DOI: http://dx.doi.org/10.26483/ijarcs.v12i1.6683

Volume 12, No. 1, January-February 2021

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A REVIEW ON DATA SECURITY ISSUES IN CLOUD COMPUTING FOR ANALYSIS OF INTEGRITY AND CONFIDENTIALITY

Utkarsh Pandey
Department of CSE
RITS, Bhopal, India

Chetan Agarwal
Department of CSE
Asst. Prof., RITS, Bhopal, India

Bhavana Verma
Department of CSE
Asst. Prof., RITS, Bhopal, India

Abstract: The advent of technological upgradation day by day results in improvement in computing processes, increasing no. of user of computing over cloud for exchanging and sharing data, figures and details. Though even with lots of capable resources in processing there is also the safety barriers in cloud computing system for example data loss, malfunctioning, unwanted change in data, unauthorised access, data intruders barriers etc. thus prime focus on vital measures need to be made in order to overcome such security issues. In order to keep eye on working over cloud two model testing including integrity test on various information, detail files and authentication test on multiple file needs to be made to check out any correction, unauthorised change. In today's era too the traditional factors are still noticed along with some hash function works on key basis. Although among various designs no one is completely relaxed from damages and attacks. Currently too no. of options available with are capable along with safety measures so that the data integrity is still maintained in outsourcing functions too. This paper provides a survey of the main research results of the previous studies.

Keywords: Cloud Computing; Security; Privacy; Integrity Checking; Authentication

I. INTRODUCTION

One of the widely prevalent models which is even growing day by day in the computing field is Cloud Computing. Web of internet allows different services over various computers [1]. Also, with pros some issue that still comes in to existence due to such computing gets solved to extent through programming model. The details use cloud computing becomes enduring stock over server. Regularly used processed information, details or figures on extraordinary high demand depicts cloud itself. The advent model used for long lasting storage of various user's information thus enabling user to use such data as per their need with same payment system which allows to pay only for the time it is used. The speedy solution with avoidance of rigidity complex is the foremost objective in cloud computing pattern that enable users to use data, information etc smoothly and enjoy the specialized services of cloud computing for example speed, turn as per situation nature.

There are 3 methods to achieve the extent;

- Various types of techn0logies have been developed in past years and get merged in this manner this concept of Cloud Computing comes into existence.
- As base of technology makes it famous and broadly prevalent.
- In this stream of evolving technologies, development based computing over cloud there is similarity of processes in traditional era and development zone.

The anticipatory statement by the sir S. Zissis, D. Lekkas et al. at 2015 that the concept of computing over cloud will become broadly prevalent computing and achieve heights in nearly future. The group of computing assets ingress over network termed as Cloud Computing. Retaining secure data in cloud from malicious acts of mal-users, data intruders has become easy as processed information is safely stored over cloud due to security imparted through use of firewall. Other vital term is virtualization, to give rise to internet topology virtual switching is tremendously useful as in equipment work virtually. Pressure on server impacts the presentation of information, data and the application of software. To examine the efficiency of circuit switching in order to pay attention to elevated bandwidth is slightly typical [2]-[5].

The concept of examination of services over cloud has came into picture by Ashraf I 2014 et al. 2013. To checkout the efficiency and the features of application is termed as testing of software. To what extent it accomplish once requirement is also to be tested. Thus the concept of testing is vital in current

era, in regards to use, safety. security and capability. It is surely expensive choice to test itself also includes concerns of data security. Thus cloud computing is the bunch with all level security, testing, processing and reduces the burdens of individual in regards such as security, testing , also save user from regular caring, improvisation etc, results in low cost at users part [6].

II. SAFETY BARRIERS IN COMPUTING PROCESS OVER CLOUD

Security of information, details, processed data on cloud and in whole computing process is critical issue & vital too. Thus main focus must be on safety of data stored over cloud. if security is missing is safeguarding data thus the question on using cloud computing in comparison to old method of computing arises [7]-[10].

Malfunction Issues: Many time bad users also come in front who applies the information from cloud for improper and illegal acts, may also used the details to do crime. In many ways malfunction mis utilise the details like using cloud to defeat code, involving in making available pirated data to various no. of individuals, use of lucrative means such as advertisements that further encourages user to impart personal information ultimately results in fraudulent act and the innocent user comes in web spread by malfunction. Also illegal acts by information collected from user which is personal can be performed. These all are the examples of cloud abuse.

Application proven to be unsafe and weak: Interface of programmable application is the only key enable accessing of Data and services of cloud which are programmable. Bugs coming in front in API redirect the data and services to user unevenly without his choice. Apache Web Server also faces the risk barriers which allow user to work on whole server. Without safety terms structure of API results in API which is actually weak. Exchanging data wrongly to no. of users due to bugs in cloud sharing services or the wrongly functions at API. Designing of API can also be done without considering safety by malfunction sometimes.

Insider issues like stealing: Not every employee working under CSP will be loyal all the times, it may happen employee with intention to undue advantage and gain indulge himself in criminal and illegal works and also to achieve his goals uses information, data available. Also, the cases have come infront where some CSP company is indulged in sharing of data. Information indoor to gain extra[11].

Safety barriers coming across due to Virtualization: Individual that uses IaaS service, because the advent of virtualization is capable to make various machines over same server virtually. Thus, the approach of individual on internal machine is too generally seen with the clarification of no. of virtual machine function on such server, thus the virtual machine can also causes various attacks and can steal information such as CPU, key times, traffic rate on internet and use of cache files that all can become possible after installing virtual machine on such server.

Consolidated services: Interdependency of services on many other services is common phenomenon over cloud. In such computational process information, data is send to various services providers for performing various services, this information may involve all type of information including sensitive information which may be mis utilized by backend without getting known who are the users.

Loss or destruction of data: Safety of data is the vital need in whole computing process. Data destruction may be in two phases; 1.May be due to some natural causes, and 2. Artificial causes. Example of phase one causes are destruction may taken place due to nature's call at server address tornado, earthquake, fire in main servers area, any other kind of physical damage to server, hardware barriers that makes recovery of data inability where replica server only becomes option. The concept of replica server proves to be costly and unsafe. Other kind of phase includes manmade causes likely stealing data, hiding information , deleting details in order to making own motive fulfilled, without permission accessing data, changing data, converting it to unfruitfulness, it involves malfunctioning of services may be due to malfunction voluntary act. To avoid such barriers coming in front due to manmade causes many ways like allowing access to only authorized personnel, checking regularly functions, services over cloud, selective person authorized to regular maintenance of server, proper use of passwords locking only known to one who authorized to work on server, regular checking etc.

The term; Eavesdropping: The one of bad habits of many human give it name called as Eavesdropping which includes the many individual's common nature to listen privately communication going on between others from back except their knowledge. Thus the meaning of Eavesdropping in technological phase becomes little bit differ which involves similarity of cheaply in silent getting personal chat information, reading private texts, listening audios, videos, viewing pictures privately shared etc. MIMA is the term recently used for Eavesdropping which have full form as Man in the middle attack. Thus, the wrong user generally connect himself in first step to cloud and thus through wrong acts indulge in getting private chats, messages information as the user thought to give information to cloud which the malfunction gains and retransferred it to his storage machines. Thus the malicious user uses the similar web page that appears as real one and the user get wrapped in the web laid down by malfunction.

III. LITERATURE REVIEW

Currently the shared details have totally enlarged, with high no. of allotment, the computing process over cloud said as platform with high scope in coming years [7]. The capacitive way is the solution that allows applications of multiple assets as per their capacity with all other features of such assets as timeliness, speed balance, less errors, as per requirement needs fulfilment. As with upgradation in technologies barriers have also been discovered with are the main focuses now a days to be considered such as safety and security of processed information, details [8][9]. Integrity of data, files also gets hamper due to high barriers relating to security [10]-[12]. In order to solve the barrier and minimize the adverse impact various ways have been searched which includes hash functions which are fully depend on key so the preserve integrity of files, documents with authenticity. Also, the researcher came up with new solution which involves amalgamation of one concept of steganography with value called as hashed value for the safely exchange [13]-[17]. Also, way like sequence mapping is applied for LSBs stands for least significant bits in picture in form of cover picture to unrevealing some values, thus enable to unrevealing capabilities and may be behind many safety barriers. To achieve the objectives of data security and integrity only additional some hash features of cryptography are applied along with conventional factors. There are always vulnerability factor due to some conventional method's adverse risk factors results into general and frequent barriers. Concurrently modification after interval in harsh elements in merger with hash features of cryptography reduces the anticipated risks from multiple insecurities. Also, the emerging concept of applying key once like one-time password term as one-time authentication approach that clarifies the integrity and test authentication [18][19]. Also one time biokey is used. The benefits from biometric method is clearly represented in such approaches which involves application of effective characters emerged through local binary pattern filter (LBP) histogram with further attachments of signatures of both receivers and sender so as to create bio-key on moment [20]. The amalgamation is with MAC-SHA-1. The consequence of such solution gives authentication clarity through message on moment. Such codes addition is termed as MACLESS which is in unrevealed form through a cover picture with use of LSBs [21] and also through recent concept of steganography involves DWT stands for discrete wavelet transformation [21]. Stealing of controversy involved in MACLESS is just because of the respectively created design that too for single moment pixel unconditionally through Rivest Cipher 4 (RC4) [22]. The service provider need is different in different levels as with such concept configuration level service provider is to be different from that in run time. Thus use of one time MACLESS [23] which allow to keep eyes on integrity and authenticity of files, folders, documents is broad. One form of strong way also been emerged with characters like signature in handwriting so as to frame a stegno-key and bio-key on moment symmetrically. Hence this approach to sustain the integrity and authenticity of details, documents, files is broadly used. Easy to apply feature of such approach makes it prevalent. Application of Homomorphic linear authenticator to assure and also there is way termed as random masking to again give assurance about the functions in TPA that such system only gets information from the data maintained and shared over cloud and not above that [24]. Thus in between the huge implementation of auditing the other barriers like over pressure due to costly phases in audit functions get avoided along with elimination the hardships due to outsourcing causes confidentiality issues.

IV. EXISTING APPROACHES

Normally, the capacity with various present concepts helping in examination is high , and also the fact is examination can be inhouse too to ensure data, documents integrity. The approach itself enables the principal having data or the agent working on behalf of principle to examine the integrity of files, details, documents and the data. Also the concept of outsourcing verification work can be employed as by imparting examination work to Third Party Auditor with respecting specialized skills and knowledge with authorities and reach [25]. This can also be termed as relationship with triple line factor which can be seen via given below in the Figure 1.

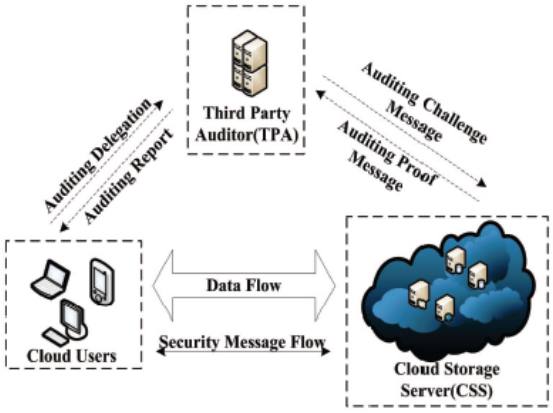

Figure 1. Third party auditor [25]

The two levels of audit system in public are Setup and Audit phase:

- Setup: the use of two different measurements like one is public and another one is secret with proactive processes so as to frame the examination metadata. The process involves the general steps like storing original data and removing the copy with keeping the framed metadata. Extra metadata if needs the storage at server as per need modification , additional, expansion in data over cloud can be done.
- Audit: While auditing process the way files are kept over cloud is the text that is given by TPA process. The feedback feature is also available in response to asked text to the cloud server through data file saved, along with saved files some metadata that have been framed as the result of examination over cloud computing process about

data integrity and authenticity. the examination of received feedbacks are also subject matter handled by TPA. Application of TPA also provides us with two ways for verification with regards to integrity are given as below.

MAC-based Solution: The authentication process through MAC based method involves again two available methods putting of sites the blocks of processed information to server together with respective MACs and also involves TPA responsible for sending secret key correspondingly [25]. Unconditionally getting blocks in combination with own MACs is key feature and the trueness is required to be examined. Later, the TPA can randomly retrieve blocks with their MACs and check the correctness via secret key. Except with lots of barriers present in computations and intercommunications , the information about the examinations of data file blocks is necessary in TPA. Deceiving the needs of data in the process of examination through TPA, such examination can be prohibited, and only equality verification involved.

HLA-based Solution: The technical development results into new featured method called as HLA method that favours audit publicly helps except recovering needs of data blocks [25]. The term HLAs is also the vital examination metadata as MACs ensures the integrity and authenticity examinations of data block. The contradiction is only combined form in HLAs in diversion from MACs, so data blocks individually aggregated in the linear form gets authenticated.

PDP: The model termed as random oracle model depicts the capable examination of data that is outsourced and the respective safety clues with use of PDP (provable data possession). The foremost policy that enables with worth examination even blockless along with on moment checking publicly. RSA signature is the foundation of such policy [26].

DPDP: During the examination of data file to ensure integrity, where checking is done based on file data examination metadata consists of table of contents of file blocks, so there are the chances to get impractical results due to alteration, expansion, and block removal is happened. So to get rid from such barrier as the suggested method is capable of strongly imparts assistance to such amendments, as per the architecture of authentication skip list which is rank based, so the suggested system is Dynamic PDP [27].

Public Auditing of Dynamic Data: The authenticity of data is maintained through application of the Merkle hash tree with the assistance if such policy given for both progressive data and audit in public together. The vital hashes in such file blocks are leaf nodes, and that too are ordered which is of MHT. The worth and location of blocks of data can be authenticated by the method of MHT authenticate Private key supports the hash functions performed by clients whose foundation is authentication metadata [28].

V. CONCLUSION

The interpretation builds up as a result of examination of data that was outsourced in multiple scenarios through statistical researches on various strong and safe algorithms and models. The interpretation about emblematic model is built up. As few objectives have been accomplished now the only focus is integrity examination of data which is outsourced in computing process over cloud and day by day process is going on. The emerging period is advancing day by day rapidly about applications programmes growth, data scaling. The effective computation of cryptographic algorithm is becoming possible now. Only the vital barriers may appear nearly about audit of data integrity.

REFERENCES

[1] Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger and Dawn Leaf, " NIST Cloud Computing Reference Architecture" US Department of Commerce, Gaithersburg, MD, 2011.

[2] P. Mell and T. Grance, "The nist definition of cloud computing, special publication 800-145," US Department of Commerce, Gaithersburg, MD, 2011.

[3] Bhaskar Prashad Rimal, Eunmi choi, Ian Lumb, "A Taxonomy and Survey of Cloud Computing System", International Joint Conference on INC, IMS and IDC, IEEE, 2009.

[4] Armbrust M, Fox A, Griffith R, Joseph D A, Katz H R, Konwinski A, Lee Gunho, Patterson A D, RabkinA, Stoica A, Zaharia M, "Above the clouds: A Berkeley view of Cloud Computing", UC Berkeley, EECS, 2010.

[5] Bhaskar Prasad Rimal, Admela Jukan, Dimitrios Katsaros, Yves Goeleven, "Architectural Requirements for Cloud Computing Systems: An Enterprise Cloud Approach", Journal of Grid Computing, Springer, 2010.

[6] Rajkumar Buyya, Karthik Sukumar, "Platforms for Building and Deploying Applications for Cloud Computing", CSI Communications, 2011.

[7] T. Rethika, I. Prathap, R. Anitha, and S. V. Raghavan, "A novel approach to watermark text documents based on Eigen values," Proceedings of the Ninth International Conference on Network and Service Security (N2S'09), France, IEEE, pp.1-5, 2009.

[8] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," Wireless Communications and Mobile Computing, John Wiley, vol. 13, no. 19, , pp. 1587-1611, Dec. 2012.

[9] A. T. Velte, T. J. Velte, and R. Elsenpeter, Cloud Computing: A Practical Approach, McGraw-Hill Companies, 1st Edition, 2010.

[10] J. Shen and K. Liu, "A Novel Approach by Applying Image Authentication Technique on a Digital Document," Proceedings of International Symposium on Computer, Consumer and Control (IS3C), Taichung, Taiwan, pp. 119-122, June, 2014.

[11] J. Qiu and P. Wang, "An Image Encryption And Authentication Scheme," Proceedings of Seventh International Conf. on Computational Intelligence and Security (CIS), China, pp. 784-787,Dec, 2011.

[12] N. Jamil and A. Aziz, "A Unified Approach to Secure and Robust Hashing Scheme for Image and Video Authentication," Proceedings of 3rd IEEE International Congress on Image and Signal Processing (CISP), Yantai, China, Oct., pp. 274-278, 2010.

[13] Z. Liu, H. S. Lallie, L. Liu, Y. Zhan, and K. Wu, "A hash-based secure interface on plain connection," Proceedings of the sixth International Conference on Communications and Networking in

China (ChinaCom'11), Harbin, China, pp. 1236-1239, IEEE, 2011.
[14] N. Rabadi and S. Mahmud, "Drivers anonymity with a short message length for vehicle-to-vehicle communications network,"Proceedings of the fifth IEEE Consumer Communications and Networking Conference (CCNC'08), Las Vegas, NV, USA, IEEE, pp. 132-133, Jan. 2008.
[15] S. I. Naqvi and A. Akram, "Pseudo-random key generation for secure HMAC-MD5," Proceedings of the 3rd IEEE International Conference on Communication Software and Networks (ICCSN), Xi'an, China, pp. 573-577, May, 2011.
[16] C. Chaisri, N. Mettripun, and T. Amornraksa, "Facsimile Authentication Based on MAC," IT Convergence and Services, Lecture Notes in Electrical Engineering, vol. 107, pp. 613-620, 2012.
[17] K. Alla, G. G. Shankar, and G. B. Subrahmanyam, "Secure Transmission of Authenticated Messages using New Encoding Scheme and Steganography," Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology, Coimbatore UNK, India, pp. 749-752, 2012.
[18] J. Song and S. Han, "One-time key authentication protocol for PMIPv6,"Proceedings of the Third International Conference on Convergence and Hybrid Information Technology (ICCIT'08), South Korea, IEEE, pp. 1150-1153. 2008.
[19] J. Y. Park, D. Lee and H. H. Lee, "Data Protection in Mobile Agents; one-time key based approach", Proceedings of the 5th International Symposium on Autonomous Decentralized Systems (ISADA'05), USA, IEEE, pp.411-418. 2001.
[20] M. A. Ferrer, F. Vargas, A. Morales, and A. Ordonez, "Robustness of offline signature verification based on gray level features," IEEE Trans. Inform. Forensics Security, vol. 7, no. 3, pp. 966-977, Jun. 2012.
[21] P. Wayner, Disappearing Cryptography: Information Hiding: Steganography & Watermarking, Morgan Kaufmann, 3th Edition, 2009.
[22] W. Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall, 6th Edition, 2013.
[23] Zaid Ameen Abduljabbar, Hai Jin, Ali A.Yassin, Zaid Alaa Hussien, "Robust Scheme to Protect Authentication Code of Message/Image Documents in Cloud Computing", IEEE, 2016.
[24] Solomon Guadie Worku, Chunxiang Xu, Jining Zhao, Xiaohu He, "Secure and efficient privacy-preserving public auditing scheme for cloud storage", Computers and Electrical Engineering, Elsevier, 2013.
[25] Cong Wang, Sherman S.M. Chow, Qian Wang, KuiRen, and Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage" IEEE Transactions on Computers, 2013.
[26] G. Ateniese, R. B. Johns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07), pp. 598-609, 2007.
[27] C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," in Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS□09), Chicago, pp. 213-222, USA, 2009.
[28] Q. Wang, C. Wang, K. Ren, W. Lou and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847 – 859, 2011.

