International Journal of Emerging Technologies in Engineering Research (IJETER)
Volume 4, Issue 3, March (2016) www.ijeter.everscience.org

Trust Management in Distributed Cloud Environment

V.JaganRaja
M.E Computer Science and Engineering (with Specialization in Networks),
The Kavery Engineering College, Mecheri.

P.Sathish Kumar
Head of department/Computer Science and Engineering, The Kavery Engineering College, Mecheri.

Dr.V.Venkatachalam
Principal, The Kavery Engineering College, Mecheri.

Abstract – Cloud is nascent and rapidly evolving model, with new aspects and capabilities being announced regularly. It is better to prevent security threats before they enter into the systems and there is no way how this can be prevented without knowing where they come from. Many existing trust mechanisms played a vital role and done their best in giving trust but even though still best is needed. So we done our best in this survey paper to examine risks, trust, trends and solutions to consider when using cloud computing in a mathematical way using Policy Based trust and some encryption techniques.

Index Terms – Cloud, Security, Threats, Encryption.

1. INTRODUCTION

Trust is a critical factor in cloud computing; in present practice it depends largely on perception of reputation, and self-assessment by providers of cloud services. We begin this paper with a survey of existing mechanisms for establishing trust. We can define trust in general Definition of trust a mental state with three elements:

- Expectancy: the trustor expects a specific behavior from the trustee.
- Belief: the trustor believes the expected behavior occurs based on the Evidence of trustee.
- Willingness to take risk: the trustor is willing to take risk for that belief

2. EXISTING TRUST MECHANISMS IN THE CLOUD

- Reputation based trust.
- SLA verification based trust.
- Cloud transparency mechanisms.
- Trust as a service.
- Formal accreditation, audit, and standards

Each of them is not enough by itself: only address one aspect of the problem.

2.1. Reputation based trust

Reputation based trust had idea to a score reflection the overall opinion; a small number of scores on several major aspects of performance. And it has a complexity of too many cloud providers and users. Reputation is helpful only when initially choosing a service, but not afterwards [1].

2.2. SLA verification based trust

It has an idea to verify and reevaluate the trust after establishing the initial trust. Service level agreement (SLA): legal contract between cloud users and service providers. SLA verification based trust has a constraints that cannot deal with “invisible” elements: security and privacy Cloud users cannot evaluate on their own, require professional third party (cloud broker, cloud trust authority).

2.3. Cloud transparency mechanisms

In Cloud transparency trust Cloud provider gives self-assessments and it has a disadvantage of dishonest service provider: filter out or change data.

2.4. Trust as a service

It Introduce third-party professionals (commercial trust brokers) , treat trust as a service (Cloud Trust Authority). Trust as a service Hard to establish basis for trust relation between cloud users and commercial trust brokers.[2]

2.5. Formal accreditation, audit and standards

This method has a trusted independent authority. Problem of Formal accreditation, audit and standards is Perfect idea, just does not exist. No formal process for assessment of cloud service by third parties.

2.6. Evidence-based trust

Idea of Evidence-based trust is to Use attributes as evidence to make trust decision (how to use semantics of trust to model trust in cloud).

How to define trust (in performance and or in believe $\mathrm{believe}(x,\mathrm{attr}_1(y,v_1)$^…$\mathrm{believe}(x, \mathrm{ttr}_n(s,v_n))\rightarrow \mathrm{trust}\__{*}(u,s,x,c)$.

- x: trustor ; y : trustee; x:information created by y ; c:a specific context.
- $_{*}$: either belief or performance.

- $attr_k(y,v_k)$: y has attribute k with value v $_k$

In Evidence-based trust how do define believe
trust_p(x,a,attr(y,v),c)^madeBy(attr y,v),a,c)^inContext(c)→believe(u, attr (s,v))

- y : trustee; x: trustor; c : a specific context ; a: attribute authority
- madeBy(attr (y,v),a;,c): a makes assertion that s have attribute with value v under c.
- trust_p(x,a, attr (y,v),c): as defined above.

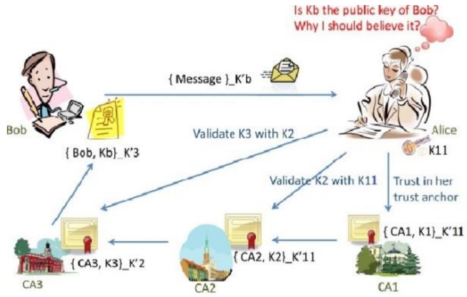
to define the attribute for evidence-based trust
Attributes for evidence-based trust (two dimensions)

- Domain-specific expectation: performance, security, privacy
- Sources of trust: competency, good intention, consistency

Different cloud users may consider different trust attributes. Relationship with policy-based trust: the belief that an entity conforms to a trusted policy implies the belief that the entity has a set of attributes associated with that policy.[4]

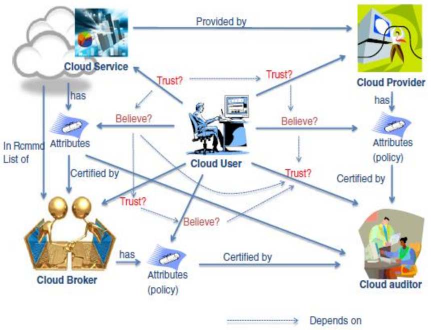
2.7. Policy Based Trust

Alice has a digital document supposedly signed by Bob using his private key K_b. To validate, she needs Bob's public key Kb. Assume that Alice trusts only her trust anchor certification authority CA1, and she knows only K11, her trust anchor's public key. In order for her to verify the signature on the document as being Bob's, she needs to discover a certification path (a chain of certificates) from CA1 to CA3 who has issued Bob's public key certificate.



As shown in above figure, Alice uses CA1's public key K11 to validate CA2's public key K2; because Alice trusts CA1 on public key certification, and CA2's public key is certified by CA1, Alice can believe that CA2's public key is K2; then Alice uses K2 to validate CA3' public key K3; and finally uses K3 to validate Bob's public key Kb. The main issue is why Alice should believe K3 is CA3's public key and Kb is Bob's public key? Essentially, to infer belief in a statement "Bob's key is Kb", Alice needs to trust CA3, the creator of that assertion, with respect to the truth of the statement; however, this raises questions that ask about the foundation of that trust, and how the trust is inferred or calculated. Some research suggests that the trust comes from recommendations along the chain of certificates by those certificate issuers [3]; but the practice of digital certification and validation in real PKI systems suggests that the trust comes from compliance with certain certificate policies.

Chains of trust relations in clouds.



The above figure illustrates some chains of trust focusing on policy-based attribute and evidence-based attribute mechanisms.

3. SUMMARY AND FURTHER RESEARCH

Cloud computing is growing rapidly according to recent strategy Iaas offerings are expected to grow at a CAGR of 31% through by year 2018.Enterprise public cloud spending is expected to reach $127 billion by the year 2018. We trust a system less if it gives us insufficient information about its expertise. Mere claims such as "secure cloud" or "trust me" don't help much to boost the trust level of consumers Establishing Trust in Cloud Computing unless sufficient information is presented with the services. The future research will based on Policy based trust mechanisms with best encryption algorithm in a mathematical way to give more Trust for the users.

REFERENCES

[1] Reputation-Based Trust Management _Vitaly Shmatikov and Carolyn Talcott Computer Science LaboratorySRI International Menlo Park, CA 94025 USA{shmat,clt}@csl.sri.com

[2] Trust as a service: a framework for trust Management in cloud environments Talal h. Noor and quan z.Sheng School of Computer Science,The Universityof Adelaide, Adelaide SA 5005, Australia {talal,qsheng}@cs.adelaide.edu.au

[3] Maurer UM (1996) Modelling a public-key infrastructure. In: In: ESORICS '96: Proceedings of the 4th European symposium on research incomputer security. Springer-Verlag, London, pp 325–350

[4] Trust mechanisms for clouding computing Jingwei . Huang David. M Nicol Information Trust Institute University of Ilinois at Urbana-Champaign presented by Ji Wang

[5] Establishing Trust in Cloud ComputingKhaled M. Khan and Qutaibah Malluhi, Qatar University