www.ijiarec.com

ISSN:2348-2079

Volume-7 Issue-1

International Journal of Intellectual Advancements and Research in Engineering Computations

Two-factor information security assurance component for distributed storage framework

Ms. G. Gowthini[1], Mrs. K.E.Eswari, M.C.A., M.Phil., ME[2].,

[1]Final MCA Department of MCA, Nandha Engineering College (Autonomous), Erode-52.

[2]Associate professor/MCA, Department of MCA, Nandha Engineering College (Autonomous), Erode-52.

ABSTRACT

In the two-factor data security protection mechanism with factor revocability for cloud storage system. Our system allows a sender to send an encrypted message to a receiver through a cloud storage server. The sender only needs to know the identity of the receiver but no other information (such as its public key or its certificate). The receiver needs to possess two things in order to decrypt the cipher text. The first thing is his/her secret key stored in the computer. The second thing is a unique personal security device which connects to the computer. It is impossible to decrypt the cipher text without either piece. More importantly, once the security device is stolen or lost, this device is revoked. It cannot be used to decrypt any cipher text. This can be done by the cloud server which will immediately execute some algorithms to change the existing cipher text to be un-decrypt able by this device. This process is completely transparent to the sender. Furthermore, the cloud server cannot decrypt any cipher text at any time. The security and efficiency analysis show that our system is not only secure but also practical.

Index Terms: Cloud storage system, Cloud security, Cloud protection, Two-factor data security protection.

INTRODUCTION

There are such an oversized variety of advantages, to store the data within the cloud storage. Data within the cloud storage server can be facilitated whenever and where as long as network access. Cloud service provider provides services to the cloud users; they can get any amount of a lot of resources any time. It provides no risk of data Storage maintenance tasks, like exploit further storage capability, is unloaded to the responsibility of a service provider easy to data sharing between numerous clients. in the event that sender needs to share a little of data, as an example, video, text, audio so forth to receiver it would be difficult for sender to send it by email as a result of the scale of data.

Instead of that sender transfers the information into the cloud storage then receiver will easily transfer anytime from anywhere. Cloud storage usually refers to a proposal object storage services like Microsoft Azure and Amazon S3 Storage.

There are totally different important challenges in cloud computing for securing information, provision of services and storage of data within the internet from differing kinds of attacks. Cloud computing provides an together with area for data storage, computer processing power, shared pool of resources, networks, user applications and specialized corporate. Cloud computing may be a lot of refined.

It is simple to forecast that the protection for data protection within the cloud storage ought to be improved. In any cases, these applications go through a possible risk concerning component revocability that will limit their possibility. An expandable and flexible Two-Component encoding mechanism is actually a lot of appropriate within the term of cloud computing that prompt our System.

Author for correspondence:
Department of MCA, Nandha Engineering College (Autonomus), Erode-52.

Cloud computing may be a common term for anything that involves scalable services, delivering hosted services like accessing, information sharing, etc. over the online on demand basis. Generally, user shares numerous kinds of documents through cloud storage networking application like Drop box, cloud me, Google drive.

Citrix Cloud computing is thought as an alternative to traditional technology as a result of its low-maintenance and better resource-sharing capabilities. The most goal of cloud computing is to provide high performance energy of computing for numerous field like military and analysis organization for performing billions of computations.

The essential security demand is attained by combining each the cryptographically cloud storage together with searchable encoding scheme.

In cloud system overall value of data storage is less because it does not need managing and maintaining expensive hardware. Within which information owner first encrypts all information before storing on a cloud in such approach that only user whom having decoding keys is decipher or fetch the data.

Figure 1.1: Architecture of Cloud Storage

RELATED WORK

In this scheme presents encoded cloud storage based on attribute-based encoded and a brand new keyword search notion: fine-grained access management aware keyword search. During this system initial group the decoded able files of users before execution the keyword search. It decreases data outpouring from the query method.

A lot of system uses the easy search approach wherever for looking one encrypted keyword, the cloud server should look round all encrypted files on the storage to check that encrypted keyword to each keyword index, and this disadvantage is removed. Focused on drawback of Identity-Based proxy re-encryption, during which cipher-text are convert into one identity to a different. Proxy re-encryption scheme is used to convert the encrypted cipher-text into decrypted cipher text while not in behalf of underlying plaintext.

This drawback removes in Inter-domain identity-based proxy re-encryption. The authors share information and privacy protective auditing theme with massive groups within the cloud. They are utilizing group signature to cipher verification data on shared data. That is the TPA those able to audit correctness of shared data however cannot reveal the identity of the signers on every block.

The original user will efficiently add new users to the group and close the identities of signers on all blocks. This paper describes a system Identity based encoding in commonplace model and has distinct disadvantage of existing system like specifically, computation capability, less public framework and a compact safety reduction. Stronger assumption is based on personal key generation quires created by attacker to reduce this disadvantage using linear diff-hell man Exponent assumption.

This paper focuses on trace out information for security concern. Using a log based audit services that concentrate on privileged information utilize and additionally contemplate their period of time of utilization for this instance information trace go into the cloud storage.

This technique overcome numerous operations on information, additionally repeated creation of tag and sampling. In planned cloud storage systems is used to hold on cipher-text existing access management strategy are not any longer helpful, disadvantage cipher text-Policy Attribute-

Based encoding (CP-ABE) may be a technique for access management of encrypted information.

METHODOLOGY

This paper describes a novel two-factor security protection mechanism for data stored in the cloud. This mechanism provides the subsequent nice features: the system is associate IBE (Identity-based encryption) - primarily based mechanism. That is, the sender only needs to recognize the identity of the receiver in order to send associate encrypted information (cipher text) to him/her.

No different data of the receiver (for example public key, certificate etc.) is required. Then the sender sends the cipher text to the cloud wherever the receiver will transfer it at any time. The system provides two-factor encoding protection. So as to decode the data hold on within the cloud, the user must possess two things. First, the user must have his/her secret key that is hold on within the computer.

Second, the user must have a novel personal security device which is able to be used to connect with the computer (for example USB, Bluetooth and NFC).

It is impossible to decode the ciph*er text while not either piece.* A lot of significantly, the system, for the primary time, provides security device (one of the factors) revocability. Once the safety device is stolen or lost, this device is revoked. That is, exploitation this device you can no longer decode any cipher text.

The cloud can immediately execute some algorithms to alter the existing cipher text to be un-decrypt ready by this device. While, the user must use his new/replacement device (together together with his secret key) to decode his/her cipher text; this method is completel*y transparent to the sender.* The cloud server cannot decode any cipher text at any time.

Benefits of planned System: one. the answer not only enhances the confidentiality of the information, however additionally offers the revocability of the device so once the device is revoked; the corresponding cipher text are updated automatically by the cloud server with none notice of the data owner.

The cloud server cannot decode any cipher text at any time. during this implementation we have five Modules, 1) personal Key Generator 2) Security Device establishment 3) Sender Module 4) Receiver Module 5)Cloud Server Module.

Modules Description: one. Personal Key Generator: a non-public Key Generator may be a trustworthy party responsible for issue the private key for each user.

Security Device establishment (SDI)

A Security Device establishment may be a trustworthy party responsible for issue security device for each user.

Sender

This user is that the sender and also the creator of the cipher text. The sender only is aware of the identity as an example email address of the receiver however nothing else associated with the receiver. When the sender has created the cipher text, he/she sends to the cloud server to let the receiver for download.

Receiver

This user is that the receiver of the cipher text and includes a unique identity as an example email address. The cipher text is holding on cloud storage whereas he/she will download it for cryptography.

The receiver contains a personal key (stored in his computer) and a security device (that contains some secret data associated with his identity). They are given by the PKG. The decoding of cipher text needs each the personal key and also the security device.

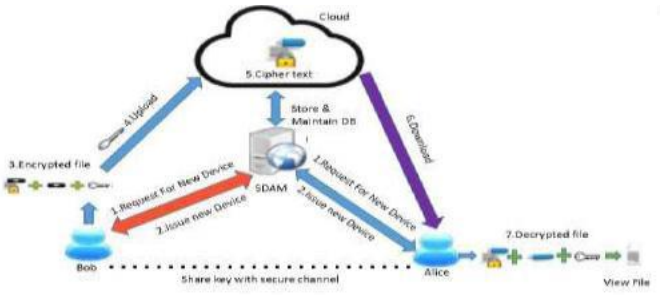

Figure 3.1: Proposed System Architecture

Cloud server

The cloud server is responsible for storing all cipher text (for receiver to download). Once a user has reportable loss of his/her security device (and has obtained a new one from the PKG), the cloud acts as a proxy to re-encrypt the entire past and future cipher text equivalent to the new device. That is, the recent device is revoked.

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, and 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.

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.

The sender needs to know the serial number/ public key of the security device, in additional to the users identity/public key. That makes the encryption process more complicated.

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

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.

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.

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.

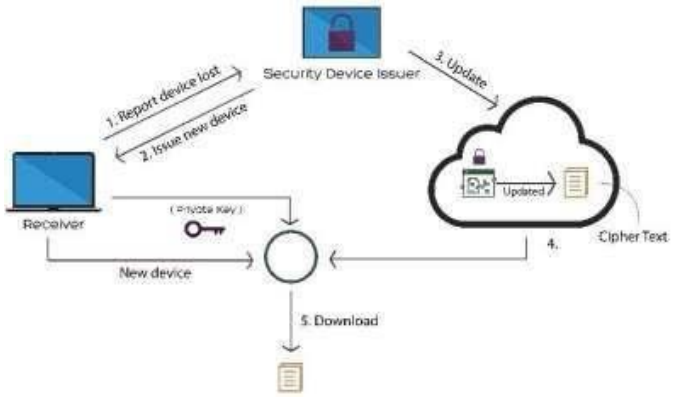

Fig 3.2: update cipher text after issuing a new security device..

- 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.
- The cloud server cannot decrypt any cipher text at any time.

CONSTRUCTION

We have two diverse encryption innovations: one is IBE and the other is conventional Open Key Encryption (PKE). At first we enable a client to produce at first level figure message under a collector's personality. The fisrt level figure content will be additionally changed into a moment level figure content comparing to a security gadget. The subsequent figure content can be unscrambled by a legitimate collector with mystery key and security gadget. Here, one may question that our development is an insignificant and clear blend of two distinct encryptions. Shockingly, this isn't valid because of the way that we have to additionally bolster security gadget revocability. A unimportant mix of IBE and PKE can't accomplish our

Objective

- Setup phase: the setup phase generates all public parameters and master secret key used throughout the execution of system.
- The SDI finally delivers the security device to a user ID.
- First-level cipher text generation phase: a data sender encrypts a data under the identity of a data receiver, and further sends the encrypted data to the cloud server.
- Second-level cipher text phase: after receiving the first level cipher text of a data from the data sender, the cloud server generates the second-level cipher text
- Device updated phase: Once a device of a user needs to be updated due to some incidences (e.g., it is either lost or stolen), the user first reports the issue to the SDI. The SDI then issues a new device for the user.
- Cipher text updated phase: The SDI notifies the cloud server to update the cipher text of the user by sending a special piece of information.
- Data recovery phase. A data receiver uses a decryption key and a device to recover the data as follows.

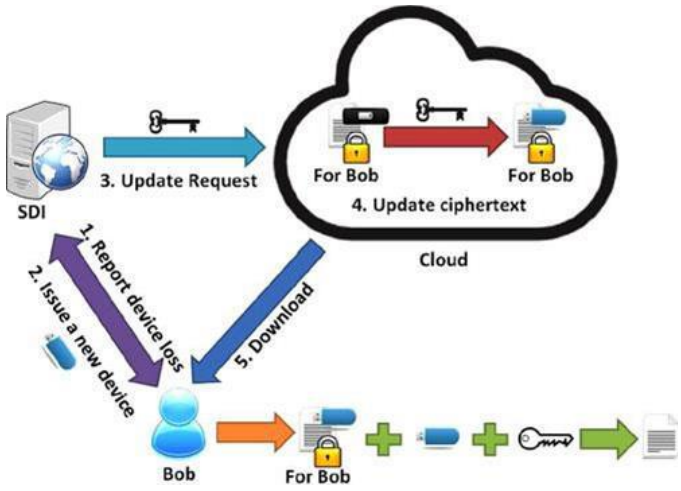

Fig 4.1: Update cipher text after issuing a new security device

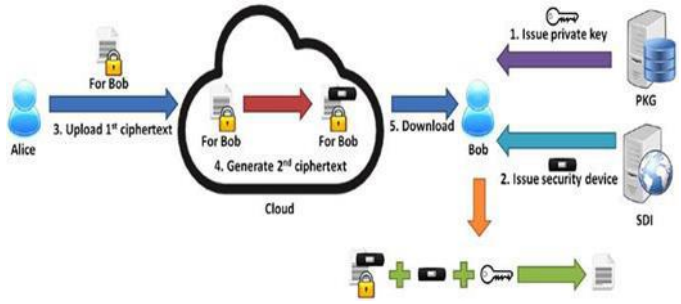

Fig 4.2: Ordinary data sharing.

SYSTEM EVALUATION

Security Analysis

We separate two security levels for our scheme: one is allowing an adversary to achieve the secret key of user but not the corresponding secure device, and the other is the reversed case. For Type-I Security. Here we allow an adversary to obtain the secret key of a user but not the corresponding security device. We analyze the security of our scheme under the model of Type-I. Practical analysis: An adversary A now is given the secret key skIDi of user IDi. We show that cannot recover the underlying message by only leveraging knowledge of skIDi as follows.

Schemes	[2]	[20]	Ours
Secret Key Generation	$2C_e$	C_e	$2C_e$
Security Device Generation	$\perp$	$\perp$	$2C_e$
Ciphertext Generation	$C_e + C_{\hat{e}} + 3C_p$	$4C_e + C_p$	first-level Ciph.: $3C_e + C_{\hat{e}}$ second-level Ciph.: $4C_e + C_{\hat{e}}$
Ciphertext Update	$\perp$	$2C_e + 5C_p$	$5C_e + 6C_p$
Device Update	$\perp$	$\perp$	$2C_e$
Data Recovery (From Original Ciph.)	$C_e + C_p$	$4C_e + 2C_p$	$8C_e + 2C_p$
Data Recovery (From Updated Ciph.)	$\perp$	$C_e + 2C_p$	$7C_e + C_{\hat{e}} + 2C_p$

Efficiency Analysis

We analyze the efficiency of our mechanism as well as its comparison with (the most efficient two-secret protection system but no revocability) and (the most efficient single secret system with revocability) in terms of computational and communicational cost. We present the theoretical comparison in Tables for computation and communication complexity, respectively. From Table, it can be seen that our system requires additional computation cost in security device generation and update, whereas others do not need any cost. This is because ours supports security device revocability.

In cipher text generation, our system does not require any pairings operation, and it is worth of mentioning that the second level cipher text generation cost can be offloaded to a cloud server. Compared to for other metrics, our system only requires slight extra cost; while we just need an additional pairing in cipher text update.

A similar phenomenon does exist in Table in the sense that our system needs extra communication cost in delivery of security device. Except for this, our communication complexity is much closer to that of others.

CONCLUSION

Various techniques are available to provide security for cloud storage data. Among them, two-Factor Data Security Protection mechanism only provides confidentiality of the data and revocability for cloud data by using secret key and unique personal device. The efficiency and security analysis show that the system is secure as well as practically implemented.

REFERENCES

[1]. Sahai, H. Seyalioglu, B. Waters. Dynamic credentials and cipher text delegation for attribute-based encryption. In: Advances in Cryptology– CRYPTO 201 Springer Berlin Heidelberg. 2012, 199-217.

[2]. Libert, D. Vergnaud. Unidirectional chosen-cipher text secures proxy re-encryption IEEE Transactions on Information Theory, 57(3), 2011, 1786-1802.

[3]. Wang, S.S. Chow, Q. Wang, K. Ren, W. Lou. Privacy-preserving public auditing for secure cloud storage IEEE Transactions on computers, 62(2), 2013, 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. IEEE Transactions on Parallel and Distributed Systems, 25(2), 2014, 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, 8209, 2013, 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 Computers, 63(1), 2014, 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, 206, 2012, 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]. C.-K. Chu and W.-G. Tzeng, “Identity-based proxy re-encryption without random oracles,” in Proc. 10th Int. Con. Inf. Security, SSS, 2007, 189–202.