Trust Based Security for Cloud Systems

Dinesh Sriram

Murali Medisetty

Problem Statement

Even though Security, Privacy and Trust issues exists since the evolution of Internet, the reason why they are widely spoken these days is because of the Cloud Computing scenario. Any client/small organization/enterprise that processes data in the cloud is subjected to an inherent level of risk because outsourced services bypass the "physical, logical and personnel controls" of the user [1]. When storing data on cloud, one might want to make sure if the data is correctly stored and can be retrieved later. As the amount of data stored by the cloud for a client can be enormous, it is impractical (and might also be very costly) to retrieve all the data, if one's purpose is just to make sure that it is stored correctly. Hence there is a need to provide such guarantees to a client.

Hence, it is very important for both the cloud provider and the user to have mutual trust such that the cloud provider can be assured that the user is not some malicious hacker and the user can be assured of data consistency, data storage [2] and the instance he/she is running is not malicious. Hence the necessity for developing trust models/protocols is demanding.

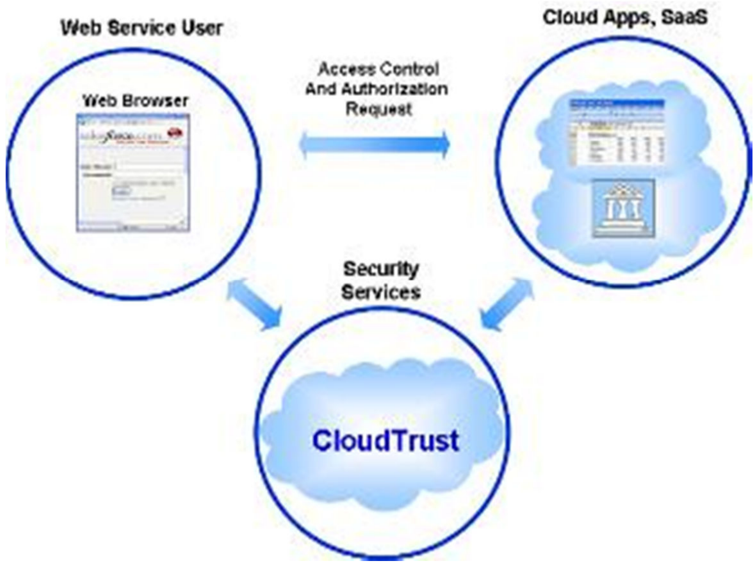
What needs to be done to solve this problem?

Both the user and the cloud provider instance must make sure that whatever requests/response they get is from a trusted source by estimating the correctness of data that they receive. This can be done by implementing a trust based protocol that runs between the user and the instance before they start transferring any "real requests/responses". The protocol/model will determine the trust at both the ends by probing each other with challenges and then decide whether the other end is legitimate to handle requests/provide responses.

What has been done?

Already existing trust protocols for Distributed Systems/Wireless Networks are currently being extended to Cloud Computing.

- *Trusted Computing Group* [3] has updated to its IF-MAP (Meta-data Access Protocol) used to enable standardized data sharing among a wide variety of devices and applications, including cloud security. TCG's IF-MAP, or Metadata Access Protocol, is based on a powerful publish/subscribe model. IF-MAP is being used today to support network security applications using equipment from different vendors, and is expected to be used in cloud computing to enable real-time communication among devices including network infrastructure devices and servers



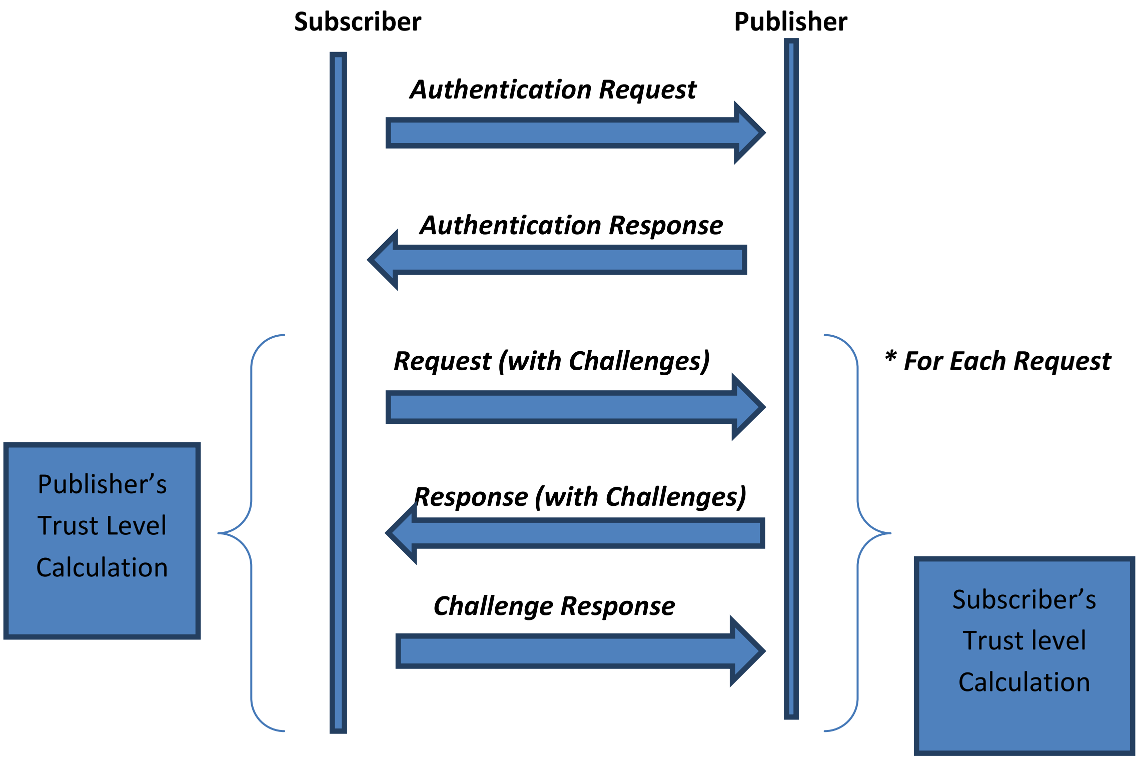
- *CloudTrust* (Part of CYLab, CMU) [5] provides trust protocol that supports strong authentication and access management. CloudTrust provides comprehensive security solutions for Cloud Integration and Application Access Management. It enables secure and authorized data access – web services can share only data that is authorized by the user or that is defined in the corporate data access policy.

What can be done?

One possible solution is to send a set of challenges along with some initial set of requests/response and determine the authenticity of the receiver. [4] (Care must be taken such that the receiver could not distinguish between the challenges and the requests) Depending on the response of the receiver, the trust level is determined. If the trust level is high, some sensitive information can be transferred or processed between the user and the cloud instance. If the trust level is low, the user / cloud instance can repeat the probing for specific number of times and then terminate the instance that he/she is running for processing if the trust level still doesn't meet the threshold.

To provide assurance about the data storage, we can survey the already existing works which use protocols for assuring a client that his data is retrievable with high probability, under the name of Proofs of Retrievability (PORs) and Proofs of Data Possession (PDP). After the survey we plan to identify (or extend) a best scheme and implement it to check the performance overhead that would incur on clients.

Our ultimate aim is to develop a trust protocol that allows computation of trust at both the ends. (i.e. at the user's end and the instance end).


Subscriber
Publisher
Authentication Request
Authentication Response
Request (with Challenges)
* For Each Request
Publisher's Trust Level Calculation
Response (with Challenges)
Challenge Response
Subscriber's Trust level Calculation

Proposed Trust Based Model

What we have done?

We have been reviewing research papers pertaining to trust and privacy in cloud systems. The knowledge from the already existing technology and research could be used to modify/extend trust models. We are now trying to do a performance analysis of the existing trust models to decide which model can be further extended.

References :

[1] http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853

[2] Cachin, C., Keidar, I., and Shraer , A. Trusting the cloud. *ACM SIGACT News,* 20:4 (2009), pp. 81-86.

[3] http://www.net-security.org/secworld.php?id=9862

[4] Eugen Staab, Volker Fusenig, and Thomas Engel, Towards Trust-Based Acquisition of Unverifiable Information, Proceedings of the 12th international workshop on Cooperative Information Agents XII

[5] http://www.cloudtrustinc.com/

[6] B. Krebs. Amazon: Hey spammers, get off my cloud, July 2008.