ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 3, March 2017

CloudShield: A Reputation-Based Trust Management Framework delivering TaaS

A.Vinay Kumar[1], B. V. Kiranmayee[2], Dr. S. Nagini[3]

M.Tech Student, Department of Computer Science, VNR VJIET, Hyderabad, India [1]

Assoc. Professor & HOD, Department of Computer Science, VNR VJIET, Hyderabad, India[2]

Assoc. Professor, Department of Computer Science, VNR VJIET, Hyderabad, India [3]

Abstract: Cloud computing or simply called as "The Cloud" is a network of scalable resources and its adoption & expansion is dependent on the trust management. Cloud services are dynamic, and it presents several challenges such as confidentiality, security and availability. Confidentiality means keeping the data private. Data protection be it the personal information of consumer which may be sensitive and confidential but also metadata and transactional data which may involve important information. In addition to this protection of cloud services from users who give deceptive feedbacks to affect the cloud service is also important. Now a day's consumer's feedback is proved to be an effective source to measure the total trustworthiness of cloud services. So, a trust management framework to manage and analyse the generated feedbacks is proposed which includes different mechanisms to provide TaaS (Trust as a Service). This Framework incorporates following key factors, A protocol to ensure the trust feedback credibility and to safeguard user's privacy. A credibility model to measure the trust feedbacks credibility, this credibility model should be adaptive and robust. Finally, an availability model for feedback management using multiple distributed nodes in a decentralized way.

Keywords: *Cloud computing, trust as a service, trust management service, credibility, feedback, security, privacy, availability, reputation attacks.*

I. INTRODUCTION

NIST definition states that the important characteristics of cloud computing are resource pooling, on-demand service, elasticity, wide network access, and measured services. Cloud environment is fragmented into three "service models" (platform, infrastructure, and software) and into four "deployment models" (public, private, community, and hybrid) to deliver cloud services [1].

Cloud computing is growing phenomenon in the IT world. The flexibility and on-demand resources of cloud services and applications pushing the organizations and firms towards cloud environment. Dynamism of cloud services possess trust and security as a significant challenge for the global growth of cloud environment [2] [3] [4] [5]. Trust generates reputation, reputation in general is an opinion about an individual person or a firm. Reputation of a cloud service in the cloud environment is of significant importance, as the consumers are more inclined to choose more reputable service provider. Service-Level Agreements which forms an understanding between household owners and customers addresses many issues regarding the cloud computing and binds the involving parties into legal bond. But to establish trust among cloud providers and customers, Service-level Agreements alone are not sufficient because of its ambiguous and not so consistent clauses [9]. So, we need a new approach to assess the trustworthiness of the services provided in the cloud. Here feedbacks given by consumers becomes a reliable source as they form the opinion of the end user. Many researchers acknowledged the importance of trust management and presented several mechanisms to assess trust based on the feedbacks given by the customers. The quality of the trust feedbacks that are collected are different from one individual to another based on the experience of that individual. But this introduces new challenges, it's not uncommon for cloud service experience malicious behaviours from its users which can be termed as reputation attacks. These reputation attacks include collusion attacks & Sybil attacks. In this paper we propose appropriate way to measure trust feedback credibility and also protect those trust feedbacks, in turn improving trust management in cloud environments. Privacy and protection are key issues of the trust management in cloud:

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 3, March 2017

• **Consumers' Privacy:** Privacy is the main area of concern for consumers who move their business towards cloud. Dynamic interaction between users and cloud providers, involve exchange of confidential information. Many privacy issues have been identified such as privacy breaches resulting in leaks of personal data (e.g., mobile number and address) or behavioural data (e.g., interaction of consumers other entities, consumer interest in the different cloud services, etc.).

• **Cloud Services Protection:** Often cloud services experience malicious behaviour from its users for different reasons. These malicious users try to affect the reputation of a cloud service by submitting misleading feedbacks which is called as reputation attacks. These reputation attacks are differentiated into collusion attacks, giving multiple deceptive feedbacks or Sybil attacks, submitting misleading feedbacks through several accounts. Dynamism of Cloud services presents a major challenge in detecting of such attacks. Moreover, a single user may have multiple accounts which makes detection of the Sybil attack difficult. Predicting the occurrence of malicious behaviour whether they are strategic behaviour or occasional behaviour is challenging.

II. LITERATURE REVIEW

According Privacy Risk, Security, Accountability in Cloud Platform - Marianthi Theoharidou, Nick Papanikolaou, Siani Pearson and Dimitris Gritzalis, the authors quoted on, transferring applications or services into the cloud presents new threats and challenges to the business which should be assessed properly. Concentration of this paper is on issues like assessment of privacy risk, identifying new threats and weaknesses in the cloud. Measuring Privacy compliance and accountability various guidelines that should be implemented are also illustrated. Various risks of data storage in cloud are discussed namely multi-tenancy, dynamicity and transparency in cloud are assessed. Quoting the UK ICO's guidelines (2012) [11], Encryption is must to protect the data from interception while transferring between different locations. Dynamism of cloud makes existing static risk assessment methods like OCTAVE or CRAMM unsuitable for the cloud. A different approach for assessing risks and accountability is needed and also for determining the cloud risk management.

According to Privacy-Preserving Fine-Grained Access Control in Public Clouds- Mohamed Nabeel, Elisa Bertino, the authors quoted on, Cloud computing is rising phenomenon in the IT world thanks to its economic benefits and flexibility, many organizations are moving their information systems to the cloud. For data confidentiality, Encryption of data along with emphasized access control on the data is suggested. The attribute based access control systems are based on identity attributes i.e., security relevant properties of users. Here drawbacks of the various popular cryptographic techniques like proxy re-encryption [6] [7], attribute-based encryption [9] and various others are discussed. Existing Group Key Management schemes have various flaws like user identity attributes are not protected and existing scheme doesn't handle scalability very well. So, a new GKM scheme known as Broadcast GKM is defined which is referred as access control vector BGKM. Two new approaches for privacy preserving ABAC systems are proposed for addressing the shortcoming of above cryptographic techniques. [10] discussed about creating Obstacles to Screened networks. In today's technological world, millions of individuals are subject to privacy threats. Companies are hired not only to watch what you visit online, but to infiltrate the information and send advertising based on your browsing history. People set up accounts for facebook, enter bank and credit card information to various websites. Those concerned about Internet privacy often cite a number of privacy risks events that can compromise privacy which may be encountered through Internet use. These methods of compromise can range from the gathering of statistics on users, to more malicious acts such as the spreading of spyware and various forms of bugs (software errors) exploitation.

According to Efficient and Secure Dynamic Auditing Protocol for Integrity Verification in Cloud Storage - Priyanga.R, Maheswari.B, Karthik.S, the authors quoted on, Information owners stores the data in the cloud servers and is accessible to data consumers. However, this new model of data hosting service brings unique security and privacy challenges. Data integrity is important factor of cloud computing which can be safeguarded by introducing auditing protocols within the cloud. Given that the data is dynamically updated in the cloud some existing remote integrity checking strategies can't be applied as they solely serve for static archive information. Economical and privacy-auditing protocol scheme extends the auditing protocol. This scheme protects data privacy and also data loss by merging the cryptography mechanism and additive property of bilinear pairing with time stamp. Batch auditing for data owners and clouds is also supported in this scheme. The proposed auditing scheme reduces the computation time in comparison with other existing auditing schemes. Because of the fragmentation technique used the data tag generation

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 3, March 2017

is reduced thereby preserving the storage space. Actual information in cloud is hidden from the auditor.

According to Reputation Attacks Detection for Effective Trust Assessment Among Cloud Services - Talal H. Noor, Quan Z. Sheng, and Abdullah Alfazi, the authors quoted on, concentration of this paper is mainly on detection of reputation attacks and assessing the trust among cloud services. SLAs which are basically are contract between service providers and end users are not enough to establish trust because of its ambiguous and inconsistent clauses [8], In -fact in a recent study [19] 46.6% consumers agree SLA's terms are unclear. So, to measure the trustworthiness of cloud services feedback given by the consumers becomes a reliable source but it is not uncommon for a trust management system to experience reputation attacks. These attacks can be collusion attacks or Sybil attacks. Here the authors introduce a credibility model which detects these reputation attacks which can be strategic or occasional. Huge collection of consumer feedbacks is taken to evaluate and establish their approach. In short, the model consists of protocol called ZKC2P which proves credibility of consumer's feedback, Collusion Attacks Detection including feedback density and occasional feedback collusion, Sybil attack detection along with metrics to detect multi identity recognition and occasional Sybil attacks.

According to TrustCloud: A Framework for Accountability and Trust in Cloud Computing – Ryan K L Ko, Peter Jagadpramana, Miranda Mowbray, Siani Pearson, Markus Kirchberg, Qianhui Liang, Bu Sung Lee, the authors quoted on, the authors discuss issues of the trust and complications of the cloud environment. Above literature papers established, lack of trust in clouds by customers is key issue in expansion of cloud computing. Areas like security and privacy in cloud environment has been extensively researched by numerous researchers, but there is little focus on cloud accountability and auditability. Cloud accountability has become a key issue because of the data distribution and virtualization done in clouds. Though trust in clouds can't be exactly described, components of trust in cloud computing can be attributed to four key factors Security [12] [13], Privacy [14] [15], Accountability [15] [16], Auditability [17]. We can also classify the trust components into preventive controls and detective controls. Here cloud accountability is categorized into different phases collectively known as Cloud Accountability Life Cycle(CALC) [18]. Finally, a TrustCloud Framework is proposed for assessing cloud accountability by categorizing them into five layers.

III. PROPOSED APPROACH

CloudShield framework uses Service oriented architecture to deliver Trust as a service. SOA and Web services are the prominently used technologies in cloud environment because any kind of resources whether they are infrastructures or platforms or software are resided in clouds as services. The TMS is spread over multiple distributed nodes so that the feedbacks generated can be handled in decentralized way. Figure 1 shows the framework, consisting of three distinct layers, namely the Cloud Service Provider Layer, the TMS Layer, and the Cloud Service Consumer Layer.

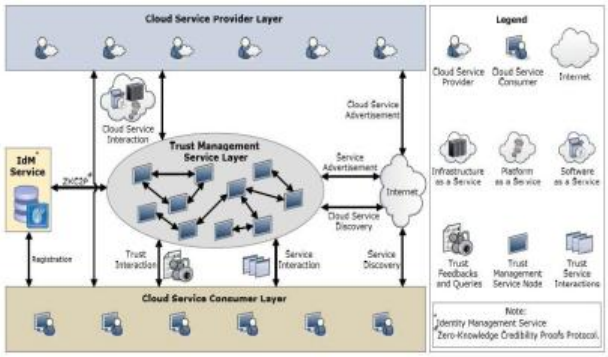

Fig.1. System Architecture

1) The Cloud Service Provider Layer.

Multiple cloud services are provisioned by the service providers which are categorized as i) IaaS or Infrastructure as a service which offers hardware, networking and hosting servers, ii) PaaS or Platform as a service which is a middle layer used by coders, programmers and developers, iii) SaaS or Software asa service built on above layers which is used by majority of users to access applications, web tools and software. Cloud service interaction between users and TMS is carried out in this layer, and cloud services advertisements where cloud providers are able to advertise their services.

2) The Trust Management Service layer.

This layer describes multiple cloud environments which are residing at distinct locations hosts numerous distributed TMS nodes. Consumers provide their feedback or inquire the trust results using the interfaces enabled by these TMS nodes. Operations of TMS layer include: i) Interactions of cloud service providers with the cloud services, ii) Advertising the services of cloud providers and TMS using service registry, iii) Discovery of cloud services and trust assessment of new cloud services by the users through web portal, and iv) A protocol to measure the credibility of the consumer's feedback known as ZKC2P protocol.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 3, March 2017

3) The Cloud Service Consumer Layer.

Finally, this layer comprises of different user base registered for cloud services. This layer includes: i) Discovery of any new cloud services and other existing services using service discovery mechanism, ii) trust interaction and service interaction where users are able submit their feedback or examine the trust results of a cloud service, and iii) Establishing the user identity by checking the credentials of the users in the IdM.

The important features of CloudShield are:

Zero-Knowledge Credibility Proof Protocol (ZKC2P). Introduction of ZKC2P ensures the users' privacy and also helps the TMS to establish the credibility of the feedback received. Trust feedback credibility is measured by ZKC2P which uses Identity Management Service (IdM), but IdM breaches the user privacy. To overcome this drawback different encryption mechanisms are investigated to safeguard the privacy of the user from such breaches. These anonymization methods mask the user identity and their interactions in the system.

A Credibility Model. Credibility of the feedbacks submitted by the users over distributed TMS nodes determine the performance of the TMS. So, the detection of the reputation attacks is important. Our proposed methods detect feedback collusion which involves, Feedback Density and also Occasional Feedback Collusion. These mechanisms differentiate credible feedbacks and misleading feedbacks into separate clusters. These collusion attacks can be of strategic or occasional behaviour depending on the length of time. We can also able to detect Sybil attacks. Detection of the reputation attacks helps us in identifying the malicious users who try to affect the reputation of the cloud service.

An Availability Model. In TMS, high availability is an essential factor. So, several distributed TMS nodes are used to manage feedbacks submitted by users. To spread the workload between TMS nodes, load balancing mechanisms are implemented and in-turn maintaining availability level. Operational power metric determines the TMS nodes required. Replication techniques are used to minimize the number of inoperable TMS nodes. Replication determination metric uses particle filtering methods to establish the availability of each node.

IV. CONCLUSION

Given the dynamism of cloud, establishing trust between users and cloud services proves to be a significant challenge for the global adoption and growth of cloud environment. To measure the trustworthiness of cloud services consumer feedback proves to be a reliable source. But cloud services often experience malicious behavior from the users who try to mislead others by giving false feedbacks against or in favor of a particular cloud service for various reasons. This type of deception is called as reputation attacks which is categorized into collusion attacks and Sybil attacks. In this paper, we analyzed and implemented various trust mechanisms which helps in detecting those attacks. We have exploited a credibility model which identifies collusion attacks and Sybil attacks over short or long time. TMS node Availability is determined using availability model. In the future we hope to increase the accuracy of the trust result by combining different trust management techniques such as reputation and recommendation. The further research work includes enhancement of the trust management performance.

REFERENCES

[1] Rajkumar Buyya, Christian Vecchiola, Thamarai Selvi, Mastering in Cloud Computing, Morgan Kaufmann, May 2013.

[2] S. M. Khan and K. W. Hamlen, "Hatman: Intra-Cloud Trust Management for Hadoop," in Proc. CLOUD'12, 2012.

[3] S. Pearson, "Privacy, Security and Trust in Cloud Computing," in Privacy and Security for Cloud Computing, ser. Computer Communications and Networks, 2013, pp. 3–42.

[4] J. Huang and D. M. Nicol, "Trust Mechanisms for Cloud Computing," Journal of Cloud Computing, vol. 2, no. 1, pp. 1–14, 2013.

[5] K. Hwang and D. Li, "Trusted Cloud Computing with Secure Resources and Data Coloring," IEEE Internet Computing, vol. 14, no. 5, pp. 14–22, 2010.

[6] S. Yu, C. Wang, K. Ren, and W. Lou. Attribute based data sharing with attribute revocation. In ASIACCS 2010: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, pages 261–270, 2010.

[7] S. Yu, C. Wang, K. Ren, and W. Lou. Achieving secure, scalable, and fine-grained data access control in cloud computing. In INFOCOM 2010: Proceedings of the 29th conference on Information communications, pages 534–542, 2010.

[8] S. Habib and et al., "Fusion of Opinions under Uncertainty and Conflict - Application to Trust Assessment for Cloud Marketplaces," in Proc. of TrustCom'2012, 2012.

[9] S. Habib, S. Ries, and M. Muhlhauser, "Towards a Trust Management System for Cloud Computing," in Proc. of TrustCom'11, 2011.

[10] Christo Ananth, P.Muppidathi, S.Muthuselvi, P.Mathumitha, M.Mohaideen Fathima, M.Muthulakshmi, "Creating Obstacles to Screened networks", International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Volume 1,Issue 4,July 2015, pp:10-14

[11] ICO. (2013, Jul.) "Guidance on the use of cloud computing," Information Commissioner's Office, UK. [Online]. Available: http://www.ico.org.uk/for organisations/data protection/topic guides/online/cloud computing.

[12] J. Brodkin, "Gartner: Seven cloud-computing security risks," Infoworld, 2008, pp. 1–3.

[13] M. Vouk, "Cloud computing—Issues, research and implementations," Proc. 30th International Conference on Information Technology Interfaces, 2008 (ITI 2008) IEEE, 2008, pp. 31-40.

[14] S. Pearson, "Taking account of privacy when designing cloud computing services," Proc. 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, IEEE Computer Society, 2009, pp. 44-52.

[15] S. Pearson and A. Charlesworth, "Accountability as a way forward for privacy protection in the cloud," Cloud Computing, 2009, pp. 131- 144.

[16] A. Haeberlen, "A case for the accountable cloud," ACM SIGOPS Operating Systems Review, vol. 44, no. 2, 2010, pp. 52-57.

[17] D. Catteddu and G. Hogben, Cloud Computing Risk Assessment, European Network and Information Security Agency (ENISA) 2009.

[18] R.K.L. Ko, B.S. Lee and S. Pearson, "Towards Achieving Accountability, Auditability and Trust in Cloud Computing," Proc. International workshop on Cloud Computing: Architecture, Algorithms and Applications (CloudComp2011), Springer, 2011, pp. 5.

[19] F. Dickmann, M. Brodhun, J. Falkner, T. Knoch, and U. Sax, "Technology transfer of dynamic it outsourcing requires security measures in slas," in Economics of Grids, Clouds, Systems, and Services. Springer Berlin / Heidelberg, 2010, vol. 6296, pp. 1–15