ISSN No: - 2456 – 2165

An Improved Cloud Services for Supporting Reputation-based Trust Managment

Ms. Sonali Nikam
Department of Computer Engineering
Jayawantrao Sawant Collage of Engineering
Hadapsar. Pune-28
Savitribai Phule Pune University, India
nikamsonali15@gmail.com

Dr. S.N.Kini
Department of Computer Engineering
Jayawantrao Sawant Collage of Engineering
Hadapsar. Pune-28
Savitribai Phule Pune University, India
snkini@gmail.com

***Abstract*— Many challenging issues such as concealment, security, and availability occur by highly dynamic, distributed, and non-transparent nature of process. Trust direction is a standout amongst the most difficult issue for the day to day life and growth of cloud computing. Deliverance customer or consumer privacy is not an easy task due to the confidential information involved in the interactions between customers and the confidence management inspection and repair. Protecting cloud service against their malicious client (e.g. such clients may give misleading feedback to specific cloud service for improving publicity of cloud) is a complicated issue. Dynamic nature of cloud environment, the availability of the cartel management service is a challenging issue for assuring. In this paper, we elaborate the purpose as well as effectuation of Cloud Armor, a reputation -based trust management arrangement which provide an arrangement of different functionality to deliver Trust as a service (TaaS), including i) a novel convention to demonstrate the believability of trust inputs of customer or user as well as save security of clients, II) Not only a versatile but also robust believability modelling for measurement the credibility of trust feedback to keep cloud avail from malicious clients and to analyze the dependability of cloud armed service , and iii) an availability model to great deal with the accessibility of the decentralized usage of the trust management service. The achievability and advantages of our methodology have been tried by a model and test studies utilizing a collection of true trust feedbacks on cloud services.**

Keywords*— Cloud computing, trust management, reputation, credibility, credentials, security, privacy, availability

I. INTRODUCTION

The cloud services provide highly dynamic, distributed, and nontransparent nature such as PaaS, SaaS and IaaS make the trust management in cloud environments a significant challenge in environment. Consumers' feedback is a best source to assess the overall trustiness of swarm table services. Researchers have known the significance of trust management as well as proposed result to assess as well as based on feedbacks manage trust collected from different participants.

The focus on proposed system is totally on improving trust management in swarm surroundings by presenting novel ways. It is so to ensure the credibleness of trust feedbacks. In particular, we differentiate the following key issues of the trust management in cloud environment. The acceptance of cloud computing increases seclusion concerns. Customers can have dynamic interaction with cloud providers. The interaction may involve spiritualist entropy. There are different cases of private breaches first is leaks of sensitive information e.g., engagement of birth as well as destination or behavioral information e.g., with whom the customer or consumer interact, the kind of cloud service the consumer showed interest etc. Undoubtedly, services which involve consumer data e.g., interaction histories should preserve their private. It is not unusual that experiences fire from its exploiter in cloud service. Attackers can disadvantage a cloud service by giving multiple misleading feedbacks or them creating several accounts. Indeed, the detection of such malicious demeanour airs various challenges. Firstly, new exploiter joins the cloud environment as well as old user parting around the clock. This consumer shuffle the detection of malicious behaviors a significant challenge. Secondly, users may contain multiple accounts for a particular cloud service, which make it difficult to detect Sybil onslaught. Finally, it is difficult to guess when malicious behaviors will occur.

II. REVIEW OF LITERATURE

In this paper, we assess how secure, confidence and privacy issues occur in the context of cloud computing and discuss ways in which they may be addressed It has the advantage of reducing price by sharing computing and storage resources, compounded with an on-demand provisioning mechanism relying on a pay per- usage business model. This makes compliance with rules referred to data handling difficult to accomplish [1].

Here paper explains about, we start this paper with a survey of existing mechanisms for establishing trust, and remark on their limitations we then address those limitations by offering more rigorous mechanisms based on evidence, attribute certification, and establishment, and conclude by suggesting a framework for integrating various trust mechanisms together to reveal chains of trust in the swarm. This organization gives an integrated perspective of the trust mechanisms for cloud computing, and analyzes the trust chains connecting cloud entities. Some cloud clients cannot make decisions close to utilizing a slow cloud service based solely on informal trust mechanisms. In this article about, The author suggest using a trustoverlay network over multiple data center to implement a reputation based system for establishing trust between service providers and data owners [2].

To protect online shared data object and massively distributed application module data coloring and software watermarking. These techniques safeguard multi-way authentication, enable

ISSN No: - 2456 – 2165

single sign-in the cloud, and tighten access control for raw data in both public and private cloud [3].

Once user move data into the cloud, they can't easily extract their data and programs from one cloud server to run on another. This leads to a data lock-in problem. Describe about, the description in Service level Agreements (SLAs) are not consistent among the cloud providers even though the other services with similar functionality [4].

This paper proposed a data coloring method acting based on cloud watermarking to recognize and ensure mutual repute. The experimental results describes that the lustiness of turnaround cloud generator can guarantee users embedded social reputation identifications in good sense. Hence, our work provides a reference solution to the critical problem in cloud security. [5].

P. Mell and T. Grance 2011. The authors not only look at what trust is but also how trust has been applied in distributed computer science. Trust manikin proposed for different broadcast system has then been refined. The trust management scheme proposed for cloud computer science. It has been investigated with particular accent on their c applicability, capability in practical heterogeneous cloud environs as well as implementabilty. Eventually, the proposed models or systems have been compared with each other based on a selected solidifying of cloud computing parameters in a tabular array [6].

L. Yao and Q. Z. Sheng 2011 propose the "Corporate trust as a Service" (TaaS) theoretical account to improvise the ways on trust direction in swarm surround. Malicious user check the feedback in cloud service. The approaches have been validated by the prototype organization as well as experimental results. All Trust management is the major destination in the variety of cloud computation environment. This system provides agency to identify the trustworthy cloud providers in terms of different attributes (e.g., security measure, functioning, compliance) assessed by multiple sources and ascendant of trust information [7].

K. Ren, C. Wang, and Q. Wang 2012. This paper listed such challenges and defines a set of security and cartel requirements that must be taken into account before swarm computation result can be fully integrated and deployed by telecommunication providers. Reputation attack to allow consumer to effectively identify trustworthy cloud services [8].

C. Dellarocas 2003. It offers a holistic view of the ranking side as good as proposed a ranking fraud sensing system for mobile Apps. Specifically, we first propose to correctly place the ranking fraud by mining the active period of time, which is called leadership sessions, of mobile Apps. These leading sessions can be leveraged for detecting the local anesthetic anomaly instead of global anomaly of App rankings. Furthermore, we investigate three eccentric of evidence , i.e., one is ranking based evidences second one is military rank based evidences and third one is revue based evidences, by fashion model Apps' ranking, rating and review deportment through statistical hypotheses mental testing. Additing to this, we propose an optimization based collecting method to integrate all the evidences for fraud spying [9].

R. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, L. Qianhui, and L. B. Sung 2011. The optimization which is founded on the aggregation method to mix all the evidence for fraud detection. Lastly, we assess the proposed organization with actual-world App data collected from the Io App Store for a long sentence period. The proposed system we detection algorithm as well as some regularity of ranking fraud activities [10].

III. METHODOLOGIES

A. Detection of Service

This layer consists of different user who use cloud services for secure data, application and different platform. For example, a new startup that has limited funding can consume services. Interactions for this layer include: i) service discovery where users are able to new cloud services and other services through the Internet, ii) trust and service interactions where client or customer are able to give their feedback the trust results of a particular cloud service, and iii) registration where users establish connection their identity through registering their credentials in IdM before using TMS.

B. Trust Communication

In a typical interaction of the reputation-based Trust Management System, a user either gives feedback regarding the trustworthiness of a specific cloud service or requests the trust assessment of the service 1. From user feedback, the behavior of a cloud service is actually a collection of invocation history record, represented by a tuple H= (C, S, F, T f), where C is the users primary identity (Name, address, phone number etc.), S is the cloud services identity, and F is a set of Quality of Service (QOS) feedback (i.e., the feedback represent several QOS parameters including availability, security, response time, accessibility, price).

C. IDM Registration

The organization purports to use the Identity, Management Service (IdM) helping TMS in measuring the credibility of a consumer response. Nevertheless, the process of the IdM information can breach the secrecy of users. One way to preserve privacy is to use cryptographic encryption techniques. However, there is no efficient way to process encrypted data, an another way is to use anonymization techniques to process the IDM information without breaching the privacy of user. Clearly, there is a trade-off between high anonymity and utility.

D. Service announcement and Communication

This layer consists of different cloud service providers who provide several cloud services such as amazon, i.e., IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Soft-ware as a Service), publicly and privately on the Web (more details about cloud services model and design can be found). These cloud service are accessible through Web portals and indexed on Web search engines like Google, Yahoo, and Baidu. Interactions for this layer are considered as Cloud service interaction with user and trust management.

IV. SYSTEM ARCHITECTURE

Given the highly moral force, distributed, and nontransparent nature of swarm armed service s, managing and establishing confidence between swarm service users and swarm serving remains a significant challenge. Substance

ISSN No: - 2456 – 2165

abusers feedback of Swarm service is a decent source to assess the whole reliance worthiness of cloud serve. However, malicious users may collaborate:

- Disadvantage a cloud service by adding turn of misleading confidence feedback (i.e., connivance tone-beginning) or
- Trick user into trusting cloud services that are not trustworthy by creating different accounts as well as adding misleading trust feedback and different response (i.e., Sybil attacks).

In this paper, the novel proficiency is introduced that gives a help in sleuthing repute based different attacks, also allowing user to effectively identify trustworthy cloud service provider. In particular, credibility model is also introduced that not only identified misleading trust feedbacks from collusion attack but also detects Sybil attacks no matter these attack happens in a long or short period of time (i.e., strategic or occasional attacks respectively). An availability model is also use to which maintain the trust management service at a particular level. To collected a large telephone number of consumers trust feedbacks given on real-world cloud services to evaluate in our techniques. The experimental solution demonstrates the applicability of our plan of attack and display the potentiality of detecting such malicious behavior. There are a few charge for our future piece of work. Plan to trust different trust management techniques such as reputation and recommendation to increase the trust results accuracy. Carrying out optimization of the trust management service is another focus of our future inquiry work.

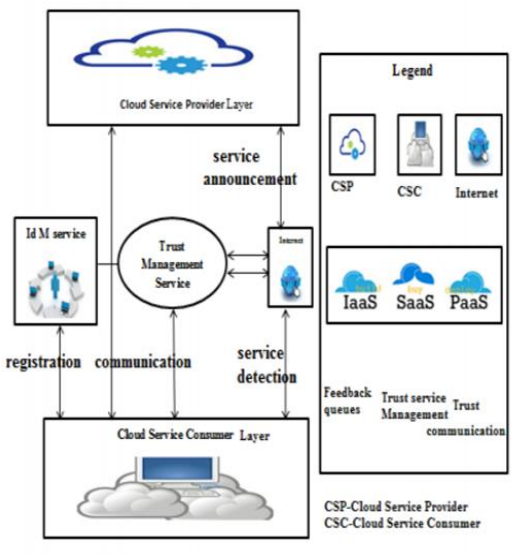


Fig.1. System Architeure of Cloud Armor

- User ’s feedback of Cloud service is a decent to assess the whole trust worthiness of swarm service In this paper , the novel techniques is introduced that gives a help in detecting reputation based fire , also allowing users to effectively identify trustworthy cloud services.
- The credibility model is also introduced that not only identifies misleading trust feedbacks from connivance blast but also detects Sybil flak no matter these attacks happens in a long or short period of sentence (i.e., strategic or occasional attacks respectively).
- We also develop an availability model that maintains the trust management service at a desired degree. We develop an availability model that maintains the trust management service at particular desired level.

A. The Cloud Service Provider Layer

The different cloud service providers who offer one or more cloud services, i.e., IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service), publicly and privately on the Web (more details about cloud services model and design). These cloud services are accessible through Web portals and indexed on Web search engines like Google, Yahoo, and Baidu. Interactions for this layer are considered as cloud service interaction with user and trust management, and cloud service advertisement where providers are able to advertise their services on the Web.

B. The Trust Management Service Layer

Trust Management nodes which are hosted in multiple cloud environments in geographical area of cloud service. These TMS nodes expose interfaces so that user can give their feedback or inquire the trust results in a decentralized way. Interactions for this layer include: i) cloud service interaction with cloud service providers, ii) service advertisement to advertise the trust as a service to user through the Internet, iii) cloud service discovery through the Internet to allow users to assess the trust of new cloud service, and iv) Zero-Knowledge Credibility Proof Protocol (ZKC2P) interactions enabling TMS to customer’s feedback.

C. The Cloud Service Consumer Layer

Finally, this layer consists of different user who use cloud service provider. For example, a new startup that has limited funding can consume different cloud services (e.g., hosting their services in Amazon S3). Interaction for this layer includes:

- User are able to discover new cloud services and other services through the Internet.
- Trust and service interactions where users are able to give their feedback or retrieve the trust results of a particular cloud service.
- Registration where user establish their identity through registering their credential in IdM before using TMS.

In this framework also exploits a web crawling approach for automatic cloud services discovery which access web information, where cloud services are automatically discovered on the Internet and stored in a cloud services repository in database. Moreover, in framework contains an Identity Management which is responsible for the registration where users register their credentials before using Trust Management and proving the credibility of a particular consumers feedback through ZKC2P.

ISSN No: - 2456 – 2165

V. CREDIBILITY MODEL

Thither is a possibility that the Trust Management Services receive inaccurate information or even malicious trust feedbacks from amateur cloud service consumers (e.g., who lack experience) or vicious cloud service consumers (e.g., who submit lots of negative feedback to disadvantage a particular cloud service, for example for particular service publicity). To overcome these issues, we are proposing a credibility model, which is centered on the cloud consumer's experience. To differentiate between expert and amateur cloud service consumers, we are considering the Majority Consensus and the Cloud Consumers Capability. It is well-known that the majority of people usually agree with different experts judgments about what is good [4]. Similarly, we believe that the majority of cloud consumers agree with Expert cloud service consumers' judgments. A cloud service provider whose trust feedback is close to the bulk of trust response is considered an Expert Cloud Service Consumer (ECSC), or an Amateur Cloud Service Consumer (ACSC) otherwise how to measure close the cloud service consumer's trust feedbacks to the majority (i.e., the Majority Consensus (J (c)) which is calculated as follows:
The numerator represents the mean of the majority trust feedbacks given by other CCS (F(l, k)) (i.e., the lth cloud service consumer, except the cloud service consumer c) to the kth cloud service. It is a common sense that older people are likely to be more experienced in judging things than younger people [14]. However, this is only true if the older people have experienced considerable number of judging use for practice. As a result, we believe that "older" cloud service consumers who have many judging practices are likely to be more experienced and capable to services. A cloud service consumer's capability (B) is measured as follows: where Vc(c) represents all good feedback (i.e., feedbacks which are close to the majority) given by the cloud service consumer c. Ag(c) denotes the virtual Age of a certain services, measured in days since the registration in the trust management. The idea behind adding the number 1 to this ratio is to increase the value of a cloud service consumer experience based on B(c) result. cloud service consumer is, the more experienced a higher B(c). It should be noted that even if a malicious cloud service consumer attempts to manipulate the capability result, the capability result will not exceed 2. The Trust feedback Management distinguishes between ECSC and ACSC through assigning the cloud service consumer's Experience aggregated weights Exp (c) to each of the cloud consumers' trust feedbacks . Exp(c) is calculated as follows: whereβ and B(c) denote the cloud service consumer's Capability factor's normal-ized weight and the factor's value respectively. The second part of the equation represents the Majority Consensus factor where μ denotes the factor's normal-ized weight and J (c) denotes the factor's value. λ represents the number of fac-tors used to calculate Exp(c) (e.g., if we only consider cloud service consumer's capability, λ = 1; if we consider both cloud service consumer's capability and majority consensus, λ = 2). We use J (c) as a penalty factor (i.e., because J (c) ranges [0,1] as described in equation). The lower J (c) is, the lower the experience of the cloud service consumer c. It is worth noting that our credibility is dynamic and is able to observe behavior changes. For example, if a cloud service consumer behaves good for a period of time (e.g., to gain credibility) and then starts misbehaving, J (c) can detect such behavior through applying the standard deviation.

$$Exp(c) = \frac{\beta * B(c) + \mu * J(c)}{\Lambda} \quad \ldots.(1)$$

Where β and B(c) denote the cloud service consumer Capability factors normalized weight and the factors value respectively. The second part of the equation represents the Majority Consensus factor where μ denotes the factor's normalized weight and J (c) denotes the factor's value. The number of factors used to calculate Exp (c)
(e.g., if we only consider cloud service consumer's capability, λ = 1; if we consider both cloud service consumer's capability and majority consensus, λ = 2). We use J (c) as a penalty factor (i.e., because J (c) ranges [0,1] as escribed in equation 3). The lower J (c) is, the lower the experience of the cloud service consumer c is. Higher B(c) means more experienced of a cloud service consumer. It is worth noting that our credibility is dynamic and is able to observe behavior changes. For example, If a cloud service consumer behaves well for a period of time (e.g., to gain credibility) and then starts misbehaving, J (c) can detect such behavior through applying the stock deviation.

VI. RESULT ANALYSIS AND EXPERIMENT

Our implementation and experiment were prepared based on the NetLogo platform 2, which was used to simulate the cloud environment. We especially focused on validating and analyzing the performance of the proposed credibility model (see Section V). In our experiments, we used the real-life, trust data set, Epin-ions3 rating data set which was collected by Massa and Avesani [13]. We prefer to use Epinions data set because its data structure is standardized (i.e., consumer opinions and reviews on specific products and services) to our cloud service con-Sumer trust feedbacks.

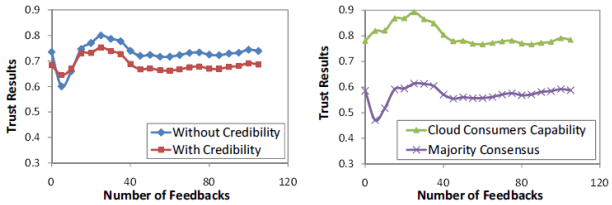
TABLE 1: EXPERIMENT FACTORS AND PARAMETERS SETUP

Experiment Design	β	μ	λ	$Exp(c)$
With Credibility Factors	1	1		2
Without Credibility Factors				1
Cloud Service Consumer's Capability Factor	1	0		1
Majority Consensus Factor	0	1		1

We are evaluate our credibility model using both analytical analysis and empirical analysis. The analytical analysis focuses on measuring the trust result accuracy when using the credibility model and without using the credibility model (i.e., we turn the Exp (c) to 1 to exclude the credibility factor). The focuses on evaluating the trust result accuracy for each agent in our credibility model (i.e., B (c) and J (c)). The parameters

ISSN No: - 2456 – 2165

setup for each corresponding experiment are depicted in Table 1.Figure 2(a) depicts the analytical analysis of the trust results for a particular cloud service. We remark that the trust result is significantly calculating the trust without considering the credibility factors than the trust with credibility factor. If the trust management receive malicious trust feedback, it is difficult to manipulate the trust result by using our credibility model. Figure 2(b) shows the empirical analysis of the cloud service. We note that trust result obtained by only considering B(c) is higher than the trust result by only considering J (c). This is use B(c) as a reward factor and the J (c) as a penalty factor. This reflect how adaptive our credibility model is where the credibility factors can easily be tweaked according to the trust needs. On the other hand, for pessimistic situations where many cloud consumers have high values of capability, the majority consensus factor (i.e., μ) needs to be increased.



(a) Analytical Analysis (b) Empirical Analysis

Fig 2. Experimental Evaluation

VII. CONCLUSION

From this Cloud Armor Supporting Reputation-based Trust Management for Cloud Services has been implemented. In cloud computing growth, the management of trust element is most challenging issue in environment. Cloud computing has produce high challenges in security and privacy by the changing of environments. Confidence is one of the most concerned obstacles to the adoption and maturation of cloud computing. Although several solutions have been proposed recently in managing trust feedbacks in cloud environments, how to determine the credibility of trust feedbacks is mostly neglected. Additionally in future, we also enhance the performance of cloud as well as the security.

We introduced an adaptive credibility model that assesses cloud services trustworthiness and distinguishes between credible and malicious trust feedbacks. We particularly introduced the cloud service consumer's in calculating the trust of a cloud service for Capability and the Majority Consensus factors. In TMS allows trust feedback assessment and storage to be managed different way. In the future, we plan to deal with more challenging problems such as the Sybil attack and the Whitewashing attack. Performance optimization of TMS is another focused work.

References

[1] Talal H. Noor, Quan Z. Sheng, Lina Yao, Schahram Dustdar and Anne H.H. Ngu "CloudArmor: Supporting Reputation-Based Trust Management for Cloud Services" IEEE Transactions On Parallel And Distributed Systems, Volume: PP, Issue: 99, January 2015

[2] S. M. Khan and K. W. Hamlen, "Hatman: Intra-cloud trust management for Hadoop," in Proc. 5th Int. Conf. Cloud Comput., 012,pp. 494–501

[3] E. Bertino, F. Paci, R. Ferrini, and N. Shang, "Privacy-preserving digital identity management for cloud computing," IEEE Data Eng. Bull, vol. 32, no. 1, pp. 21–27, Mar. 2009.

[4] Yu-Chao Liu, Yu-Tao Ma, Hai-Su Zhang, De-Yi Li and Gui-Sheng Chen, "A Method for Trust Management in Cloud Computing: Data Coloring by Cloud Watermarking", International Journal of Automation and Computing, pp 280-285, 2011.

[5] S. Habib, S. Ries, and M. Muhlhauser, "Towards a trust management system for cloud computing," in Proc. 10th Int. Conf. Trust, Security Privacy Comput. Commun., 2011, pp. 933–939.

[6] P. Mell and T. Grance. (2011, Sep.). The NIST definition of cloud computing.

[7] L. Yao and Q. Z. Sheng, "Particle filtering based availability prediction for web services," in Proc. 9th Int. Conf. Service-Oriented Comput., 2011, pp. 566–573.

[8] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Comput., vol. 16, no. 1, pp. 69–73, Jan./Feb. 2012.

[9] C. Dellarocas, "The digitization of word of mouth: Promise and challenges of online feedback mechanisms," Manage. Sci., vol. 49, no. 10, pp. 1407–1424, 2003

[10] R. A. Wagner and M. J. Fischer, "The string-to-string correction problem," J. ACM, vol. 21, no. 1, pp. 168–173, 1974.

[11] R. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, L. Qianhui, and L. B. Sung, "TrustCloud: A framework for accountability and trust in cloud computing," in Proc. IEEE World Congr. Services, 2011, pp. 584–588.

[12] J. Huang and D. M. Nicol, "Trust mechanisms for cloud computing," J. Cloud Comput., vol. 2, no. 1, pp. 1–14, 2013.

[13] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," IEEE Internet Comput., vol. 14, no. 5, pp. 14–22, Sep./Oct. 2010.

[14] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, 2010.

[15] I. Brandic, S. Dustdar, T. Anstett, D. Schumm, F. Leymann, and R. Konrad, "Compliant cloud computing (C3): Architecture and language support for user-driven compliance management in clouds," in Proc. 3rd Int. Conf. Cloud Comput., 2010, pp. 244–251.

[16] W. Conner, A. Iyengar, T. Mikalsen, I. Rouvellou, and K. Nahrstedt, "A trust management framework for service-oriented environments," in Proc. 18th Int. Conf. World Wide Web, 2009, pp. 891–900.

[17] T. H. Noor, Q. Z. Sheng, and A. Alfazi, "Reputation attacks detection for effective trust assessment of cloud services," in Proc. 12th Int. Conf. Trust, Security Privacy Comput. Commun., 2013, pp. 469–476.

[18] S. Pearson and A. Benameur, "Privacy, security and trust issues arising from cloud computing," in Proc. 2nd Int. Conf. Cloud Comput., 2010, pp. 693–702.

[19] E. Bertino, F. Paci, R. Ferrini, and N. Shang, "Privacy-preserving digital identity management for cloud computing," IEEE Data Eng. Bull, vol. 32, no. 1, pp. 21–27, Mar. 2009.

[20] E. Friedman, P. Resnick, and R. Sami, "Manipulation-resistant reputation systems," in Algorithmic Game Theory. New York, USA: Cambridge Univ. Press, 2007, pp. 677–697.

[21] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Comput., vol. 16, no. 1, pp. 69–73, Jan./Feb. 2012.

[22] F. Skopik, D. Schall, and S. Dustdar, "Start trusting strangers? bootstrapping and prediction of trust," in Proc. 10th Int. Conf. Web Inf. Syst. Eng., 2009, pp. 275–289.

[23] H. Guo, J. Huai, Y. Li, and T. Deng, "KAF: Kalman filter based adaptive maintenance for dependability of composite services," in Proc. 20th Int. Conf. Adv. Inf. Syst. Eng., 2008, pp. 328–342.

[24] T. Dillon, C. Wu, and E. Chang, "Cloud computing: Issues and challenges," in Proc. IEEE 24th Int. Conf. Adv. Inf. Netw. Appl., 2010, pp. 27–33.

ISSN No: - 2456 – 2165

[25] Y. Wei and M. B. Blake, "Service-oriented computing and cloud computing: Challenges and opportunities," IEEE Internet Comput., vol. 14, no. 6, pp. 72–75, Nov./Dec. 2010.

[26] P. Mell and T. Grance. (2011, Sep.). The NIST definition of cloud computing [Online]. Available: http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

[27] O. David and C. Jaquet. (2009, Jun.). Trust and identification in the light of virtual persons pp. 1–103 [Online]. Available: http://www.fidis.net/resources/deliverables/identity-of-identity/

[28] B. Fung, K. Wang, R. Chen, and P. Yu, "Privacy-preserving data publishing: A survey of recent developments," ACM Comput. Surv., vol. 42, no. 4, pp. 1–53, 2010.