International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 09
August 2017

A Review on Security Concern with Trusty Supporting Reputation-based Management for Cloud Services

G. Vinay Kamal[1], M.Ashok Kumar[2], B.Suresh[3]

[1]M.Tech (CS), Vikas Group of Institutions, A.P., India.

[2-3] Assistant professor, Dept. Of CSE, Vikas Group Of Institutions, A.P., India.

Abstract *— cloud computing is gaining a considerable momentum as a new computing paradigm for providing flexible services, platforms, and infrastructures on demand. In cloud services make the trust management in cloud environments a significant challenge. According to researchers at Berkeley, trust and security is ranked one of the top 10 obstacles for the adoption of cloud computing. Cloud computing(CC)helps IT companies to focus on their business or strategic projects rather than technical aspects. Mainly three service model are offered by cloud which are Infrastructure as a service (IaaS), Platform as a Service (PaaS) and Software as a service (SaaS). At SaaS level applications are hosted by providers on network, these services are used by customers over internet on demand basis. A web browser is used to access different software's from the cloud providers. A user need not to install software on his machine, only an instance of software is needed. For example Google Apps, SQL Azure. In PaaS model as name implies it gives platform to build various applications. Various facilities offered by PaaS to deploy applications include application designing, development, testing and hosting. In the process one of the most challenging issues for the adoption and growth of cloud computing. For improvements in the classical work is enhanced using simulated annealing that is very effective and making use of metallurgy based implementations. In metallurgy, the temperature factor is taken for the forging and development of metal components. The freezing point is achieved in a loop of down level temperature. In this work, the simulated annealing based implementation is used with the integrated with dynamic security key for enhanced security trust architecture. The proposed META (Metaheuristic Enhanced Trust Assessment) architecture is giving effective results in terms of turnaround time, security factor, cost, complexity and trust value.*

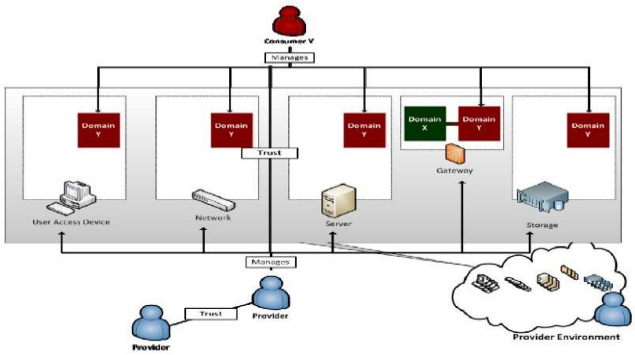
Keywords — ***Cloud Computing, Trust Management, Confidentiality, META Approach, Security Concerns.***

1. INTRODUCTION

Trust is a social problem. There are lots of definitions of trust. Basically trust refers to confidence or belief of one entity on other. One cannot build trust in a day. It is normally based upon provider's position in market. As users are putting their resources on provider's datacentres so there is major concern about the trustworthiness of providers and services. Two parties are involved in any trusted relationship: one is trusting party (i.etrustor) and other party to be trusted (i.e trustee) [1]. Various risks are involved: location security risk, data disclosure

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 09
August 2017

problem, data misplacement issue, data investigation concern. In cloud environment hostile user can add malicious code and take CPU space, resources and time. To model attractive cloud computing, trust should be introduced and there should be some trustworthy regions where users can deploy their applications and use resources safely. The highly dynamic, distributed, and nontransparent nature of cloud services make the trust management in cloud environments a significant challenge. According to researchers at Berkeley, trust and security is ranked one of the top 10 obstacles for the adoption of cloud computing. Indeed, Service-Level Agreements (SLAs) alone are inadequate to establish trust between cloud consumers and providers because of its unclear and inconsistent clauses. Consumers' feedback is a good source to assess the overall trustworthiness of cloud services. Several researchers have recognized the significance of trust management and proposed solutions to assess and manage trust based on feedbacks collected from participants. In reality, it is not unusual that a cloud service experiences malicious behaviors (e.g., collusion or Sybil attacks) from its users. This system focuses on improving trust management in cloud environments by proposing novel ways to ensure the credibility of trust feedbacks.



2. RELATED WORK

THE highly dynamic, distributed, and nontransparent nature of cloud services make the trust management in cloud environments a significant challenge. According to researchers at Berkeley, trust and security are ranked one of the top 10 obstacles for the adoption of cloud computing. Indeed, Service-Level Agreements (SLAs) alone are inadequate to establish trust between cloud consumers and providers because of its unclear and inconsistent clauses. Consumers' feedback is a good source to assess the overall trustworthiness of cloud services. Several researchers have recognized the significance of trust management and proposed solutions to assess and manage trust based on feedbacks collected from participants. In reality, it is not unusual that a cloud service experiences malicious behaviors (e.g., collusion or Sybil attacks) from its users. This paper focuses on improving trust management in cloud environments by proposing novel ways to ensure the credibility of trust feedbacks. In particular, we distinguish the following key issues of the trust

management in cloud environments:

• *Consumers' Privacy.* The adoption of cloud computing raise privacy concerns . Consumers can have dynamic interactions with cloud providers, which may involve sensitive information. There are several cases of privacy breaches such as leaks of sensitive information (e.g., date of birth and address) or behavioral information (e.g., with whom the consumer

interacted, the kind of cloud services the consumer showed interest, etc.). Undoubtedly, services which involve consumers' data (e.g., interaction histories) should preserve their privacy.

• *Cloud Services Protection.* It is not unusual that a cloud service experiences attacks from its users. Attackers can disadvantage a cloud service by giving multiple misleading feedbacks (i.e., collusion attacks) or by creating several accounts (i.e., Sybil attacks). Indeed, the detection of such malicious behaviors poses several challenges. Firstly, new users join the cloud environment and old users leave around the clock. This consumer dynamism makes the detection of malicious behaviors (e.g., feedback collusion) a significant challenge. Secondly, users may have multiple accounts for a particular cloud service, which makes it difficult to detect Sybil attacks. Finally, it is difficult to predict when malicious behaviors occur (i.e., strategic VS. occasional behaviors).

• *Trust Management Service's Availability.* A trust management service (TMS) provides an interface between users and cloud services for effective trust management. However, guaranteeing the availability of TMS is a difficult problem due to the unpredictable number of users and the highly dynamic nature of the cloud environment. Approaches that require understanding of users' interests and capabilities through similarity measurements or operational availability measurements (i.e., uptime to the total time) are inappropriate in cloud environments. TMS should be adaptive and highly scalable to be functional in cloud environments. In this paper, we overview the design and the implementation of Cloud Armor (cloud consumers credibility Assessment & trust management of cloud services): a framework for reputation-based trust management in cloud environments. In Cloud Armor, trust is delivered as a service (TaaS) where TMS spans several distributed nodes to manage feedbacks in a decentralized way. Cloud Armor exploits techniques to identify credible feedbacks from malicious ones. In a nutshell, the salient features of Cloud Armor are:

• *Zero-Knowledge Credibility Proof Protocol (ZKC2P).* We introduce ZKC2P that not only preserves the consumers' privacy, but also enables the TMS to prove the credibility of a particular consumer's feedback. We propose that the Identity Management Service (IdM) can help TMS in measuring the credibility of trust feedbacks without breaching consumers' privacy. Anonymization techniques are exploited to protect users from privacy breaches in users' identity or interactions.

• *A Credibility Model.* The credibility of feedbacks plays an important role in the trust management service's performance. Therefore, we propose several metrics for the feedback collusion detection including the *Feedback Density* and *Occasional Feedback Collusion*. These metrics distinguish misleading feedbacks from malicious users. It also has the ability to detect strategic and occasional behaviors of collusion attacks (i.e., attackers who intend to manipulate the trust results by giving multiple trust feedbacks to a certain cloud service in a long or short period of time). In addition, we propose several metrics for the Sybil attacks detection including the *Multi-Identity Recognition* and *Occasional Sybil Attacks*. These metrics allow TMS to identify misleading feedbacks from Sybil attacks.

3. LITERATURE SURVEY

Universally Composable Multiparty Computation with Partially Isolated Parties

It is well known that universally composable multiparty computation cannot, in general, be achieved in the standard model without setup assumptions when the adversary can corrupt an arbitrary number of players. One way to get around this problem is by having a trusted third party generate some global setup such as a common reference string (CRS) or a public key infrastructure (PKI). The recent work of Katz shows that we may instead rely on physical assumptions, and in particular tamper-proof hardware tokens. In this paper, we consider a similar but strictly weaker physical assumption. We assume that a player (Alice) can partially isolate another player (Bob) for a brief portion of the computation and prevent Bob from communicating more than some limited number of bits with the environment. For example, isolation might be achieved by asking Bob to put his functionality on a tamper-proof hardware token and assuming that Alice can prevent this token from communicating to the outside world. Alternatively, Alice may interact with Bob directly but in a special o_ce which she administers and where there are no high-bandwidth communication channels to the outside world. We show that, under standard cryptographic assumptions, such physical setup can be used to UC-realize any two party and multiparty computation in the presence of an active and adaptive adversary corrupting any number of players. We also consider an alternative scenario, in which there are some trusted third parties but no single such party is trusted by all of the players. This compromise allows us to signi_cantly limit the use of the physical set-up and hence might be preferred in practice.

Efficient and Secure Dynamic Auditing Protocol for Integrity Verification In Cloud Storage

In cloud computing, information homeowners host their information on cloud servers and users (data consumers) will access the information from cloud servers. As a result of the information outsourcing, however, this new paradigm of knowledge hosting service additionally introduces new security challenges, which requires associate freelance auditing service to ascertain the information integrity within the cloud. Some existing remote integrity checking strategies can solely serve for static archive information and, thus, can't be applied to the auditing service since the information within the cloud are often dynamically updated. Thus, economical and secure dynamic auditing protocol is desired to convert information homeowners that the information area unit properly holds on in the cloud. Economical and privacy-preserving auditing protocol was proposed to provide data integrity. Then, this scheme extends the auditing protocol to support the information dynamic operations, that is economical and incontrovertibly secure in the random oracle model. Also auditing protocol supports batch auditing for each multiple homeowners and multiple clouds, without exploitation any sure organizer. The analysis and simulation results show that projected auditing protocols area unit secure and efficient, particularly it scale back the computation value of the auditor.

Trusted Cloud Computing with Secure Resources and Data Coloring

In recent days more attention is paid towards data hiding, this paper aims at providing confidentiality and integrity towards both the data as well as image. Reversible data hiding (RDH) in encrypted images provides excellent property that the original cover can be losslessly recovered. All the previous methods of embedding data by reversibly vacating room after encryption may subject to some errors on the data as well as image extraction. In this paper I propose a novel method by reserving room before encryption with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted images. The proposed method can achieve real reversibility, that is data extraction and image recovery are free from any error. Experiments show that this novel method can embed more than 10 times lager payloads (i.e) efficiency for the same image quality as the previous methods.

4. CONCLUSION & FUTURE ENHANCEMENT

Given the highly dynamic, distributed, and nontransparent nature of cloud services, managing and establishing trust between cloud service users and cloud services remains a significant challenge. Cloud service users' feedback is a good source to assess the overall trustworthiness of cloud services. However, malicious users may collaborate together to i) disadvantage a cloud service by giving multiple misleading trust feedbacks (i.e., collusion attacks) or ii) trick users into trusting cloud services that are not trustworthy by creating several accounts and giving misleading trust feedbacks (i.e., Sybil attacks). In this paper, we have presented novel techniques that help in detecting reputation based attacks and allowing users to effectively identify trustworthy cloud services. In particular, we introduce a credibility model that not only identifies misleading trust feedbacks from collusion attacks but also detects Sybil attacks no matter these attacks take place in a long or short period of time (i.e., strategic or occasional attacks respectively). We also develop an availability model that maintains the trust management service at a desired level. We have collected a large number of consumer's trust feedbacks given on real-world cloud services (i.e., over 10,000 records) to evaluate our proposed techniques. The experimental results demonstrate the applicability of our approach and show the capability of detecting such malicious behaviors. There are a few directions for our future work. We plan to combine different trust management techniques such as reputation and recommendation to increase the trust results accuracy. Performance optimization of the trust management service is another focus of our future research work.

REFERENCES

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

[2] 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.

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

[4] 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.

[5] 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," *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.

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

[7] 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. Of CLOUD'10*, 2010.

[8] W. Conner, A. Iyengar, T. Mikalsen, I. Rouvellou, and K. Nahrstedt, "A Trust Management Framework for Service-Oriented Environments," in *Proc. of WWW'09*, 2009.

[9] T. H. Noor, Q. Z. Sheng, and A. Alfazi, "Reputation Attacks Detection for Effective Trust Assessment of Cloud Services," in *Proc. of TrustCom'13*, 2013.

[10] T. H. Noor, Q. Z. Sheng, S. Zeadally, and J. Yu, "Trust Management of Services in Cloud Environments: Obstacles and Solutions," *ACM Computing Surveys*, vol. 46, no. 1, pp. 12:1–12:30, 2013.

[11] S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising From Cloud Computing," in *Proc. CloudCom'10*, 2010.

[12] 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, 2009.

[13] E. Friedman, P. Resnick, and R. Sami, *Algorithmic Game Theory*. New York, USA: Cambridge University Press, 2007, ch. Manipulation-Resistant Reputation Systems, pp. 677 697.

[14] T. H. Noor, Q. Z. Sheng, and A. Alfazi, "Reputation Attacks Detection for Effective Trust Assessment of Cloud Services," in *Proc. of TrustCom'13*, 2013.

About authors:

Mr. G.VINAY KAMAL is a student of **VIKAS GROUP OF INSTITUTIONS**, Nunna, VIJAYAWADA. He is presently pursuing his M.Tech degree from JNTU,Kakinada.

Mr. M.ASHOK KUMAR is presently working as Assistant professor in CSE department,Vikas group of institutions , Nunna ,Vijayawada.

Mr. B.SURESH is presently working as Head of the Department in CSE department, Vikas group of institutions , Nunna, Vijayawada.