Volume 4, No. 5, May 2013

Journal of Global Research in Computer Science

ISSN-2229-371X

RESEARCH PAPER

Available Online at www.jgrcs.info

DATA INTEGRITY USING ENCRYPTION IN CLOUD COMPUTING

*1 Regil V Raju, 2M.Vasanth, 3Udaykumar P
1The department of CSE, BharathUniversity ,Chennai, Tmail Nadu, India
2The department of CSE, BharathUniversity ,Chennai, Tmail Nadu, India
3The department of CSE, BharathUniversity ,Chennai, Tmail Nadu, India

Abstract:- Data integrity is an important phase in cloud computing. Since the previous couple of years the protocols that was evoked during this field has reached greater heights.[1] Existing protocols with the assistance of a third-party auditor in an exceedingly previous work, Sebe´et al propose a data integrity verifying protocol that supports information dynamics[2]. During this paper, we adapt Sebe´et al.'s protocol to support information authentication. The outlined protocol supports information verification while not facilitate of a third-party auditor [3]. In addition, the projected protocol doesn't leak any personal data to third-party verifiers. Through a correct diagnosing we are going to be measurement however sensible will the system works. After that, through thorough analysis, we will show that the protocol encompasses a sensible performance.

Keywords: Cloud server, Third party auditor, Homo-morphic token, cloud service.

INTRODUCTION

Organisations nowadays are progressively moving towards Cloud Computing as a replacement revolutionary technology promising to chop the price of development and maintenance and still reach extremely reliable services [4]. The Cloud technology could be a growing vogue and remains undergoing voluminous experiments. Cloud guarantees vast price advantages, speed and improvement in business [5]. All business information and computer code are keep on servers at a foreign location brought up as information centers [6]. Information center setting permits enterprises to run applications much quicker, with easier ways to manage few maintenance efforts, and additional promptly scale resources like servers, storage, and networking to satisfy daily fluctuating business desires [7].

The data center in cloud environment holds valid information's that end-users would conventionally have stored on their computers. This raise issues concerning user privacy protection because users should must their information [8]. The movement of information to centralized services may have an effect on the privacy and security of users' interactions with the files keep in cloud cupboard space[9]. The use of virtual infrastructure may be used as a launch pad would possibly introduce new attacks to user's information[10].Data integrity is outlined because the accuracy and consistency of keep information, in absence of any alteration to the information between two updates of a file or record[11]. Cloud services ought to guarantee information integrity and supply trust to the user privacy[12]. though outsourcing information into the cloud is economically appealing for the price and complexness of long-run large-scale information storage, it's lacking of giving robust assurance of information integrity and convenience may impede its wide adoption by each enterprise and individual cloud users[13. Cloud computing poses privacy concerns primarily, as a result of the service supplier at any point in time, might access the information that's on the cloud.

The Cloud service supplier may accidentally or deliberately alter or delete some information from the cloud server. Hence, the system should have some style of mechanism to make sure the safety of the information integrity [14]. The present Cloud security model relies on the idea that the user/customer ought to trust the supplier. , this is usually ruled by a Service Level Agreement (SLA) that normally defines mutual supplier and user expectations and obligations[15].In order to make sure the integrity and convenience of information in Cloud and enforce the standard of cloud storage service, Efficient ways that change on-demand information correctness verification on behalf of cloud users ought to be designed[16].However, the actual fact that users do not have physical possession of information within the cloud prohibits the direct adoption of ancient ++ primitives for the aim of information integrity protection[17]. Hence, the verification of cloud storage correctness should be conducted while not express data of the whole information files [18]. The information kept within the cloud may not be uniquely accessed however even be frequently updated by the users, as well as insertion, deletion, modification, appending, etc [19]. Thus, it's conjointly imperative to support the combination of this dynamic feature into the cloud storage correctness assurance, that makes the system style even more difficult [20] .during this paper, we have a tendency to analyze a way for coding and information recovery just in case of failures [21].

RELATED WORK

Using Cloud Storage, users will remotely store their data and revel in the on-demand prime quality applications and services from a shared pool of configurable computing resources, while not the burden of native knowledge storage and maintenance. However, the actual fact that users not have physical possession of the outsourced knowledge makes the information integrity protection in Cloud Computing a formidable task, particularly for users with unnatural computing resources. Moreover, users ought to be able to simply use the cloud storage as if it's native, without concern concerning the requirement to verify its integrity.

Thus, sanctioning public auditability for cloud storage is of important importance in order that users will resort to a 3rd party auditor (TPA) to see the integrity of outsourced knowledge and be worry-free. To firmly introduce a good TPA, the auditing method ought to herald no new vulnerabilities towards user knowledge privacy, and introduce no further on-line burden to user. during this paper, we have a tendency to propose a secure cloud storage system supporting privacy-preserving public auditing. we have a tendency to more extend our result to change the TPA to perform audits for multiple users at the same time and with efficiency. in depth security and performance analysis show the planned schemes square measure incontrovertibly secure and extremely economical.

Cloud Computing has been visualized because the next generation design of IT Enterprise. In distinction to ancient solutions, wherever the IT services square measure underneath correct physical, logical and personnel controls, Cloud Computing moves the applying computer code and knowledge bases to the massive data centers, wherever the management of the info and services might not be absolutely trustworthy. This distinctive attribute, however, poses several new security challenges that haven't been well understood. During this article, we tend to target cloud knowledge storage security, that has invariably been a crucial side of quality of service. to confirm the correctness of users' knowledge within the cloud, we tend to propose a good and versatile distributed theme with 2 salient options, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-coded knowledge, our theme achieves the mixing of storage correctness insurance and knowledge error localization, i.e., the identification of misbehaving server(s). in contrast to most previous works, the new theme any supports secure and economical dynamic operations on knowledge blocks, including: knowledge update, delete and append. intensive security and performance analysis shows that the planned theme is very economical and resilient against Byzantine failure, malicious knowledge modification attack, and even server colluding attacks.

In an ageing world, maintaining healthiness and independence for as long as potential is important. rather than hospitalization or institutionalization, the senior and disabled may be power-assisted in their own atmosphere twenty four h each day with various 'smart' devices. The conception of the sensible house is a promising and cost-efficient approach of rising home look after the senior and also the disabled during a non-obtrusive approach, permitting larger independence, maintaining healthiness and preventing social isolation. Sensible homes ar equipped with sensors, actuators, and/or medicine monitors. The devices operate during a network connected to an overseas centre for information assortment and process. The remote centre diagnoses the continuing scenario and initiates help procedures pro re nata. The technology may be extended to wearable and in vivo implantable devices to watch folks twenty four h each day each within and out of doors the house. This review describes a range of comes in developed countries on sensible homes examining the varied technologies accessible. Blessings and drawbacks, also because the impact on fashionable society, ar mentioned. Finally, future views on sensible homes as a part of a home-based health care network are given.

Wireless home automation networks comprise wireless embedded sensors and actuators that change observance and management applications for home user comfort and economical home management. This text surveys the most current and rising solutions that square measure appropriate for WHANs, together with ZigBee, Z-Wave, INSTEON, Wavenis, and IP-based technology.

EXISTING SYSTEM

Security problems are going to be occurring throughout the transmission. User will be able to modify the information throughout the transmission. Unwanted information are going to be delivered to the user who can access the cloud server. We will not predict whether or not the information ought to be correct or not. Security is the major issue to be mentioned within the Cloud Computing method. Internet threats square measure increased thus information security is to be mentioned is to be maintained

PROPOSED SYSTEM

Existing system fails to predict the information consistency. thus we have a tendency to introduce a replacement concept, to observe the packets by voucher. Voucher checks the blocks of knowledge arbitrarily by causing a challenge request and substantiating challenge response from that packet when voucher is authorize mistreatment its public key. If the challenge and challenge response is matched then the block is traditional. If challenge response is differed from the expected challenge response then the block is affected. Voucher can offer awake to the user who is all the one using the cloud server. By using this technique we will access remote system with none losses or malicious. the information keep during a Cloud Server is split into blocks. The Integrity of the blocks area unit verified arbitrarily by the Third Party voucher. Voucher can offer its public key then the Challenge to a specific Block. The lock can respond with Challenge Response. The voucher verifies the cr, if it's real then |the information is in safe condition; if not data Access is blocked.

MODULE DISCRIPTION

Cloud Server:

An entity, who has data to be stored within the cloud and depends on the cloud for information storage and computation, may be either enterprise or individual client an entity, who has information to be hold on within the cloud and depends on the cloud for data storage and computation, may be either enterprise or individual customers. Here cloud user will register for accessing the cloud. When user will login into the cloud then User wish to store their data into cloud server. Before that user will transfer the data and send the data securely with facilitate of TPA

Third party auditor (tpa):

Third Party Auditor (TPA): AN elective TPA, who has experience and capabilities that users might not have, is trustworthy to assess and expose risk of cloud storage services on behalf of the users upon request. TPA can receive the information from the cloud user. When receiving the information TPA can generate the information into the token exploitation the homo-morphic methodology. Then TPA sends and stores the information firmly in multiple servers through the CSP. TPA can make sure the server and information .If any of a cloud get affected means that with the assistance of the third party auditor .we simply recover the data's from cloud. Byzantine failure, malicious information modification attack and even server Colluding attacks overcome by TPA.

Homomorphic token:

Upon receiving challenge, every cloud server computes a brief "signature" over the specified blocks and returns them to the user. quick localization of information of error: to effectively find the malfunctioning server once data corruption has been detected. By utilizing the homo-morphic token with distributed verification of erasure-coded information, our theme achieves the storage correctness insurance as well as information error localization. Our main theme is for ensuring cloud data storage is bestowed during this section. The primary a part of the section is dedicated to a review of basic tools from writing theory that's required in our theme for file distribution across cloud servers. Then, the token is introduced

Cloud service supplier:

Cloud Server (CS): an entity, that is managed by cloud service supplier (CSP) to supply data storage service and has important storage space and computation resources so as to attain assurance {of information storage correctness and data error localization at the same time, our theme entirely depends on the pre-computed verification tokens. Later, once the user needs to create positive the storage correctness for the information within the cloud, he challenges the cloud servers with a collection of haphazardly generated block indices.

CONCLUSION

In this paper, we tend to propose a brand new remote information integrity checking protocol for cloud storage. The projected protocol is appropriate for providing integrity protection of customers' necessary information. The projected protocol supports information insertion, modification, and deletion at the block level, and additionally supports public verifiability. The projected protocol is evidenced to be secure against associate un-trusted server. It's additionally non-public against third-party verifiers. Each theoretical analysis and experimental results demonstrate that the projected protocol has superb potency within the aspects of communication, computation, and storage prices. Currently, we tend to square measure still acting on extending the protocol to support information level dynamics. the issue is that there's no clear mapping relationship between the info and therefore the tags. within the current construction, information level dynamics will be supported by mistreatment block level dynamics. Whenever a chunk of information is changed, the corresponding blocks and tags square measure updated. However, this could bring reserve computation and communication prices. we tend to aim to realize information level dynamics at stripped prices in our future work.

REFERENCES

[1]. F. Sebe, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J.-J. Quisquater, "Efficient Remote Data Possession Checking in Critical Information Infrastructures," IEEE Trans. Knowledge and Data Eng., vol. 20, no. 8, pp. 1034-1038, Aug. 2008.

[2]. R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the Fifth Utility," Future Generation Computer Systems, vol. 25, no. 6, pp. 599-616, 2009.

[3]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-609, 2007.

[4]. R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple- Replica Provable Data Possession," Proc. 28th Int'l Conf. Distributed Computing Systems (ICDCS' 08), 2008.

[5]. G. Ateniese, R. Di Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. Fourth ACM Int'l Conf. Security and Privacy in Comm. Networks (SecureComm '08), 2008.

[6]. C. Erway, A. Ku¨ pc¸u¨ , C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), pp. 213-222, 2009.

[7]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality of Service (IWQoS '09), pp. 1-9, July 2009.

[8]. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," Proc. 14th European Conf. Research in Computer Security (ESORICS), Sept. 2009.

[9]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, Mar. 2010.

[10]. Y. Deswarte and J.-J.Quisquater, "Remote Integrity Checking," Proc. Sixth Conf. Integrity and Internal Control in Information Systems (IICIS '04), pp. 1-11, 2004.

[11]. D.L.G. Filho and P.S.L.M. Barreto, "Demonstrating Data Possession and Uncheatable Data Transfer." Cryptology ePrint Archive, Report 2006/150, http://eprint.iacr.org/, 2006.

[12]. M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," Proc. 11th USENIX Workshop Hot Topics in Operating Systems (HOTOS), 2007.

[13]. C. Wang, S.S.-M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," Cryptology ePrint Archive, Report 2009/579, http://eprint.iacr.org/, 2009.

[14]. Y. Zhu, H. Wang, Z. Hu, G.-J.Ahn, H. Hu, and S.S. Yau, "Cooperative Provable Data Possession," Cryptology ePrint Archive, Report 2010/234, http://eprint.iacr.org/, 2010.

[15]. Z. Hao and N. Yu, “A Multiple-Replica Remote Data Possession Checking Protocol with Public Verifiability,” Proc. Second Int’l Data, Privacy and E-Commerce Symp.(ISDPE ’10), 2010.

[16]. O. Goldreich, Foundations of Cryptography. Cambridge Univ. Press, 2004.

[17]. I. Damga°rd, “Towards Practical Public Key Systems Secure against Chosen Ciphertext Attacks,” Proc. 11th Ann. Int’l Cryptology Conf. Advances in Cryptology (CRYPTO ’91), 1992.

[18]. M. Bellare and A. Palacio, “The Knowledge-of-Exponent Assumptions and 3-Round Zero-Knowledge Protocols,” Proc. Cryptology Conf. Advances in Cryptology (CRYPTO ’04), pp. 273-289, 2004.

[19]. G.L. Miller, “Riemann’s Hypothesis and Tests for Primality,” Proc. Seventh Ann. ACM Symp.Theory of Computing (STOC ’75), pp. 234-239, 1975.

[20]. Z. Hao, S. Zhong, and N. Yu, “A Privacy-Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability,” Technical Report 2010-11, SUNY Buffalo CSE Dept., http://www.cse.buffalo.edu/tech-reports/2010-11.pdf, 2010.

[21]. Multiprecision Integer and Rational Arithmetic C/C++ Library, http:// www.shamus.ie/, 2011. For more information on this or any other computing topic, please visit our Digital Library at www.computer.org/publications/dlib