IJITKM Volume 8 • Number 1 June-Dec 2014 pp. 50-54 (ISSN 0973-4414)

A Survey on Trust Based Security and Privacy Issues of Cloud Computing Framework

Usvir Kaur[1]
Research Scholar, I.K. Gujral Punjab Technical University, Jalandhar, Punjab, India,

Dr. Dheerendra Singh[2]
Professor, Dept. of Computer Science & Engineering Shaheed Udham Singh College of Engineering and Technology, Tangori, Mohali, Punjab, India.

***Abstract*— Usage of cloud computing services have been increasing day by day since it introduced. Due to the increasing factor of usability and dependability of the internet by individuals and organizations, today every small/large scale organization is demanding the services of cloud computing, it provides lots of very good and advance services like (PaaS), (SaaS), (IaaS), which delivers very cost effective and advance solution's regarding the daily usability's of the organizations, but if cloud computing has lot of benefits then it has also some problems, like the main problem is "Trust based relationships". In this paper we briefly describes the security and privacy issues of cloud computing because security and privacy are the two very important factors of trust based relationships, which are the reasons behind the problems of trust based management systems between the clients and the service providers. We also describes some more aspects of cloud computing based on parameters such as data integrity, reliability and vendor-lock-in problems.**

Keywords*— *Cloud computing; Qos; SLA; Cloud audit; Data reliability; Data security; Data privacy; Trust management system; Data integrity; Attribute certification;

I. INTRODUCTION

Today we know cloud computing has become very powerful and provides very advance solution's to the IT and computing sectors. All small/large scale organizations, institutions and individual users are using cloud services, these type of services provide by the cloud service providers and they charge such amount for these services on the bases of "Pay As You Go", means we just need to pay only amount of money according to our usage of cloud services, but there are some issues have been rising for some last years and these issues are related to the security and privacy of the users, which are using cloud services as for individual purposes or businesses purposes and we can say that the problem of cloud computing services is "Trust", which is the main factor behind the relationship between the users and the service providers, because trust plays a vital role in the usage of cloud computing services in commercial environments.

We know cloud computing transform the resources into reality of dreams called "Utility Computing", with this capability we can use on-demand-services any time from any location, no need to plan expensive infrastructures to start IT based company, and cloud computing services fulfilled everything that related to software, platform and infrastructure. In this service has great potential for instant access, utility and scalability features, but on the other hand there some security related gaps are available in the cloud computing services, which includes many problems of trust, threats, security and privacy.

Cloud computing infrastructure provides very good capabilities to their customers, which includes network, on-demand, storage space, online and offline applications etc. Cloud computing infrastructure provides the power to user, to control and use cloud services according to their needs. But invasion of security is a very critical and serious problem of the cloud services, because it can be possible employees of the service provider company threat or corrupt the data of the users from the cloud servers. So trust based security and privacy is very important for the CSP's to insure the quality of service for the customers.

II. BACKGROUNDS AND RELATED WORK

There are lots of models and security tools have been introduced to solve the problems of security and privacy issues, some of which have been extensively discussed from different contexts, but they still lacks and don't pictured fully to the context of problems. The Trust mechanisms for cloud computing by Jingwei Huang [1] identified all the trust based attributes and objects to clarify actually where the trust factor stands in the cloud computing and what is the importance of trust in relationship between the users and the service providers. They evaluate all the trust based factors in detail like semantics of trust in cloud computing, how to work trust mechanism, poly based trust mechanism, proof based trust mechanism and many more important things which evaluate the trust factors. Trust factor is an important thing for the strong and trust based relationship between the CSP's and customers.

The question is how to measure the trust factor of a cloud computing service providers, how to know about the service is good or not on the prospective of security and privacy. According to the Paul Manuel [5] we can measure the trust in two ways. First, we notice about the present capabilities and service feedbacks of the vendor. Second, we look at past user feedbacks and credentials about the service provider. This is because past feedbacks and credentials about the vendor tells us the past service record and reputation of that vendor and present credentials and service tells us, what is offered in

present by a particular vendor. It includes service and what type of resources vendor provides for the cloud computing like reliability, security and privacy, trust management system conditions, data integrity, turnaround time, availability. Recourses of cloud computing includes the present status of environment security level, average throughput of computing power, processor capabilities and speed, RAM size of the system, capacity of hard disk. So it is very important, first look at these present and past records and feedbacks, when you are selecting a service provider for the cloud computing services.

In paper [2] author purposed trust based relationship model, which uses compliance based monitoring mechanism for the trust relationship between users and service providers. According to the author cloud computing services reduce the expenses of initial capital, which invests by the organization for their businesses and it also enhance the reliability, scalability and availability of the structure of the organizations workflow, but today still due to the unreliability of these cloud services users don't like to go with these options, which provides by the cloud service providers. Although (Service Level Agreement) SLA has introduced, which is a legal agreement between a client and service provider, but the problem is still available about the security and privacy, whether it is from service provider or from a user, which uses a service of cloud computing.

Virtualization is an important part of cloud computing because without it, cloud computing could never became like as it is today. In paper [3] author describes about the virtualization, what is the virtualization and actually how it effects on the security and privacy issues of cloud computing. To monitor the virtual machines (VM's) behavior on cloud computing infrastructure is critical for the cloud services. Today running infrastructures of cloud computing with virtual machines are very sensitive against the malicious behaviors, such that many of malicious attacks they cannot capture on the single and individual virtual machines with specific functions that cannot be used for VM's that are currently running with single cloud node of heterogeneous functionality, which causes the problems of security and privacy of users and service providers in cloud computing infrastructure.

III. CLOUD SERVICE MODELS

In this section, we briefly describes the cloud service models, which are very important part of the cloud computing framework and we can also say that without these service models cloud computing is nothing. We can see these all three important cloud service models in Fig.1, which are working together and independently without any problem. These all three service models plays a vital role in cloud computing.

These models are working with on-demand module schemas like if somebody demands data storage space or web space and software service on-demand, then we will use Software as a Service (SaaS) model to fulfill the need of a particular user. Similarly, software developers will choose Platform as a Service (PaaS) model because they can choose any platform for the development purposes and Infrastructure as a Service (IaaS) offers core networking related services for the network developers. Actually these three service models provides the access from physical infrastructure to the end user.

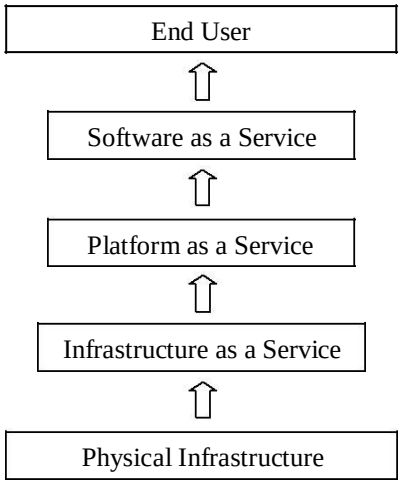

Fig. 1. Block diagram of cloud service models.

A. SaaS

SaaS stands for Software as a Service, in this model the service of applications and software's provide by the service providers to the users with on demand or pay as you use basis. Each customers has used his separate capabilities of service, which is different from the other users. In this service users can share the resources of his application with the other users like online slide shows, word processing tools, spreadsheet tools and customer relationship management tools etc. The important benefit of this service model is, it is easy to understand, no need to learn special skills for this service model. We can use this service with a little bit knowledge about the software's, which we have been used in our daily lives.

B. PaaS

Platform as a Service is also very important service model of the cloud computing, this model provides some high level configuration services like in this model we can use a whole platform for our work purposes. PaaS is normally used by the software developers, they can use any particular platform for their development needs. In this service model developers easily use a runtime environment, they can develop any of software with API's and configure them remotely, which demands a particular platform and runtime environment.

C. IaaS

It gives a huge opportunity to the users, it stands for Infrastructure as a Service, and in this service we can use resources of a computer as a service, which includes operating systems, virtual machines and hardware's. Resources can be use with the help of service Application Programming Interface (API). These all resources can be use through rent packages or pay as you go bases. All the resources are dynamically scalable, customer can change and upgrade any

of resources according to their needs. This service model mostly prefers by the network developers because with the help of Infrastructure as a service (IaaS), they can use all the resources as service with on single platform. Service providers also provides lot of internal API programs, which allow the users to use these services independently and easily without any problem.

IV. TRUST BASED SECURITY AND PRIVACY ISSUES

Security and Privacy are the two different but very important factors of any technology, which provides a service to the users but here we are talking about the cloud computing, which is today facing lot of serious problems regarding these two factors whether service is using by users or providing by service providers both are facing the problem. In this section we briefly describes the all issues of security and privacy of cloud computing services. In figure 2 we can see some important issues of cloud computing.

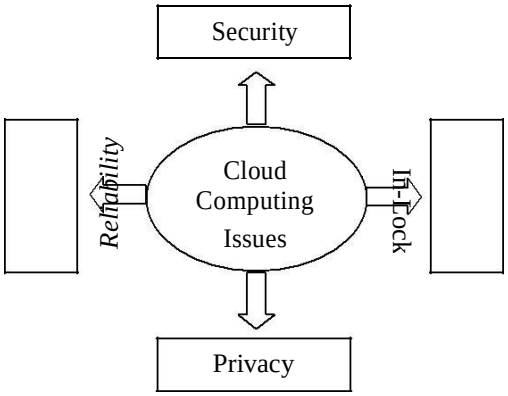

Fig. 2. Block diagram of cloud computing issues.

A. Privacy Issues

There are lot of privacy risks are available in the area of cloud computing, which are differ according to the type of cloud services. Some of cloud service areas have low risk factors but some cloud service areas have very high privacy risk factors like when we are using simple sharing services of information of our data, which we set as a public and we can share our information with anybody, so in this type of cloud service the risk of privacy is very low however if the service delivers dynamically allocations of personalized information of a particular user according to location, network topologies, social networks and preferences then it is a great deal for service providers to handle privacy threats, in this condition of service the potential risk of privacy threats is very high.

1. Lack of control

We know cloud computing provides us very good and advance technology, which delivers the capabilities to use our tools and software's from a single source based system, which used multiple nodes to handle heterogeneous type of work loads. Now the question is, what is our control on our applications and personal data?, which shuffled and stored from local systems to cloud servers, because client data processed and assessed in the server side on machines, users have not any control on the data. So there are many chances of data theft, data lose, data corruption, unauthorized access etc.

2. Unauthorized distribution of data

According to the author of paper [8], there are so many risk factors in the agreements and legal terminologies regarding cloud computing data distribution. Data may be distribute to the companies for unauthorized access, because there are not any legal terminologies given in the agreements, if the cloud company is acquired by another company or for some reason cloud company becomes bankrupt then there are not any guarantee, what purposes new company will use the data. For example, they can sale the data to another competitor companies or they can use the data for their personal gain.

3. Risks over data transfer

We know cloud computing is a service and users can assess these cloud based services via remote servers. So the connection between customers and service providers is always not protected. Every transaction of transfer or retrieval of data is facing many problems like risks of data threaten, Denial of Service and DNS spoofing attacks. Today every single person is using a smart phone and due to the cloud computing popularity, every smart phone is using the functionality of these services like sharing personal data via cloud service, even data which can be transferred locally to one device to another device, often users using the cloud service to transfer that data. Therefore users take risks of their private data without knowing actually what are the risks and problems of cloud computing services, users always assumes that, data which they are transferring to another device transferred locally.

B. Security Issues

Today in cloud computing, security perimeter factor is a main and important factor to create trust based relationship between the user and service provider. According to the author of paper [8] cloud computing infrastructure has been using a firewall model for security, which model was actually developed for the internet end hosts security purposes. Internet firewall system or we can say protocol is not properly working with the cloud computing infrastructure based services, because cloud based infrastructure made with a mixture of public and private deployment. In cloud computing sector, public cloud systems are facing many issues regarding the security concerns, because in a recent user survey results have showed, public cloud sectors have been facing top challenges in the security related problems. So this is the main reason why security perimeter of cloud computing becomes sophisticated and because of this problem chances of data threaten is increasing rapidly, so there is a need to develop and introduce new security infrastructure, which solves the problems of traditional security systems and handle the new and powerful mechanism of cloud computing security.

1. Data accessibility risks

Data accessibility is very critical problem in the cloud computing systems, we know when we are using cloud services, our data has stored on the cloud servers, which are situated in the different places of the world. Problem is begins here, because every cloud server is situated in a separate place, where government of that place has may be legal rights to access the users data and users may not be notified for this action of the government. Second we know security is an important issue of cloud computing and security of data is more critical then malicious activities, when it is processing in the cloud. Risks of data security threat is larger in the staff of cloud service providers, because they are highly trained and privileged to access the data.

2. Data backup and availability

We know today every business sector enhance the capabilities of work to shuffle with cloud computing services, but there are some major issues of cloud computing services like data backups and data threat possibilities. It is very serious problem for the business sectors, if they lose important and secret data on the cloud servers. There are not any assurance policy of cloud computing service providers regarding the data lose or threaten by the malicious behaviors or by internal official highly trained workers. Secondly service providers are not giving any information about the data storage, like where and on which servers they are storing users' data. So chances of data theft has being increased.

3. Multi-Tenancy with Virtual Machines

To provide the cloud computing services to users, with multi-tenancy architectural, some service provider vendors use resource management and job scheduling mechanisms, in which software's are designed for the virtualized distribution of work load on the different machines, so that each organization can use the customized virtual resources. But most of the service providers are using fully virtualized mechanism for the equal destitution of resources, because due to the virtualization it can be possible to distribute a single machine power equally for services between each users and completely isolated from each other. But the use of virtualization also introduce some new type of security related permeability, such as cross VM related side channel security attacks [10], which extract important information's from the same VM machine, which is using by a different user. So therefore strong security parameters are needed for the visualization mechanism.

4. Cloud Audit

Today cloud auditing has become a service that every organization wants to use to increase the audit related capabilities. But cloud service providers need to create the internal audit monitoring controls rather than external monitoring controls. Because cloud computing infrastructure is showing lot of new challenges of an audit related services, so existing environment for audit should be enhanced for the present and future requirements. Transactions which recorded for the auditing should be properly made and scanned, so that important and secure data not use publicly for the auditing purposes [7]. It should be important for data owner to trust on the environment, so that there are not any untraceable transactions take place in the cloud audit services.

V. RELIABILITY AND VENDOR-LOCK-IN

Reliability and Vendor-Lock-In are the two most common and serious problems, which are found in cloud computing services. So it is very important to the service providers to improve these problems, if they want to gain trust between them and customers. In this section we briefly explained what is the reason behind these two problems and how can service providers improve to the trust factor.

A. Reliability

Reliability and trust are the two very important factors between the users and cloud service providers but due the security and privacy issues in the cloud computing services, trust factor of users is decreasing day by day from the cloud computing services. So cloud computing service provider should take some steps like risks and issues of cloud services are well defined in the agreements, which signed between the customer and service provider, it should be mentioned in agreement about the storage and processing of data transparency related rules and if service providers provides the information about locations where the data of users is saved then trust and reliability can be increase between the user and cloud service provider.

B. Vendor-Lock-In problem

Vendor-Lock-In is very serious problem in cloud computing, it takes harassments to the customers, because in vendor-lock-in condition customer cannot easily migrate the data to new service provider. Customers are facing lot of problems when they want to change to a new service provider. It is happening, because the technology of cloud computing is comparably new and it follows the old standards, protocols and tools, this is the reason why migration is complicated and expensive on cloud computing but new standards still have being developed day by day according to the problems, which customers have being faced.

VI. CONCLUSION

In this paper we briefly described the backgrounds of cloud computing and its issues regarding the trust based relationships, which today have being faced by many customers. Cloud computing is a new and advance service, but the problem, which is today facing by all the customers, is old standards, that adopted by the cloud computing service providers. These old standards are not properly fit in the cloud computing scenario. So it is must to create the new standards and rules for the cloud computing. Also, cloud service providers need to improve the security and privacy mechanisms regarding the data, which stored by the customers on the cloud servers. It is very important for the service providers to ensure that security and privacy of customer's data will not be compromised at any condition. It is the only single factor, which creates trust among the all customers for

trust based adoption of cloud computing based services, because without the trust, customers will be afraid to use cloud computing based services. Protection of security and privacy makes trust based relationship between the users and service providers. So it is very important for the service providers to create a good environment, which gives the transparency to the customers on the bases of security and privacy factors.

Acknowledgement

Authors are highly thankful to the department of RIC, IKG Punjab Technical University, Kapurthala, Punjab, India for providing the opportunity to conduct this research work

REFERENCES

[1] Jingwei Huang, David M Nicol, "Trust mechanisms for cloud computing," in Proc. Journal of Cloud Computing: Advance, Systems and Applications 2013, 2:9, pp. 1-14.

[2] Jagpreet Sidhu, Sarbueet Singh, "Compliance based rustwortiness calculation mechanism in cloud environment," in Proc. International Workshop on Intelligent Techniques in Distributed Systems 37, 2014, pp. 439-446.

[3] Deqing Zou, Wenrong Zhang, "Design and implementation of a trusted monitoring framework for cloud platforms," in Proc. Future Generation Computer Systems 29, 2013, pp. 2092-2102.

[4] Imad M. Abbadi, Muntaha Alawneh, "A framework for esblishing trust in the cloud," in Poc. Computers and Electrical Engineering 38, 2012, pp. 1073-1087.

[5] Xiaonian Wu, Runlian Zhang, "A trust evaluation model for cloud computing," in Proc. Information Technology and Quantitative Management 17, 2013, pp. 1170-1177.

[6] Md. Tanzim Khorshed, A.B.M. Shawkat Ali, "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing, " Future Generations Computer Systems 28, 2012, pp. 833-851.

[7] Hall, J.A. & Liedtka, "The sarbanes-oxley act: implications for large-scale IT outsourcing," Communications of the ACM, 50(3), 2007, pp. 95-100.

[8] Wenjuan Fan, Harry Perros, "A novel trust management framework for multi-cloud environments based on trust service providers," Proceeding in Knowledge-Based Systems 70, 2014, pp. 392-406.

[9] Wei Wang, Guosun Zeng, "Cloud-DLS: dynamic trusted scheduling for cloud computing" Expert Systems with Applications 39, 2012, pp. 2321-2329.

[10] T. Ristenpart, E. Tromer, "Explorign information leakage in third-party compute clouds," CCS'09, ACM, Chicago, Illinois, 2009.

[11] Younis A. Younis, Kashif Kifayat, "An access control model for cloud computing," in Proc. Journal of Information Security and Applications 19, 2014, pp. 45-60.

[12] M.K. Munchahari, S.K. Sinha, "A new trust management architecture for cloud computing environment," in: Proceedings of 2012 International Symposium on Cloud and Services Computing (ISCOS), 2012, pp. 136–140.

[13] Siani Pearson, Axxedine Benameur, "Privacy, security and trust issues arising from cloud computing," in: Proceedings of 2010 IEEE Second International Conference on Cloud Computing technology and Science (CloudCom), 2010, pp. 693-702.

[14] S. Song. K. Hwang, "Fuzzy trust integration for security enforcement in grid computing," in: Proceedings of the Int'l Symposium on Network and Parellel Computing, LNCS 3222, Springer-Verlag. Berlin, 2005, pp. 9-21.

[15] C. Ngo, Y. Demchenko, "Toward a dynamic trust establishment approach for multi-provider intercloud environment," in: Proceedings of 2012 IEEE 4th International Conference on vloud Computing Technologyand Science (CloudCom), 2012, pp. 532–538.

[16] B. Gao, L. He, L. Liu, "From mobiles to clouds: developing energy-aware offloading strategies for workflows," in: Proc. of the 2012 ACM/IEEE 13th International Conference on Grid Computing, IEEE Computer Society, 2012, pp. 139-146.

[17] B. grobauer, T. Walloschek, E. Socker, "Understanding cloud-computing vulnerabilities," IEEE Security and Privacy, 2010.

[18] L. Yan, C. Rong, G. Zhao, "Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography," Cloud Computing, 2009, pp. 167-177.

[19] W. Lou, K. Ren, "Security, privacy, and accountability in wireless access networks," in: Proc. Wirless Communications IEEE 16, 2009, pp. 84-106.

[20] A. N. Khan, M. Mat Kiah, S. U. Khan, "Towards secure mobile cloud computing: A survey," in: Proc. Future Generation Computer Systems 29, 2013, pp. 1278-1299.

[21] H. Wang, S. Wu, "Security protection between users and the mobile media cloud," in Proc. Communications Magazine, IEEE 52, 2014, pp. 73-79.

[22] Abbadi IM., Alawneh M., Martin A., "A. Secure virtual layer management in clouds," Proc. in the 10th IEEE international conference on trust, Security and privacy in computing and communications (IEEE TrustCom-10), 2011, pp. 99-110.