International Journal of Research
Special Issue in UGC Approved Journal
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 11
September 2017

Improved Data Protection Mechanism for Cloud Storage with the usage of Two Components

Mohammed Nadeemuddin[1], Md Ateeq Ur Rahman[2]
[1] Department of CSE, SCET, Hyderabad
nademdba@gmail.com.

[2]Professor and Head, Department of CSE, SCET Hyderabad,
mail_to_ateeq@yahoo.com

ABSTRACT— ***This proposed approach is an enhance data protection mechanism for the cloud usage by employing of two components. In this system sender sends an encrypted message to a receiver with the assist of cloud mechanism. The sender requires to capture identification of receiver but no need of various information which incorporates certificate or public key. To decrypt the cipher text, receiver desires elements. The first data or is a unique non-public protection device or some hardware device connected to the laptop system. Second one is personal key or secrete key stored inside the computer. Without having those matters cipher text by no means decrypted. The important component is the safety tool lost or stolen, then cipher text can't be decrypted and hardware tool is revoked or cancelled to decrypt cipher textual content. The performance and security evaluation display that the device is secure in addition to practically applied. The device makes use of a new hardware device. To decrypt the cipher textual content together with the non-public key. This paper proposes Identity based and attribute based encryption approach of cloud storage which may be implementable on cloud platform. The record analyses the feasibility of the applying encryption set of policies for data safety and confidentiality in cloud Storage with all kind of modern algorithms.***

1.INTRODUCTION:

There are such a lot of benefits, to store the records in the cloud storage. Data accessed in the cloud storage server may be hosted at any time and any place or anywhere so long as community access. Cloud Service provider gives services to the cloud users, they can acquire any amount of greater resources any time. It gives no threat of information Storage maintenance duties, such as obtaining additional storage capacity, can be unloaded to the duty of a service provider. Very clean to records sharing among many users. If sender wants to percentage a chunk of statistics consisting of video, textual content, audio etc. To receiver, it can be tough for sender to send it by way of e mail due to the level of information. Rather than, User uploads the document into the cloud storage after that receiver can effortlessly down load each time from any area. Cloud storage typically refers to a proposal object storage services like Microsoft Azure and Amazon S3 Storage. There are extraordinary considerable challenges in cloud computing for securing records, provision of offerings and storage of statistics inside the net from exceptional varieties of assaults. Cloud

computing provides an which includes space for data storage, laptop processing energy, shared pool of resources, networks, user programs and specialized company. Cloud computing is a more sophisticated. It is easy to forecast that the security for data safety in the cloud storage have to be enhance. In any instances, those packages go through a potential hazard about component revocability that may restriction their opportunity. An expandable and bendy Two-Component encryption mechanism is in reality extra suitable inside the time period of cloud computing that set off our System. Cloud computing is a common term for something that involves scalable offerings, delivering hosted services like accessing, data sharing, and so on. Over the net on call for basis. Cloud computing is called an alternative to standard technology because of its low-upkeep and higher resource-sharing abilities. The main goal of cloud computing is to offer excessive overall performance strength of computing for diverse control like navy and research company for performing billions of computations. The important safety requirement can be attained via combining both the cryptographic cloud storage at the side of searchable encryption scheme. In cloud system overall price of records storage is much less as it does no longer require managing and preserving pricey hardware. In which information owner firstly encrypt all data before storing on a cloud in such manner that only person whom having decryption keys may be decrypt or fetch the data.

Encryption can protect records as it's miles being transmitted to and from the cloud provider. It can similarly protect information that is saved on the provider. Even there's an unauthorized adversary who has won get entry to to the cloud, as the data has been encrypted, the adversary cannot get any information approximately the plaintext. Asymmetric encryption permits the encrypt to apply only the general public statistics (e.g., public key or identity of the receiver) to generate a cipher textual content even as the receiver makes use of his/her own mystery key to decrypt. This is the maximum handy mode of encryption for records transition, due to the elimination of key management existed in symmetric encryption. Cloud storage way "the storage of information online on the cloud" in which a employer's information is stored in and reachable from more than one disbursed and related resources that include a cloud. Cloud storage can provide the blessings of greater accessibility and reliability; rapid deployment; robust safety for backup, archival and disaster, recovery purposes; and decrease general storage fees due to no longer having to purchase, control and keep expensive hardware. But, cloud storage does have the security and compliance worries

2. RELATED WORK.

In this paper, recommend a two-data or information protection safety mechanism with aspect revocability for cloud storage system. System permits a sender to send an encrypted files or messages to a receiver via a cloud storage server. The sender simplest needs to know the identity of the receiver. The receiver desires parts a good way to decrypt the cipher-text. The first aspect is a unique non-public security tool which connects to the laptop. The second data or is his/her master key stored inside the computer. It is impossible to decrypt the cipher-textual content without both pieces. More importantly, once the security tool is stolen or misplaced, this tool is revoked. To trade the prevailing cipher text to be un-

decrypt able by using this tool. This process is absolutely understandable to the sender. Furthermore, the cloud server can not decrypt any cipher-text at any time. This paper offers the data approximately characteristic of low preservation. Cloud computing provides financially and efficient solution for sharing datas organization aid amongst cloud users, the scheme is likewise very flexible, it may be truly prolonged to guide more advanced looking question. We conclude that this provide a great building block for the construction of comfy services within the cloud storage which are not trusted by consumer. As we are able to proportion only unmarried key the storage area required turns into much less and more efficient. This paper focuses on hint out data for security difficulty. Using a log primarily based audit services that focus on privileged information utilize and also allow in mind their time period of utilization for this example information hint out in the cloud storage. This machine overcome numerous operations on information, also repeated advent of tag and sampling. In proposed cloud storage structures is used to stored cipher-textual content present access control approach are not useful, disadvantage cipher text-Policy Attribute-Based Encryption (CP-ABE) is a technique for get right of entry to manipulate of encrypted information. In this scheme gives cryptographic cloud storage based on characteristic-based totally cryptosystems and a brand new key-word seek belief: best-grained get entry to control aware key-word seek. In this device first Group the decryptable documents of users earlier than executing the key-word search. It decreases records leakage from the query manner. Many gadget uses the truthful search approach wherein for searching one encrypted key-word, the cloud server ought to appearance round all encrypted documents on the storage to examine that encrypted keyword to every key-word index, this disadvantage is eliminated . In attention on trouble of Identity-Based proxy re-encryption, in which cipher-textual content are convert into one identity to some other. Proxy re-encryption scheme is used to convert the encrypted cipher-text into decrypted cipher text with out in behalf of underlying plaintext. This disadvantage gets rid of in Inter-domain identification-based proxy re-encryption. The authors share statistics and privatives maintaining auditing scheme with massive corporations within the cloud. They are making use of institution signature to compute verification information on shared records. That is the TPA the ones capable of audit correctness of shared data however cannot screen the identity of the signers on every block. The unique consumer can efficaciously upload new users to the organization and close the identities of signers on all blocks. This paper describes a gadget Identity Based Encryption in popular version and has distinct disadvantage of current system including namely, computation functionality, less public framework and a compact safety reduction. Stronger assumption is based on non-public key technology quires made by means of attacker. To lessen this drawback the use of Bilinear diff hell man Exponent assumption.

3. FRAME WORK

There exists cryptographic primitive called “leakage-resilient encryption”. The protection of the scheme is still guaranteed. if the leakage of the name of the game secret is up to certain bits such that the understanding of those bits does no longer assist to recover the entire mystery key. However, although the usage of leakage resilient primitive can guard the leakage of certain bits, there exists another realistic

difficulty. Say, a part of the secret secret's stored into the safety device. If the tool receives stolen, then the person desires a alternative to continue to decrypt his corresponding secret key. One of the solution is to duplicate those bits (that inside the stolen tool) to the replaced device by using the personal key generator (PKG). This set of rules permits a sender to send an encrypted message to a receiver through a cloud storage server. The sender finest desires to recognize the identity of the receiver however no different records (inclusive of its public key or its certificate). The receiver wishes to possess things in order to decrypt the cipher text. The first data or is his/her secret key saved inside the computer. The second element is a precise personal security device which connects to the laptop. It is not possible to decrypt the cipher textual content with out either piece.

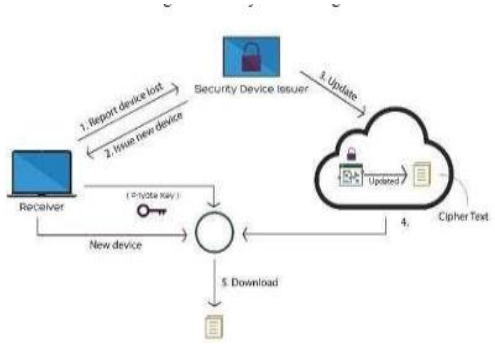

Figure 1: Update cipher text after issuing a new security device.

The encryption procedure is completed twice. First encrypt the plaintext corresponding to the general public key or identification of the person. Then encrypt it again similar to the public key or serial wide variety of the safety tool. For the decryption stage, the security tool first decrypts as soon as. The in part decrypted cipher text is then exceeded to the computer which makes use of the consumer secret key to in addition decrypt it. Without both part (consumer secret key or security tool) one can't decrypt the cipher text. If the person has lost his security device, then his/her corresponding cipher text in the cloud can't be decrypted all the time! That is, the method cannot support safety tool replace/ revocability. Our system is an IBE (Identity-based totally encryption)- based mechanism. That is, the sender simplest wishes to recognize the identification of the receiver so that you can ship an encrypted statistics (cipher text) to him/her. No other information of the receiver (e.g. Public key, certificates etc.) is needed. Then the sender sends the cipher text to the cloud where the receiver can down load it at each time. Our system gives two-component data encryption safety. In order to decrypt the data saved inside the cloud, the person needs to possess two matters. First, the person wishes to have his/her mystery key which is saved in the laptop. Second, the user needs to have a completely unique personal safety device which might be used to connect to the laptop (e.g. USB, Bluetooth and NFC). It is impossible to decrypt the cipher text without either piece. More importantly, our device, for the primary time, gives safety device (one of the elements) revocability. Once the security tool is stolen or reported as lost, this tool is revoked. That is, using this tool can now not decrypt any cipher text (corresponding to the person) in any condition. The cloud will immediately execute some algorithms to alternate the existing cipher text to be un-decrypt able with the help of this tool. While the person needs to apply his new / substitute tool (collectively with his mystery key) to decrypt his/her cipher text. This manner is absolutely transparent to the sender. The cloud server cannot decrypt any cipher text at any time.

4. EXPERIMENTAL RESULTS

We leverage extraordinary encryption technology: one is IBE and the alternative is conventional Public Key Encryption (PKE). We first allow a person to generate a first degree cipher text underneath a receiver's identification. The first level cipher textual content will be similarly converted right into a second level cipher text similar to a safety tool. The resulting cipher textual content can be decrypted through a legitimate receiver with secret key and security device. Here, one may doubt that our creation is a trivial and simple aggregate of two distinct encryptions. Unfortunately, this isn't always proper because of the reality that we want to further support security tool revocability. A trivial mixture of IBE and PKE can't acquire our aim. To help revocability, we rent re-encryption generation such that the a part of cipher textual content for an old protection device can be up to date for a brand new tool if the vintage device is revoked.

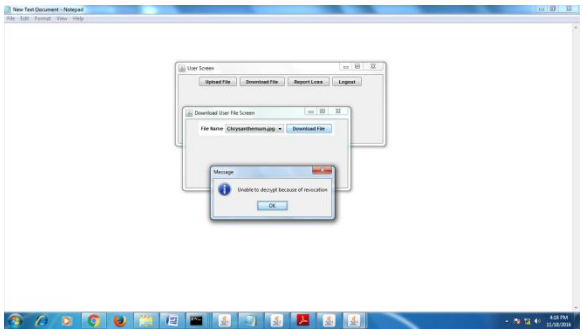

Figure 2: Key Revocation Process

Meanwhile, we want to generate a unique key for the above cipher textual content conversion. We also assure that the cloud server cannot achieve any information of message by gaining access to the special key, the antique cipher textual content and the up to date cipher text. We similarly use hash-signature technique to "sign" cipher text such that after a thing of cipher text is tempered by means of adversary, the cloud and cipher text receiver can tell. From the Above presentations, we can see that our two data or protection system with security device revocability can't be obtained by means of trivially combining an IBE with a PKE.

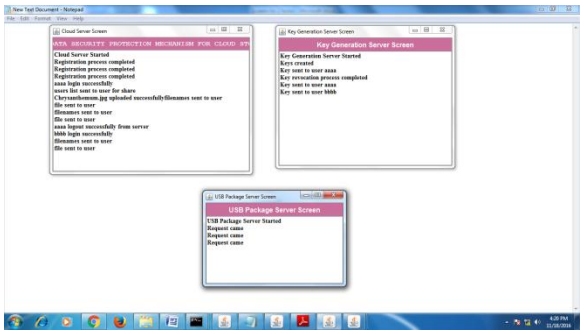

Figure 3: Cloud Server, USB and Key servers

5. CONCLUSION

We introduced a unique Two-data protection mechanism for cloud storage system, in which a records sender is acceptable to encrypt the statistics with understanding of the identity of a receiver, while the receiver is required to use each his/her anonymous key and a protection tool to advantage access to the information. Our answer not handiest complements the confidentiality of the data, however additionally gives the revocability of the device in order that as soon as the tool is evoked the corresponding cipher textual content will be updated mechanically by way of the cloud server with none be aware of the statistics owner. Furthermore, we offered the safety proof and performance analysis for our machine. Our answer no longer handiest complements the confidentiality of the statistics, however additionally gives the revocability of the tool so that once the tool is revoked, the

corresponding cipher text will be updated mechanically by using the cloud server without any be aware of the information owner. Furthermore, we provided the protection proof and performance analysis for our machine.

6. REFRENCES

[1] A. Akavia, S. Goldwasser, and V. Vaikuntanathan, "Simultaneous hardcore bits and cryptography against memory attacks," in Proc. 6th Theory Cryptography Conf., 2009, pp. 474–495.

[2] S. S. Al-Riyami and K. G. Paterson, "Certificate less public key cryptography," in Proc. 9th Int. Conf. Theory Appl. Cryptal., 2003, pp. 452–473.

[3] M. H. Au, J. K. Liu, W. Susilo, and T. H. Yuen, "Certificate based (linkable) ring signature," in Proc. Inf. Security Practice Experience Conf., 2007, pp. 79–92.

[4] M. H. Au, Y. Mu, J. Chen, D. S. Wong, J. K. Liu, and G. Yang, "Malicious KGC attacks in certificate less cryptography," in Proc. 2nd ACM Symp. Inf., Compute. Common. Security, 2007, pp. 302–311.

[5] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in Proc. Int. Conf. Theory Appl. Cryptographic Techn., 1998, pp. 127–144.

[6] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proc. ACM Conf. Comput. Commun. Security, 2008, pp. 417–426.

[7] D. Boneh, X. Ding, and G. Tsudik, "Fine-grained control of security capabilities," ACM Trans. Internet Techn., vol. 4, no. 1, pp. 60– 82, 2004.

[8] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in Proc. 21st Annu. Int. Crypto. Conf., 2001, pp. 213– 229.

[9] R. Canetti and S. Rosenberger, "Chosen-cipher text secure proxy re-encryption," in Proc. ACM Conf. Compute. Common. Security, 2007, pp. 185–194.

[10] H. C. H. Chen, Y. Hu, P. P. C. Lee, and Y. Tang, "NCCloud: A network-coding-based storage system in a cloud-of-clouds," IEEE Trans. Compute., vol. 63, no. 1, pp. 31–44, Jan. 2014.