NATIONAL CONFERENCE ON ICT EMPOWERED TEACHING, LEARNING AND EVALUATION (NCICT-2016)

International Journal of Advanced Scientific Technologies in Engineering and Management Sciences (IJASTEMS-ISSN: 2454-356X) Volume.2,Special Issue.1Dec.2016

SURVEY ON TRUST SCHEME MANAGEMENT IN CLOUD COMPUTING

P. Jyothi

Assistant Professor, CSE Department, P.V.K.K Institute of Technology

Sanapa Road, Rudrampeta, Anantapuramu-515001

E-mail: jyophani.reddy@gmail.com

Abstract -Technology enrichments renovating many devices in a flourishing sector of IT organizations. Cloud Computing endows scalable and distributed environments through internet. Augment in services and technologies on other side will cause major impact on security. The customer information will be at risk when the data is kept in cloud because data will be accumulated on various physical machines which are unknown to the user and also customer should have trust to store their crucial data on remote data centre of cloud service provider. To defend customers data in cloud there should be some security gauges has to be taken to establish confidence among trading partners. Trust scheme management plays a substantial role between end user and service provider to establish confidence for storing customer's data on remote data centre of service provider.

Keywords: Trust, Feedback, Time stamp, Security.

I. INTRODUCTION

Cloud computing benefits have been utilizing by number of organizations in day to day environments to share resources such as storage, networks, server, applications and services and also organizations to address their information technology they adopt cloud based benefits in need of hardware and software. Services [1] provided by cloud computing are SaaS[Software as a Service], PaaS[Platform as a Service], IaaS[Infrastructure as a Service]. SaaS allows the customers to use software applications, run time environment is provided by PaaS for developments as well as implementations and access to fundamental resources is provided by IaaS such as for virtual storage, physical machines. These amenities can be deployed at different levels as public, private and hybrid cloud.

Cloud applications vary according to the complexity, some are static websites and others are dynamic. Based on need of users, the services of cloud are provided as private, public and community cloud. Many issues will come across in cloud such as confidentiality, integrity and availability. Overall trustworthiness of resources of cloud are based on calculation of algorithmic sum of trusted values which are available to all parts of a computing system.

II. BACK GROUND

Cloud computing guarantees reliable services to be provided to costumers by next generation data centers which are built on internet. Cloud computing plays a major role due to its scalability, flexibility and reduction of cost in its computing resources [3]. Some of the security issues arises in cloud computing depend on development model on which it is delivered. Public cloud has much impact of security issues [9] on data when compared to private cloud. But where as in hybrid cloud the issue will arise with respect to location, so the hybrid cloud has to take care of both the location along with data.

One more factor in storage in cloud is data outsourcing. Data will be transmitted from one location to another due to the lack of enough space to store huge data of customers in one particular place in cloud; vendors will request other organizations to store the requested data which makes user data outsourced to some other firm. There will be single organization which takes responsibility for user data before outsourcing; whereas after outsourcing no organization will take single responsibility in control of users data because of distribution of storage to several organizations. This will make security issues in the cloud.

To overcome security issues [6] in the cloud, cryptographic cloud is introduced which provides authentication and authorization. To provide protection for data, cryptographic measures alone will not be sufficient. Security has to be further extended by combining cryptographic measures along with encryption. Many algorithms for encryption are proposed to secure the data which provides a better solution to safeguard information of end user [10]. Encryption is one measure to provide solutions to security issue when any chance for the client data to be compromised. One more problem arises when same encryption key is used among all clients, so different encryption key had been proposed for each client according to dependence of service provider. Public key cryptography [11] known as Identity based cryptography and Public key Infrastructure.

III. RELATED WORK

To establish trust relationship [5] between trading partners, a trust management [2] had proposed as soon they complete their transaction successfully. Thus level of trust is mainly based on past experience of provider [7]. The feedback is analyzed, aggregated and publicly available to the interested parties. Due to possibility of malicious participants involvement while providing feedback ratings of trust management [8] will make susceptible to some threats and attacks. Threats will cause damage to the accuracy of information whereas attacks will disable service for individual or group of participants such as denial of service which does not allow occurrence of normal operation. These threats and attacks will make weakness in trust management.

Malicious participants may place unreliable feedback ratings on management system, which makes this false rating to be compromised among overall trustworthiness of parties that are participated. Valuation of trust can be done in two ways which are direct and indirect. In direct trust [4], depending on n successful transactions host node belief on other node honesty, responsibility and capability based on its own transactions.

Indirect trust, the value will be assessed based on recommendations of the other nodes those had already transactions with host node. With the help of verifying scheme the feedback verifier will generate ratings and considered as good ratings which fall within timestamp by considering the calculations of both direct and indirect trust. The feedback will be based on past experience which is given by certificate authority (CA) [12] .Involvement of malicious ratings will decrease when we consider timestamp based ratings along with feedback of both participants and by certificate authority.

IV. CONCLUSION

Trust management scheme is introduced to build confidence among the trading partners and providers to transmit data for their storage within the cloud. Feedback ratings of providers based on their timestamps and past experience which is issued by certificate authority can be combined to calculate the trust value of providers by negotiating the ratings of malicious participant's feedback. The future work can be extended by completely negotiating feedback ratings of malicious customer's consideration when calculating trusted values of providers.

according to management scheme [8] to know the trust level which depends on the ratings of provider's feedback

REFERENCES

[1] Foster, Y. Zhao, I.Raicu, S.Lu, "Cloud Computing and GridComputing 360-Degree Compared," CoRR, abs/0901.0131, 2009

[2] Albert S. Horvath III and Rajeev Agrawal, "Trust in Cloud Computing"Proceedings of the IEEE Southeast Con - Fort Lauderdale, Florida, April9 - 12, 2015.

[3] F.Sabahi, "Cloud Computing Security Threats and Responses,"International Conference on Communication Software and Networks (ICCSN) , IEEE, 2011.

[4] M. B. B. K. Thomas Beth, "Valuation of Trust inOpen Networks."

[5] Soon-keowChonga, JemalAbawajyb, Masitah Ahmad, IsredzaRahmiA.Hamid "Enhancing Trust Management in Cloud Environment".

[6] MutumZicoMeetei, Anita Goel "Security Issues in Cloud Computing"

[7] MerrihanB.Monir, Mohammed H.AbdelAzi2, AbdelAziz A Abdelhammid, El-Sayed M. El-Horbaty "Trust Management in Cloud Computing :A Survey"

[8] Xiaodong Sun, Guiran Chang, Fengyun Li "A Trust Management Model to enhance security of Cloud Computing Environments"

[9] MahrooshIrfan, Muhammad Usman "A Critical Review of Security Threats in Cloud Computing"

[10] Amland, S. (1999). Risk based Testing and Metrics. International Conference on Testing Computer Software, Washington, D.C., USA.

[11] D. Boneh, M. Franklin.,Identity-based encryption from the weil pairing" in advances in cryptology,volume 2139.,New York,USA:Springer-verlag,2001,pp. 213-229.

[12] Nida, Bhupendra Kumar Teli" An Efficient and Secure Means for Identity and Trust Management in Cloud"