnection network. Apart from all benefits and advantages there are some concerns as well related to cloud computing, as in cloud computing data is put outside the control of the end user on a location that is unknown to the user. Due to this, Cloud computing also raises to various security issues. [4] End user is concerned about the integrity of data that is stored in cloud, as user's data can be modified by attackers or even in some cases due to employee espionage.

The cloud server is just used to save the encrypted blocks of data for the user. By using the auditing approach processing overhead of cloud server and verifying authority can be largely reduced. Cryptography is an effective technique that helps to assure user's data accuracy. The Cryptographic techniques can be used in cloud to protect the data from attackers. In this paper, the significance of cryptography is discussed by which possibility of attacks on cloud data can be reduced. This paper covers some of the existing cryptographic methods that ensure the security of cloud data. In this paper auditing scheme is presented using cryptographic techniques and by using the auditing scheme based on the cryptography user data becomes more secure, that leads to enhancement of trust between the end user and cloud provider. Cloud data auditing is necessary for securing data in cloud storage since it facilitates cloud users to verify the integrity of their outsourced data effectively and efficiently.

Keywords
Cloud Server, IaaS, PaaS, SaaS, TPA .

1. INTRODUCTION
Cloud computing is gaining attention nowadays due to its benefits. It is a growing technology in which large volume of data is distributed and stored at different physical locations. Cloud computing has become a revolution in information and communication technology world due to its innovative and promising vision. In clod computing possibilities are generally unlimited and different types of services made available to the end users at a nominal price [17] .

Among all the services provided by the cloud computing one of the service is cloud storage, which provides unlimited storage to cloud users. Apart from the storage capacity there are some other advantages of cloud storage as well. Some benefits of cloud storage can be listed as:

- It provides cost effective solution to the user as there is no need to invest heavily in hardware purchase
- Reduce the user's overhead to maintain and manage the storage space
- It provides the data accessibility remotely irrespective of the geographical location
- Scalability is another feature

According to the recent survey around 80% of the organizations prefer to choose the It outsourcing [18].

User can save both money and time by making use of Cloud computing services. Cloud computing provides different resources and applications to the end user with the help of internet [19].

Apart from this there are various advantages of Computing; some of them can be listed as

Data portability: With the help of Cloud Computing user can access the data from any physical location with the help of internet.

Numerous Storage Capacity: Cloud Computing provides the users almost unlimited storage capacity.

Reliability: Hardware or software failures are the responsibility of cloud service providers, hence Cloud computing provides better reliability

Data sharing: Data can be shared easily among the trusted parties

So due to its various benefits as discussed, we can say Cloud computing is quite promising for its end users. Apart from all the benefits there are various concern and issues that might compromise data Integrity, availability and confidentiality. This can happen due to various internal and external security attacks, which exploits the weakness of security system and harm the user's data.

So we can say security is one of the biggest concern and is a barrier in the way of Cloud adoption. Apart from security some other issues in adoption of Cloud computing can be privacy of data, end user's trust on cloud service provider and some other factors [20].

So the major goal is to enhance the security and integrity of user's data stored at remote locations due to critical nature of Cloud computing and numerous amount of data contained by Cloud storage. But to provide security to the cloud data and maintain integrity of the user's data is an uphill task. One of the possible solution to such problems can be by using remote data auditing which can be implemented using available cryptographic technique, that can be adopted, such that information leakage and privacy of user get maintained.

The Third party auditor is much more expert than the end user and Third party auditor can time to time check the integrity of user's data by which user can get benefitted and also improves the user's trust in cloud computing. Apart from helping the users, the results achieved by third party auditor, also provides input to cloud service providers so that they can improve their services. We can say auditing service can play a vital role by which both the end user and cloud service provider get benefitted [21]. In this paper, auditing scheme is discussed by which user can trust on cloud computing based services.

2. PAPER ORGANIZATION

The rest of the paper is organized as follows. In Section 3, extensive literature survey has been done. In Section 4, various gaps are discussed regarding literature review which needs to be solved. In Section 5, Third party auditing scheme is discussed. We conclude the paper in Section6.

3. LITERATURE REVIEW

The work carried out by the following researchers in the area of proposed research has been reviewed as under: -

3.1 Lifei Wei et all," Security and privacy for storage and computation in cloud computing ", Elsevier [2014].

Cloud computing is growing as the latest computing paradigm whose aim is to provide cost effective, customized, reliable and guaranteed quality of service working environments for cloud users. In Cloud Computing user data and applications are placed at large centralized data centers, known as Cloud. Due to global replication and migration, resource virtualization, the physical absence of machine and data in cloud, cloud data and the evaluated results may not be well managed and completely trusted by the cloud users. Almost all the previous work on the cloud computing security aims on the storage security rather than considering the computation security together with storage security [5].

3.2 An Na Kang et all," A strengthening plan for enterprise information security based on cloud computing", springer [2013]".

Large number of security threats and security accidents are reporting in cloud computing paradigm nowadays. Most of the countries are promoting security policies for cloud computing in order to counter various threats and security accidents. For example, USA, make announcement of the imposition of cloud computing security policy and guidelines which helps in information protection. NIST (National Institute of Standards and Technology) was in charge of cloud computing security strategy for the federal government of the USA. NIST was responsible for providing technical support that is required for applying cloud based system to federal government, such as standard development of security of data, interoperability, and mobility of data. United Kingdom government announced some plans for governmental cloud computing and some frameworks for information protection. Japan has been actively researching on different ways to provide cloud data security and have raised awareness of the importance of security in cloud computing by announcing the execution plan for Smart Ubiquitous Networks and guidelines to data protection for cloud service [6].

3.3 Mark D. Ryan," Cloud computing security: The scientific challenge, and a survey of solutions", Elsevier [2013].

Cloud computing security comprises all the topics the of computing security, including the designing of security based architectures, reduction of attack surfaces, protection from various malware, and enforcement of access control mechanism. But some aspects of cloud computing security appear to be specific to that particular domain

1. The cloud is generally a collection of shared resources, and some of these sharers (called tenants) may be attackers.
2. Cloud based data is generally accessed through potentially APIs and insecure protocols across various public networks.
3. Data stored in the cloud storage is vulnerable to being lost (e.g., accidentally deleted) or incorrectly modified by the cloud handler.
4. Data in the cloud is widely accessible by the cloud service provider and its employees.

From these mentioned problems 1 to 3 are solved but there are no such methods that provides solution to the 4th problem. It is open problem and one of the biggest challenge to achieve in cloud computing [4].

3.4 Cindhamani.J et all," An enhanced data security and trust management enabled framework for cloud computing systems, IEEE [2014].

In past generation people use to store their useful data in their own hard disc, but nowadays a Cloud computing also provides that feature. Cloud computing is an internet based development in the 20th century. Cloud computing provides large amount of services in which users can access their data from anywhere at any time from all around the network. Cloud is used for various business applications, it mainly provides the platform as a service, infrastructure as a service and software as a service. People are mainly attracted to the Cloud computing because it provides resources on demand. Cloud storage service provides automated storage, purveying, and simple reporting. It also improves the overall efficiency with high quality. Trusted third parties are used in cloud environment where the information is stored on behalf of other entity. Trust third parties do not ensure the security factors like integrity, confidentiality, identification [7].

3.5 Kaiping Xue et all," A Dynamic Secure Group Sharing Framework in Public Cloud Computing" ,IEEE [2014].

In the last decade the demand of outsourcing data has increased at large extent. To fulfill the requirement for data storage and large scale computation with high performance, many cloud computing service providers have worked and provide solution in their own way, such as Amazon Simple Storage Service (Amazon S3), Google Drive, Microsoft One Drive, Dropbox and many more. There are mainly two advantages of storing the data in Cloud data servers: 1) With the help of Cloud storage end user need not to worry about the trouble of buying extra cloud storage servers and hiring server

maintenance and management engineers 2) Data sharing becomes easy for the data owner, as the data can be share within a single link among the recipients.

Apart from the various advantages as discussed about cloud storage, there are some challenging obstacles as well while adopting cloud storage method, among which, the security and privacy of user's critical data remains two major issues. Mostly, the data owners use trusted servers to store their data, and these trusted servers are controlled by fully trusted administrator. However, the cloud is basically managed and maintained by a semi-trusted third party. Due to this, traditional security mechanism for storage technologies can't directly applied in the case of cloud storage. As data owner share their data with multiple users in cloud computing, it poses an even more difficult problem to cloud data owner since data owner must make sure that apart from the intended recipients and cloud service provider no one can gain access to cloud data. [8].

3.6 Meng Liu et all," A Decentralized Cloud Firewall Framework with Resources Provisioning Cost Optimization" ,IEEE [2015].

Cloud computing is gaining popularity as the upcoming infrastructure of computing platform in the field of Information Technology.

With numerous hardware and software based resource pooling and delivery of information and data on demand, cloud computing gives rapid elasticity to its end users. Cloud computing have service-oriented architecture, in which cloud services are broadly categorized in three forms: as-Software as a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure -as-a-Service (IaaS) [9][10] .

Irrespective of the promising model and in talks everywhere about its features, data security becomes the barrier in the way of cloud computing, due to which most of the users hesitate to move their existing applications to clouds.

Security and privacy are the major issues due to these people hesitate to move their applications to cloud. Traditional attacks such as Distributed Denial of Service, viruses, worms and phishing attacks still exist in clouds. On the other hand, some new attacks arises day by day and becomes a headache to the security experts, these attacks are Economic Denial of Sustainability (EDoS) attack [11], cross Virtual Machine (VM) attack, and many more attacks.

3.7 Nektarios Georgios Tsoutsos et all," The HEROIC Framework: Encrypted Computation Without Shared Keys", IEEE [2015].

Due to availability and affordability of Cloud computing services nowadays, the option of outsourcing computationally demanding applications is very encouraging. The advantages of performing computation in the cloud computing environment generally includes large scalability, negligible upgrade or maintenance cost, and pay-as-per use service options. Unfortunately, these advantages are sometimes outweighed by users concerns about data security and privacy in the cloud environment, and other threats that are associated with Cloud computing [12].

Apart from this at the infrastructure end, the known exploitation of hypervisor technologies keeps increasing. With reference to the privately maintained datacenters, where many access controls ensure the security and privacy of the data and executed applications, in a cloud setting users are asked to trust a third party with full control on their sensitive information. This can only be possible if user trust the cloud service provider on the basis of its previous track record regarding security. If the user is not fully sure about this, then user can refuse to store or send the sensitive information in the cloud. So, on the basis of discussed points many security techniques need to be worked out so that trust improves between the end user and Cloud service provider [13].

3.8 Nektarios Georgios Tsoutsos et all," An analysis of security issues for cloud computing" Springer [2013].

Cloud computing is a cost effective, flexible, and proven service delivery platform for providing services or business over the internet. With the time importance of Cloud computing is increased at a greater pace and it becomes very popular in the scientific and industrial organizations. Cloud computing is nowadays in consideration as one of the topmost technologies and with a better prospect in successive years by different organizations.

Cloud computing provides ubiquitous, easy, on demand network access to a large pool of shared resources (these configurable resources can be services, servers, storage, applications, and networks). All of these resources can be rapidly provisioned whenever required and these resources can also be released with minimum of management effort or cloud service provider interaction [12].

As discussed there are so many benefits of using Cloud computing, but there are also some significant barriers to adoption. One of the major barrier to adoption of cloud is security, followed by several issues regarding legal matters, privacy and compliance [14], because Cloud computing a new computing model, so the security achievement is quite challenging and how security techniques can be applied to cloud computing. With all the issues taken into consideration it is quite difficult to ensure security in cloud computing and this becomes a major concern for information executives.

3.9 Jin He et all," NetSecCC: A scalable and fault-tolerant architecture for cloud computing security" Springer [2014].

Cloud computing is influential computing paradigms in recent years, due to this cloud computing not only reduces capital expenditures, but it also improves computational efficiency to a great extent, and due to such benefits, it successfully attracts extensive attentions everywhere. Due to this, cloud computing is widely accepted and currently used in different IT services whether it is utility computing, load distributing, service oriented computing, parallel computing and many more computing paradigms.

But beside all the good features to provide network security using virtual machine based cloud computing remains a widely open challenge. Due to rapid development of cloud computing this challenge needs to be solved. Although few solutions still exist, but they do not provide complete protection. Unless network security in cloud computing is properly imposed and ensures, all cloud computing based services are prone to a high risk of attacks [15].

3.10 Rajkumar Buyya ,"Introduction to the IEEE Transactions on Cloud Computing",IEEE[2013].

Cloud computing is rapidly growing computing paradigm that promise to turn the vision of "computing utilities" into reality. Cloud computing started with a no risk concept: In which IT infrastructure is set up by someone and end user use it and pay according to shat end user uses. The service that offer various computing resources is known as Infrastructure as a Service (IaaS) and various application software's are offered as Software as a Service (SaaS). An operating environment that is used for designing, deploying and testing of applications is called PaaS (Platform as a Service). Various business organizations are adopting public Cloud services to save their capital expenditure and operational costs by opting for Cloud computing as it has features like elastic scalability and market-oriented costing. But apart from all these benefits public Cloud computing also have limitations like data security, data transfer security, performance issues, and level of control [16].

4. EXISTING GAPS IN THE LITERATURE

With the help of Cloud computing services, application potential of companies has increases. In other words, companies can outsource surplus parts of their IT infrastructure for Cloud computing, and the maintenance and servicing of these systems may be carried out by the Cloud provider. This will reduce the financial burden on the companies.

However, the biggest challenge is the building of trust between the end user and cloud service provider. End user may think that he has no control over his/her data that is saved somewhere else in the cloud data center. If this information is made available to the end users, then security mechanisms may be employed from user side to secure the data.

As observed in literature review, most of the security related problems deals with the stationary cloud data, but security for the data in transit has not been discussed in the reviewed literature. Also in some of the cases weaknesses of virtualization can expose cloud computing atmosphere to numerous security attacks and threats such as Information leakage from committing information, service breakage due to sharing and centralizing resources. Apart from this here is no such method that can control the attack if an attacker takes control over the hypervisor. As discussed at present there are not many techniques available to show, where the user's data reside in the cloud.

By taking these issues into consideration in the upcoming section third party auditing scheme is discussed, using which the trust between the end user and cloud service provider got strengthen. In the third party auditing scheme security is enhanced using different types of available cryptographic techniques, due to which the trust factor between the users and cloud service provide will improve.

5. TPA AUDITING SCHEME

To secure data in the cloud storage, a mechanism called Data auditing is introduced. Data auditing is used to verify the user data which can be carried either by the user or by a third-party auditor. Data auditing also helps to maintain the data integrity in cloud storage systems. Auditing authority roles can be classified in two ways

1) Private auditability, in which only end user and auditor is permitted to check the integrity of the data that is stored in cloud, but by applying this scheme user's overhead got increased due to verification process.

2) Public auditability, in which anyone can challenge the server and performs data verification check by taking the help of auditor [22].

5.1 Solution using TPA scheme

Given Fig 1 shows the auditing model provides data integrity checking on the basis of identity-based auditing mechanism. In the model four entities are involved.

1) End user who wish to store large amount of data on cloud server, user can be an individual or enterprise.

2) A cloud server that provides almost unlimited amount of storage space to users.

3) A third party auditor (TPA) who is expert in providing security and auditing to user's data, and also ensures the integrity of data.

4) A key generator (KG) that generates keys for different users by using the user's identity information [17].

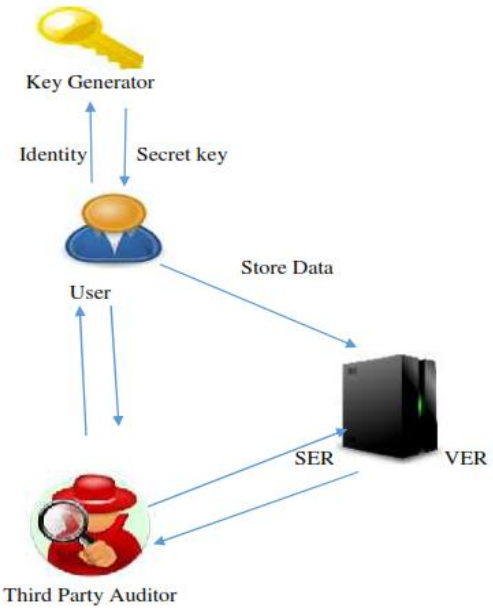

Fig 1: auditing model provides data integrity

By using the auditing scheme end user gets several benefits like confidentiality, integrity, storage correctness. Auditing can be done periodically or whenever required by the user.

Auditing schemes are developed to verify the correctness or integrity of cloud data with the help of third party auditor [17].

The proposed auditing scheme consists of three entities which works in cooperation with each other to provide security to the data, these are cloud server, end user and third party auditor. Roles of each entity are well defined.

1. End user is responsible for organising the data in the form of blocks, encrypting the data blocks using AES, generating hash value for each of the block using SHA 2 algorithm, concatenating these generated secure blocks and finally applying digital signature on data. Data blocks can also be saved on the basis of sensitivity of data. Sensitive data blocks can be clubbed in one group and can be organised separately. These secured sensitive blocks need more attention, so these blocks can be audited frequently by the third party auditor, also cloud server can use enhanced security schemes to save these blocks of data.

2. Cloud server is responsible for storing encrypted blocks of data send by the user. Cloud server can provide enhanced security to the sensitive blocks of data.

3. Third entity is the third party auditor. Whenever a client request for auditing of data, third party auditor request the desired blocks of data from cloud server and checks the blocks for integrity purpose by verifying the hash values. Same hashing algorithm is used by the auditor; which client use for auditing. After generating the hash value for the encrypted blocks of data, auditor generates digital signature on data blocks. For digital signatures RSA scheme can be used.

During verification signatures kept by auditor which was generated by the client, and one generated on the data received from cloud server are matched. If both the signature matches, it means data is not modified by any user or attacker. If signature does not match, then data considered to be tempered or affected by attack. All these result or data integrity checks are provided to the end user or data owner. Fig 2 given below is showing the proposed scheme workflow.

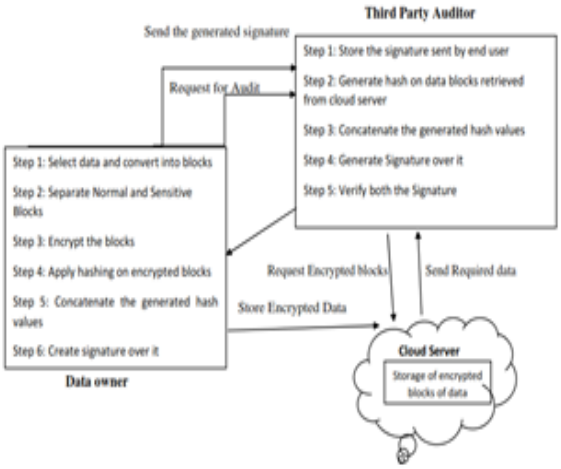

Fig 2: Proposed Scheme for security

In the auditing scheme Data owner plays a vital role and is most responsible related to data. Data owner needs to register with the cloud server and auditor in the proposed auditing scheme, to use the services, the data owner first performs login and registration with cloud server and the auditor, for which user first need to register to become active member. When user successfully logged in data owner selects the files to be stored in cloud server. All these must be splitted and encrypted before applying hashing to them. All these steps make the system more secure. All the encrypted blocks sent to cloud server for storage purpose. And hashed data is made more secure using RSA signature, and this data is send to third party auditor. Given figure 3 shows the working of a data owner.

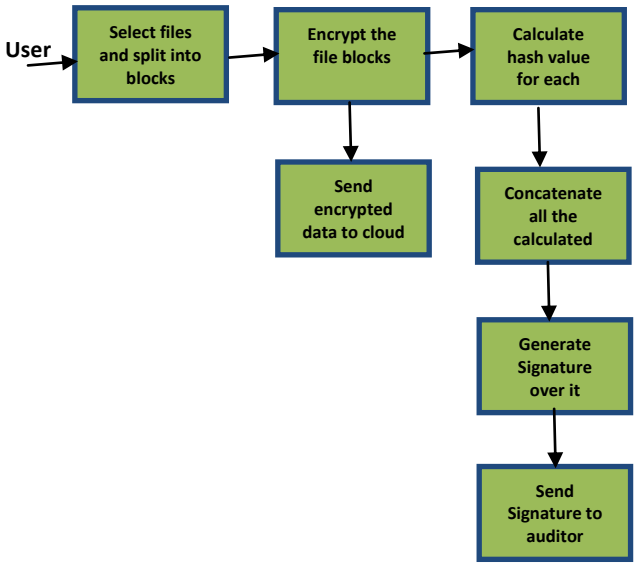

Fig 3: working of data owner

Second most important role in the scheme is played by the auditor. Auditor audits the user data either on the request of owner or it can randomly check the sensitive data for its integrity. When a client request for the data auditing, auditor starts the auditing process, as the auditor stores the owner signature, auditor again calculate the signature values on the data received from the cloud server and if both values match, it verify that data is not modified at cloud server. After all the process of verification, results are provided to the end user.

6. CONCLUSION AND FUTURE SCOPE

In this paper, the third-party auditing scheme is discussed which provides data integrity by which sensitive data get better security. Various cryptographic techniques are used by the end user or data owner, and third party auditor to enhance the level of security. The cryptographic techniques help to address cloud data security issues. Also, in the proposed scheme sensitive data is separated from the normal data and continuous monitoring via auditor can make such data more secure. Thus, the data can be securely shared with the authorized users by adopting the cryptographic techniques. In the current scheme, only data integrity can be ensured, but in future some enhancement can be done using which user can perform dynamic operations such as updating, deletion, insertion.

7. REFERENCES

[1] Mell, Peter, and Timothy Grance. "The NIST definition of cloud computing (draft).", NIST special publication 800.145 (2011).

[2] Zhang, L.-J., Zhou, " CCOA: cloud computing open architecture.",In: 2009 IEEE International Conference on Web Services (2009), pp. 607–616.

[3] Ye Du , Ruhui Zhang , Meihong L, "Research on a security mechanism for cloud computing basedon virtualization", Springer Science+Business Media New York (2013) ,pp 19-24.

[4] Mark D. Ryan, " Cloud computing security: The scientific challenge, and a survey of solutions", Elsevier, The journal of system and software (2013) ,pp 2263-2268.

[5] Lifei Wei, Haojin Zhu,, Zhenfu Cao,, Xiaolei Dong,, Weiwei Jia, Athanasios V. Vasilakos," Security and privacy for storage and computation in cloud computing ", Elsevier,Information Sciences (2014) ,pp 371-386.

[6] An Na Kang , Leonard Barolli ,Jong Hyuk Park ,Young-Sik Jeon," A strengthening plan for enterprise information security based on cloud computing ",Springer Science+Business Media (2013) ,pp 703-710.

[7] Cindhamani.J, Naguboynia Punya, Rasha Ealaruvi, L.D. Dhinesh babu ," An enhanced data security and trust management enabled framework for cloud computing systems", 5th ICCCNT – 2014 July 11-13, 2014, Hefei, China, IEEE(2014)

[8] Kaiping Xue, Peilin Hong ," A Dynamic Secure Group Sharing Framework in Public Cloud Computing" , IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 2, NO. 4, OCTOBER DECEMBER (2014) ,pp 459-470. 11

[9] Meng Liu, Wanchun Dou, Shui Yu, Zhensheng Zhang, "A Decentralized Cloud Firewall Framework with Resources Provisioning Cost Optimization", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 26, NO. 3, MARCH (2015),pp 621-631.

[10] M.Armbrust,A.Fox,R.Griffith,A.D.Joseph,R.Katz,A.Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M.Zaharia, "A view of cloud computing," Commun. ACM (2010), vol. 53, no. 4, pp. 50–58.

[11] C. Hoff.," Cloud computing security: From ddos attack (distributed denial of service) to edos (economic denial of sustainability)" [Online]. Available: http://www.rationalsurvivability.com/blog/?p=66(2008)

[12] Nektarios Georgios Tsoutsos, , Michail Maniatakos, "The HEROIC Framework: Encrypted Computation Without Shared Keys", IEEE TRANSACTIONS ON COMPUTER-AIDED DESIGN OF INTEGRATED CIRCUITS AND SYSTEMS, VOL. 34, NO. 6, JUNE (2015),pp 875-888.

[13] IBM Security Solutions, "2010 Mid-year trend and risk report,".http://www-05.ibm.com/fr/pdf/IBM_X-Force2010_Mid-Year_Trend_and_Risk_Report.pdf (Aug. 2010).

[14] KPMG's 2010 Cloud Computing survey. http://www.techrepublic.com/whitepapers/fromhype- to-futurekpmgs-2010-cloud-computing-survey/2384291.

[15] Jin He , Mianxiong Dong , Kaoru Ota , Minyu Fan Guangwei Wang," NetSecCC: A scalable and fault-tolerant architecture for cloud computing security", Springer Science+Business Media New York,(2014).

[16] Rajkumar Buyya ,"Introduction to the IEEE Transactions on Cloud Computing", IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 1, NO. 1, JANUARY-JUNE (2013),pp 3-21.

[17] Yong yu,Liang Xue,Man Ho Au,Willy Susilo, Jianbing Ni,Yafang Zhang,Athanasios V. Vasilakos,Jian Shen," Cloud data integrity checking with an identity-based auditing mechanism from RSA", Elsevier, Future generation Computing systems (2016) .

[18] M. Xie, H. Wang, J. Yin, X. Meng, "Integrity auditing of outsourced data, in: Proceeding of VLDB'07", University of Vienna, Austria, (2007), pp. 782–793.

[19] Zissis, Dimitrios, Dimitrios Lekkas" Addressing cloud computing security issues", Future Generation computer systems ,March (2012),pp. 583-592.

[20] Swapnali More,Sangita Chaudhari," Third Party Public Auditing scheme for Cloud Storage", 7th International Conference on Communication, Computing and Virtualization, Procedia Computer Science ,2016 , pp 69 – 76.

[21] Cong Wang, Member, Sherman S.M. Chow, Qian Wang, Kui Ren, Wenjing Lou, "Privacy Preserving Public Auditing for Secure Cloud Storage", IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 2, FEBRUARY (2013).

[22] Cong Wang, Sherman SM Chow, Qian Wang, Kui Ren, and Wenjing Lou. Privacy Preserving Public Auditing for Secure Cloud Storage. http://eprint.iacr.org/2009/579.pdf