Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 50 (2015) 103 – 108

Procedia
Computer Science

2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)

An Extended Trust Management Scheme for Location Based Real-Time Service Composition in secure cloud computing

C.Bharathi[a], V.Vijayakumar[b], K. V. Pradeep[c]*

[a]*Research Scholar, VIT University, Vandalur – Kelambakkam Road, Chennai – 600048, India*
[b]*Professor, VIT University,Vandalur – Kelambakkam Road, Chennai – 600048, India*
[c]*Research Scholar, VIT University, Vandalur – Kelambakkam Road, Chennai – 600048, India*

Abstract

Available trust measures for cloud computing does not provide rigid control, which needs more enhanced security measures. We propose an extended trust management scheme which uses various attributes of the cloud computing environment. The trust computing performed with user profiles, and key based mechanism does not support the firewalls for successful operating and performance development. Here the location information of the user is used to avoid services from targeting by malicious users. It also uses a time variant hashing mechanism to compute secret keys for the legitimate users. On the scope of being secure the services from target attacks, we used a real time service composition approach, which combine necessary services according to the location of the user and other metrics.

Keywords: Cloud Security; Cloud Services; Trust Management.

1. Introduction

The increased growth of information technology makes everything as simple task in the computational world and the cloud computing is one of the recent emerging technology. Like grid computing, the cloud also intended to share resources among various users apart from locations. The loosely coupled nature of cloud environment

* Corresponding author. Tel.: +918056499193.
*E-mail address:*bharathi.c2013@vit.ac.in

doi:10.1016/j.procs.2015.04.068

makes the system more prone to different kind of malicious threats and access. In cloud platform the user identity could not be verified as easier than other platforms. There exist various layers of services which are offered by variety of service providers. Also the trustworthy of the users could not be maintained by the service providers, because anybody can register the trust cloud and access according to the trust scheme. The identity of the user who requests the service will not be known to the service provider, which will be maintained by the controller or a third party.

Trust management is the procedure presents in cloud computing where the identity and authenticity of the user who request the service access is verified. In order to access the data present in the cloud server, the requesting user must have rights and registered to the cloud. Only if the user is registered to the cloud and has rights to access, he will be able to access the data. In general cloud architecture the security enforcements are performed and handled by the third party auditor. The TPA maintains the security measures to control the access of cloud resources. The user could succeed the authentication process only if he present in the trust cloud.

General key based authentication mechanism has been implemented in various cloud security mechanism but suffers with different type of network attacks. The cloud security mechanism must be reliable and less time consuming. In key based authentication procedure the computation of keys and verification procedure takes more time when the number of users goes in millions. So that the security mechanism must be less time consuming one to support higher throughput of the system.The location details of the user could be used as one of the supporting factor in improving the performance of the cloud environment. The same set of service may be deployed at different locations and has to be fetched according to the location of the user where the location identification has to be done. Once the trustworthy of the user is verified then the location information can be used to select and compose the required services at runtime.

2. Background:

A Tabu Search Algorithm for the Location of Data centers and Software Components in Green Cloud Computing Networks [1], presents a planning problem and an extremely efficient tabu search heuristic to optimize the cloud data centers locations and components of the software while concurrently discovering the routing information and capacities of the network link. The objectives are to optimize the operational expenditures (OPEX), the capital expenditures (CAPEX), the CO2 emissions and the network performance. The problem is modelled using a mixed-integer programming model and solved with both an optimization solver and a tabu search heuristic.

Virtual Data Center Embedding across Distributed Infrastructures [2], is proposed to maximize the cloud provider's revenue while ensuring that the infrastructure is as environment-friendly as possible. To evaluate the effectiveness of the proposal, extensive simulations of four data centers connected through the NSFNet topology is conducted.

Modeling and Analysis of State-of-the-art VM-based Cloud Management Platforms [3], provide analysis, modeling, and three open source verification of state-of-the-art in VM-based cloud platforms: (a) Nimbus, (b) Eucalyptus, and (c) Open Nebula. To model and analyze the structural and the behavioral properties of systems, High-Level Petri Nets (HLPN) is used. Furthermore, Z3 Solver and Satisfiability Modulo Theories Library (SMT-Lib) are used to verify the models. 100 VMs are modelled to verify the feasibility and correctness of the simulations.

On the Characterization of the Structural Robustness of Data Center Networks [4], analyse the state-of-the-art DCNs robustness. Multi-layered graph modeling of several DCNs is presented and the classical robustness metrics is studied by considering the different failure scenarios for the performance of comparative analysis. The inadequacy of classical network robustness metrics is presented to properly evaluate the robustness of DCN and innovative procedures are proposed to quantify the robustness of DCN.

3. Proposed Method:

The proposed trust management scheme has four stages namely: Multi-Attribute Hashing function, Real-time service composition, Location Based service selection and extended trust management scheme. We discuss each of the functional stages in the coming chapters.

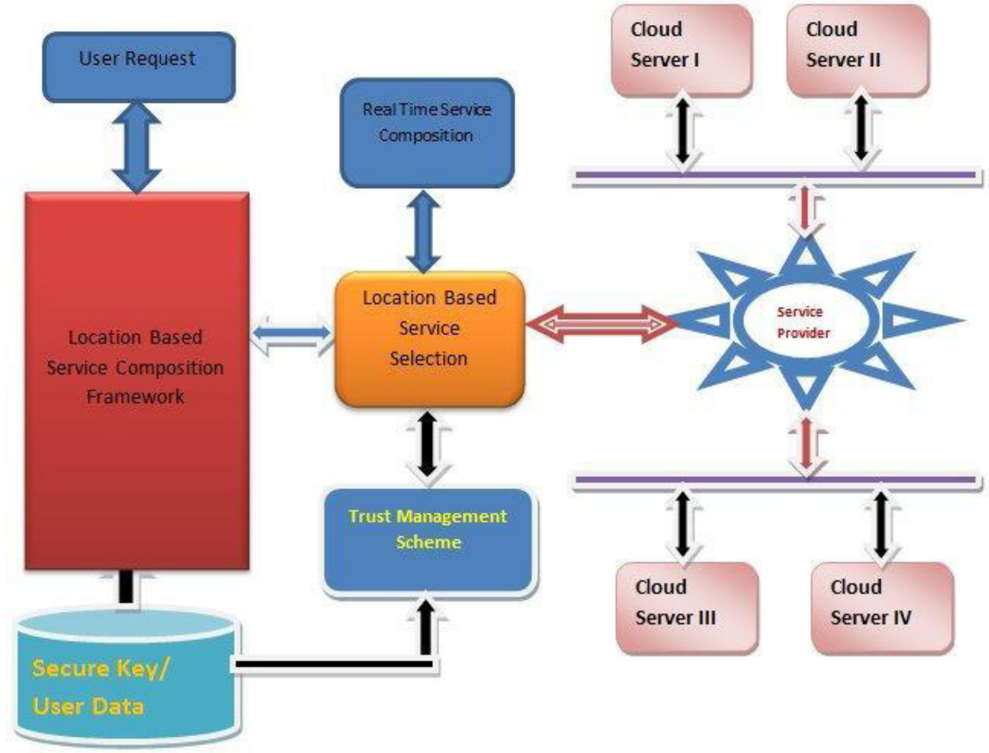

Fig. 1. Proposed architecture

3.1 Multi-Attribute Hashing Function:

The multi attribute hashing function uses various parameters to compute the key for distinct user. The cloud authority generates secret key for each registered user and distributes them to the user which will be verified at the time of access. For a user U_i, registered from location L_i, with access grade G_i, the secret key sk will be computed as follows

```
Key Generation Hash Function:
Input: User U, Locations L.
Output: Secret key sk.
Compute Nu = Number of user from location L.
          Nu = $\Omega(U \times L)$.
          Generate Random Number R.
                    R= Rand×(Size (S)).
          Scheme SS = S(R).
                    Create SecretKeysk.
                    Initialize sk= zeros(8).// 8 bit integer.
                                        // First 2 bit- for user no
                                        //$2^{nd}$ 2 bit for cloud id
                    // $3^{rd}$ 2bit for service id-
                    // last two bit is location no

                User number un  =         $\int_1^{Ur} Rand \times pol(1,Ur)$

                Compute cloud id cid  =   $\int_1^{C} C \times Ser(1,Ci)$

                Compute service id Sid =  $\int_1^{S} Ser \times C(1,S)$

    Construct sk = {Un,Cid,Sid,L}.
Return Sk.
```

3.2 Signature Verification:

The signatureverification is performed as reverse to the key generation mechanism. The received key is computed with the size and then manipulated accordingly. We extract the field values of user number, trust cloud id, service id and user location.

```
Signature Verification
Mechanism: Input:sk
Output: Boolean
Read Input key sk.
Read secret key base Kb from data base Db.
    D = compute size of sk.
    If D==8 then
        Split sk into 2bit segment.
        User number Un = sk(0-2).
        Trust cloud id Tid= sk(3-4).
        Service id Sid= sk(5-6).
        Location L= sk(7-8).
    Match all the parameters with the key from key
    base. For each $kb_i$ from Kb
        Compute Un,Tid,Sid,L = $\int kb_i$(Un,Tid,Sid,L).
        If($Kb_i$(Un,Tid,Sid,L)== Un.Tid.Sid.L)
            True;
        End
    End.
Return bool.
```

3.3 Trust Management:

The trustworthy of each user in the cloud is maintained using the trust management scheme where the trustworthy of different users are computed in different way. The registered internal users are verified using public and private keys whereas the normal customers are verified using the provided secret key sk. Upon receiving the request from the user his identity is verified using the signature verification process and the access history of the user will be taken into account for his behaviour analysis. We compute the behaviour metric which shows the genunity of the user on accessing the cloud service. It is compute using the access details and malformed behaviour details.

3.4 Real time service Composition:

From set of services available particular set of services will be selected based on the frequency of successful access and number of times being accessed at each time frame. We compute the successful frequency of access and based on the frequency value we select set of services and compose them based on location information.

4. Result Discussion:

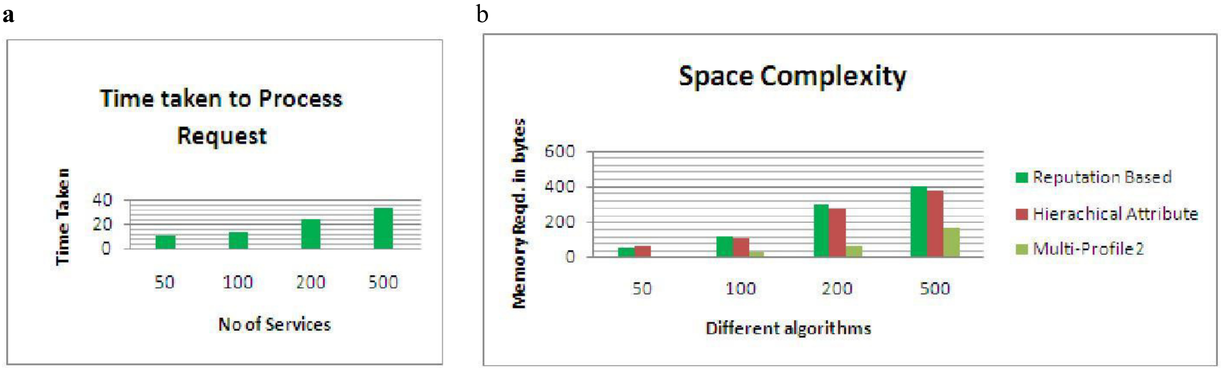

Fig. 2. (a) Graph1 time taken to process the user request between numbers of services (b) Space complexity graph of proposed system

Table1: Comparison and Computation Complexity

Operation	HASBE	Proposed
System setup	O(2N)	O(N)
Key verification	O(2N+M)	O(N)
User Revocation	O(1)	O(1/N)

Table 1 shows the comparison result of computation complexity between two algorithms. The Hasbe algorithm takes O(2N) time for set up where N is the no. of attributes used, whereas this methodology takes N only. Key verification and user revocation process time also much lesser than the earlier HASBE algorithm.

5. Conclusion:

The proposed trust management scheme has used various parameters for secure cloud computing. The hashing function has used all the parameters like user id, cloud id, service id and location information. The compute key is only 8 bit and reduces the overhead of generation and verification of secret keys. We also used the access history of services and user, based on which a service is selected and trust computing is done. The proposed method has produced higher efficient results than previous methods.

References

1. Federico Larumbe, A Tabu Search Algorithm for the Location of Data Centers and Software Components in Green Cloud Computing Networks, IEEE Transaction on Cloud Computing, Vol: 1, Issue 1, 2013.

2. Amokrane A, Greenhead: Virtual Data Center Embedding across Distributed Infrastructures, Ieee Transaction on cloud computing , vol:1 issue 1, pp:36-49, 2013.

3. Malik S.U.R , Modeling and Analysis of State-of-the-art VM-based Cloud Management Platforms, IEEE Transaction on cloud computing, vol1. Issue1, pp:1, 2013.

4. Bilal K, On the Characterization of the Structural Robustness of Data Center Networks, IEEE Transaction on Cloud Computing, Vol:1, Issue 1, PP: 1, 2013.

5. XinYu Lei, Outsourcing Large Matrix Inversion Computation to A Public Cloud, IEEE Transaction on Cloud Computing, vol 1, issue 1, pp :1 , 2013.