ISSN:2229-6093

G C Priya et al,Int.J.Computer Technology & Applications,Vol 3 (2), 691-695

A Trust, Privacy and Security Infrastructure for the Inter-Cloud

Ms. R. Parameswari [1], Ms.G.C.Priya [1] and Dr.N.Prabakaran [2]

1 Asst. Professors, Department. of Computer Applications, Saveetha Engineering College, Thandalam, Chennai, Tamil Nadu, India.

2 Senior Lecturer, Department. of Computer Applications, Rajalakshmi Engineering College, Thandalam, Chennai, Tamil Nadu, India.

{eswari.sai82, pri.gcbabu}@gmail.com and prabakaran_om@yahoo.com

Abstract-- Cloud Computing is one of the most important security challenges to manage and assure a secure usage over multi-provider Inter-Cloud environments [1] with dedicated communication infrastructures, security mechanisms, processes and policies. Based on the collection of various Inter-Cloud usecases and scenarios within the private and public sector like DMTF (Distributed Management Task Force), NIST (National Institute of Standards and Technology), GICTF (Global Inter- Cloud Technology Forum) and ENISA (European Network and Information Security Agency) we analyzed and summarized the range of requirements are trust and reputation management, sticky polices with fine grained access control, privacy preserving delegation of authority, federated identity and security management. The cloud service providers are then able to offer a reliable privacy preserving Infrastructure-as-a-Service to their clients.

Keywords: Cloud Computing, Trust, Privacy, Security, Inter-Cloud, Audit Service, Trust Negotiation, Delegation Service.

I. INTRODUCTION

The Cloud Computing is commonly known "as a Service" model [2,3], comprised of technological nodes that are coordinated analytically to perform services for user in the form of software, platform and infrastructure provided by Cloud Provider (CP). It follows "pay-by-use" model. The commonly accepted definition is from National Institute of Standards and Technology (NIST) that defines it as " Cloud computing is a pay-per-use model for enabling available, convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications,) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is comprised of five key characteristics, three delivery models, and four deployment models". Security concerns arising because both customer data and program are residing in Provider Premises.

Table 1: Common Security Requirements

GOAL	DESCRIPTION
CONFIDENTIALITY	Ensuring that information is not decided to unauthorized persons.
INTEGRITY	Ensuring that information held in a system is a proper representation of the information intended and that it has not been modified by an unauthorized person.
AVAILABILITY	Ensuring that the information processing resources are not made unavailable by malicious action.
NON – REPUDIATION	Ensuring that agreements made electronically can be proven to have been made.

Cloud computing offers dynamically scalable resources provisioned as a service over the Internet. The third-party, on-demand, pay-per-use and seamlessly scalable computing resources and services offered by the cloud paradigm promise to reduce capital as well as operational expenditures for hardware and software.

Cloud Service Providers show that this has been recognized and partially already adopted by cloud users [1]. As one consequence of this success, the number of cloud service providers offering cloud services increased so that cloud users now have a rich set of services to choose from. One way of categorizing clouds takes the physical location from the viewpoint of the user into account [3]. A ***Public Cloud*** is offered by third-party service providers and involves resources outside the user's premises. In case the cloud system is installed on the user's premise—usually in the own data center—this setup is called ***Private Cloud***. A hybrid approach (a combination of Private and Public Cloud) is denoted as ***Hybrid Cloud***. This paper will concentrate on Public Clouds, since these services demand for the highest security requirements but also this paper will start arguing which includes high potential for security prospects.

Another categorization depends on the type of resources or a service delivered by the cloud and distinguishes three distinct layers[3]. ***Infrastructure-as-a-Service*** **(IaaS)** is the name for cloud

environments that provide their users with basic infrastructure facilities including CPU, memory, and storage instances. These infrastructure components are operated and maintained by the IaaS provider. The most prominent examples of this type of cloud services are Amazon's Elastic Compute Cloud (EC2) [4], the aforementioned Amazon's Simple Storage Service (S3) [5], Savvis Symphony [6], and Rack Space Cloud [7]. ***Platform-as-a-Service*** **(PaaS)** describes a platform delivery model. Here, the cloud provider offers specific runtime environments to be used in the user's own application contexts. Examples would be providing database services or specific application runtime environments. On top of these platforms, the cloud user is able to implement and operate own applications. Hence, the PaaS provider is responsible for providing the hardware and the particular platform (including update management and bug fixing), and the cloud user is responsible for the specific implementations that use the given platform APIs. Examples for PaaS offerings are Google's App Engine [8] for Web application development, Microsoft SQL Azure [9] for databases, and Cloud scale for real-time data analysis tasks. ***Software-as-a-Service*** **(SaaS)** refers to the approach of providing a full software application most commonly via browser-based techniques. Here, the cloud provider is responsible for all parts of the application stack: hardware, operating system, application runtime, and the software implementation itself. The cloud users in this scenario are humans that interact with the cloud services via browser interfaces. Popular examples include Sales force for a Customer Relationship Management (CRM) system and the provisioning of office suites by Google and Zoho.

II. RELATED WORK

The Trusted Architecture for Securely Shared Services proposes to develop and implement architecture with trusted services to manage and process distributed personal information. This architecture will be dependable, robust but at the same time it is cost-effective and reliable. The personal information that will be processed and managed can consist of any type of information that is owned by or refers to people.

The proposed architecture therefore has to be generic and cross-domain applicable. The Trusted Architecture for Securely Shared Services will focus an instantiation of this architecture in the employability and e-health sector allowing users and service providers in these two sectors to manage the lifelong generated personal employability and e-health information of the individuals involved. The personal information includes the interests, current and previous activities, and future objectives, where the service providers will then be able to use these preferences to propose career paths that are compatible with the worker's objectives. For the last three years the EC TAS3 integrated project has been building a trust, privacy and security (TSP) infrastructure for web services. TAS3 has set out to provide an answer to the user-controlled, trusted sharing of personal information in a user-centric, demand-led services economy. A key task of the Demand-led Innovation is the promotion of dialogue between users and service providers. User-led innovation is promoted in traditional e-health sectors, in private and public services, and in sectors which generate new demand. The resulting TPS infrastructure is provided as a set of web services, so that cloud IaaS, PaaS and SaaS providers can build their own TPS applications or platforms. A cloud PaaS provider will add its own platform tools in addition to the TPS ones, even as a cloud SaaS provider will provide fully operational TPS enabled applications to its users.

III. TRUST NETWORK INFRASTRUCTURE SERVICES

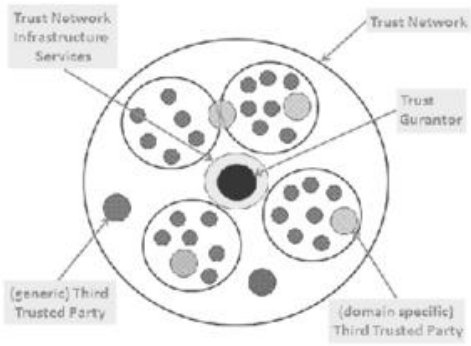

Figure 1: Trust Network Infrastructure

The Trust Network is a set of services called the Trust Network Infrastructure Services (TNIS) providing a core trust infrastructure supporting information exchange based on user control in the trust networks. The Trust Network is generally foreseen to be a public and nonexclusive entity: anyone, User, Service Provider, or even Trusted Third Party operator, willing to be certified can participate. Trust Networks may compete on issues such as cost, trust level, terms of use and even competence of members (i.e. specialists). That being said, TAS3 Trust Networks do not exclude the possibility to run private exclusive networks.

From that perspective a Trust Ecosystem (consisting of several Trust Networks) becomes

possible that are made up of component TN systems. This would allow some parties to seek and to develop private, closed or exclusive networks that are compatible with the TAS3 infrastructure but not subject to it. In itself this may enable some information transfers across providers that are both in public and private networks in order to service particular customer needs, but would not necessarily imply that such private providers were under the TAS3 Governance model or direct oversight

Trust Network participants will be subject to a general framework contract. This covers the overall rules of engagement for any user (end-user or service provider) of the Network and creates the needed relationships for obligations to be enforced against service providers. For these service providers, this general framework agreement is then supplemented with role and transaction based contracts, covering not only what is allowed within the Trust Network, but also how data acquired for specific purposes should be handled beyond the reach of the TNIS (Trust Network Infrastructure Services) monitoring Systems.

The trust guarantor is the technical operator of the trust network and its Trust Network Infrastructure Services (TNIS). Central to the operation of the network based trust infrastructure is the use of specific Trusted Third Parties (TTPs) for mechanical & legal validation of services (providers + requesters) and end users in the networks. The trusted third parties also interface with a higher level definition of trust metrics overseen by a top level Trust Guarantor. It is visualize that cross Trust Network communication will be enabled by co-operation between Trust Guarantors. This eventually will result in a Trust Ecosystem. The main Components of a Trust Network Technically the top level Trust Guarantor have a fundamental role in Introducing, Monitoring, and Auditing the end2end assurance of trust between the transacting parties.

IV. TRUST, SECURITY AND PRIVACY (TPS) INFRASTURCTURE

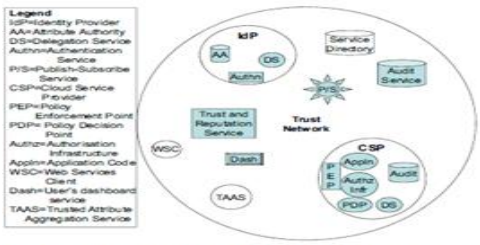

Figure 2: Components of the Cloud Trust, Security and Privacy Infrastructure

Each TPS infrastructure requires a trusted third party, the Trust Network Operator (TNO) to oversee its operation and ensure that all the required services are optional. In order to offer a TPS-enhanced service, a Cloud Service Provider (CSP) must "join the TN" by asking the TNO to perform a series of validation test to confirm that its TPS service is running correctly. The CSP then signs a contract with the TNO to say that it will honor users' privacy policies and provide the TN's audit service summary of all accesses to its users' personal information. It further agrees that in cases of disputes with its users, the TN auditor may inspect its detailed audit trails to determine the sequence of disputed events and make a judgment. The CSP then joins the trust networks, its services are entered in the TN's directory of services, and it publishes its terms and conditions to prospective users.

At the highest level, the high level policies and obligations are set forth in a Trust Network Management. The binding to polices, practices and technical requirements is supported by an intake process where the capacity of prospective CSP's to meet the requirements is evaluated. These concepts and governance structure are built with the objective of enhancing trust across a complex ecosystem of service providers that may not be in direct contact or even known to an individual using a particular CSP. It is not possible for individuals to control or comprehend the myriad options and delivery mechanisms of CSPs. This may not be the case where in individual has a defined service provided by a known provider, but cloud services are progressively including multiple service providers and multiple services creating a need to enable trust across the cloud ecosystem. Prospective users may search the TN's service directory to find candidate CSPs offering the services they require. The user's Web Services Client (WSC) may then enter into a trust negotiation session with each of the CSPs to determine the most suitable one to use without actually invoking a given CSP service. The purpose of trust negotiation is: to determine whether or not it and the CSP possess the required attributes (authorization credentials) in order to access the service (i.e to enable the WSC and the CSP to establish mutual trust); and in cases where both the WSC and the CSP do posses they require attributes/credentials, which subset of them, disclosed by the WSC to the CSP, is sufficient to grant access to the resource. After choosing the most suitable /trustworthy /cost effective CSP, and prepares to submit their personal and/or sensitive data to the cloud service. Users are entitled to set their own sticky privacy policies when they submit their policy remains with this data during its lifetime.

Furthermore the CSP will, at the user's request, ensure that a summary audit trail of accesses to this data is forwarded to the user as well as to the TN's audit service.

TAS3 provides a Federated Identity Management (FIM) infrastructure to ensure mutual authentication of WSCs and CSPs, based on the Liberty Alliance specifications, which are themselves based on SAMLv2. We have enhanced the Liberty Alliance Scheme in number of ways. Firstly we have introduced the Level of Assurance (LoA) concept based on the NIST scheme. This tell the CSP how strongly the user has been authenticated which allows the CSP to better control access to its resources by ensuring that the user has been authenticated strongly enough for the requested mode of access. We have introduced attribute aggregation into the FIM infrastructure through the introduction of a Trusted Attribute Aggregation Service which links users IdP accounts together. This allows the user to merge attributes from different IdPs into a single session with a CSP.

The secure publish subscribe infrastructure allows the distribution of summary audit messages and sticky policy updates though out the TN. Every CSP that receives a sticky policy must subscribe for updates and must publish summary audits. The user's dashboard, which records the user's interactions with the TN, contains an audit service to receive the summary audits, and sticky policy update service to publish changes to the user's sticky policy.

V. USERS TRUST PERCEPTION

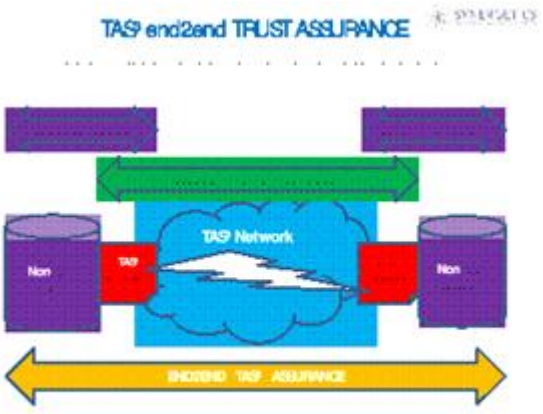

Figure 3: Trust Perception

Users should be able to join trust networks by agreeing the terms and conditions of use. The User can then allow his personal information to be shared within the network in order to become a part of distributed composite applications & services. It is the central focus of TAS3 that when users present their personal information to a TAS3 Trust Network, they can trust that it will not be used out of context of the terms that they agreed when joining the network and the policies set out for the actual transaction. The trust is based on the end2end assurance provided by the Trust Guarantor, and relies on a combination of technical monitoring and enforcement capabilities and legal contracts signed by all involved parties. More specifically, legal contracts extend the reach of enforcement beyond the TN perimeter and beyond the service providers' firewall. The perception of a TAS3 trust network, its' trust model works foremost on the user defining policies for their own personal information when joining a network and at the time of the transactional network decisions based on the users' information.

VI. CONCLUSION

A Trust, Privacy and Security Infrastructure for the Inter-Cloud initiated from a need for trusted sharing of personal information, thus Trust Networks arise from two angles: With the user as the ONLY 'lifelong' gamut within Trust Networks, the variety and scope of the TN is likely to be fitted around the users' health wealth and happiness. And second one, from a service providers perspective we see two orthogonal axis or attraction pools: regional development, interests & communality. We expect a bottom-up approach with smaller, local initiatives being used as reference cases and national governments overseeing the results and eventually building momentum for larger, possibly national roll-outs, where different trust networks can be interlinked into Trust Ecosystems. In fact the Trust Ecosystem level could be the goal of the TAS3 project guiding principles, standards & methods, promoting them to new candidate Trust Networks. It may also be the correct level to discuss cross-country issues. Security Management areas that describe all identified functional aspects. This set will serve as a foundation of our future development towards security management architecture for the Inter-Cloud.

REFERENCES

[1] D. Bernstein, E. Ludvigson, K. Sankar, S. Diamond and M. Morrow, Blueprint for the Inter Cloud - Protocols and formats for cloud Computing Interoperability, In Proceedings of the Fourth International Conference on Internet and Web Applications and

Services, 2009.
[2] J. Voas and J. Zhang, "Cloud Computing: New Wine or Just anew Bottle?," IT Professional, vol. 11, pp. 15-17, 2009.

[3] P. Mell and T. Grance, "The NIST Definition of Cloud Computing, Version 15," National Institute of Standards and Technology, Information Technology Laboratory, 2010.[Online]. Available: http://csrc.nist.gov/groups/ SNS /cloudcomputing/

[4] Amazon Web Services, "Amazon Elastic Compute Cloud (Amazon EC2)." [Online]. Available: http://aws.amazon.com / ec2/

[5] "Amazon Simple Storage Service (Amazon S3)." [Online]. Available: http://aws.amazon.com/s3/

[6] Savvis, "Savvis Symphony." [Online]. Available: http: //www.savvisknowscloud.com/services/

[7] RackSpace, "RackSpace Cloud." [Online]. Available: http: //www.rackspacecloud.com/index.php

[8] Google, "Google App Engine." [Online]. Available: https: //appengine.google.com

[9] Meiko Jensen, J¨org Schwenk, Jens-Matthias Bohli, Nils Gruschka, Luigi Lo Iacono "Security Prospects through Cloud Computing by Adopting Multiple Clouds" in proceeding of 4th International Conference on Cloud Computing, 2011, IEEE .

[10] David W Chadwick, Jerry I den Hartog, Andreas Pashalidis, Joseph Alhadeff, "My Private Cloud Overview" in proceeding of 4th International Conference on Cloud Computing, 2011, IEEE .