Security in Cloud Computing Based on Third Party Auditor: A Survey

Mohamed Ben Haj Frej, Julius Dichter, Navarun Gupta
Department of Computer Science and Engineering
University of Bridgeport, Bridgeport, CT

Abstract
This paper surveys security in cloud computing based on Third Party Auditor (TPA) also known as Trusted Third Party (TPP). There are various security models for safeguarding the client’s data in cloud. TPA provides secure connections between the user and the cloud server. Cloud Service Provider (CSP) Provides the clients with cloud storage and service. TPA has access to the client’s cloud data and all the critical information. There are many security models for making the TPA more reliable so the clients can trust the third party for storing their data. In this paper, we survey mostly the types of security models based on Third Party Auditing in cloud. We also discuss how these security models enable the third party to gain the clients trust. The classification has been based on the adopted security method as well as on the kind of threats they are addressing.

Introduction
• Cloud computing is based on pay as you use computing rather than having local servers or personal devices to handle applications.
• Computing services, such as database transactions, storage, software, computing, and applications, are delivered to local devices through Internet.

There are four delivery models in cloud computing, namely:
- Public cloud,
- Private cloud,
- Community cloud,
- Hybrid cloud.

Based on the services, the cloud is divided into three models:
- Infrastructure as a Service (IaaS).
- Platform as a Service (PaaS).
- Software as a Service (SaaS).

The third party auditor has expertise and capabilities that the user and CSP does not have. TPA is trusted to assess the CSP’s storage security upon request from the user and the provider so the data is free from:
- Byzantine failures,
- Malicious data,
- Data modification attack
- Server colluding attacks

Security Threats:
- Confidentiality: only authorized parties or systems having the ability to access protected data.
- Integrity: assets can be modified only by authorized parties or in authorized ways.
- Availability: the property of a system being accessible and usable upon demand by an authorized entity.
- Access Control: the data is legally accessed due to astringent access control, Authentication and Identification that is due to multi-tier security resulting into interoperability defects.

Cloud Vulnerabilities: for the third party management models, most security problems stem from:
- Loss of control
- Lack of trust
- Multi-tenancy

Methods for improving security in TPA

Recapitulation Table

<table>
<thead>
<tr>
<th>Security Model</th>
<th>Security Requirement</th>
<th>Threats</th>
<th>Advantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>TPA based on RSA</td>
<td>Non-repudiation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TPA based on ElGamal</td>
<td>Non-repudiation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public Key Infrastructure</td>
<td>Non-repudiation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TPA based on ECC</td>
<td>Non-repudiation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TPA based on Hash</td>
<td>Non-repudiation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TPA based on Identity</td>
<td>Non-repudiation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TPA based on Key Exchange</td>
<td>Non-repudiation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TPA based on Certificate</td>
<td>Non-repudiation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TPA based on Proxy</td>
<td>Non-repudiation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TPA based on Privacy</td>
<td>Non-repudiation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TPA based on Trust</td>
<td>Non-repudiation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TPA based on Audit</td>
<td>Non-repudiation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TPA based on Identity</td>
<td>Non-repudiation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TPA based on Key Exchange</td>
<td>Non-repudiation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TPA based on Certificate</td>
<td>Non-repudiation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TPA based on Proxy</td>
<td>Non-repudiation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TPA based on Privacy</td>
<td>Non-repudiation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TPA based on Trust</td>
<td>Non-repudiation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TPA based on Audit</td>
<td>Non-repudiation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Conclusion
In this paper, we have surveyed the main security models and the techniques they are using to overcome the security issues. The focus is centered on Third Party Auditor in cloud computing which does the auditing process on behalf of the client, establishes the secure connection and guarantees the integrity of the data. The classification has been based on:
- The adopted security methods
- The kind of threats these methods are addressing.

References