International Journal of Scientific Research in Computer Science and Engineering
Vol.6, Issue.3, pp.31-34 , June (2018)
Survey Paper
E-ISSN: 2320-7639

Cloud reliability enhancement mechanisms: A Survey

Vikas Mangotra[1*], Richa Dogra[2]

Dept. of CSE, GCET,Gurdaspur ,PTU Kapurthala, Punjab, India
Dept. of CSE, GCET,Gurdaspur , Punjab, India

Available online at: www.isroset.org

Received: 03/Jun/2018, Revised: 12/Jun/2018, Accepted: 20/Jun/2018, Online: 30/Jun/ 2018

***Abstract*—** In today's era cloud computing becomes the hottest topic due to its ability to reduce the cost associated with computing. Cloud computing provides the on demand services like storage, servers, resources etc. to the users without physically acquiring them and the payment is according to pay per use. Since cloud provides the storage, reduces the managing cost and time for organization to the user but security and confidentiality becomes the one of the biggest obstacle in front of us. The major problem with cloud environment is, the number of user is uploading their data on cloud storage so sometimes due to lack of security there may be chances of loss of confidentiality. To overcome these obstacles a third party is required to prevent data, data encryption, and integrity and control unauthorized access for data storage to the cloud. To optimize better results we will review some paper and find the better results to remove the security barriers.

***Keywords*—** *Cloud Computing, security, and confidentiality*

I. INTRODUCTION

With the rapid development of hardware and software cloud computing brings the revolution in the business industry[1]. It provides resources like computational power, storage, computation platform ad applications to user on demand through internet. Some of the cloud providers are Amazon, IBM, Google, Salesforce, Microsoft etc. Cloud computing features included resource sharing, multi-tenancy, remote data storage etc. but it challenges the security system to secure, protect and process the data which is the property of the individual, enterprises and governments. Even though, there is no requirement of knowledge or expertise to control the infrastructure of clouds; it is abstract to the user. It is a service of an Internet with high scalability, quality of service, higher throughput and high computing power[2]. Cloud computing providers deploy common online business applications which are accessed from servers through web browser. Data security is the biggest issue in cloud computing and it is not easy to resolve it. In our review paper we will review the different ways to manage the confidentiality of the data[3].

II. OBJECTIVES

With the rapid development of hardware and software cloud computing brings the revolution in the business industry[1]. It provides resources like computational power, storage, computation platform ad applications to user on demand through internet. Some of the cloud providers are Amazon, IBM, Google, Salesforce, Microsoft etc. Cloud computing features included resource sharing, multi-tenancy, remote data storage etc. but it challenges the security system to secure, protect and process the data which is the property of the individual, enterprises and governments. Even though, there is no requirement of knowledge or expertise to control the infrastructure of clouds; it is abstract to the user. It is a service of an Internet with high scalability, quality of service, higher throughput and high computing power[2]. Cloud computing providers deploy common online business applications which are accessed from servers through web browser. Data security is the biggest issue in cloud computing and it is not easy to resolve it. In our review paper we will review the different ways to manage the confidentiality of the data[3].

III. SECURITY ISSUES IN CLOUD COMPUTING

In cloud environment usual data transmission occurs between client and server using third party. So the confidentiality of your data becomes the primary problem. Security issues for a significant number of these frameworks and innovations are pertinent to distributed computing[5]. For instance, the system that interconnects the frameworks in a cloud must be secure and mapping the virtual machines to the physical machines must be completed safely. Information security includes encoding the information and additionally guaranteeing that suitable strategies are implemented for information sharing[6]. Cloud security isn't to be mistaken for "cloud-based" security benefit over the conventional danger. This security administration can be upgraded with the distributed computing, ensuring against DDOS, Trojan, Virus and Spam memory[7].

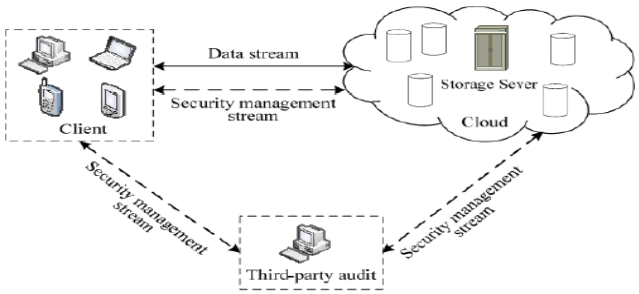

Figure 1: Data storage structure of Cloud Computing

However, the qualities of distributed storage make clients' information looked with numerous security dangers, incorporates: (1) the conventional security district parcel is invalid. On account of the distributed storage benefit must be adaptable, security limits and assurance hardware can't be unmistakably characterized, which builds some trouble for the usage of particular assurance measures; [8](2) the distributed storage transmits information through the system. The benefit interferences, information devastation, data stolen furthermore, altered caused by the noxious assaults in the organize represent a serious test to the security of information correspondences, get to confirmation and classification; [9](3) from the client's view, the distributed storage of information makes distributed computing specialist co-op gets the information get to control, and the client's information is looked with protection security dangers. Individuals stress over that the touchy individual information will be exposure, abuse or missing by putting the information in cloud condition[10].

To tackle the above issues, as of late, scientists made a parcel of research work in the information security to control systems, information respectability, confirmation, cipher text to recover and information encryption system of cloud figuring condition[11].

There are heaps of security issues with distributed computing in light of advances usage including systems, working frameworks, databases, asset booking, virtualization, stack adjusting, exchange administration, memory administration and simultaneousness control. For instance, the system ought to be secure on cloud with the goal that mapping the virtual machines to the physical machines must be done securely [12]. Information security includes scrambling the information as well as gives surety of proper approaches. Distributed computing experiences some different security concerns which are given beneath.

- Application access becomes easy
- Transmission mechanism simplified
- VM Protection and access management
- Cryptography and security of network
- Data Encryption and security
- Data access right protection
- Data validity and availability
- Locality of data
- Data merging and collaboration
- Data aggregation and filtering
- Strategies of security and protection
- Batch performance and administration

IV. Cloud Security Challenges

Some of the cloud security challenges that come in front of users are given below:

A. Authentication

The data on the internet is available to all the unauthorized users. Therefore the confidentiality of the data can be lost.

B.Access Control

Access control ensures that data is accessible only by the authorized user only. Access rights could be read only, write , delete etc. The user who is given the access of reading cannot write the data hence they can perform the operation for which they have permission [13].

C.Policy Integration

There are many cloud providers they use their own policies and approaches. Some of them are Amazon, Google who provides services to end users.

D.Service Management

Service management is accomplished by the use of group of cloud service providers. The hybridization of services in case of heavy user environment is provided. The services commonly merged by Google, Amazon etc.

E.Trust Management

Trust management in servicing is critical to ensure trust is maintained with the cloud service provider. In case trust is lost users of the cloud may be reduced.

V. Outsorced Feature in Cloud Computing

There are several main challenges for building assurance to the user:

A. Outsourcing

Outsourcing chops down both capital utilization and operational use for cloud customers. Regardless, outsourcing

furthermore suggests that customers physically lose control on their information and endeavors. The loss of control issue has ended up being one of the fundamental drivers of cloud uncertainty[14]. To address outsourcing security issues, at first, the cloud provider ought to be solid by giving trust and secure figuring and information storing; second, outsourced information and calculation may be clear to customers to the extent order, trustworthiness, and other security organizations. Moreover, outsourcing will perhaps achieve security infringement, due to how fragile information is out of the proprietor's control[2].

B. *Massive data and intense computation*

Cloud computing is fit for handling mass data stockpiling and intense computing assignments. Thusly, customary security components may not do the trick because of terrible computation or correspondence overhead. For instance, to check the respectability of data that is remotely put away, it is unreasonable to hash the whole data set. To this end, new systems and conventions are normal[15].

VI. SECURITY ISSUES

Organization seeks security and reliability consideration seriously since information stored within the database is critical for the user. To tackle the issue, cloud service providers deal with the service security through security mechanisms implementations.

A. Data Security

Information Security raises as a mystery, reliability and openness. These are the huge issues for cloud shippers. Arrangement is portrayed as a security of information. Mystery is proposed to keep the sensitive information from unapproved or wrong individuals[16]. In this stores the encryption key information from enormous business C, set away at mixed arrangement in huge business D. That information must be secure from the specialists of enormous business D. Uprightness is portrayed as the rightness of information, there is no consistent techniques exist for attested information exchanges. Availability is portrayed as information is open on time.

B. Administrative Compliance

Clients are over the long haul capable when the security and climatic phase of their own information is taken by an expert co-op.[17] Traditional pro associations more slanted to outsource diagrams and security affirmation. Distributed computing providers reject to tolerate the examination as hailing so these customers can simply make utilization of unimportant operations.

C. Data Locations

At the point when customers use, they likely won't know absolutely where their information will encouraged and which zone it will secure in. Honestly, they won't not appreciate what country it will be secured in. Master associations ought to be asked whether they will accomplish to securing and change information particularly tact, and on the preface of their customers will they make a sensible accomplishment to take after neighborhood assurance need[18].

D. Special client access

Client may require data or information at any moment of time. For this purpose special access to client may have to be granted. This feature is provided within the cloud through SLA.

E. Put stock in Issue

Trust is critical in ensuring the cloud is used effectively by the user. Cloud is house of data stored by the user. In case this information is lost or corrupted than trust is lost but cloud user strength maintenance is target of every cloud service provider. [19].

F. Data Recovery

This is the mechanism of recovering the information which is corrupted or lost due hardware or software failure.

VII. USING THE SECURITY SOLUTIONS

Four typical aspect are reviewed in this paper for evaluation so that any of the technique can be selected for future enhancement..

Table 1: Cloud Security Solutions

Security solutions	Description
Continuation Mechanism	This the mechanism of migrating service from one cloud service provider to another cloud service provider
IDM	Trust insurance security enhancement mechanism by which size of user community is increased in cloud
Data security	Security is ensured using cryptography, encryption etc.
virtualization security	Virtualization mechanism ensures that resources are available as and when required.

A. Continuation of service from traditional platform to cloud platform

In this era every person is shifting his business applications on cloud. Even though, it is a good technology but it brings some risks in front of them. [20]

B. Identity and access management

Unauthorized access to the information on the cloud becomes a big issue because all the confidential data is on internet so anybody can access or trap the network. So it must be require updating the traditional approach of identity mechanism in order to get higher level of security. Identity federation, security assertion markup, biometric sensors are some of the ways to secure data from unauthorized access.

C. Data Security

Data security is the common issue in the cloud environment. In order to maintain confidentiality of data, availability and completeness some encryption techniques can also be applied. For more security data wiping is also necessary so that sensitive information can't be leaked out[21].

D. Virtualization Security

Virtualization guarantees the cost saving, ease of administration etc. Virtual environment includes access control, virtual machine monitor; virtual firewall which provides security to the user that data is secure on the system.[22]

VIII. CONCLUSION

Distributed computing gives the assets to the clients as well as give a major test of security. There are securities necessities for the two clients and cloud suppliers yet at times it might struggle somehow. Security of the cloud relies on put stock in registering and cryptography. In our audit paper a few issues identified with information area, security, stockpiling, accessibility and uprightness. Building up confide in the cloud security is the greatest prerequisite. These issues said above will be the examination hotspot of distributed computing. There is almost certainly that distributed computing has splendid future

REFERENCES

[1] GX. Yu, "Intelligent Urban Traffic Management System Based on Cloud Computing and Internet of Things," pp. 2169–2172, 2012.

[2] B. Mills, T. Znati, and R. Melhem, "Shadow Computing: An energy-aware fault tolerant computing model," *2014 Int. Conf. Comput. Netw. Commun.*, pp. 73–77, 2014.

[3] V. M. Sivagami, "Survey on Fault Tolerance Techniques in Cloud Computing Environment," no. 9, pp. 419–425, 2015.

[4] R. Jhawar, V. Piuri, and M. Santambrogio, "A Comprehensive Conceptual System-Level Approach to Fault Tolerance in Cloud Computing," pp. 0–4, 2012.

[5] C. A. Chen, M. Won, R. Stoleru, and G. G. Xie, "Energy-efficient fault-tolerant data storage and processing in mobile cloud," *IEEE Trans. Cloud Comput.*, vol. 3, no. 1, pp. 28–41, 2015.

[6] S. S. Lakshmi, "Fault Tolerance in Cloud Computing," vol. 04, no. 01, pp. 1285–1288, 2013.

[7] R. Buyya, C. S. Yeo, and S. Venugopal, "Market-oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities," *Proc. - 10th IEEE Int. Conf. High Perform. Comput. Commun. HPCC 2008*, pp. 5–13, 2008.

[8] Z. Xiao, W. Song, and Q. Chen, "Dynamic Resource Allocation Using Virtual Machines for Cloud Computing Environment," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 6, pp. 1107–1117, Jun. 2013.

[9] U. Wajid, C. Cappiello, P. Plebani, B. Pernici, N. Mehandjiev, M. Vitali, M. Gienger, K. Kavoussanakis, D. Margery, D. G. Perez, and P. Sampaio, "On Achieving Energy Efficiency and Reducing CO 2 Footprint in Cloud Computing," vol. 7161, no. c, 2015.

[10] Y. Xie, H. Wen, B. Wu, Y. Jiang, and J. Meng, "Transactions on Cloud Computing," vol. 13, no. 9, 2015.

[11] D. Ardagna, G. Casale, M. Ciavotta, J. F. Pérez, and W. Wang, "Quality-of-service in cloud computing : modeling techniques and their applications," pp. 1–17, 2014.

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

[13] S. Saha, S. Pal, and P. K. Pattnaik, "A Novel Scheduling Algorithm for Cloud Computing Environment," vol. 1, 2016.

[14] A. Farahzadi, P. Shams, J. Rezazadeh, and R. Farahbakhsh, "Middleware technologies for cloud of things-a survey ☆," *Digit. Commun. Networks*, no. April, pp. 1–13, 2017.

[15] J. P. D. Comput, B. Javadi, J. Abawajy, and R. Buyya, "Failure-aware resource provisioning for hybrid Cloud infrastructure," *J. Parallel Distrib. Comput.*, vol. 72, no. 10, pp. 1318–1331, 2012.

[16] J. Mohammed, C.-H. Lung, A. Ocneanu, A. Thakral, C. Jones, and A. Adler, "Internet of Things: Remote Patient Monitoring Using Web Services and Cloud Computing," in *2014 IEEE International Conference on Internet of Things(iThings), and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom)*, 2014, pp. 256–263.

[17] X. Cui, B. Mills, T. Znati, and R. Melhem, "Shadow replication: An energy-aware, fault-tolerant computational model for green cloud computing," *Energies*, vol. 7, no. 8, pp. 5151–5176, 2014.

[18] D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya, "Energy-efficient data replication in cloud computing datacenters," *Globecom Work. (GC Wkshps), 2013 IEEE*, pp. 446–451, 2013.

[19] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure Ranked Keyword Search over Encrypted Cloud Data," in *2010 IEEE 30th International Conference on Distributed Computing Systems*, 2010, pp. 253–262.

[20] H. Wang, Z. Kang, and L. Wang, "Performance-Aware Cloud Resource Allocation via Fitness-Enabled Auction," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 4, pp. 1160–1173, Apr. 2016.

[21] [21] Z. Amin, "Review on Fault Tolerance Techniques in Cloud Computing," vol. 116, no. 18, pp. 11–17, 2015.

[22] P. Zhang, S. Hu, J. He, Y. Zhang, G. Huang, and J. Zhang, "Building cloud-based healthcare data mining services," *Proc. - 2016 IEEE Int. Conf. Serv. Comput. SCC 2016*, pp. 459–466, 2016.

[23] J. Abawajy, S. Member, M. Chowdhury, and A. Kelarev, "Hybrid Consensus Pruning of Ensemble Classifiers for Big Data Malware Detection," vol. 3, no. 2, pp. 1–11, 2015.

