# Trust as a Service: A Framework for Trust Management in Cloud Environments

2012 Honours Project By Jeriel Jian En Law| Supervised By Dr. Michael Sheng and Mr Talal H Noor

## Project Aims

Among a growing trend of Internet technologies, cloud computing is a fast emerging computing paradigm that promises elasticity of resources like computational power and storage. In addition, it provides the flexibility and convenience for cloud consumers to utilize applications, platforms and infrastructure on the fly. While the use of cloud computing has many advantages, it also attracts many obstacles including trust [1]. How will a cloud consumer know which cloud service to trust their essential data? By definition of trust, it involves determining the credibility of trust feedbacks to aid in the identification of a trustworthy cloud service.

This project aims to create and implement a trust management framework[2] to counteract the problem of trust in a dynamic cloud environment. We seek to explore feasible solutions on various trust issues of handling malicious attacks, trust management availability and feedback credibility.

## Cloud-Armor

The TMS framework is implemented as a Web service known as Cloud Armor, designed to create a user-friendly cloud environment for cloud consumers (the users) as well as for cloud service providers. Cloud consumers can discover, add feedbacks and assess the trust level of cloud services in one of the links labelled 'trust assessment'. On the other hand, cloud service providers can advertise their cloud services in Cloud Armor to be evaluated and utilized by cloud consumers. We envisage the win-win benefits both parties stand to gain when they use Cloud Armor..

## Architecture of the Trust Management Service Framework

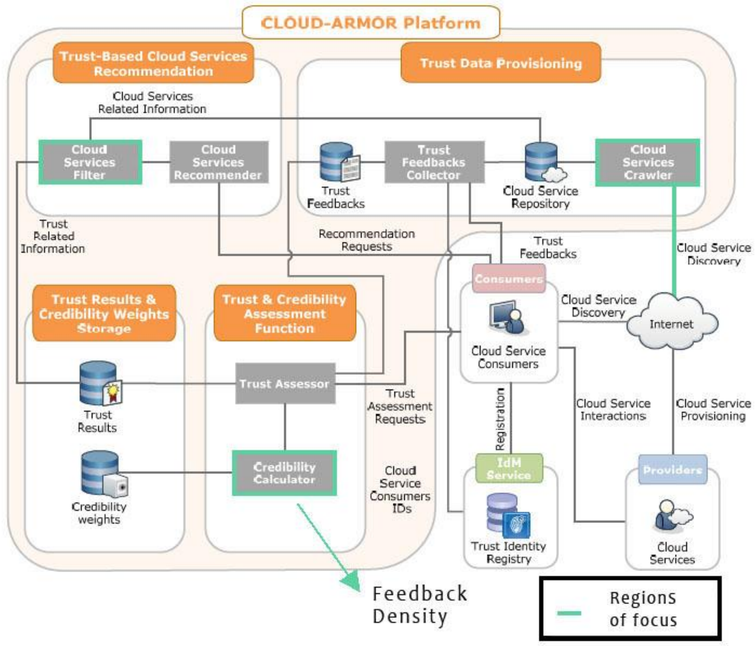
The main focus of the project consists of four parts, three of which have already been integrated into the framework.

1) *Cloud Services Crawler* module which automatically discovers cloud services on the Web.

2) *Cloud Services Filter* which distinguishes cloud services.

3) *Feedback Density Model*, one of several factors used to calculate the credibility of trust feedbacks.

4) *Availability Model*, which provides availability and dynamic distribution of work load among all TMS instances.




## Cloud Service Discovery and Filtering

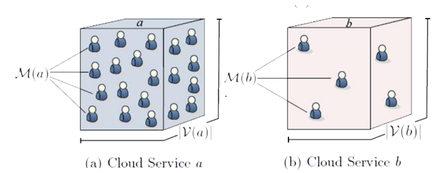
The cloud service discovery module finds cloud services automatically on the Web. It deploys a crawler, modified from an open source, java code named "crawler4j" (http://code.google.com/p/crawler4j/). Given a collection of seeds, it is capable of crawling thousands of webpages and downloading them into various formats like html, WSDL (Web Service Description Language), XML and WADL (Web Application Description Language). Subsequently, more cloud service information from the collected data are obtained, specifically the URL, ID, logo and description. After which, all information are stored in the *Cloud Services Repository*.

*Cloud Service Filtering* is carried out once information is ready from the repository. It is an iterative process, categorising a cloud service's home page based on well known cloud computing terms namely, software as a service (SaaS) , platform as a service (PaaS) and infrastructure as a service (IaaS). According to formal definitions, a cloud service is considered to be SaaS when it has keywords such as "application", "storage", PaaS when it has "library", "API" and IaaS when it has "infrastructure", "hosting".

A total of 5890 validated cloud services around the world are collected, out of 487360 links parsed by the *Cloud Services Crawler*.

## Feedback Density Model

The TMS uses the feedback density to detect whether a service is under a *self promoting attack*, which happens when a cloud consumer decides to add multiple feedbacks to a cloud service out of self-interest. Hence feedback density is required to calculate the credibility of a cloud service.




(a) Cloud Service $a$ (b) Cloud Service $b$

From the picture above, we can tell that the lesser the density of feedbacks is given to a cloud service, the lower the credibility. Therefore, cloud service *a* is more credible than cloud service *b*.

## Conclusion

Today, the rapid adoption of cloud services around the world has already given rise to a host of problems in trust and security. Given the urgent attention of the situation, we came up with a solution by producing the TMS framework.

The TMS has progressed into a complete implementation of a single instance, capable of executing operations on real data. The results will be shown during the demonstration.

## References

[1] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia. A view of cloud computing. Communications. ACM, 53(4):50-58, April 2010

[2] Credibility-based Trust Management for Services in Cloud Environments. Talal. H. Noor and Quan Z. Sheng. The 9th International Conference on Service Oriented Computing (ICSOC 2011). Paphos, Cyprus, December 5-8, 2011.