Security Issues in Cloud Computing: A Review

[1]Anmol Bhandari, [2]Sonia Sharma
[1,2]Dept. of CSE, Guru Nanak Dev University, Amritsar, Punjab, India

Abstract
Now days, Cloud Computing is the most transpiring trend in Information Technology. Due to its salient features and advantages like scalability, easy and cheap access, throughput and on demand up and down grading of Iaas, Paas and Saas, it is attracting many organizations around the world. Besides all the advantages and pros of cloud environments, there are some risks and challenges also. The biggest of all the challenges is Privacy and Security. In this paper, a review of different security issues like trust, authenticity, encryption, confidentiality, resource sharing and key management are presented along with the efforts made on how to resolve these issues and threats.

Keywords
Cloud Computing, Security Issues, Trust, Confidentiality, Authenticity, Encryption

I. Introduction

With the advancement in technology, the IT infrastructure has changed completely. In thepast, an organization had to deploy expensive infrastructure to perform their routine tasks and store the operational data of the organization. Normally data was stored in Relational Databases on one or more servers located inside the organization and the clients needed to request data from the seserver machines. This was quite costly as the organization needed to hire personnel for deploying, managing and maintaining the infrastructure.

In the last decades, concept of Clusters [1] and Grid Computing [2] opened new ways for information architecture and storage. It became possible to store data on clusters or in the form of grids that were loosely coupled, heterogeneous and geographically dispersed [3]. The concept of Cloud Computing [4] is relatively a new concept originating its basis from Clusters [2] and Grid Computing [3]. It uses the same idea of broad network access and resource pooling but it is different from the cluster and grids as it can provide on-demand self- services [5] to it susers.

No doubt, Cloud Computing has provided many exciting services and features like flexibility, reliability, unlimited storage, portability and the quick processing power but cloud security is still a big issue [6]. Security issues including lack of trust, the risk of malicious insiders and the failing of cloud services have been discussed in [7]. This paper reviews different security threats to Cloud Computing like trust, privacy, confidentiality, Authenticity, encryption and discusses the presented solutions to overcome these issues. Each of the security threat will be discussed separately in different sections along with the viable solution in given domain.

This paper is composed into IV sections. Section I introduces cloud computing, its features and dilemmas. Section II is about background work incloud computing. Section III discussed indetail the problems and proposed solutions to tackle these problems. Section IV is the discussion of these issues and their solutions. In the end conclusion and future work is given.

II. Background Work

Being the most trending technology of the age, the research is being done widely on Cloud Computing and especially on cloud security. In December 2008, Cloud Security Alliance (CSA) [8] was formed with the aim to provide assured security within cloud computing environment. CSA launched “Security Guidance for Critical Areas of Focus in Cloud Computing” [9]as their initial product to help users get better insight about clouds and the security parameters. The Cloud Computing Interoperability Group and the Multi-Agency Cloud Computing Forum have made lot of efforts to deliver efficient and effective controls to provide information security in Cloud environment [31].

For now, many efforts have been made to find main security issues in cloud. It is described that privacy and the trust are the major security issues faced by the cloud computing [10]. Security and privacy challenges to cloud computing are discussed indetail in [11]. Where [12] also addresses the security issue. It is declared that cloud systems can’t grow without resolving security and privacy issues [13]. A cloud computing framework and information as set classification model were proposed so that to help cloud users choosing different delivery services and models [31].

III. Security Issues and Solutions

This section discusses the problems related to cloud computing and their proposed solutions.

A. Trust

Trust between customer and service providers is the main issue faced by cloud computing now days. Customer is never sure whether the Service is trust worthy or not and whether his data is secure from the intruders or not. The customer and Service provider are boundby Service Level Agreement (SLA) document. This is a type of an agreement between the customer and the service provider; it contains the duties of service provider and his future plans [7]. But unfortunately there are no standards for SLA.

Many efforts have been made till now to resolve the issues of trust and privacy to resolve the security issues incloud. A trust model is presented in [10] to enhance the security and interoper ability of cloud computing environment. Husky Healthcare Social Cloud [14] presentsa trustrating mechanism to secure the cloud environment in collaboration with social media. SLA Framework [15] is used in [16] to propose a trust management model for security in cloud environment.

B. Confidentiality

Confidentiality means to prevent the disclosure of private and important information. Since all the information is stored on geographically scattered locations, confidentiality becomes a major issue. Many methods are used to preserve confidentiality from which, encryption is the most used method. But it is relatively an expensive method.

To preserve privacy, a secure cloud storage service [17] is designed that is built upon the public cloud structure and by using cryptographic techniques, privacy is achieved. A new approach proposed by [18] uses hierarchy of P2P reputation system to preserve privacy. It gains it with virtualized defense.

[19] Describes that the attribute-based cryptography can be used to preserve privacy and maintain security in a cloud based EHR system and patients can share data in a flexible, scalable and dynamic manner.

C. Authenticity

Integrity is also a main issue faced by cloud computing. It refers to the improper modification of information. As the data resides indifferent places inacloud sothe access control mechanism should be very secure and each user must be verified as an authentic user.

Authentication problem can be solved by using the digital signatures but even after having access to digital signatures a user can't get access and verify the subsets of data.

An access control scheme presented by [20] is a decentralized and robust access control mechanism where the cloud user identity is verified by the cloud without knowing the user's identity before storing information. Information can be decrypted by only the authentic users. Replay attacks are also prevented in this scheme.

Another scheme [21] new setting is presented where the users are independent from the service providers and they don't need to register witht hem. Data owner provides the user the credential information. The username and password pair generates the identity information for each user that is provided to the service provider by the data owner. This scheme proves to be very scalable.

D. Encryption

To secure the data in cloud computing, the most widely used method is Encryption. But it also have some failure. High computational power is needed in encryption. Whenever a query is executed, the encrypted data need to be decrypted which results in the reduction of overall database performance. There are many methods present to make sure that better encryption in terms of better security and operations are provided.

A method proposed by [22] explains that instead of using only one cryptographic method, usage of multiple cryptographic methods can increment the overall throughput. Data is encrypted by using these methods in each and every cell of a table in a cloud. Whenever a user wants to make or execute a query, the query parameters are checked and evaluated against the data stored. The query results are decrypted by the user itself but not the cloud in order to increase the performance.

Another technique known as end-to-end policy based encryption[23] use different policy to encrypt data and different policy to decrypt data. The Trust Authority releases decryption keys which enables a user to get fine grained access control in public clouds. Another method known as fully Homomorphic encryption[24] is a latest trend that provides results of calculation performed on encrypted data rather than the raw data. It increments the confidentiality of data and provides better encryption.

E. Keymanagement

While doing encryption, we need encryption/decryption keys and managing these keys it self is a big security issue incloud environment. Storing these encryption keys on cloud is a bad option. It is easy to store single encryption key but for the real time systems it become a complex task to store these keys. This may require a separate small database to store the keys locally in a protected database. But again, that's not a good idea because the purpose for which we are shifting our data to clouds will become worthless. As by doing so we will need additional hardware and software resources and the cost issues will also arise. The only solution to key management may be through two-level encryption [25]. This can be very helpful to store encryption keys incloud.

F. Data Splitting

Data splitting may be the better alternative to encryption. It is surely very fast as compared to encryption itself.The main idea behind it is to split the data overmultiple hosts that are non-communicable. Whenever a user needs its data back, he must have access to both service providers to recollec this original data. No doubt it is very fast technique but it has its own security issues.

Multi-Cloud Database Model [7] is a method for data splitting where multiple clouds and different techniques are used toensure the integrity and availability of data after splitting it. In this way the security is very much enhanced as the data is stored and replicated inmultiple clouds and there are fewer chances of the intruders to attack. These clouds share data using secret sharing algorithm [26] and TMR technique [27].

G. Multitenancy

In a cloud environment, different resources and services are shared among different application sat different geographic locations. This is done to solve the issues of resource scarcity and to eliminate cost that is the main purpose of the cloud. But the sharing of the resources of an organization gives birth to confidentiality issues. These systems and applications must be isolated to some extent inorder to keep confidentiality alive. Otherwise it is very difficult to supervise the data flow and the insecurity is suesarise [28].

Data and applications in a cloud may be stored on virtual servers as well as on the actual hardware. In both of thecases there are security issues involved. If these are stored virtually, there are chances that one virtual machine hosting a malicious application can affect the performance of other machines. If these are stored on actual hardware, there may be security issues because of multi-core processing. Cloud providers should employ Intrusion Detection Systems to keep their customers safe incloud environment [29]. Anarchitecture to deploy IDS is presented in [29]. Trusted cloud computing platform (TCCP) is designed to provide better security of the virtual machines [30].

VI. Discussion

Cloud Computing has provided many exciting services and features like flexibility, reliability, unlimited storage, portability and the quick processing power but cloud security is still a big issue. Major security issues faced by the cloud like Trust, Confidentiality, Integrity, authentication, encryption and recourse sharing issues were discussed along with their solutions.

One main problem discussed is to define the proper format of SLA document to make it clear in service provider as well as in customers mind that what services the cloud is intended to provide and what the customers expect from the cloud.

Another major issue faced by cloud computing is encryption and to solve this issue, different mechanisms have been deployed like end-to-end policy based encryption [23], Cryptographic methods [22] and fully Homomorphic encryption [24].

Different trust management models [10], [14], [15], [16] are also discussed. Secure cloud storage service [17], Virtualized defense [18] and attribute-based cryptography [19]are discussed as the major confidentiality preserving techniques.Data splitting technique is discussed as an alternative to encryption and its model [7] is also described.

V. Conclusion

In this study, different security issues faced by cloud computing are discussed along with the possible available remedies to these problems. It can be concluded that the data encryption and trust are the two major issues in this regard followed by the authenticity and dataintegrity.

VI. Futurework

Cloud computing is relatively a new and widely emerging domain and it must have to overcome the security issues in order to bemore and more prominent technology of the future. A lot of research is being done in this regard to solve these major issues but still many problems are unseen and unknown and the doors for futurere search are always open.

References

[1] Buyya,Rajkumar,"High performance cluster computing", New Jersey: F'rentice (1999).

[2] Foster, Ian, Carl Kesselman, edsm.,"The Grid 2: Blueprint for a new computing infrastructure", Elsevier, 2003.

[3] What is grid computing? - Gridcafe. E- [Online Available: http://sciencecity.orgRetrieved2014-06-18.

[4] Armbrust, Michael, etal.,"Aviewofcloud computing", Communications of the ACM 53.4 (2010), pp. 50-58.

[5] Mell, Peter, Timothy Grance,"The NIST definition of cloud computing (draft)", NIST special publication 800.145(2011):7.

[6] Weis, J., Alves-Foss, J.,"Securing Database asaService", IEEE Security and Privacy, pp. 49-55, 2011.

[7] AlZain, M., Soh, B., Pardede, E.,"A New Approach Using Redundancy Technique to Improve Security in Cloud Computing.IEEE, 2012.

[8] Messmer, Ellen (March 31, 2009),"Cloud Security Alliance formed to promote best practices". Computer world.Retrieved May 02, 2014.

[9] "Security Guidance for Critical Areas of Focus in Cloud Computing". Cloud Security Alliance. Retrieved May 02, 2014.

[10] Li, Wenjuan, Lingdi Ping,"Trust model to enhance security and interoper ability of cloud environment", In Cloud Computing, pp. 69-79. Springer Berlin Heidelberg, 2009.

[11] Ko, RyanKL, etal.,"Trust Cloud:A framework for accountability and trust in cloud computing," Services (SERVICES), 2011 IEEE World Congress on. IEEE, 2011.

[12] Pearson, Siani, Azzedine Benameur,"Privacy, security and trust issues arising from cloud computing", Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on. IEEE, 2010.

[13] H. Takabi, J.B.D.Joshi, G.Ahn,"Security and privacy challenges in cloud computing environments. IEEE Security & Privacy; 8 (6), pp. 24–31, 2010.

[14] Wooten, Ryan, etal.,"Designandimplementation of a secure healthcare social cloud system", Cluster, Cloud and Grid Computing (CCGrid), 2012 12th IEEE/ACM International Symposium on. IEEE, 2012.

[15] M. Alhamad,"Conceptual SLA Framework for Cloud Computing", Accepted for IEEE DEST 2010 on 15 March 20-10-2010.

[16] Alhamad, Mohammed, Tharam Dillon, Elizabeth Chang,"Sla-based trust model for cloud computing", Network-Based Information Systems (NBiS), 2010 13th International Conference on. IEEE, 2010.

[17] Kamara, Seny, Kristin Lauter,"Cryptographic cloud storage", Financial Cryptography and Data Security. Springer Berlin Heidelberg, pp. 136-149, 2010.

[18] Hwang, Kai, Sameer Kulkareni, Yue Hu.,"Cloud security with virtualized defense and reputation-based trust mangement", Dependable, Autonomic and Secure Computing, 2009. DASC'09.Eighth IEEE International Conferenceon. IEEE, 2009.

[19] Narayan, Shivaramakrishnan, Martin Gagné, Reihaneh Safavi-Naini,"Privacy preserving EHR system using attribute-based infrastructure", Proceedings of the 2010 ACM workshop on Cloud computing security workshop. ACM, 2010.

[20] Yu, Shucheng, et al.,"Achieving secure, scalable, and fine-grained data access control in cloud computing", INFOCOM, 2010 Proceedings IEEE. IEEE, 2010.

[21] Yassin, AliA., etal.,"Efficient Password-based Two Factors Authentication in Cloud Computing", International Journal of Security & Its Applications 6.2, 2012.

[22] Purushothama. B., Amberker,B.,"Efficient Query Processing on Out sourced Encrypted Datain Cloud with Privacy Preservation, 2013.

[23] Pearson, Siani, et al.,"End-to-endpolicy-based encryption and management of data inthe cloud", Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on. IEEE, 2011.

[24] Tebaa, Maha, SaïdElHajji, AbdellatifElGhazi. "Homomorphic encryption applied to the cloud computing security", Proceedings of the World Congress on Engineering. Vol. 1, 2012.

[25] Wang, Guojun, Qin Liu, Jie Wu.,"Achieving fine-grained access control for secure data sharing on cloud servers", Concurrency and Computation: Practice and Experience 23. 12(2011): pp. 1443-1464.

[26] Shamir, Adi.,"How to share a secret" Communications of the ACM 22. 11(1979), pp. 612-613.

[27] Lyons, RobertE., Wouter Vanderkulk.,"The use of triple-modular redundancy to improve computer reliability", IBM Journal of Research and Development 6.2(1962), pp. 200-209.

[28] Behl,A.,Behl,K.,'An Analysis of Cloud Computing Security Issues. IEEE, pp. 109-114, 2012.

[29] Roschke, Sebastian, Feng Cheng, and Christoph Meinel. "Intrusion detection in the cloud." Dependable, Autonomic and Secure Computing, 2009. DASC'09. Eighth IEEE International Conferenceon. IEEE, 2009.

[30] Santos, Nuno, KrishnaP. Gummadi, Rodrigo Rodrigues, "Towards trusted cloud computing", Proceedings of the 2009 conference on Hottopics in cloud computing, 2009.

[31] Onwubiko, Cyril.,"Security issues to cloud computing", Cloud Computing. Springer London, 2010. pp. 271-288.