Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 45 (2015) 380 – 389

Procedia Computer Science

International Conference on Advanced Computing Technologies and Applications (ICACTA-2015)

Trust Model for Measuring Security Strength of Cloud Computing Service

Rizwana Shaikh[a], Dr. M. Sasikumar[b]

[a]*Assistant Professor, SIES Graduate School of Technology, Nerul. Navi Mumabi,India*
[b]*Associate Director, CDAC Kharghar, Navi Mumabi, India*

Abstract

Cloud computing has become a part of the competitive market today. Various cloud computing service providers are available with their services in the cloud environment. Techniques adopted by various providers to achieve security are of varying nature. To analyze and measure a particular service based on its security properties is a challenge. This paper presents such a measurement by using a trust model. A trust model measures the security strength and computes a trust value. A trust value comprises of various parameters that are necessary dimensions along which security of cloud services can be measured. CSA (Cloud Service Alliance) service challenges are used to assess security of a service and validity of the model. Adequacy of the model is also verified by evaluating trust value for existing cloud services. Trust model acts as a benchmark and ranking service to measure security in a cloud computing environment.

Peer-review under responsibility of scientific committee of International Conference on Advanced Computing Technologies and Applications (ICACTA-2015).

Keywords: Cloud Computing; Trust; Trust model; Security;

1. Introduction

Cloud computing has captured significant portion of the competitive market today. Many organizations make use of cloud services. Although cloud computing services is growing and gaining popularity, the fear about the usage of cloud services is still an open issue. Various issues deterring adoption are identified in the literature; one of the major issues is security. Security risks in the area of cloud computing has attracted attention since its beginning. New protocols and tools are always in demand to enhance and assess the security strength of a cloud computing service or service provider.

Corresponding author. Dr. M. Sasikumar
E-mail address: the.little.sasi@gmail.com

Peer-review under responsibility of scientific committee of International Conference on Advanced Computing Technologies and Applications (ICACTA-2015).
doi:10.1016/j.procs.2015.03.165

Security of a cloud service should cover many aspects like authentication, authorization data protection etc. These are the basic security goals which constitute principles of security and become crucial while moving towards the cloud. Therefore a tool that assesse and evaluates these security concerns with respect to cloud services before selection is the necessity in the cloud environment. Our focus here is on a framework for such an evaluation of service security in a cloud environment. Here we propose a trust model that is used to evaluate cloud service security strength. It consists of a trust value that is overall security strength of the cloud service. Trust value can be evaluated by a list of parameters that covers almost all relevant aspects of security. A trust based evaluation is formulated to evaluate trust value. A list of such parameters is identified. Cloud service features and specifications are used to evaluate the trust value and termed as static trust. Value of trust is affected, based on user experience and transactions over a period of time. A refined set of parameters are formulated to evaluate the trust dynamically. Static and dynamic trust altogether determines security of the cloud services.

Thus trust model acts as a security strength evaluator and ranking service for cloud application and services. It can be used as a benchmark to setup the cloud service security and to find the shortcomings and improvements in cloud infrastructure. The rest of the paper is organized as follows. Section two covers literature survey where solutions from the literature are analyzed. Section 3 deals with the proposed trust framework with the trust model. Model is detailed with the different parameters in this section. Section4 describes extending this model into a dynamic trust model with a set of dynamic parameters. Section 5 discusses incorporating the model in cloud computing environment. Accuracy and validity of the trust model is analyzed in Section 6. Finally conclusion and future scope as section 7 ends the paper.

2. Literature Review

Security issues and trust in the area of cloud computing is active area of research. Trust evaluated by Jingwei H. et al in [1] is based on evidences and subjective logic and is used to evaluate security breaches based on the historical data. A framework for secure application execution is proposed by the authors Satyjeet N et al in [2]. It provides modified hypervisor that secures the processor architecture, thereby making secure execution environment. Trust model for data security in private cloud is proposed in [3] by Edna D. et al. Authors make use of recommendations and interactions records of past transactions to calculate the trust. Trust based approach is applied using trusted computing at IaaS level by Hamid Banirostam et al in [4]. Secure use of virtual machines is provided to provide confidentiality and accuracy in IaaS cloud. Trust management framework is proposed by Monoj Kumar M. et al in [5], which makes use of feedback and credibility to calculate trust value. Hyukho K. et al in [8] present a trust model where trust calculations are made to achieve reliability of the resources. A collaborative trust model for Cloud Environment is proposed by Zhimin Yang et al in [9]. Trust model is compatible with firewall without affecting its performance. A protocol to establish trust and confidentiality while accessing data is proposed by Mahbub Ahmad et al in [10]. User behavior trust evaluation based on time, abnormal degree of behavior and access times is discussed by Tian L. et al in [11]. Trust management system for ubiquitous computing is proposed by Azzedine B et al [12]. Trust values are used for providing secure access for well-behaved nodes in the communication. Trust for data storage for cloud computing is proposed by Barsoum A. et al in [13]. User control for the data access and modification are the key contributions.

Data access control mechanism is also proposed by Kan Yang et al in [14]. It is efficient in terms of access cost but with weak security considerations. Evaluation of security metrics based on SLA is studied by the authors in [15]. A questionnaire based approach is selected as the best one to evaluate the security. A detailed survey about the security and trust in various collaborative environments is discussed in [16]. Calculating cloud security by estimating parameters and functions is the proposed outcome of the survey. Various approaches for security and its quantification measure are proposed in the literature. CSA security guidance [17] provides list of areas for analyzing and evaluating the cloud services. It provides the various factors to be considered for determining risk before moving on to the cloud.

We have studied and identified that a model to incorporate all aspects of security quantification measure for cloud computing application and service is still the necessity. Here we present a trust model that incorporates various security challenges and can be used to evaluate the security strength of the service.

3. Trust Model –TM

Evaluating a cloud service security is the necessity for any organization moving towards the cloud. We have identified a comprehensive list of security parameters that are necessary and sufficient to measure security with respect to cloud computing environment. These parameters are incorporated in our trust model and a trust value is the outcome. Trust value can be a single value giving the notion of overall security of a cloud service. It can also be broken down to various aspects of security based on the parameters and represented as a vector. A user can select a cloud service based on its requirement and demands either for identity, data protection or any other measure listed in the trust value vector. Trust model consists of various parameters that depend on sub parameters and functions. Functions are non-breakable and can be used for measurement of strength. Figure1 indicates the conceptual structure of the trust model with the individual parameters elaborated with their sub parameters and functions

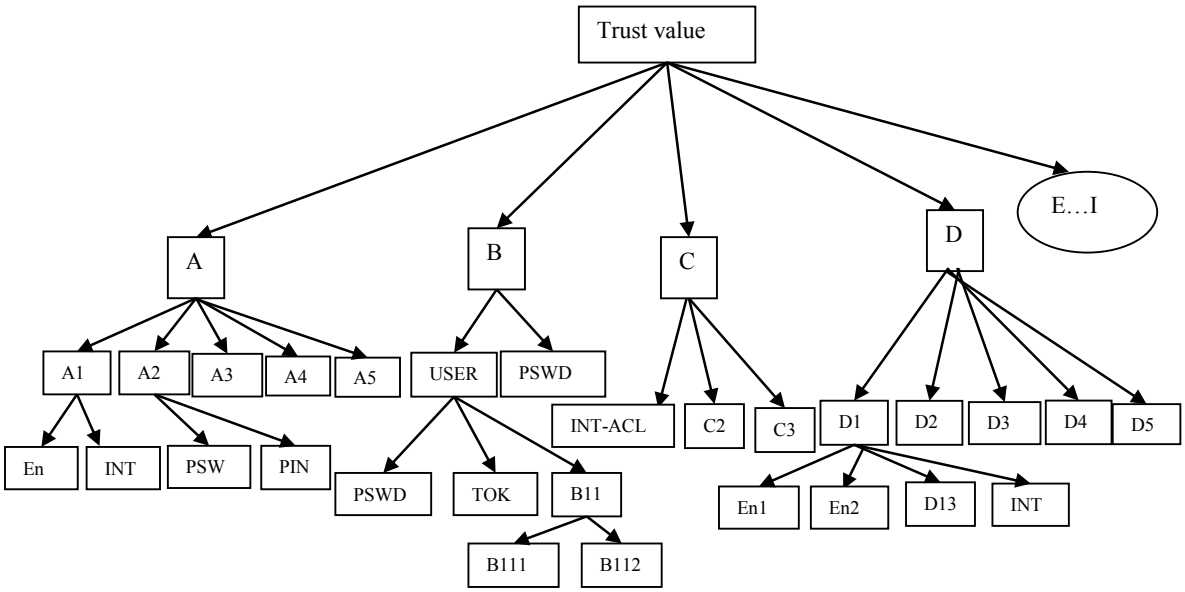

Fig.1.Trust Model conceptual view

The individual parameters are described briefly below, and the respective sub-tree is elaborated in the subsequent sections.

1) Identity management-IDM-A: IDM is a key element of the security eco-system for cloud, and in general for any internet applications. Every cloud service has a process of generating identities for the cloud users. This process can be examined to determine security strength associated with it. It forms one of the trust components as IDM strength. Various parameters relevant to the IDM process include identity creation, storage and the life cycle management of the identity. These processes can be measured against the IDM strength component of the trust model.
2) Authentication-B: To increase user confidence at the time of login and identity verification process, authentication check is required. It is a two sided process, for user accessing a service from authentic provider and for provider to give services to the legitimate user. Therefore, authentic use of cloud service by a legitimate provider can be determined by the strength of authentication that forms one of the components of the trust model. It measures the process provided by a cloud service for authentication check for user as well as service.
3) Authorization-C: A user should not be able to use any actions not authorized for. This property can be checked against the authorization strength. An action including service access, performing any operations, and all input/output related activities requires authorizing users at these stages. A cloud service provides authorization

by using various methods. The effectiveness of the method is measured with respect to the authorization strength. It is measured with respect to the stored ACL (Access Control Strength) integrity, Presence of PMI (Privilege Management Information) and the process of performing validation check of user.

4) Data Protection-D: The crucial asset of a user as well as any organization moving on to the cloud is data. Data privacy issues are at great concerns while moving data to and from cloud environment. A data protection mechanism exhibit by various services possesses characteristics that need to be measured while evaluating the data protection strength. These can be measured by the data protection trust value component of the model. Data Confidentiality, Integrity and Availability can be measured with respect to the data protection strength.
5) Confidentiality-E: A cloud service should protect the secrecy of the communication between a cloud user and provider and all other actions performed in various activities. This property can be measured by confidentiality parameter. Techniques for achieving privacy of the data, message, Identity generation and all other communications between provider and user can be measured with respect to the confidentiality strength provided by the service.
6) Communication-F: Data or messages passed in the cloud computing environment prone to eavesdropping or leakage. The communication strength measures the provision provided by the cloud service at the time of data or message transmission. Therefore the communication strength measures strength of standards used for message transmission and communication.
7) Isolation-G: Multitenant feature of cloud computing infrastructure leads to the problem of isolation of resources among multiple users. Security breaks and violations are the key factors that are caused mainly due to isolation. Cloud service isolation strength determines the level of protection provided to eliminate the security breaks and restrict user access areas. The isolation strength measured by the trust model, determines the level of protection at resource, application and data that is provided by the cloud service.
8) Virtualization-H: The concept of cloud computing is incomplete without the virtualization feature. A virtualized infrastructure is more prone to attacks then the physical one. Techniques should be provided to secure the virtualized environment. The parameter that measures the effectiveness of the security applied to protect the virtualized environment is virtualization. It determines the security consideration at virtualization layer of a cloud computing architecture. It includes strength of VM (Virtual Machine), VMM (VM Monitor), Guest VM protection strength and other monitoring tools.
9) Compliance-I: A compliance approval indicates the method and process of a particular cloud service have been quantified by the known and authorized agencies. Security of a cloud computing service provider and a service can also be determined by the approval or certification from various compliance or standards.

The parameters cover almost all aspects of security. The above parameters are measured individually and can be combined to calculate the overall strength of a cloud computing service and application. The collective value of all the parameters in a form of vector is used to measure the overall security strength. For example a cloud service say S1 has strength value of A=0.8, B=0.7 and so on. Security strength of S1 can be represented as (0.8, 0.7…). The average of all the applicable parameters gives overall security trust value.

Trust value evaluated so far gives the static trust of the cloud service at any point of time. To make it more realistic the dynamic nature of the cloud service also needs to be observed. Usage pattern of the service and web log research can be used to evaluate user satisfaction about the service. Dynamic parameters can be drawn from these sources and leads to evaluating dynamic trust. Dynamic trust along with static trust value can be used to evaluate the security strength of a cloud computing application or service.

The calculations of detailed parameters are discussed in the next section. The parameter is indicated by the tree structure determined by the root name. Level next to root indicates sub parameters and leaf node indicates functions. Nodes represent parent-child relationship. Parent node can be the weighted sum of its child nodes. The weights are different for different levels and are discussed in each of the parameters descriptions. These weights are decided based on the type of function used and time to break the achieved security using them. The actual parameters are described as a collection of weighted sum of its corresponding sub parameters and functions. Finally the root node which indicates a trust value is the vector sum of all the parameters. The individual parameters are discussed in the next sections.

3.1. Identity Management System-(A)

Identities corresponds to the entities and consisting of attributes and identifiers. An identity management system describes the management of individual identities, their authentication, authorization, roles, and privileges within or across system [18]. Storing and managing of identities are very crucial security concerns for cloud services to get confidence from the user. These issues are also crucial for the cloud user to increase their trust towards a cloud provider and services. Various challenges for implementing identity management systems are; trust a provider for authenticating their users, authentic and integrated storage of identities and recycling of identities etc. Every cloud service has a method of managing identities may address some or all these challenges. The techniques and methods used can be measured by the identity management component strength.

We are proposing a set of sub parameters that contribute towards the IDM strength measurements. Each of these are depends upon further sub parameters and functions to determine the security strength of the overall identity management system. Table1 indicates these sub parameters, which are the function of measurable values used for calculating strength.

Table 1- Identity management system-A

Sub-Parameter	Dependency	Description	Function	Example
Storage of identities in terms of Cryptosystem- A1	Strength of (Cryptosystem Key)	The time required to guess a key is determined by checking all possible permutations	Time to break -Key length (En)	2^64 << 2^128 << 2^256
	Strength of Stored information integrity (Integrity Check)-INT	Storing encrypted form of data / Encrypted file	Time to break- En	Strength of encryption key for each credential record
		Using hash with plain data	Strength of Hash algorithm(Size of message digest generated)	MD5 - 128 Bits SHA1- 160 Bits SHA2-256 Bits
		Use of encrypted Hash	Strength of encryption Key size and hash algorithm key	Encrypted checksum or Hash
		Plain data with parity check	Strength of parity check	Only detection or detection & correction
Policy for Authorized Access of Cryptosystem- A2	Strength of password	Security of password	Length of password	Sufficiently large
			Randomness	combination of number, characters and special symbol
	Strength of unblock pin	Unblock pin required if multiple attempts to access cryptosystem fails	Length of pin	Sufficiently large and random number
Identity provisioning- A3	Strength of Identity Provisioning	How system generates identities	Cycle Length (of random numbers used for generating identities)	short cycle length less secure then long cycle length
	Strength of Identities	Identity itself generated should be secure	Length of identity	Large Random number is more secure then short length for identities
Communication Security- A4	Strength of communication Security	Securely passing the identity to user.	Strength of Encryption key (if identities are passed in encrypted form)	Strength of Encryption

			Use of certificate for encryption	Public key of user can be used to encrypt the identity
			Use of soap message encryption	Soap envelop can be used to encrypt the identity in the message itself
Life Cycle Management- A5	The method of identity creation, management and destroy	How the identities are deleted	Complete delete or inaccessible or reuse	Value of strength if complete delete, partial delete or reuse

Identity management strength depends on various sub parameters and functions; the hierarchical tree structure is given in figure2.

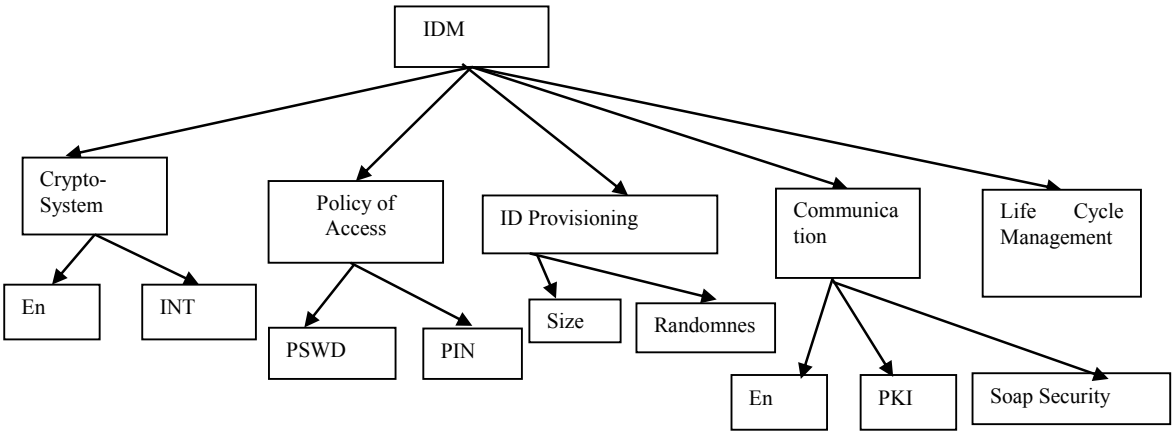

Fig.2. parameter-IDM

Following are the sub-parameters of IDM;

1) CryptoSystem: A provision for storing user identities is one of the factors to be analyzed while measuring the IDM strength. The identities can be stored and managed at a central location as cryptosystem that can be accessed by administrator. Strength of which is determined by measuring the policy of access and the integrity strength of the stored information i.e. user credentials. Therefore cryptosystem strength is measured by key strength that is required to access the cryptographic system and integrity strength of the stored user credentials.

2) Policy of Access: The strength of policy applied to access the cryptosystem in the form of secure storage of identities is measured by this sub parameter. To access crypto system a password is used which can be combination of letters, alphabets or special symbol. If various attempts are made with the unknown password then the system will block. To overcome that an unblock pin is required. Therefore strength associated with policy of access parameter is depends on the password used to access cryptosystem and unblock pin that is required if several un-successful attempts have been made.

3) Provisioning: Another component of the IDM system is Identity provisioning. It is the method of generating the identities. Every cloud service have some or the other method of generating identities. The effectiveness of provisioning method is measured in terms of strength. Strength of provisioning is determined by size and randomness of identities generated.

4) Communication: Generated identities are passed to the user by communication channel. The strength of which is determined by the encryption key (En) used to pass the encrypted form of identity, communication standard used i.e. using public key cryptography (PKI) and soap message security if present.

The overall strength of IDM is proposed as the weighted sum of the above sub parameters depending on their breaking time contribution towards the overall strength. Thus;

IDM = Sum (0.2(cryptosystem), 0.3(process of access), 0.2(Provisioning), 0.2(communication), 0.1(life cycle management))

The parameter IDM discussed determines the security strength in various aspects of identity.

Collection of all the parameters as vector value can be used to determine the security strength of a cloud service. These trust value of a cloud computing service calculates security at any point of time and termed as static trust.

4. Making the Trust Model Dynamic

Over a period of time the service used by various users can be analyzed in terms of feedback and comments. Web research and user feedback can be used to evaluate the dynamic nature of the service. A set of parameters are identified to evaluate a cloud service security. They are;

a) Specific attacks: White papers, articles and social media may give information about a particular cloud computing service over a period of time. It may include specific attacks that has been occurred and handled by the service provider. Also the new technology introduction by means of white papers and articles can also brought the attention towards such attacks.
b) Frequency of attacks: Specific attack occurring frequently will also not acceptable for a reputed cloud service. Therefore this parameter is also considered while choosing the service depending on the requirements.
c) Loss of data protection/ Data leakage: The policy for data protection and provision for data leakage should be carefully checked while moving the valuable data to the cloud computing storage.
d) Improvements in Technology, Security standards and quality: Over a period of time along with the user demands and technology change, a cloud provider must comply with the competitive market needs. Improvements in the technology, security policies and quality attracts user for a cloud provider and its service. A cloud service with increased user demand should possess these characteristics.

Proposed parameters are based on survey and study of the service usage, customer satisfaction and increase in demand and security.

5. Trust Model in Cloud Environment

Trust model can be used in a cloud environment. A trust calculation environment is prepared which includes

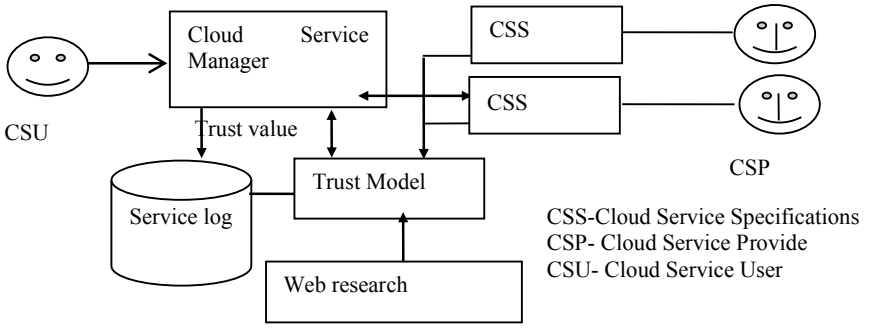

Fig.3.Architecture for trust evaluation in Cloud Environment

various components. A framework is designed for calculation of trust in a cloud environment with multiple cloud service providers and their respective services. The architecture in figure3 shows the various components of trust evaluation in cloud environment.

Major components are:

a) Cloud Service Manager: Details about a specific cloud service like type of service, Service provider and number of users registered for that service and other accounting information is available with a cloud service manager. Lists of all the available services are accumulated in it. Along with that it also maintains trust value associated with a cloud service that gives its security strength. A cloud service has to get registered with the cloud service manager for the first time by the cloud service provider before its use. At this point of time the static trust calculation is done with respect to static parameters. Over a period of time with the service usage dynamic parameters are also considered and dynamic trust is evaluated. Any user who wants to select a particular cloud

service will get the detailed information about the service and its strength from the cloud service manager and accordingly selects a cloud service.

b) Trust Model: It is the trust evaluator that makes use of service details to calculate static or base trust values. It also uses service log and web for calculating dynamic trust.

c) Service log: It is the database of log information about the services. It consists of the log records comprising of information like; service utilization, number of successful and failed transaction, response time and many more. These are made available to trust model to calculate the trust value associated with a specific service.

d) Web Research: It includes the sources of user feedback and comments to draw the conclusions about dynamic security of cloud services.

The trust model calculates the values for various cloud services. Cloud users want to utilize one of the cloud services depending upon their requirements. A cloud user can approach to a cloud service Manager for the required service. A cloud service manager includes details about all the available services along with their security strengths in terms of trust values. Based on the user demands and security strength a cloud service is selected.

Trust model acts as raking service to determine the security strength of the cloud services. It evaluates both the static and dynamic trust value in terms of security that can be used by the users to determine security and reputation of cloud services.

6. Implementation and Testing

6.1. Implementation

Implementation of the trust model requires first preparing a test bed. It is a cloud computing environment that is required as the first step towards our implementation. Various tools are used as a part of our implementation to check their feasibility. A comparative study shows in [16] the various parameters are drawn and analysed during the implementation that can be used as the basis for development of cloud by using any of these tools. Also trust model is implemented as a .Net service and observations are recorded. Trust values are measured by giving inputs for various parameters and sub parameters. A cloud service manager holds a repository that includes the database for all the cloud services and can be used by the cloud service users to select one amongst the available with respect to their requirement and demand for security.

6.2. Testing and Validating TM

Trust model can be used to measure the security strength of cloud services and applications. One of the concerns when looking at any new model is its adequacy for the domain. Does our cloud trust model cover all the aspects of security relevant to cloud computing? To check the validity and adequacy of our trust model following analysis is done. One is using CSA service challenges for application security. Answer to these challenges from trust model proves the adequacy of it in almost all aspects of security. The other approach of evaluating the trust model is by calculating service strength of the existing cloud services. Cloud services are evaluated and trust value is calculated as a vector of values. This measurement gives significant use of trust model in evaluating the overall strength of any cloud application or service.

6.2.1-Evaluating Adequacy of the Model

CSA is an international organization working with security and other areas of computing. They publish comprehensive analytic reports and guidelines concerning various challenges and shortcomings faced in cloud computing. We have attempted to validate our trust model against their published list of challenges in [19]. A questionnaire is prepared from these security challenges. The proposed TM was analyzed with respect to this questionnaire. The questionnaire prepared and what part of our TM corresponds to the question and how well the issue is addressed is prepared in tabular form. Only few of the questions are presented in table2.

Table2: Security challenges addressed by the TM

Sr.No.	Challenges	Measures provided by TM
1	Is the theft of Identity is being taken care of?	Crypto-strength of IDM
2	Does Vendor lock-in issue addressed	IDM-En
3	How unauthorized access is prevented	IDM- Policy of Access
4	What is the provision for insider threat?- eavesdropping	IDM-Communication strength
5	Does privileged escalation possible?	Authentication and Authorization Strength
6	Is non-repudiation is achieved?	Confidentiality and Communication strength
7	Does the delegation of authorizations/ entitlement appropriate?	Authorization strength

8	How to control excessive access or access privilege?	Authorization strength
9	What is the provision for fraud detection?	Authentication Strength
10	How privacy is achieved?	Central Privacy- Data protection Strength
11	Do the providers and clients have separate interfaces?	Crypto system by providers and identity management by users
12	Preventive measure for attack on identity?	Identity strength
13	How password management is done?	Password strength at the time of Id generation process
14	How resource hogging is prevented?	Authentication strength
15	How the complete removal of identity information at the end of life cycle.	Identity life cycle management strength
16	Is real time provisioning and de provisioning is adequate?	Communication strength, ID-Prov strength
17	Is the IDM is portable?	Yes , various components can be configured separately
18	How the transparency to the user is maintained?	User data Encryption key, hash, Id and password selection form the user side
19	Does a user centric access control is possible?	Yes – Grouping set of user based on preferences
20	How Interoperability with existing IT systems possible?	Independent components as required can be integrated to provide the strength

List of challenges and the corresponding measures of strength given by the trust model indicates its validity. Any cloud service can be validated against these challenges and can be measured by using the trust model. As the table shows, the model incorporates almost all aspects that are required to measure the security strength of the cloud services

6.2.2 Evaluating Fairness of the Model

A second aspect of evaluating a trust model is to validate it against actual services, and see if the values computed are meaningful and indicative of the "trust-ability" of the service. For this purpose, we evaluated the trust model against a number of existing cloud service providers. Security issues handled by various cloud service providers vary. Some are providing authentication using password and other may use two factor authentication schemes. Similarly methods of providing data protection also vary. Some of the cloud services considered for our evaluation and the observations are recorded in table3.

Table3: TM and Cloud services parameters strength

Parameters	Sub-Parameter	AWS	Bluelock	Netmagic	Google App	AT&T	Critix	Gogrid
Strength of Identity management	Storage of identities in Crypto-system	Central control of all the identities	Provides VDC-Virtual Data Center	Policy based access control using web control tool	Authorized access	Token based service	Single control	Role based access control RBAC
	Policy for Authorized Access of Crypto-system	MFA-(Multi factor authentication) Pin, Password			Role based access	Enable single connection Hub	password reset and auto password change	
	Identity provisioning	Randomness	NAV	NAV	NAV	NAV	Active directory support	NAV
	Communication Security	Http, Soap message, X.509		SSL digital certificate	TLS	MPLS-VPN	VPN – Virtual Private Network	Private Network Transfer
	Life cycle management	NAV		NAV	NAV	NAV	NAV	NAV
	Overall strength	0.8	0.8	0.6	0.5	0.6	0.8	0.5

Services are analysed and the techniques of providing the security are investigated to determine the security strength. We have analysed all the parameters from these services as per our model as applicable to these providers, and computed the strength values. For presenting here only one parameter is shown. Table3 indicates the method of analyzing security parameters with respect to the trust model, and the trust values computed. NAV (not available) is used wherever the parameter information is not available and NAP (not applicable) indicates that the parameter is not applicable to that service.

7. Conclusion

Trust based evaluation is proposed in the form of trust model. Trust value is the output of the trust model that measures the security strength. Trust model can be effectively used by the user to select a particular service. It can also be used by providers as a benchmark to find out the shortcomings and improvement areas of a cloud service or application. Trust model can be integrated with the cloud services and their descriptions as a cloud service manager. Cloud service manager stores trust value repository of registered cloud providers and their services. The trust value measures can be used to select a service globally by the users.

References

1. Jingwei Huang, David M Nicol, “Trust mechanisms for cloud computing”, http://www.journalofcloudcomputing.com/content/2/1/9, Journal of cloud computing, Springer, 2013.
2. Satyajeet N Srujan Kotikela, Mahadevan Gomathisankaran, “CTrust: A framework for Secure and Trustworthy application execution in Cloud computing”, International Conference on Cyber Security, 2012.
3. Edna Dias Canedo, Electr. Eng. Dept., Univ. of Brasilia-UNB -, Asa Norte, Brazil ; de Sousa, R.T. ; de Carvalho, R.R. ; de Oliveira Albuquerque, R., “Trust Model for Private Cloud”, IEEE International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012.
4. Hamid Banirostam, Alireza Hedayati, Ahmad Khadem Zadeh, Elham Shamsinezhad, “A Trust Based Approach for Increasing Security in Cloud Computing Infrastructure”, 15th International Conference on Computer Modelling and Simulation, 2013.
5. Monoj Kumar Muchahari, Smriti Kumar Sinha, “A New Trust Management Architecture for Cloud Computing Environment”, IEEE International Symposium on Cloud and Services Computing (ISCOS), 2012.
6. Rizwana Shaikh, M. Sasikumar, “Trust Framework for Calculating Security Strength of a Cloud Service”, IEEE International Conference on Communication, Information & Computing Technology (ICCICT), 2012.
7. Rizwana Shaikh, M. Sasikumar, “Trust Model for Calculating Security Strength of a Cloud Service”, IEEE International Conference on Computational Intelligence & Computing Research (ICCIC), 2012.
8. Hyukho Kim, Hana Lee, Woongsup Kim, Yangwoo Kim, “A Trust Evaluation Model for QoS Guarantee in Cloud Systems”, International Journal of Grid and Distributed Computing, March, 2010.
9. Zhimin Yang, Lixiang Qiao, Chang Liu, Chi Yang, Wan Guangming, “A Collaborative Trust Model of Firewall-through based on Cloud Computing”, 14th International Conference on Computer Supported Cooperative Work in Design, China, 2010.
10. Mahbub Ahmed, Yang Xiang, Ali S, “Above the Trust and Security in Cloud Computing: A Notion towards Innovation”, IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, Australia, 2010.
11. Tian Li, Chuang Lin, Yang Ni, “Evaluation of User Behavior Trust in Cloud Computing”, International Conference on Computer Application and System Modeling -ICCASM, China, 2010.
12. Azzedine Boukerche, Yonglin Ren, “A trust-based security system for ubiquitous and pervasive computing environments”, Computer communications, 2008.
13. Barsoum, A. and Hasan A, “Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems”, IEEE Transactions on Parallel and Distributed Systems. December 2012.
14. Kan Yang. Xiaohua Jia, Kui Ren. Bo Zhang and Ruitao Xie, “DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems”, IEEE Transaction on Information Forensics and Security, August 2013.
15. Nia Ramadianti Putri and Medard Charles Mganga, Enhancing Information Security in Cloud Computing Services using SLA Based Metrics, School of Computing, Blekinge Institute of Technolog, Sweden, January 2011.
16. Rizwana Shaikh, M. Sasikumar, “Cloud Security issues: A Survey”, International Journal of Computer Applications, April 2012.
17. CSA, Security Guidance for Critical areas of focus in Cloud Computing V3.0, 2011.
18. Kathy Bergsma (University of Florida) on September 23, 2009.
19. Cloud Computing Market Maturity Study Results, CSA Cloud Security Alliance, 2012.