

Risk Analysis approach

To ensure that all security risks are eliminated, cloud service providers are trying to implement different security mechanisms.

There are two important questions regarding the security risks:

1. *How to estimate data security risk before placing data in the cloud?*
2. *How to assure customers that their data is safe with various service providers within the cloud network?*

With the help of a proper risk analysis approach, the cloud service providers can gain trust from their customers. Current security technology such as Secure Socket Layer (SSL), digital signatures and authentication protocols lack effective trust management.

Figure represents a risk analysis approach using a Trust Matrix.

For the trust matrix two variables, namely Data Cost and Provider's History are considered.

- a) Data cost is considered as one of the variables because the users can assign a cost to the data based on the data's criticality.
- b) Provider's History is considered as another parameter since it includes the record of the past services provided by the provider to the customers.
- c) The variable parameter Data Location is used to provide details about the data located in sensitive sites.

A trust matrix can be generated with the variables represented along the axes.

- a) x axis represents the data cost.
- b) y axis represents the service provider's history.
- c) z axis represents the data location.

The trust matrix consists of areas representing the Low Risk/ High Trust Zone and High Risk/ Low Trust Zone. A common cloud computing scenario is considered with some past statistics from the service providers. Thus the trust has been measured and can be used for all the future transactions

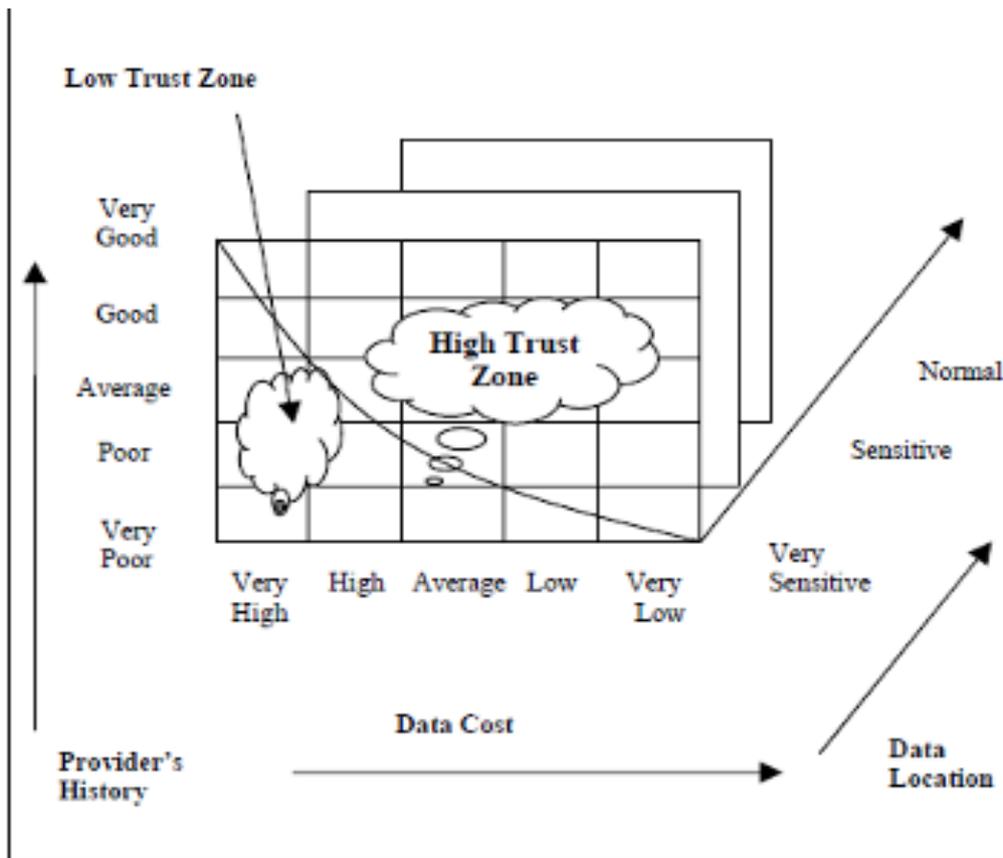


Figure: A Trust Matrix for Risk Analysis

Now, it is obvious that a high data cost with poor service provider history combining with a very sensitive location will result in a higher risk/lower trust.

High trust zone signifies the region of high trust. It can specify the security risk for the current transactions and also for future transactions with that service provider. Similarly, low trust zone signifies the region of low trust.

As a risk preventive approach, a *trust action* can be taken as part of a preventive or reactive measure. For example, an added level of authentication and/or verification can be used for the activities which are related to the low trust zone.