A Novel Approach for Enhancing the Authentication Process in Cloud Computing

Shubha Bharill a, Praveen Lalwani b, T.Hamsapriya c
Department of Computer Science and Engineering, Oriental Institute of Science and Technology, Bhopal, Madhya Pradesh, India

Abstract—A cloud computing is a new computing model which is a successor of grid computing, utility computing, parallel computing, distributed computing and other Virtualization technologies. The cloud is a metaphor for the Internet and is an abstraction for the complex infrastructure it conceals. Cloud Computing provides the capability to use computing and storage resources on meter basis and reduce the investments in an organization’s computing infrastructure. Although data stored in third party storage systems like the cloud might not be secure since integrity, confidentiality and authenticity of data are not guaranteed. Cloud is a third party service and so, a client cannot trust the cloud service provider to store its data securely within the cloud. Hence, many organizations and users are still not willing to use the cloud services to store their data in the cloud until certain security guarantees are made. So to avoid this insecurity of user’s data there is a need to authenticate a client before using the services.

In this paper an authentication model is proposed for cloud computing based on Kerberos protocol using threshold cryptography to provide more security and to increase the availability of key. This model can also benefit by filtering the unauthorized access and to reduce the burden of computation and memory usage of cloud provider against authentication checks for each client. It acts as a third party between cloud server and clients to allow authorized and secure access to cloud services.

Index Terms—Cloud Computing, Kerberos Authentication model, Ticket Granting Server, Multiparty Authentication

I. INTRODUCTION

Cloud Computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files on any computer with internet access. This technology allows for much more efficient Computing by centralizing data storage, processing and bandwidth. Cloud storage is used by a large number of individuals and enterprises. All data stored on their hard drive is not cured by the user and no one knows where exact data saved. The security in the cloud is one of the most important issues. Already many researchers, survey cloud security problem. But we add another service to enhance the security issues. This service is Kerberos authentication service. In this theory, admin defines any IP address for using the cloud server provider. It means admin makes restrict for some user. At the next step the user with that IP address can connect to the Kerberos and after this service it should connect to the cloud service provider for sending the data. So with this long filtering we can enhance the security problem in the cloud. We will discuss the
whole process of Kerberos Authentication model in section 3. Although the Kerberos is alone not a perfect model for authentication because the single Kerberos server is prone to failure, so in this paper we are proposing a Cryptography algorithm known as a Threshold cryptography algorithm for increasing the security and availability of data. A threshold public key encryption system is a public key system where the private key is distributed among n decryption servers so that at least k servers are needed for decryption. The key can be retrieved by performing computation on at-least k no. of participants. Less than k no of participants are not useful to retrieve the key. Such a scheme is called a \((k, n)\) threshold scheme. It is easily computable when have the necessary data available.

II. RELATED WORK

<table>
<thead>
<tr>
<th>Title of the Paper</th>
<th>Concept</th>
<th>Future Work</th>
<th>Year of Publication</th>
<th>Conference/Journal Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1] SAPPHIRE: Anonymity for Enhanced Control and Private Collaboration in Healthcare Clouds</td>
<td>Proposed a paradigm shift in the interaction of users with cloud services that removes unwarranted trust in the cloud service provider and provisions accessibility for collaborators.</td>
<td>Extended SAPPHIRE through the implementation of a collaborative toolkit for matching records to further enhance privacy and collaboration. Also, we look to incorporate privacy-preserving sensor reporting for pervasive health. Finally, we hope to add confidential auditing and usage controls using health care workflow models.</td>
<td>2012</td>
<td>IEEE 4th International Conference on Cloud Computing Technology and Science</td>
</tr>
<tr>
<td>[2] Ensuring Security in On-demand File Replication System</td>
<td>Proposed security mechanisms to fully secure the on-demand logical resource (file) replication scheme through the use of symmetric and asymmetric keys as they are required for fulfilling the confidentially, integrity, availability requirements of the system efficiently.</td>
<td>In future the X.509 certificates shall be incorporated in this approach. Certificates will be assigned to different FRS by the central trusted authority. Through certificates the FRS will be able to authenticate themselves to other FRS. The inclusion of the certificates will make the system more scalable and secure.</td>
<td>2012</td>
<td>Third International Conference on Computer and Communication Technology</td>
</tr>
<tr>
<td>[3] Coding For Trusted Storage In Untrusted Networks</td>
<td>Proposed an encoding scheme that exploits the algebraic properties of structured matrices to ensure both confidentiality and fault-tolerance over a set of untrusted and unreliable networks.</td>
<td>The adoption of a stronger threat model involving Byzantine attackers, capable of corrupting some of the coded data stored in multiple untrusted networks.</td>
<td>2012</td>
<td>IEEE Transactions On Information Forensics And Security</td>
</tr>
<tr>
<td>[4] Applying Agents to the Data Security in Cloud Computing</td>
<td>Presented a data security model for cloud computing, and introduces agents to data security module in order to provide more reliable services.</td>
<td>There are still some studies to be done in the future for instance, further reducing the user waiting time, speeding up data access, and further increasing data availability.</td>
<td>2012</td>
<td>IEEE International Conference on Computer Science and Information Processing (CSIP)</td>
</tr>
<tr>
<td>[5] Security concept and implementation for a cloud based e-Science infrastructure</td>
<td>Presented a novel security concept for e-Science infrastructures based on the MIT Kerberos implementation, highlight its challenges, and discussed the implemented solution and its evaluation within the distributed ABA framework to implement user authentication down to the lowest (database) level.</td>
<td>The complete security concept is domain independent and thus can be used for other cloud-based infrastructures.</td>
<td>2012</td>
<td>Seventh International Conference on Availability, Reliability and Security</td>
</tr>
<tr>
<td>[6] Privacy preserving public auditing for data storage security in cloud computing</td>
<td>Utilized and uniquely combined the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system.</td>
<td>To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously.</td>
<td>2011</td>
<td>Presented in ieee computer society</td>
</tr>
<tr>
<td>[7] Enabling Public Auditability and Data Dynamics for Storage Security in</td>
<td>This work studies the problem of ensuring the integrity of data storage in Cloud Computing. In particular, we consider the task of</td>
<td>To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our</td>
<td>2011</td>
<td>Presented in ieee transactions on parallel and distributed</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>Conference/Year</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud Computing</td>
<td>allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud.</td>
<td>systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[8] Above the Trust and Security in Cloud Computing: A Notion towards Innovation</td>
<td>Derived a secure protocol by successively eliminating the dangling pitfalls that remain dormant and thereby hamper confidentiality and integrity of information that is worth exchanging between the INO and the CSP. Entities like AS and TGS as incorporated in proposed protocol scheme are yet to be further made resilient and trusted in compromised and devastated situations to be envisaged. An experimental outcome showing the analytically found improvement of proposed scheme over SSL is yet to be done along the line of confidentiality in setting up secure trusted channel between INO and CSP.</td>
<td>IEEE/IFIP International Conference on Embedded and Ubiquitous Computing 2010</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[9] How to Manage Information Security in Cloud Computing</td>
<td>Discussed the Key Success Factors (KSFs) that determine the management information security in cloud computing and applied Fuzzy Analytic Hierarchy Process (Fuzzy AHP or FAHP) to overcome the seeming failure of general Analytical Hierarchy Process (AHP) in dealing with respondents impersonal differences in paired comparison. Reviewing empirical studies on KSFs may provide different answers, which the FAHP analysis evidently pointed out.</td>
<td>IEEE 2011</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[10] MCDB: Using Multi-Clouds to Ensure Security in Cloud Computing</td>
<td>Proposed a Multi-clouds Database Model (MCDB) which is based on Multi-clouds service providers instead of using single cloud service provider such as in Amazon cloud service also presented the architecture of the proposed MCDB model and described its components and layers. Comparison can be made of proposed model with other multi-clouds models or systems to go further in our comparison until the best and improved model found.</td>
<td>Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing 2011</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[11] A quantitative analysis of current security concerns and solutions for cloud computing</td>
<td>Identified and classified the main security concerns and solutions in cloud computing, and proposed a taxonomy of security in cloud computing, gave an overview of the current status of security in this emerging technology. Deeper study on current security solutions to manage cloud computing virtual machines inside the cloud providers should be the focus of future work in the area.</td>
<td>Third IEEE International Conference on Cloud Computing Technology and Science 2011</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[12] Role Of Cloud Computing For Smart Grid of India And Its Cyber Security</td>
<td>Focused on secure and dependable data storage centre, worked upon proposed a internet connectivity device model instead of having C.P.U. and discs, for cloud computing. The adoption of advanced technologies is necessary to enable significant environmental benefits and more efficient use of our grid.</td>
<td>IEEE computer society 2011</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[14] A Trust Based Approach for Increasing Security in Cloud Computing Infrastructure</td>
<td>A new approach called Trusted Cloud Computing Infrastructure is proposed, presenting a User Trusted Entity (UTE) to make cloud computing infrastructures reliable in order to enable infrastructure service developers to provide a closed execution environment. Proposed work is specifically designed only for IaaS environment. It can be elaborated for PaaS and SaaS environment also.</td>
<td>IEEE, UKSim 15th International Conference on Computer Modeling and Simulation 2013</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
III. PROPOSED WORK

In cloud data storage system, users store their data in the cloud and for accessing must refer to cloud server provider. Thus the correctness of the user being referred to the distributed cloud server must be guaranteed because the data stored in the cloud may be frequent, updated with user including, insertion, deletion, modification, appending, reordering, etc. To ensure this updating is under correctness user is important so in this paper we introduce one model based on Kerberos. In this model each user to gain the cloud server must be registered and authenticated with third party. For avoiding some limitations of Kerberos in this paper we are implementing a new algorithm at TGS known as Threshold Cryptography algorithm. This algorithm will avoid single point of failure to increase the availability and also make a multiparty authentication system which is beneficial from the security point of view. We will discuss both in detail one by one.

A. Kerberos

Here Kerberos is used for providing authentication for a client who want to access the applications stored at server side. Some another reasons for using Kerberos is, in Kerberos user password never travel over the network, never stored in any form on the client machine and it never be stored in unencrypted form and mutual authentication. Awareness of authenticity of user and server to each other is known as Mutual authentication.

Authentication Server: AS Issues a Ticket Granting Ticket to user. User sends their user name to server. Server responds with TGT encrypted with user’s password. User enters password on client-if correct the TGT is successfully decrypted.

Ticket Granting Server: Logically different from the AS but may reside on the same server. User contacts when a network service is desired. Service ticket request is encrypted with session key provided by the in the TGT, not user’s password. TGS authenticates tickets and issues a ticket for the resources as well as the encryption key to use with communication with the service.

Network Server: Client sends resource ticket and authenticator to the service encrypted with the client/server key. Server verifies both and issues a return message with a modified version of timestamp in the authenticator encrypted with client/service key. Client views message- if timestamp is modified correctly the service is genuine and ready to process request.

Since all authentication is controlled by a centralized Key Distribution Centre, compromise of this authentication infrastructure will allow an attacker to impersonate any user by getting the knowledge about the key. So we use Threshold Cryptography algorithm to divide Ticket Granting Server into multiple parts to allow multiparty authentication, it means one cannot decrypt the key until the predefined numbers of parts of TGS are not available. Second reason for using Threshold Cryptography algorithm is to provide more availability to the TGS. In a traditional Kerberos authentication system if TGS got deactivated due to any reason, then all the system get affected and the whole procedure of authentication get shut down. To avoid this type of system failure in this paper we are proposing a Threshold Cryptography algorithm which will divide our TGS into n parts and at least k parts are need to make an useful information. Here k is always smaller than n.

B. Threshold Cryptography Algorithm

Reason for using threshold cryptography is to provide more security to the key used by the secret sharing scheme. In this scheme data D is divided into n pieces and knowledge of some pieces k enables to derive secret data D. Knowledge of any pieces k-1 makes secret data D completely undetermined. Such a scheme is called a (k, n) threshold scheme. This scheme is easily computable when have the necessary data available. This is a safe and convenient method to provide security for key.

C. Mathematical Derivation of Threshold Cryptography Algorithm:

Suppose using (k, n) threshold scheme to share our secret S. Choose at random k-1 coefficients and \(a_0, a_1, \ldots, a_{k-1}\). Let \(a_0 = S\). Then we can build the polynomial to divide the key as:

\[
q(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1}
\]

Construct \(D_1 = q(1), D_2 = q(2), \ldots, D_n = q(n)\). Given any subset of k pairs, can find S using interpolation. The secret is a constant term \(a_0\). For an Example:

\[
S = 1234, n = 6, k = 3
\]

Randomly two numbers: \(a_1 = 166, a_2 = 94\) are used to produce the polynomial:

325
Six points are obtained from the polynomial: (1, 1494); (2, 1942); (3, 2578); (4, 3402); (5, 4414); (6, 5614). So that each participant can get different single point (both x and q(x)).

To reconstruct the secret:
In order to reconstruct the secret $S$, $k$ points will be enough. Let $k=3$ and consider (2, 1942); (4, 3402); (5, 4414). It is possible to construct $q(x)$ by using Lagrange’s polynomial, and the value of $S$ can also be derived. Let us consider $(x_0, y_0) = (2, 1942); (x_1, y_1) = (4, 3402); (x_2, y_2) = (5, 4414)$.

Lagrange’s polynomials can be computed as:
\[
\begin{align*}
l_0 &= \frac{x - x_1}{x_0 - x_1} \frac{x - x_2}{x_0 - x_2} = \frac{x - 2}{2} \frac{x - 5}{2} = \frac{1}{2} x^2 - 1 \frac{1}{2} x + 3 \frac{1}{2} \\
l_1 &= \frac{x - x_0}{x_1 - x_0} \frac{x - x_2}{x_1 - x_2} = \frac{x - 2}{4} \frac{x - 5}{4} = - \frac{1}{2} x^2 + 3 \frac{1}{2} x - 5 \\
l_2 &= \frac{x - x_0}{x_2 - x_0} \frac{x - x_1}{x_2 - x_1} = \frac{x - 2}{5} \frac{x - 4}{5} = - \frac{1}{3} x^2 - 2 x + 2 \frac{2}{3}
\end{align*}
\]

The Lagrange’s polynomial is:
\[
f(x) = \sum_{j=0}^{2} y_j l_j(x) = 1734 \left( \frac{1}{6} x^2 - \frac{1}{2} x + 3 \frac{1}{3} \right) + 2634 \left( -\frac{1}{2} x^2 + 3 \frac{1}{2} x - 5 \right) + 3234 \left( \frac{1}{3} x^2 - 2 x + 2 \frac{2}{3} \right)
\]
\[
= 1234 + 150 x + 50 x^2.
\]

Remember that the secret is the free coefficient, which means that $S=1234$, and as it is similar to the equation 5.2.

**IV. WORKING MODEL**

In Kerberos, Threshold Cryptography is applied at TGS. The process of authenticating a client by AS is similar as discussed in section 3.1.1 and 3.1.2. TGS uses a polynomial function which will logically divide...
the single TGS into multiple TGS ($n$). After authenticated by AS, client sends the request to k number of TGS for requesting services. TGS will send reply to the client. At client side reply from at-least $k$ number of TGS are required to perform computation to retrieve the Client/Server session key. After retrieving the Client/Server session key client will communicate to the Service Server to use the requested services. Working model using threshold Cryptography in Kerberos Authentication system is discussed in Fig. 2.

A. Initial Authentication of client

Whenever a client wants to access a service from cloud server it requires a Kerberos ‘Ticket’ before it serves the clients’ request. On the basis of this ticket the cloud server will grant access to all the subscribed services to the client. This ticket proves client authentication to the server similar as section 5.2.1 and 5.2.2. This removes the overhead of cloud server for performing authentication checks and also saves cloud processing and storage.

B. Ticket Granting Ticket

The Ticket Granting Ticket exchange needs to obtain service granting ticket. Client next sends the Ticket Granting Ticket to a Ticket Granting Server (TGS). In traditional Kerberos Authentication Model there is only one TGS, so if the master key (also known as client/server session key) sent by TGS is known by someone, then one who is not authorized can use the services provided by the cloud server. It makes data unsecure. To avoid this drawback, an efficient security algorithm known as Threshold Cryptography Algorithm, is applied at TGS:

- In this algorithm instead of single TGS, multiple TGS ($n$) have been used where at-least ($k$) number of TGS are needed to decrypt the master key (where $k < n$).
- The client sends a request for the master key to $k$ number of TGS. If $k$ number of TGS replies, then the client can get the required master key.
- Otherwise the client will send the request to $(k + 1)^{th}$ TGS and wait for the reply.
- This process of sending request to $(k + 1)^{th}$ TGS will be continue, until at-least $k$ number of TGS will not reply.
- After getting the master key client can request the required service from the service provider. This whole procedure is illustrated in fig.1.
- The server either rejects the ticket or accepts it and performs the service.
- The master key granted to client can only be decrypted by the cloud server with the secret key shared between the cloud server and TGS.

Any unauthorized user will never be able to decrypt the master ticket. Since the ticket that the client has received from the TGS is time-stamped. So it allows clients to make additional request using the same ticket within a certain time period (typically, 8 hours) without the need to prove authentication again. As the ticket is valid for a limited period of time, this makes fewer chances that anyone else will be able to use it later. A flow chart for understanding the working of the new authentication model is described in Fig 3. Kerberos Authentication model is responsible for providing authentication to the client. By using Threshold Cryptography in Kerberos Authentication model the security of the data stored at server side as well as the availability of secure key increases. In traditional approaches, the key may be lost due to some environmental problems such as storm, earthquake or any weather disaster or some other administrative problems such as an employee involved in a major project leaving in the middle of the project. In our approach multi party authentication is provided to the key.

V. RESULT ANALYSIS

Here we are taking a comparative analysis between Traditional Authentication model and in our approach. In Traditional Authentication model if an attacker attacks on single Kerberos server then he is able to decrypt the data in a given time for a given length of key as shown in fig. 3. But using the multi authentication system it will take the to decrypt the key in multiple of $k$. It means by using our approach for authentication, complexity for an attacker to decrypt the data will be increase in multiple of $k$. Where $k$ is no. of $n$ participants to decrypt the data. So our approach is making the whole Kerberos Authentication model more secure.
Fig. 2. Kerberos using Threshold Cryptography where n=5 and k=3[15]

TABLE II. COMPARATIVE RESULT ANALYSIS BETWEEN SINGLE TGS AND MULTI TGS AUTHENTICATION SYSTEM

<table>
<thead>
<tr>
<th>S. no.</th>
<th>Key Size (bits)</th>
<th>Broken Time for single TGS=T</th>
<th>Broken Time for multiple TGS=k.T</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>56</td>
<td>399 (sec.)</td>
<td>k.399 (sec.)</td>
</tr>
<tr>
<td>2.</td>
<td>128</td>
<td>$1.02 \times 10^{38}$ (yr)</td>
<td>k.$1.02 \times 10^{38}$ (yr)</td>
</tr>
<tr>
<td>3.</td>
<td>192</td>
<td>$1.872 \times 10^{37}$ (yr)</td>
<td>k.$1.872 \times 10^{37}$ (yr)</td>
</tr>
<tr>
<td>4.</td>
<td>256</td>
<td>$3.31 \times 10^{36}$ (yr)</td>
<td>k.$3.31 \times 10^{36}$ (yr)</td>
</tr>
</tbody>
</table>
VI. CONCLUSION AND FUTURE WORK

In this paper we discussed the need for authentication in a cloud computing environment and a new approach for authentication. There has a lot of work already been done for providing security to clouds and also to provide authenticated user and services but in this paper a novel approach based on Kerberos authentication using threshold cryptography have given for a stronger and more secure protocol. Kerberos provides a centralized authentication server whose function is to authenticate the user to the cloud server and the cloud server to the user. Although due to some limitation of Kerberos it is not sufficient for authentication procedure. So that in our paper we proposed Threshold Cryptography algorithm to avoid the single point of failure in Kerberos, we have merged the concept of Threshold Cryptography with Kerberos authentication model to make it more valuable. This method is providing the concept of multiparty authentication. Using this algorithm we have seen that a client might not be able to access the services until the required no. of server does not reply. This concept is useful to increase the security and also to improve the availability of key (used to authenticate a client).

In order to provide the authentication to the user, using Threshold Cryptography in Kerberos there is a need to work on time complexity also. In future, this work can be extended by using the concept of parallel processing algorithm to enhance the efficiency of the overall system. To incorporate confidentiality and integrity along with the authentication, can be the another aspect to explore the perspective of security in cloud computing environment.

REFERENCES