Trust Managemement Parameters in Cloud Computing Environments

Zafeiroula Georgiopoulou
Department of Digital Systems,
University of Piraeus
Piraeus, Athens
e-mail: roulageorgio@ssl-unipi.gr

Costas Lambrinoudakis
Department of Digital Systems,
University of Piraeus
Piraeus, Athens
e-mail: clam@unipi.gr

Abstract— In cloud computing environments, successful trust management can compensate the countermeasures that have been adopted for mitigating the security and privacy risks that the cloud comes across. This paper identifies the parameters that a trust model should include. These parameters are presented together with a detailed analysis of how, each of them, could be applied/utilized by the trust model for quantifying the trust of the cloud providers to their users.

Keywords- Cloud Computing; Trust; Trust Managemen;' Trust Models; Privacy; Trust metric

I. INTRODUCTION

Cloud computing is a technology that has emerged in all aspects of modern Information Technology infrastructure providing comparative advantages to organizations. However, this deployment and cloud tenancy create major security concerns and loss of trust that mainly comes with the loss of physical perimeter control. During the previous years, several scientists have addressed the issue of proper trust management [1].

A fine-tuned trust management would be a very good countermeasure for many security and privacy risks in cloud environments. The main reason for such a conclusion is that having in place proper trust management mechanisms, users can select providers based on their requirements and trustworthiness and, at the same time, providers can reject or accept users based on how trustful they are.

The novelty of the trust management model proposed in this paper is that it allows cloud providers to monitor in real-time the users of their services. Based on our previous literature review research [1], we propose a list of trust parameters, together with an in depth description of how trust management can be applied per parameter. Furthermore, the proposed model includes a trust metric that will be capitalized for quantifying trust [3].

The structure of the paper is as follows: The next section defines the trust modeling parameters that should be considered for facilitating proper trust management of the users by the cloud providers. Section III explains how the aforementioned trust parameters could be combined in order to produce the "trust metric" that will quantify the trust of cloud providers to their users. The last section concludes the paper and provides pointers for future work.

II. TRUST PARAMETERS

Defining the correct trust parameters is a key point for successful trust management. They should take into account all the aspects and factors of a cloud architecture that could affect trust. The proposed list of trust parameters follows next.

A. Trusted Access Points

A user typically connects to the cloud from a pre-defined range of devices. By device we mean any electronic device that a cloud user could employ for accessing cloud services (Laptops, desktops, mobile phones, tablets, etc.). The range of devices that have been already used for connecting to the cloud, and thus fulfill the security policy criteria of the provider, will be referred as "Trusted Access Points".

A trust security policy should take into account the access point and extra attention should be paid in the case of new devices. In favor of "Trusted Access Points", a table with the principal characteristics per device, as listed next, should be maintained in a central repository within the perimeter of the cloud provider.

a) User ID: Uniquely identifies every user in the cloud.

b) Unique Device ID: Uniquely identifies each device that a client is utilizing to access the cloud. This unique identifier is the result of a salted encrypted combination of the Device Type and its MAC address.

c) Type: Categorization of device (Mobile, Laptop, Desktop, Tablet etc.)

d) Operating System: The device's operating system will be stored since it affects the security parameters. For instance, an Android device is considered less safe from a Windows Server device.

e) Date of Last Connection: Information on the date and time that a specific device accessed the cloud.

All the above will be maintained from a "Trusted Access Point Agent", which will monitor the devices employed by each user.

Every time that a user requires to access the cloud an identification / authorization process will be invoked specifically for the purposes of the "Trusted Access Point". The identification part aims to verify if the user's device has been already whitelisted, by checking a central repository named "Trusted Access Points". If the user attempts to

 ISBN: 978-1-61208-529-6

access the cloud with an unknown device, a security flag will be raised, initiating a process that will check whether the specific device can be included in the Trusted Access Points repository or not.

The unknown devices must be identified and should fulfill the security policy's minimum requirements. For instance, mobile devices can be prohibited from the security policy [4].

B. Location

Determining the geo-location of a device is the process of defining, in a precise manner, the latitude/longitude coordinates of the device together with some other characteristics like country, city, address, zip code and time zone. Based on Isaca's definitions [5], Geolocation data are generated and collected either in an active mode, referred as user-device-based geolocation, or in a passive mode, referred as table look-up or data correlation server-based geolocation. Table 1 [5] summarizes these modes and the technologies that each mode employs.

TABLE I. MODES OF GEOLOCATION DATA GENERATION AND COLLECTION

Mode	Collection Method	Technologies Involved
Active: User—Device-based	• Uses firmware and software on user's computer or wireless device • Location determined via GPS chip and/or triangulation using cellular tower information • Request-response model	• GPS • Assisted GPS (A-GPS) •Wi-Fi—Wireless positioning • 3G/4G •Mobile applications—iPhone, Android devices, BlackBerry®
Passive: Data-lookup—Sever-based	Involves use of third-party geolocation service providers, e.g., Quova®, NetGeo,Bering Media • Based on nonlocation-specific IP address acquired from user device or service set identifiers (SSIDs) for wireless networks • Correlation with stored IP or SSID databases obtained from purchase records, user-provided information, network analysis of trace routes and domain name system (DNS) host names	• IP location—Whois lookup, DNS LOC, geographic names in domain name user or application information, timing data using ping inference based on routing data, e.g., traceroute monitoring of Internet service provider (ISP) networks • 3G/4G •Wi-Fi—Wireless positioning

A far as privacy issues are concerned, the proposed model will need the IP Geolocation. Assuming that an accurate method for retrieving the location of a cloud client exists, we will consider how this affects the trustfulness of the client, justifying the fact that a trust security policy should take into account geolocation information [5]-[8].

A user usually accesses the cloud from specific locations. This range of locations will be referred as "Trusted Geolocation Coordinates". To maintain this information, the main characteristics of each user location, as listed next, will be recorded in a central repository within the perimeter of the cloud provider.

a) *User ID: Uniquely identifies every user in the cloud*
b) *Location: Latitude and longitude coordinates of each user location*
c) *IP address: The IP address that the user is utilizing to access the cloud*
d) *City: The City from which the user is accessing the cloud*
e) *Zip: The Zip code of the user's access location*
f) *Time Zone: The Time Zone of the user's location*
g) *Last Access: Information about the date and the time that a user accessed the cloud for the last time form a specific location.*

All the above will be maintained from the "Location Agent". Then, an allowed zone of latitude/longitude coordinates will be defined that a user could be pinpointed. This zone comes from the combination of coordinates and an acceptable distance that has been specified at the initial configuration of the model. Every time a user accesses the cloud an identification and authorization method regarding geolocation characteristics is initiated. The identification process checks a central repository named "Trusted Geolocation Coordinates", in order to verify if the user has been allowed before to access the cloud from the same location and its allowed perimeter. If the user is trying to access the cloud from an unknown location a security flag is raised until a decision of whether that location should, or should not, be included in the list of trusted locations is reached. Clearly, the Location Agent should invoke mechanisms against IP spoofing.

C. Behavior

In all types of systems (cloud and conventional), a user follows a similar pattern of actions (behavior). In other words, the behavior of a user is expected to be similar within different sessions [1] [10].

A trust security policy should take into account the behavior characteristics of its users. More specifically it is necessary to monitor the data that a user is typically accessing and to consider cases of abnormal behavior. The typical user behavior, in terms of the data that he is accessing and the actions that he is performing, will be referred as "Trusted Behavior". In order to monitor the behavior of a user the cloud provider should monitor the following information.

a) *User ID: Uniquely identifies every user in the cloud.*
b) *Application Unit: During the initialization of the proposed model, the cloud resources are logically separated in isolated application units.*
c) *Authorization granted: Boolean value of whether the user has the appropriate rights to access the specific application unit.*

 ISBN: 978-1-61208-529-6

d) *Type of action: Monitors the user actions; i.e. the user tried to view, write, update or delete information.*

e) *Last Action: Information about the date and the time that a user performed a specific action.*

The audit trail for data access, maintained in the "Trust Behavior Table", will be aggregated by the Trust Behavior Agent. Indicative overall aggregated values follow:

a) *The average number of accesses to each data category.*

b) *The average user throughput (bandwidth for upload and download).*

c) *Volume of data transfers from CSP to the user.*

d) *Volume of data transfers from the user to CSP.*

e) *Average duration of user access.*

f) *Unauthorized modification or view access endeavors.*

The thresholds related to data access should be clearly defined. As a minimum, one threshold for every aggregated value is needed. The Trust Behavior Agent will monitor all users' data accesses and if any of the aforementioned thresholds has been violated a security warning will be raised from the agent. A relevant algorithm will process the information and will decide if the specific user should be excluded from the trusted data access behavior or not.

D. Resources

A cloud user typically consumes specific resources while using the cloud. By Resources we refer to network and hardware components that the user consumes while connected to cloud. The various resources utilized by a user during a specific session will be monitored and will be referred as "Trusted Resources".

The trust security policy of the proposed model will take into account the resources consumed by a user and in case of excessive use a security warning will be issued. In order to maintain a "Trusted Resources" table, the following information will be traced:

a) *User ID: Uniquely identifies every user in the cloud.*

b) *Unique Device ID: Uniquely identifies each device that a client is utilizing. Maintained in the Trusted Access Point table.*

c) *Session Length: The total session time.*

d) *Bandwidth: Bandwidth of cloud network used.*

e) *Device Memory: Device memory used; depicted as percentage of the total device memory.*

f) *Cloud Memory: Cloud memory used; depicted as percentage of the total cloud memory.*

g) *CPU Threads: CPU usage on user's device.*

h) *Network Ports: List of ports that the user it utilizing on the cloud.*

i) *Volume of data sent: Number of bytes sent by the user during the current session.*

j) *Volume of data received: Number of bytes received by the user during the current session.*

The above information will be maintained by a Trust Resource Agent. Thresholds, regarding the resource limits, are necessary. During each session the Trust Resource Agent will monitor the consumption of cloud resources and in case that the thresholds are violated a security warning will be issued.

E. Authentication

Another major parameter of the proposed trust model is the authentication behavior of the cloud user. To this end, the following information will be monitored:

a) *User ID : Uniquely identifies every user in the cloud.*

b) *Unsuccessful Logins: Number of times that the user tried to access the cloud services without success.*

c) *Token Used: Metric regarding the security of the tokens used*

d) *Wrong authentication method: In cloud environments that support multiple authentication methods the endeavor to use the wrong method should be monitored.*

The above information will be processed by a "Trust Authentication Agent". A trust authentication value per user will be calculated/updated, based on pre-defined values, during every authentication process. When the value for a user falls below a specific threshold, he will not be considered a trusted user any more. Log in will be banned and further procedures will be required in order to reestablish trust.

F. Feedbacks

In cases of outsourcing, feedback on consumers who had transactions with other service providers is required. Specifying a common feedback trust metric, regarding trustfulness, between providers, will facilitate the consideration of this information. To this end a "Feedback Trust Table", should be maintained in a central repository within the perimeter of the cloud provider:

a) *User ID : Uniquely identifies every user in the cloud.*

b) *Unsuccessful Logins: Number of times that the user tried to access the cloud services without success.*

c) *Token Used: Metric regarding the security of the tokens used*

d) *Wrong authentication method: In cloud environments that support multiple authentication method the endeavor to use wrong method should be monitored.*

The above information will be processed by a "Provider's Feedback Agent". Every time a user endeavors to access the cloud, the agent will search the relevant table for feedbacks. If the overall feedback value is below a threshold, the user will not be considered trusted and relevant actions should be taken.

 ISBN: 978-1-61208-529-6

G. Access Point Security

Since trust management is part of the security policy, it is evident that the security of the access point – user's computer, phone tablet, etc. – should be taken into account as an important parameter in the trust metric. To this respect, a Security Evidence collector should be available on the provider's side and assuming that the user gives his consent, the agent will collect information regarding the user's device security. The most important items that should be checked are the following:

a) Use of antivirus
b) Use of firewall
c) Operating System's Updates and Patches are installed
d) List of Software installed

Based on the collected data, an access point security value will be assigned to every user's device. If the security value for a user device is below some threshold, it will not be allowed to enter the cloud.

III. TRUST METRIC

The definition of a Trust Metric facilitates the quantification of the degree to which a cloud user can be trusted by a cloud provider and it is necessary to establish trust between the two entities. A simple way to implement this trust metric could be the use of a binary discrete model where the trust values are set 'high', for a highly trusted entity, or 'low' for an untrusted entity.

In order to measure trust with the proposed model, a metric that will quantify, in a general manner, the trustfulness of each user is necessary. The range of trust values (TV) is set to be between 0 to 10; 0 being the minimum trust value and 10 the maximum. Furthermore, the proposed trust metric will employ a weighting factor for every of the aforementioned trust parameters. The weighting factors will represent the importance of each trust parameter and are:

- WAP : Weighting of Trusted Access Point
- WL : Weighting of Geo-location characteristics
- WDA : Weighting of Data Access
- WR : Weighting of Resources
- WA : Weighting of Authentication
- WF : Weighting of Feedback
- WAS: Weighting of Access Point Security
- WFP1…N : Weighting of future parameters

Weights will take values between 0 to 1. The proposed Trust Metric will be:

$$T_{AP}*W_{AP} + T_L*W_L + T_{DA}*W_{DA} + T_R*W_R + T_A*W_A + T_F*W_F + T_{AS}*W_{AS} + T_{FP1}*W_{FP1} + T_{FP2}*W_{FP2} + \ldots\ldots + T_{FPn}*W_{FPn}$$

IV. CONCLUSIONS & FUTURE WORK

Cloud Computing is a widely accepted technology but it raises a lot of security issues. The goal of our work is to improve the current status by applying proper trust management methods and surpass security risks. In this paper the trust parameters that a cloud trust model should take into account are presented together with an analysis of how these parameters can be monitored. Furthermore, the need for a trust metric, that will quantify the trust of the cloud provider to the user, has been highlighted.

For the future, we aim to provide an overall simulation of the proposed trust model, presenting experimental results from measurements of the trust parameters and the way they are used to calculate the trust metric.

ACKNOWLEDGMENT

This work has been partially supported by the Research Center of the University of Piraeus.

REFERENCES

[1] L. Wenjuan, P. Lingdi, and P. Xuezeng, "Use trust management module to achieve effective security mechanisms in cloud environment," in International Conference on Electronics and Information Engineering (ICEIE), vol. 1, Kyoto, Japan, 2010, pp. 14-19.

[2] Z. Georgiopoulou, C. Lambrinoudakis,"Literature Review of Trust Models for Cloud Computing", International Conference On Cloud Computing And Big Data (CloudCom-Asia), Hong Kong, 2016.

[3] P. D. Manuel, T. Selve, and M. I. Abd-EI Barr, "Trust management system for grid and cloud resources" in First International Conference on Advanced Computing (ICAC 2009), Chennai, India, 2009, pp. 176-181.

[4] Y. Zhimin, Q. Lixiang, L. Chang, Y. Chi, and W. Guangming, "A Collaborative Trust Model of Firewall-through based on Computing" in 14th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Shanghai, China, 2010, pp. 329 - 334.

[5] Geolocation: Risk, Issues and Strategies, ISACA, Geolocation: Risk, Issues and Strategies

[6] B. Tang , R. Sandhu, "Cross-Tenant Trust Models in Cloud Computing", Information Reuse and Integration (IRI), 2013 IEEE 14th International Conference on 14-16 Aug. 2013.

[7] B. Eriksson, P. Barford, J. Sommersy, and Robert Nowak, "A Learning-based Approach for IP Geolocation NIST Interagency Report 7904, December 2012

[8] E. K. Banks, M. Bartock, K. Fiftal, D. Lemon, K, Scarfone, U. Shetty et al., "Trusted Geolocation in the Cloud: Proof of Concept Implementation", International Journal of Computer Science and Information Technologies, Vol. 3 (2) , 2012, 3328 – 3333.

[9] B. K. Dewangan1, P. Shende2, "The Sliding Window Method: An Environment To Evaluate User Behavior Trust In Cloud Technology", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 2, February 2013.

[10] T. Li-qin, L. Chuang "Evaluation of User Behavior Trust in Cloud Computing" 2010 International Conference on Computer Application and System Modeling (ICCASM 2010)

 ISBN: 978-1-61208-529-6