International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018

Improved Data Security Protection Mechanism for Cloud Storage System

Ashish Ladda & V.Achyuth

[1] Assistant Professor, Department of CSE, Balaji Institute of Technology & science, Warangal District, Telangana, India.

[2] M.Tech Student, Department of CSE, Balaji Institute of Technology & science, Warangal District, Telangana, India.

Abstract— *In that anticipated an improve the information security assurance instrument for cloud utilizing two parts. Amid this framework sender sends a scrambled message to a beneficiary with the help of cloud framework. The sender needs knowing personality of beneficiary however no might want of various information like endorsement or open key. To decipher the figure content, recipient wants two parts. The essential issue might be a one of a kind individual security gadget or some equipment gadget associated with the PC framework. Second one is close to home key or secretes key hang on inside the PC. While not having these two components figure message ne'er unscrambled the fundamental thing is that the security gadget lost or stolen, at that point figure content can't be decoded and equipment gadget is repudiated or scratched off to decoded the figure content.*

Index Terms-- Cloud Storage System, Cloud Security, Cloud Protection, Two-Factor Data Security Protection;

INTRODUCTION

There are such countless, to store the data in the distributed storage. Data in the cloud capacity server can be encouraged at whatever point and wherever insofar as system get to. Cloud specialist co-op gives administrations to the cloud clients, they can get any measure of more assets whenever. It gives no danger of information Storage upkeep undertakings, for example, gaining extra stockpiling limit, can be emptied to the obligation of an administration supplier. Simple to data sharing between various customers. If sender needs to share a touch of data, for instance, video, content, sound et cetera to beneficiary it may be troublesome for sender to send it by email due to the span of data. Rather than that sender moves the information into the distributed storage after that recipient can without much of a stretch download whenever from wherever. Distributed storage ordinarily alludes to an offer question stockpiling administrations like Microsoft Azure and Amazon S3 Storage. There are diverse critical difficulties in distributed computing for securing information, arrangement of administrations and capacity of information in the web from various kinds of assaults. Distributed computing gives an including space to information stockpiling, PC preparing power, shared pool of assets, systems, client applications and specific corporate. Distributed computing is a more modern. It is anything but difficult to estimate that the security for information security in the distributed storage ought to be progress. In any cases, these applications experience a potential hazard about part revocability that may restrict their probability. An expandable and adaptable Two-Component encryption component is extremely more proper in the term of distributed computing that provoke our System. Distributed computing is a regular term for anything that includes versatile administrations, conveying facilitated administrations like getting to, information sharing, and so on. over the web on request premise. For the most part, client share

different sorts of records through distributed storage organizing application like Drop box, cloud me, Google drive. Citrix Cloud processing is known as an other option to customary innovation because of its low-support and better asset sharing capacities. The principle objective of distributed computing is to give elite vitality of processing for different field like military and research association for performing billions of calculations. The fundamental security prerequisite can be accomplished by consolidating both the cryptographic cloud capacity alongside accessible encryption plot. In cloud framework general cost of information stockpiling is less as it doesn't require overseeing and keeping up costly equipment. In which information proprietor right off the bat scramble all information before putting away on a cloud in such way that lone client whom having unscrambling keys can be decode or bring the information.

Figure 1: Architecture of Cloud Storage

. RELATED WORK

In this plan presents encoded distributed storage in view of characteristic based encoded and a fresh out of the box new catchphrase seek idea: fine-grained get to administration mindful watchword look. Amid this framework introductory gathering the decoded capable documents of clients before execution the watchword seek. It diminishes information overflowing from the inquiry strategy. A great deal of framework utilizes the simple scan approach wherever to look one encoded watchword, the cloud server should look round all scrambled records on the capacity to watch that encoded catchphrase to every catchphrase file, and this detriment is evacuated. Concentrated on disadvantage of Identity-Based intermediary re-encryption, amid which figure content are change over into one personality to an alternate. Intermediary re-encryption conspire is utilized to change over the scrambled figure content into unscrambled figure content while not for sake of basic plaintext. This disadvantage evacuates in Inter-space character based intermediary re-encryption. The creators share data and security defensive evaluating topic with gigantic gatherings inside the cloud. They are using bunch mark to figure confirmation information on shared information. That is the TPA those ready to review rightness of shared information however can't uncover the character of the endorsers on each piece. The first client will proficiently add new clients to the gathering and close the personalities of underwriters on all squares. This paper depicts a framework Identity based encoding in ordinary model and has unmistakable burden of existing framework like particularly, calculation ability, less open system and a smaller wellbeing decrease. More grounded suspicion depends on individual key age quires made by aggressor to lessen this detriment utilizing straight diff-hellman Exponent presumption. This paper concentrates on follow out data for security concern. Utilizing a log construct review benefits that gather in light of favored data use and furthermore mull over their timeframe of usage for this case data follow go into the distributed storage. This method defeat various operations on data, furthermore rehashed formation of tag and testing. In arranged distributed storage frameworks is utilized to hang on figure content existing access administration methodology are no longer accommodating, inconvenience figure content Policy Attribute-Based encoding (CP-ABE) might be a system for get to administration of scrambled data.

EXISTING AND PROPOSED SYSTEM

A. Existing System

There exists cryptographic primitive called "leakage-resilient encryption". The security of the scheme is still guaranteed if the leakage of the secret key is up to certain bits such that the knowledge of these bits does not help to recover the whole secret key. However, though using leakage resilient primitive can safeguard the leakage of certain bits, there exists another practical limitation. Say,a part of the secret key is stored into the security device. If the device gets stolen, then the user needs a replacement to continue to decrypt his corresponding secret key. One of the solution is to copy those bits (that in the stolen device) to the replaced device by the private key generator (PKG). This approach can be easily achieved. Nevertheless, there exists security risk. If the adversary (who has stolen the security device) can also break into the computer where the other part of secret key is stored, then it can decrypt all cipher text corresponding to the victim user. The most secure way is to cease the validity of the stolen security device.

Disadvantages of Existing System:

1. If the user has lost his security device, then his/ her corresponding cipher text in the cloud cannot be decrypted forever! That is, the approach cannot support security device update/revocability.
2. The sender needs to know the serial number/ public key of the security device, in additional to the user"s identity/public key. That makes the encryption process more complicated.

B. Proposed System

This paper describes a novel two-factor security protection mechanism for data stored in the cloud. This mechanism provides the following nice features:

1)The system is an IBE (Identity-based encryption) - based mechanism. That is, the sender only needs to know the identity of the receiver in order to send an encrypted data (cipher text) to him/her. No other information of the receiver (e.g., public key, certificate etc.) is required. Then the sender sends the cipher text to the cloud where the receiver can download it at any time.

2) The system provides two-factor data encryption protection. In order to decrypt the data stored in the cloud, the user needs to possess two things. First, the user needs to have his/her secret key which is stored in the computer. Second, the user needs to have a unique personal security device which will be used to connect to the computer (e.g., USB, Bluetooth and NFC). It is impossible to decrypt the cipher text without either piece.

3) More importantly, the system, for the first time, provides security device (one of the factors) revocability. When the security device is stolen/lost, this device is revoked. That is, using this device you can no longer decrypt any cipher text. The cloud will immediately execute some algorithms to change the existing cipher text to beun-decryp table by this device. While, the user needs to use his new/replacement device (together with his secret key) to decrypt his/her cipher text; this process is completely transparent to the sender.

4) The cloud server cannot decrypt any cipher text at any time.

Advantages of Proposed System:

1. The solution not only enhances the confidentiality of the data, but also offers the revocability of the device so that once the device is revoked; the corresponding cipher text will be updated automatically by the cloud server without any notice of the data owner.
2. The cloud server cannot decrypt any cipher text at any time.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018

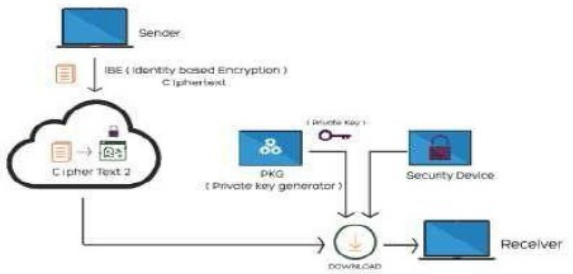

Fig. 1: Ordinary data sharing.

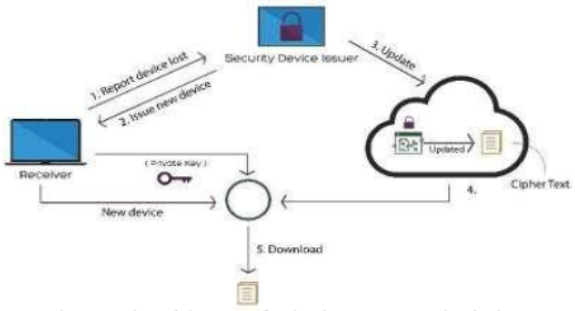

Fig. 2: Update cipher text after issuing a new security device.

EXPERIMENTAL RESULTS In our experiments, initially start the three servers like Cloud server system, Key generator system (The first factor is his/her secret key stored in the computer) , USB package server (The second factor is a unique personal security device which connects to the computer), and finally User applications in that user application initially one or more users register into the system after registration into the system authorized user login into the system after login into the system authorized user upload the file into the system the file is stored into cloud storage server while uploading the data onto cloud, we can create the access policy for different users after successfully uploading the file onto cloud The owner can download the data into local system, after that Owner/ user can report the loss of device, if they lost the device then wont able to decrypt the data after reporting the loss of device Unable to decrypt the data or unable to access the data and try to login as a different user (Owner/ user) and try to downloading the data Owner/ user can download the data to shown in below screens.

Through our implementation authorized owner upload the file into the cloud we can define the access policy for different users and also generate the keys and owner/user can download the file into the local system after that Owner/user can report the loss of device, if they lost the device then wont able to decrypt the data after reporting the loss of device Unable to decrypt the data or unable to access the data and try to login as a different user (Owner/ user) and try to downloading the data Owner/ user can download the data based on that we can send or store the data in efficient and secure manner at lower cost then compare to current methods.

CONCLUSION

In this paper, we have a tendency to presented a novel two-factor information security insurance component for distributed storage framework,

inside which information sender is permitted to code the data with learning of the personality of a recipient just, while the collector is expected to utilize every hello there/her mystery key and a security gadget to acknowledge access to the data. Our determination not just upgrades the secrecy of the data, however moreover offers the revocability of the gadget all together that once the gadget is disavowed; the relating figure content are refreshed mechanically by the cloud server with nonenotice of the data proprietor. In addition, we have a tendency to present the security verification and productivity examination for our framework.

REFERENCES.

[1] A. Sahai, H. Seyalioglu, B. Waters. Dynamic credentials and cipher text delegation for attribute-based encryption. In: Advances in Cryptology–CRYPTO 2012. Springer Berlin Heidelberg. 2012; 199-217.

[2] B. Libert, D. Vergnaud. Unidirectional chosen-ciphertext secure proxy re-encryption. IEEE Transactions on Information Theory. 2011; 57(3),1786-1802.

[3] C. Wang, S.S. Chow, Q. Wang, K. Ren, W. Lou. Privacy-preserving public auditing for secure cloud storage. IEEE Transactions on computers.2013; 62(2), 362-375.

[4] C.K. Chu, S.S. Chow, W.G. Tzeng, J. Zhou, R.H. Deng. Key-aggregate cryptosystem for scalable data sharing in cloud storage. IEEETransactions on Parallel and Distributed Systems. 2014; 25(2), 468-477.

[5] H. Guo, Z. Zhang, J. Zhang, C. Chen. Towards a secure certificate less proxy re-] encryption scheme. In: International Conference on Provable Security. Springer Berlin Heidelberg. 2013; 8209, 330-346..

[6] H.C. Chen, Y. Hu, P.P. Lee, Y. Tang. NCCloud: a network-coding- based storage system in a cloud-of- clouds. IEEE Transactions on Computers, 2014; 63(1), 31-44.

[7] J. H. Seo, K. Emura. Efficient delegation of key generation and revocation functionalities in identity-based encryption. In: Cryptographers‟ Track at the RSA Conference. Springer Berlin Heidelberg. 2013; 343-358.

[8] J. Shao, Z. Cao. Multi-use unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption. Information Sciences, 2012; 206, 83-95.

[9] J.K. Liu, F. Bao, J. Zhou. Short and efficient certificate-based signature. In: International Conference on Research in Networking. Springer Berlin Heidelberg. 2011; 167-178.

[10] J.K. Liu, K. Liang, W. Susilo, J. Liu, Y. Xiang. Two-Factor Data Security Protection Mechanism for Cloud Storage System. IEEE Transactions

[11] K. Liang, Z. Liu, X. Tan, D. S. Wong, C. Tang. A CCA-secure identity-based conditional proxy re-encryption without random oracles. In: International Conference on Information Security and Cryptology. Springer Berlin Heidelberg. 2012; 231-246. .

[12] L. Ferretti, M. Colajanni, M. Marchetti. Distributed, concurrent, and independent access to encrypted cloud databases. IEEE transactions on parallel and distributed systems, 2014; 25(2), 437-446. on Computers, 2016; 65(6), 1992-2004.

[13] M. Vimala,K.Vishnukumar. A survey on data security mechanism for cloud storage system, 2016

[14]R. R. Pavithra, V. R. Nagarajan. A survey on certificate revocation scheme using various approaches. Indian Journal of Innovations and Developments. 2016; 5(5), 1-3.

Ashish Ladda is 5+ years experienced Assistant Professor in the Department of Computer Science &

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018

Engineering, BALAJI INSTITUTE OF TECHNOLOGICAL SCIENCES-NARSAMPET, Warangal, India and his research area includes Cloud Computing , IoT, Data Mining , Network Security etc.,

V.Achyuth Currently doing M.Tech in Computer Science & Engineering at BALAJI INSTITUTE OF TECHNOLOGICAL & SCIENCES-NARSAMPET, Warangal, India. His research interests includes Cloud Computing, Network Security, Mobile Computing, etc,