International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (01), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

FACTUAL DEMONSTRATION: FOR EVALUATING THE SECURITY STRENGTH OF CLOUD COMPUTING

S Pragadeeswaran[1], V Karuppuchamy[2], H.E.Khodke[3], M.Ramkumar[4]

[1]Assistant Professor, CSE Dept, Muthayammal Engineering College,Rasipuram

[2]Assistant Professor, Computer Engineering, Sanjivani College of Engineering, Kopargaon

[3,4] Assistant Professor, Knowledge Institute of Technology Salem

ABSTRACT

Cloud computing has turned into a part of the concentrated market today. Different cloud computing service providers are accessible with their administrations in the cloud environment. Procedures embraced by different suppliers to accomplish security are of shifting nature. To dissect and measure a specific service in view of its security properties is a test. This paper shows such anestimation by utilizing a factual demonstration. A factual model measures the security strength and calculates the factual strength esteem. A factual esteem includes different parameters that are essential measurements along which security of cloud services can be estimated. CSA (Cloud Service Alliance) benefit challenges are utilized to evaluate security of an administration and legitimacy of the model. Ampleness of the model is likewise confirmed by assessing trust an incentive for existing cloud administrations. Factual model in demonstrate goes about as a benchmark and positioning administration to quantify security in a cloud computing environment.

Keywords*: *Cloud Computing, Cloud Service Alliance, Factual Demonstration, Security

I INTRODUCTION

Cloud computing has conquered a significant part of the competitive market today. Many organizations use cloud services. Although cloud services are growing and gaining popularity, the fear of using cloud services remains an open problem. There are several problems listed in the literature that prevent adoption. One of the main problems is safety. Cloud computing security risks have attracted attention since their inception. New protocols as well as tools continue to be needed to improve and measure the security strength of a cloud service. The security of a cloud service must cover many aspects, such as: Authentication, protection of authorization data and so on. These are the basic security goals that make security principles critical to the cloud. Therefore, a tool that assesses and evaluates these security issues related to cloud services before selection is the need in the cloud environment.

Here we focus on a framework for assessing service security in a cloud environment. We propose a factual demonstration model used to evaluate the strength of cloud service security. It is a factual value that represents the overall security of the service in the cloud. The factual value can be judged from a list of parameters covering almost

all relevant aspects of safety. To assess the real value, a confidence based assessment is made. A list of these parameters is identified. The properties and specifications of the cloud service are used to evaluate the factual value that are called static trust. The value of trust depends on the user experience and transactions period of time. A refined set of parameters is formulated to dynamically assess trust. Static and dynamic approval completely determines the security of cloud services. Therefore, the factual model serves as an evaluator for security and classification services for cloud applications and services. It can be used as a reference point to configure cloud service security and to detect errors and improvements to the cloud infrastructure.

II 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

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (01), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

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.

III FACTUAL DEMONSTRATION MODEL

Evaluating a cloud service security is the necessity for any organization moving towards the cloud. We have identified a complete list of the necessary and sufficient security parameters to measure security against the cloud computing environment. These parameters are embedded in our trust model and the result is a real value. The actual value can be a single value that indicates the overall security of a cloud service. It can also be broken down into several safety aspects based on the parameters and displayed as a vector. A user can select a service in the cloud based on their needs and needs an identity, privacy, or any other metric listed in the real-valued vector. The trust model consists of several parameters that depend on sub parameters and functions. Functions cannot be interrupted and can be used to measure the force. Figure 1 shows the conceptual structure of the trust model with the individual parameters developed with its sub parameters and functions.

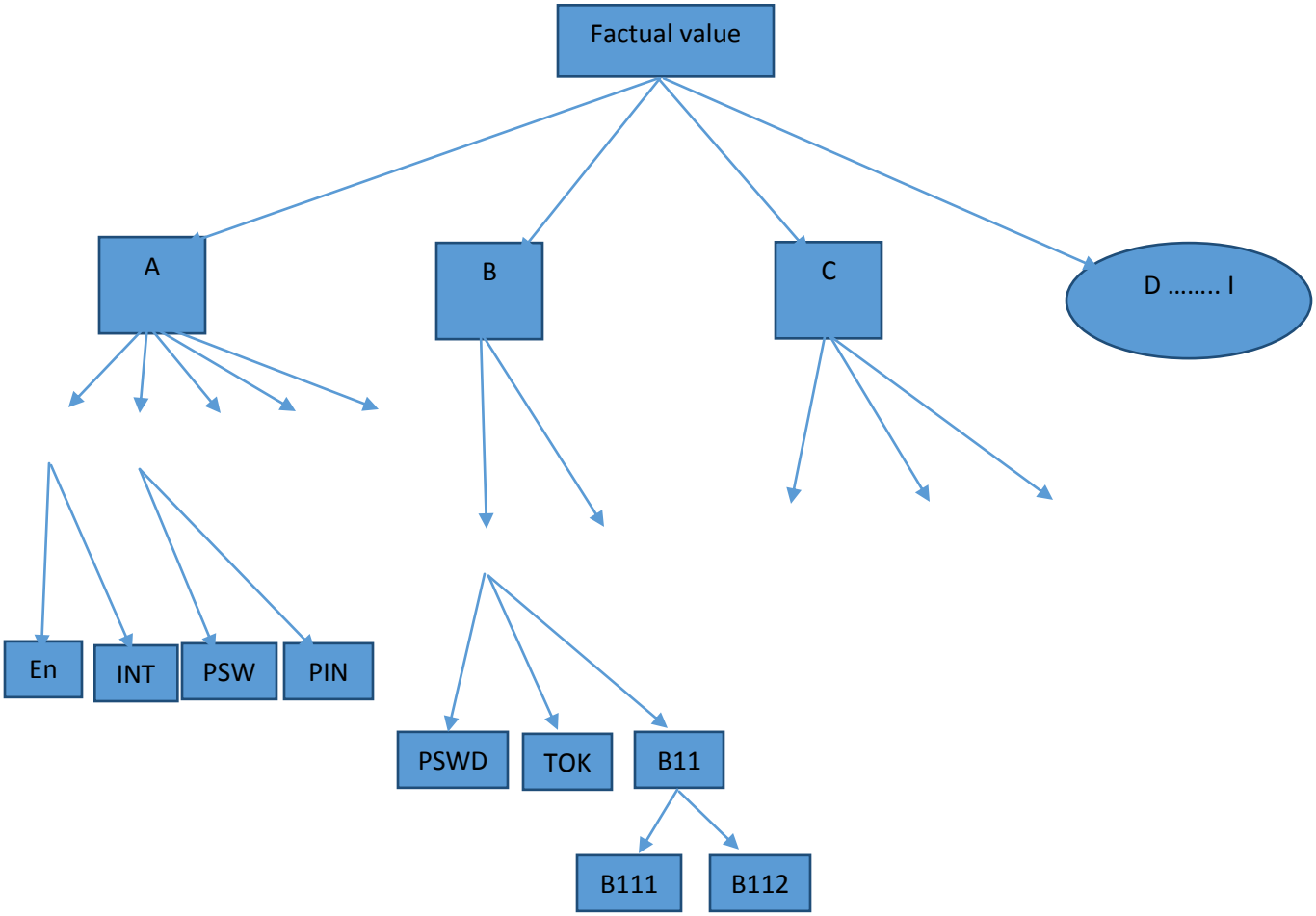

Figure 1. Factual model conceptual view

IV PARAMETERS AND METHODS

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

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 providerand 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 factual 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 factual value. Factual 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 factual 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 factual value is the vector sum of all the parameters.

V CONCLUSION

Security based assessment is proposed as factual demonstration model. Factual esteem is the yield of the factual model that measures the security quality. Factual model can be viably utilized by the client to choose a specific

administration. It can likewise be utilized by providers as a benchmark to discover the inadequacies and change territories of a cloud administration or application. Factual model can be incorporated with the cloud services and their portrayals as a cloud service supervisor. Cloud service supervisor stores factual esteem vault of enlisted cloud providers and their administrations. The factual esteem measures can be utilized to choose a service universally by the clients.

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 SrujanKotikela, MahadevanGomathisankaran, "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, AlirezaHedayati, Ahmad KhademZadeh, ElhamShamsinezhad, "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 Conferenceon 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, LixiangQiao, 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. AzzedineBoukerche, YonglinRen, "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. XiaohuaJia, KuiRen. Bo Zhang and RuitaoXie, "DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems", IEEE Transaction on Information Forensics and Security, August 2013.
15. Nia RamadiantiPutri 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. Vengatesan K., and S. Selvarajan: Improved T-Cluster based scheme for combination gene scale expression data. International Conference on Radar, Communication and Computing (ICRCC), pp. 131-136. IEEE (2012).
18. Kalaivanan M., and K. Vengatesan.: Recommendation system based on statistical analysis of ranking from user. International Conferenceon Information Communication and Embedded Systems (ICICES), pp.479-484, IEEE, (2013).
19 K. Vengatesan, S. Selvarajan: The performance Analysis of Microarray Data using Occurrence Clustering. International Journal of Mathematical Science and Engineering, Vol.3 (2) ,pp 69-75 (2014).
20.K.Umamaheswari, Dr.R.P.Singh, Dr.K.Vengatesan, "Review on Performance Analysis of Gene Expression data using Fuzzy Clustering Techniques",Internation Jounrnal of Adcance research in Sciene and Engineering, Volume 07, Special Issue 01, December 2017,297-303.
21. M.Ramkumar, Dr.R.P.Singh, Dr.K.Vengatesan, B.Narmadha," Study on Performance Measure of Statistically Significant Gene Expression Data Using Biclustering Algorithms", Internation Jounrnal of Adcance research in Sciene and Engineering, Volume 07, Special Issue 01, December 2017,417-423.
22. B.Narmadha, M.Ramkumar, K.Vengatesan, M.Srinivasan, "Household Safety based on IOT", International Journal of Engineering Development and Research (IJEDR), ISSN:2321-9939, Volume.5, Issue 4, pp.1485-1492, December 2017.
23. K.Vengatesan,R.P.Singh, Mahajan S. B , Sanjeevikumar P,Paper entitled "Statistical Analysis of Gene Expression data using Biclustering Coherent Column" International Journal of Pure and Applied Mathematics , Volume 114 No. 9 2017, 447-454 .