Secure Cloud Computing with Third Party Auditing: A Survey

Laxmikant Mishra  
M.Tech Research Scholar  
Computer Science  
Gyan Ganga Institute of Technology & Management Bhopal

Amit Kumar Sharma  
Assistant Professor  
Computer Science  
Gyan Ganga Institute of Technology & Management Bhopal

ABSTRACT
Cloud computing based technology and its impact is growing now a day. Cloud computing is used in all the area of Business, Education, Social Impact and data miner. The growing demand is because of the on demand service and pay per basis used somehow in the unlimited form. But the uses enhance the risk of data trapping and forgery. As the services are sharing within different cloud users and the accessibility are also different. So the security issues in cloud computing environment are a major concern. As the users totally rely on the cloud vendors, so there is a need of data protection and the data control from the cloud users. So the main aim of my paper finds the advancement in the related previous technology and the gaps. Based on our study some future enhancements have been suggested.

Keywords

1. INTRODUCTION
Cloud computing provide on demand resources based on pool of resources available by the cloud providers [1] [2] [3]. From the aspect of traditional computing the advantages of cloud computing are: Effective Cost, Device Independency, on demand service and scalability [4] [5]. But the security concerns are the major key aspects in the future cloud computing era. There are several security majors are suggested in [6], [7], [8], [9],[10],[5].Virtualization, high performance computing are also the greater facility aspects of cloud computing. But to achieve the performance on the parallel system and maintaining the integrity is tough [11]. All the above work shows the inclusion of efforts made to design solutions that are used to fulfill various requirements like: efficiency, verification, unbounded use of queries and irretrievability of data, etc. The two categories are private auditability and public auditability. Private and Public auditability are the two categories of the verifier [5]. Although schemes with private auditability can achieve the schemes efficiently, but it is challenging situation if the data is storing privately [5]. Virtualization is the key feature of cloud computing by which data sharing is possible between different machines of virtual existence from the data center [12]. Virtualization enables the resource migration [9] of virtual machines which is stable and take in part as the virtual machine parameters to the consumers and balance the load across physical servers in the data centers [12].

In today’s age several companies are in the great position for the cloud provider. The list of the cloud providers are [13]:

• Google- It is a provider of private cloud. It provide the services like email, document applications, data translation services, maps, web analytics, etc.[13].
• Microsoft- It has SharePoint service that mainly provides the services in the area of content and business intelligence. For this they provide tools to be moved into the cloud area [13].
• Salesforce.com- It runs the cloud application for its customers in a cloud. The main products are Force.com and Vmforce.com. It provides platforms to build customized cloud services [13]. But the security concerns are uncovered.

The cloud computing framework relies on the layers for data transportation. Cloud computing services are mainly divided into two parts cloud computing services and the deployment model. The three main service layers that comprise the cloud computing architecture based on which the on demand service will be provided [14]. According to [14] Platform as a Service (PaaS) is an environment for Cloud Computing Security Management for developing and building applications for different environments. According to Infrastructure as a Service (IaaS) mostly involves virtualization environments as purchased services rather than physical or dedicated computer equipment. The services layers are shown in figure 1.

![Figure 1: Types of Service Models in Cloud Computing](image)

In the traditional way of computing the resources are purchased locally which are sometimes higher in cost and not affordable. This limits the ways in which a user could interact with the software in that the software was only available and accessible for the original workstation [14]. But now by the use of cloud computing the Software as a Service model has transformed this methodology in such a way that software can be purchased for use over the Internet [14]. Instead of
purchasing software it is directly hosted in the cloud [14]. The main benefit of this type of system is there is no need of powerful work station as the user location but on demand resources/software can share it with rent. So if it is integrated with the security regimes it becomes powerful. The data is deployed based on three categories. First is public second is private and third is hybrid. In public cloud the resources are used in general public. The list of public cloud providers are IBM’s Blue Cloud, Elastic Compute Cloud (EC2), Sun Cloud, Windows Azure Services Platform and Google AppEngine. It is not sell as a service and it is costly. Portion of the public cloud can be migrated or clubbed as a hybrid cloud but it contains the feature of both deployment model.

In 2013, Zheng et al. [17] provides a comparison between private cloud and public cloud. Based on their study they suggest the theoretical reference to build the private cloud computing. In 2011, Li et al. [18] presented a study using online Personal Health Record (PHR), it shows the necessity of authorization capability which reduces the privacy exposure find from the search results, and establishes a scalable framework for Authorized Private Keyword Search (APKS) over encrypted data. In 2011, Yang et al. [19] suggest Storage-as-a-service is an important component of cloud computing. Authors suggest the searching capability based on private data over the encryption standard. It also provides multi-user searchable encryption, for the single-user setting. A practical multi-user searchable encryption scheme was proposed to taking the advantage consideration. In 2011, Wang et al. [20] discussed the problem of ensuring the integrity of data storage. This task is allowing a third party auditor (TPA), based on the cloud client, to judge the integrity of the data stored in the cloud. It holds good in achieving economies scale. In 2012, Naqvi et al. [21] suggest a testing way to find the scalability and homogeneity of federated Cloud security services. The goal is to impact the security functions under several operating conditions. The results based on the above scenario will help in different businesses scenario to identify the security architecture which fit in requirements. In 2012, Tianfield et al. [22] analyzes the cloud security requirements based on various parameters like integrity, confidentiality, trust, availability and compliance. In 2012, Abuhussein et al. [23] suggest volume shortage in Healthcare, education and business industry and suggest cloud computing infrastructure. But the data to the cloud and the data shifting process in not controlled at the users end. The security and privacy of the customer's is an important issue. So attributes which are responsible security and privacy are analyzed. Security provisions can make a better cloud vision in future. In 2012, Liu et al. [24] also discussed the security problem of cloud computing. Computing Systems are analyzed based on computing concepts and characters. Cloud computing security problem are not solved by single security. So traditional and latest technologies can be a better combination to solve this issue. In 2013, Pant et al. [25] discusses about security and compliance assessment with the cloud computation time and adoption mechanism. In 2013, meng et al. [26] discusses security issues, data transmission security, storage capacity and management They suggest that the universal data management may affect cloud security strategies and it may be evoked long-term development direction. In 2013, Yang et al. [27] suggested Trusted Cloud Computing Platform (TCCP) for remote attestation which provides better security for tenant. The different authentication policies, such as user password checking, image hash verification and chain measurement are the different levels of security should be adopted.

2. LITERATURE SURVEY
In 2010, Wang et al. [15] for solving the privacy preserving role of cloud a private match and min-attribute generalization approach was suggested. Privacy indexing is also suggested in the internet. In 2010, Wang et al. [16] suggest a method for cloud computing security. They named this method as private face recognition method. It has three components: user part provides face images; cloud initialization part has a face subspace and templates database; cloud private matching identification part contains the core algorithm of the method comparing two encrypted numbers under double-encrypted conditions. Their results shows that the method can ensure that cloud neither know user’s real face data, nor the face private matching identification result, to make user’s face data secure. In 2011, Zheng et al. [17] provides a comparison between private cloud and public cloud. Based on their study they suggest the theoretical reference to build the private cloud computing. In 2011, Li et al. [18] presented a study using online Personal Health Record (PHR), it shows the necessity of authorization capability which reduces the privacy exposure find from the search results, and establishes a scalable framework for Authorized Private Keyword Search (APKS) over encrypted data. In 2011, Yang et al. [19] suggest Storage-as-a-service is an important component of cloud computing. Authors suggest the searching capability based on private data over the encryption standard. It also provides multi-user searchable encryption, for the single-user setting. A practical multi-user searchable encryption scheme was proposed to taking the advantage consideration. In 2011, Wang et al. [20] discussed the problem of ensuring the integrity of data storage. This task is allowing a third party auditor (TPA), based on the cloud client, to judge the integrity of the data stored in the cloud. It holds good in achieving economies scale. In 2012, Naqvi et al. [21] suggest a testing way to find the scalability and homogeneity of federated Cloud security services. The goal is to impact the security functions under several operating conditions. The results based on the above scenario will help in different businesses scenario to identify the security architecture which fit in requirements. In 2012, Tianfield et al. [22] analyzes the cloud security requirements based on various parameters like integrity, confidentiality, trust, availability and compliance. In 2012, Abuhussein et al. [23] suggest volume shortage in Healthcare, education and business industry and suggest cloud computing infrastructure. But the data to the cloud and the data shifting process in not controlled at the users end. The security and privacy of the customer's is an important issue. So attributes which are responsible security and privacy are analyzed. Security provisions can make a better cloud vision in future. In 2012, Liu et al. [24] also discussed the security problem of cloud computing. Computing Systems are analyzed based on computing concepts and characters. Cloud computing security problem are not solved by single security. So traditional and latest technologies can be a better combination to solve this issue. In 2013, Pant et al. [25] discusses about security and compliance assessment with the cloud computation time and adoption mechanism. In 2013, meng et al. [26] discusses security issues, data transmission security, storage capacity and management They suggest that the universal data management may affect cloud security strategies and it may be evoked long-term development direction. In 2013, Yang et al. [27] suggested Trusted Cloud Computing Platform (TCCP) for remote attestation which provides better security for tenant. The different authentication policies, such as user password checking, image hash verification and chain measurement are the different levels of security should be adopted.

3. PROBLEM DOMAIN
Third party auditing and security is the greater concern today. There are few areas which are still unattended in cloud computing security such as auditing, side channels and migration of data from one cloud to another [33]. Cadence has evermore been on immutable make believe and corrupt assail but the pretence of service has not been considered. The check tick off on protean organize with cherish to respect to overcast computing is another open research issue. On touching celebration, know-how and restrictive computational intellect

![Image](image-url)
creates obstacle in conduct oneself to provide best performance to mobile user. This handbill to pieces provides percipient view of cloud computing security issues.

Brave and violent base systems are increasingly reliant on cloud computing applications in order to provide elements of functionality and achieve the associated missions. Leaning towards the in conformity and misemploy more these applications, they eat be cheerful to failures and attacks - detecting, move wink at through, recovering immigrant, and reconfiguring in response to such issues. Pliancy is break the ice as the industriousness of uphold government stroll last analysis definitely be veracious when facing swings. These changes could be anything from unanticipated failures, intrusions, accidents, and/or increased albatross. Connect of the small of brisk such percipient systems in the depressing is on-demand equipping attributes to make do nigh load and in finical to handle the highest expected load. This typically leads to “dormant”, brand-new affirmative drift we utilize to increase security and reliability.

4. ANALYSIS
The overall analysis in all the aspects are shown in table 1.

<table>
<thead>
<tr>
<th>S.no</th>
<th>Authors</th>
<th>Year</th>
<th>Work</th>
<th>Gap</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Vijay et al.[28]</td>
<td>2012</td>
<td>Authors considered an architecture where different services are hosted on the cloud infrastructure by multiple cloud customers (tenants).This model extends the node controller with the functionality of the Certification Authority to certify the behavior of the tenant virtual machines. Since the Node Controller is aware of the dynamic changes to the tenant virtual machine, it can ensure that the certified properties are satisfied by the tenant virtual machines.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Abdullah Abuhussein et al. [23]</td>
<td>2012</td>
<td>Authors identify and categorize a list of attributes which reflect the various aspects of cloud security and privacy. Quantifying metrix for promoting the attributes is missing.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Huaglory[22]</td>
<td>2012</td>
<td>Presents a comprehensive study on the challenges and issues of security in cloud computing. Security authentication mechanism are not elaborated properly.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Irina et al. [29]</td>
<td>2012</td>
<td>They suggest some of the key benefits and the major drawbacks that come around with swapping out services and infrastructure to a public cloud. Based on these benefits and drawbacks, K.O. (knock-out) criteria will be identified, which can be seen as the minimum basis for secure cloud Environment. Suggested techniques should be implemented.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Mehdì et al. [30]</td>
<td>2013</td>
<td>Authors purpose is to concentrate on cloud data storage security and to manage the user’s data in the cloud by Implementation of kerberos authentication Service. Other standard encryption techniques can also be used.</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Liu Xiao-hui et al. [31]</td>
<td>2013</td>
<td>Authors introduced cloud development status, and analyzed the security problems. The security problem has become a focus</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Azzedine Benameur et al. [32]</td>
<td>2013</td>
<td>Authors present an approach to leverage the elasticity and on-demand provisioning features of the cloud to improve resilience to availability concerns and common attacks. Need of supporting different file formats.</td>
<td></td>
</tr>
</tbody>
</table>
5. CONCLUSION AND FUTURE WORK

Security is major concern today in the cloud computing environment. Third party auditing and external security services are needed due to increasing demand of the cloud computing. So our paper main aim to study and analysis the aspects of cloud computing security. Future suggestions are following:

1) Hybridization of virtualization and Optimization may be used.
2) Trusted framework can be developed by using RSA and MD5 Algorithm [5].
3) Data mining task can be computed in cloud environment for proper data classification and categorization [36].
4) Provide secure framework for providing mobile cloud computing making data access and handling mechanism by data mining [37].
5) Data Security can be provided by RC4, RC5 etc.[38].
6) Strong user authentication is also a good choice[39].

6. REFERENCES


