ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

Facilitate Cloud Storage Auditing With Provable Outsourcing of Key Updates

N.JOTHIMALAR [1], V.MATHESWARAN [2]

1. P.G. Student, Dept. of MCA, VSB Engineering College, Karur, Tamilnadu, India
2. Assistant Professor, Dept. of MCA, VSB Engineering College, Karur, Tamilnadu, India

Abstract
Key-exposure resistance has always been animportant issue for in-depth cyber defence in many securityapplications. Recently, how to deal with the key exposure problemin the settings of cloud storage auditing has been proposed andstudied. To address the challenge, existing solutions all requirethe client to update his secret keys in every time period, whichmay inevitably bring in new local, burdens to the client, especiallythose with limited computation resources, such as mobile phones.In this paper, we focus on how to make the key updates astransparent as possible for the client and propose a new paradigmcalled cloud storage auditing with verifiable outsourcing of keyupdates. In this paradigm, key updates can be safely outsourcedto some authorized party, and thus the key-update burden on theclient will be kept minimal. In particular, we leverage the thirdparty auditor (TPA) in many existing public auditing designs, letit play the role of authorized party in our case, and make it incharge of both the storage auditing and the secure key updates forkey-exposure resistance. In our design, TPA only needs to hold an encrypted version of the client's secret key while doing all theseburdensome tasks on behalf of the client. The client only needs todownload the encrypted secret key from the TPA when uploadingnew files to cloud. Besides, our design also equips the client withcapability to further verify the validity of the encrypted secretkeys provided by the TPA.

1. INTRODUCTION

Cloud computing, as a new technology paradigm with promising further, is becoming more and more popular nowadays. It can provide users with seemingly unlimited computing resource. Enterprises and people can outsource time consuming computation workloads to cloud without spending the extra capital on deploying and maintaining hardware and software. In recent years, outsourcing computation has attracted much attention and been researched widely. It has been considered in many applications including scientific computations, linear algebraic computations, linear programming computations and modular exponentiation computations, etc. Besides, cloud computing can also provide users with seemingly unlimited storage resource. Cloud storage is universally viewed as one of the most important services of cloud computing. Although cloud storage provides great benefit to users, it brings new security challenging problems. One important security problem is how to efficiently check the integrity of the data stored in cloud. In recent years, many auditing protocols for cloud storage have been proposed to deal with this problem. These protocols focus on different aspects of cloud storage auditing such as the high efficiency, the privacy protection of data, the privacy protection of identities, dynamic data

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

operations, and the data sharing etc. The key exposure problem, as another important problem in cloud storage auditing, has been considered recently.

The problem itself is non-trivial by nature. Once the client's secret key for storage auditing is exposed to cloud, the cloud is able to easily hide the data loss incidents for maintaining its reputation, even discard the client's data rarely accessed for saving the storage space. Yu *et al.* constructed a cloud storage auditing protocol with key-exposure resilience by updating the user's secret keys periodically. In this way, the damage of key exposure in cloud storage auditing can be reduced. But it also brings in new local burdens for the client because the client has to execute the key update algorithm in each time period to make his secret key move forward. For some clients with limited computation resources, they might not like doing such extra computations by themselves in each time period. It would be obviously more attractive to make key updates as transparent as possible for the client, especially in frequent key update scenarios. In this paper, we consider achieving this goal by outsourcing key updates. However, it needs to satisfy several new requirements to achieve this goal. Firstly, the real client's secret keys for cloud storage auditing should not be known by the authorized party who performs outsourcing computation for key updates. Otherwise, it will bring the new security threat. So the authorized party should only hold an encrypted version of the user's secret key for cloud storage auditing. Secondly, because the authorized party performing outsourcing computation only knows the encrypted secret keys, key updates should be completed under the encrypted state. In other words, this authorized party should be able to update secret keys for cloud storage auditing from the encrypted version he holds. Thirdly, it should be very efficient for the client to recover the real secret key from the encrypted version that is retrieved from the authorized party. Lastly, the client should be able to verify the validity of the encrypted secret key after the client retrieves it from the authorized party. The goal of this paper is to design a cloud storage auditing protocol that can satisfy above requirements to achieve the outsourcing of key updates.

The main contributions are as follows:

(1) We propose a new paradigm called cloud storage auditing with verifiable outsourcing of key updates. In this new paradigm, key-update operations are not performed by the client, but by an authorized party. The authorized party holds an encrypted secret key of the client for cloud storage auditing and updates it under the encrypted state in each time period. The client downloads the encrypted secret key from the authorized party and decrypts it only when he would like to upload new files to cloud. In

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

addition, the client can verify the validity of the encrypted secret key.

(2) We design the first cloud storage auditing protocol with verifiable outsourcing of key updates. In our design, the thirdparty auditor (TPA) plays the role of the authorized party who is in charge of key updates. In addition, similar to traditional public auditing protocols,another important task of the TPA is to check the integrity of the client's files stored in cloud. The TPA does not know the real secret key of the client for cloud storage auditing, but only holds an encrypted version.

In the detailed protocol, we use the blinding technique with homomorphic property to form the encryption algorithm to encrypt the secret keys held by the TPA. It makes our protocol secure and the decryption operation efficient. Meanwhile, the TPA can complete key updates under the encrypted state. The client can verify the validity of the encrypted secret key when he retrieves it from the TPA. Therefore, the designed protocol satisfies the above mentioned four requirements.

(3) We formalize the definition and the security model of the cloud storage auditing protocol with verifiable outsourcing of key updates. We also prove the security of our protocol in the formalized security model and justify its performance by concrete implementation.

2. LITERATURE SURVEY

A.Privacy-Preserving Public Auditing For Secure Cloud Storage

The distributed storage benefit (CSS) eases the weight for capacity administration and upkeep. In any case, if such an essential administration is helpless against assaults or disappointments, it would convey hopeless misfortunes to the customers in light of the fact that their information or documents are put away in a dubious stockpiling pool outside the ventures. These security dangers originate from the accompanying reasons: First, the cloud bases are a great deal more intense and dependable than individualized computing gadgets, however they are still helpless to inner dangers (e.g., through virtual machine) and outside dangers (e.g., by means of framework gaps) that can harm information respectability; second, for the advantages of ownership, there exist different inspirations for cloud benefit suppliers (CSP) to carry on unfaithfully toward the cloud clients; moreover, question once in a while experience the ill effects of the absence of trust on CSP in light of the fact that the information change may not be convenient known by the cloud clients, regardless of the possibility that these debate may come about because of the clients' own particular dishonorable operations. In this way, it is fundamental for CSP to offer a productive review administration to check the respectability and accessibility of put away data. It is attractive that cloud just engages

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

confirmation ask for from a solitary assigned gathering. To completely guarantee the information respectability and spare the cloud client's calculation assets and in addition online weight, it is of basic significance to empower open examining administration for cloud information stockpiling, with the goal that clients may depend on an autonomous outsider inspector (TPA) who has skill and proficient to review the outsourced information when required. Open review capacity permits an outer gathering, notwithstanding the client himself, to confirm the accuracy of remotely put away information This extreme disadvantage extraordinarily influences the security of these conventions in distributed computing. It is an endeavor to demonstrate the security by applying different systems and legitimize the execution of proposed plans through solid trials and examinations. It is our endeavor to give security to the cloud by just basically utilizing Kerberos frameworks for open review capacity. In particular, proposed plot accomplishes group examining where various assigned inspecting undertakings from various clients can be performed at the same time by the TPA in a protection safeguarding way. [6] proposed a secure hash message authentication code. A secure hash message authentication code to avoid certificate revocation list checking is proposed for vehicular ad hoc networks (VANETs). The group signature scheme is widely used in VANETs for secure communication, the existing systems based on group signature scheme provides verification delay in certificate revocation list checking. In order to overcome this delay this paper uses a Hash message authentication code (HMAC).

B. Baf: An Efficient Publicly Verifiable Secure Audit Logging Scheme For Distributed Systems

In this paper, we concentrate on the best way to make the key overhauls as straightforward as could be expected under the circumstances for the customer and propose another worldview called distributed storage reviewing with certain outsourcing of key redesigns. In this worldview key overhauls can be securely outsourced to some approved gathering and along these lines the key-upgrade trouble on the customer will be kept insignificant. In particular, we influence the outsider inspector (TPA) in numerous current open examining outline, let it assume the part of approved gathering for our situation and make it accountable for both the capacity reviewing and secure key upgrades for key-presentation resistance. Existing arrangements all require the customer to overhaul his mystery enters in each day and age, which may definitely acquire new nearby, weights to the customer, particularly those with constrained calculation assets, for example, cell phones. In these Concepts, we concentrate on the most proficient method to make the key upgrades as straightforward as could be expected under the circumstances for the customer and propose

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

another worldview called distributed storage inspecting with evident outsourcing of key redesigns. In this worldview, key redesigns can be securely outsourced to some approved gathering, and subsequently the key-overhaul load on the customer will be kept insignificant. In particular, we influence the outsider evaluator (TPA) in numerous current open examining plans, let it assume the part of approved gathering for our situation, and make it accountable for both the capacity inspecting and the safe key upgrades for key-introduction resistance. In our outline, TPA just needs to hold a scrambled variant of thecustomer's mystery key, while doing all these difficult assignments for the benefit of the customer. We prove that BAF is secure under appropriate computational assumptions, and demonstrate that BAF is significantly more efficient and scalable than the previous schemes. Therefore, BAF is an ideal solution for secure logging in both task intensive and resource-constrained systems

C. Dynamic Provable Data Possession

In this paper, we concentrate on the best way to make the key overhauls as straightforward as could be expected under the circumstances for the customer and propose another worldview called distributed storage reviewing with certain outsourcing of key redesigns. In this worldview key overhauls can be securely outsourced to some approved gathering and along these lines the key-upgrade trouble on the customer will be kept insignificant. In particular, we influence the outsider inspector (TPA) in numerous current open examining outline, let it assume the part of approved gathering for our situation and make it accountable for both the capacity reviewing and secure key upgrades for key-presentation resistance. As of late, key presentation issue in the settings of distributed storage examining has been proposed and concentrated on.generated the key of particular concepts mainly they are read as they are mainly generated the key a particular point key are not update In this worldview, key redesigns can be securely outsourced to some approved gathering, and subsequently the key-overhaul load on the customer will be kept insignificant. In particular, we influence the outsider evaluator (TPA) in numerous current open examining plans, let it assume the part of approved gathering for our situation, and make it accountable for both the capacity inspecting and the safe key upgrades for key-introduction resistance. In our outline, TPA just needs to hold a scrambled variant of the customer's mystery key, while doing all these difficult assignments for the benefit of the customer. The customer just needs to download the scrambled mystery key from the TPA while transferring new documents to cloud. Moreover, our plan additionally outfits the customer with capacity to facilitate confirm the legitimacy of the scrambled mystery keys gave by TPA. We formalize the definition and the security model of this worldview. The

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

security confirmation and the execution reenactment demonstrate that our point by point plan instantiations are secure and productive.

2.1 EXISTING SYSTEM

Cloud storage is universally viewed as one of the most important services of cloud computing. Although cloud storage provides great benefit to users, it brings new security challenging problems. One important security problem is howto efficiently check the integrity of the data stored in cloud. In recent years, many auditing protocols for cloud storage have been proposed to deal with this problem. The key exposure problem is another important problem in cloud storage auditing.

2.1.1 Disadvantages of Existing System

1. Checking the integrity of the data inefficient
2. Once the client's secret key for storage auditing is exposed to cloud, the cloud is able to easily hide the data loss incidents for maintaining its reputation, even discard the client's data rarely accessed for saving the storage space.
3. Exiting System don't like auditing protocol with verifiable outsourcing of key updates.
4. TPA has the access to see client's secret key without encryption
5. No verification system available for client's for to check validity of the encrypted secret key when downloading them from TPA
6. All exiting auditing protocols are all built on the assumption that the secret key of client is absolutely secure and wobble not be exposed.

2.2 PROPOSED SYSTEM

We propose a new paradigm called cloud storage auditing with verifiable outsourcing of key updates. In this new paradigm, key-update operations are not performed by the client, but by an authorized party. The authorized party holds an encrypted secret key of the client for cloud storage auditing and updates it under the encrypted state in each time period. The client downloads the encrypted secret key from the authorized party and decrypts it only when he would like to upload new files to cloud. In addition, the client can verify the validity of the encrypted secret key. We design the first cloud storage auditing protocol with verifiable outsourcing of key updates. In our design, the third party auditor (TPA) plays the role of the authorized party who is in charge of key updates. In addition, similar to traditional public auditing protocols, another important task of the TPA is to check the integrity of the client's files stored in cloud. The TPA does not know the real secret key of the client for cloud storage auditing, but only holds an encrypted version. In the detailed protocol, we use the blinding technique with homomorphic property to form the encryption algorithm to encrypt the secret keys held by the TPA. It makes our protocol secure and the decryption operation efficient. Meanwhile, the TPA can

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

complete key updates under the encrypted state. The client can verify the validity of the encrypted secret key when he retrieves it from the TPA.

2.2.1 Advantages of Proposed System

1. In this protocol, key updates are outsourced to the TPA and are transparent for the client
2. The TPA only sees the encrypted version of the client's secret key, while the client can further verify the validity of the encrypted secret keys when downloading them from the TPA
3. The TPA does not know the real secret key of the client for cloud storage auditing, but only holds an encrypted version. In the detailed protocol we use the blinding technique with homomorphism property to form the encryption algorithm to encrypt the secret key held by the TPA.it makes our protocol secure and the decryption operation efficient.
4. Meanwhile, The TPA can complete key updates under the encrypted state. The Client can validity of the encrypted secret key when he retrieve it from the TPA.

3. SYSTEM MODEL

The proposed system shows the system model for cloud storage auditing with verifiable outsourcing of key updates in Fig. 1. There are three parties in the model: the client, the cloud and the third-party auditor (TPA).

The client is the owner of the files that are uploaded to cloud. The total size of these files is not fixed, that is, the client can upload the growing files to cloud in different time points. The cloud stores the client's files and provides download service for the client.

The TPA plays two important roles: the first is to audit the data files stored in cloud for the client; the second is to update the encrypted secret keys of the client in each time period. The TPA can be considered as a party with powerful computational capability or a service in another independent cloud. The whole lifetime of the files stored in cloud is divided into$T + 1$ time periods (from 0-th to T -th time periods). Each file is assumed to be divided into multiple blocks. In order to simplify the description, it does not furthermore divide each block into multiple sectors in the description of the protocol. In the end of each time period, the TPA updates the encrypted client's secret key for cloud storage auditing according to the next time period. But the public key keeps unchanged in the whole time periods. The client sends the key requirement to the TPA only when he wants to upload new files to cloud. And then the TPA sends the encrypted secret key to the client. After that, the client decrypts it to get his real secret key, generates authenticators for files, and uploads these files along with authenticators to cloud. In addition, the TPA will audit whether the files in cloud are stored correctly by a challenge-response protocol between it and the cloud at regular time.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

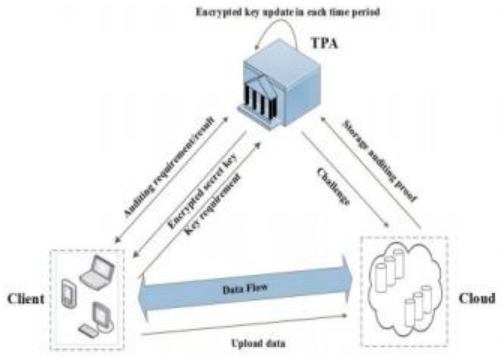

Fig. 1. System model of our cloud storage auditing.

The definition of cloud storage auditing protocol with verifiable outsourcing of key updates.

Definition 1: A cloud storage auditing protocol with secure outsourcing of key updates is composed by seven algorithms (*SysSetup*, *EkeyUpdate*, *VerESK*, *DecESK*, *AuthGen*, *Proof-*

Gen, *ProofVerify*), shown below:

1) *SysSetup*: the system setup algorithm is run by the client. It takes as input a security parameter k and the total number of time periods T , and generates an encrypted initial client's secret key *ESK*0, a decryption key *DK* and a public key *PK*. Finally, the client holds

DK, and sends *ESK*0 to the TPA.

2) *EkeyUpdate*: the encrypted key update algorithm is run by the TPA. It takes as input an encrypted client's secret key *ESKj* , the current period j and the public key *PK*, and generates a new encrypted secret key *ESKj*+1 for period $j + 1$.

3) *VerESK*: the encrypted key verifying algorithm is run by the client. It takes as input an encrypted client's secret key *ESKj* , the current period j and the public key *PK*, if *ESKj* is a well-formed encrypted client's secret key, returns 1; otherwise, returns 0.

4) *DecESK*: the secret key decryption algorithm is run by the client. It takes as input an encrypted client's secret key *ESKj* , a decryption key *DK*, the current period j and the public key *PK*, returns the real client's secret key *SK j* in this time period.

5) *AuthGen*: the authenticator generation algorithm is run by the client. It takes as input a file F, a client's secret key *SK j* , the current period j and the public key *PK*, and generates the set of authenticators _ for F in time period j .

6) *Proof Gen*: the proof generation algorithm is run by the cloud. It takes as input a file F, a set of authenticators, a challenge *Chal*, a time period j and the public key *PK*, and generates a proof P which proves the cloud stores F correctly.

7) *Proof Verif y*: the proof verifying algorithm is run by the TPA. It takes as input a proof P, a challenge *Chal*, a time period j , and the public key *PK*, and returns "*True*" if P is valid; or "*False*", otherwise.

3.1MODULE DESCRIPTION

The syste has three main modules,

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

1. Client Module
2. Cloud Module
3. Third Party Auditor (TPA)

3.1.1 CLIENT

The client is the owner of the files that are uploaded to cloud. The total size of these files is not fixed, that is, the client can upload the growing files to cloud in different time points.

3.1.2 CLOUD

The cloud stores the client's files and provides download service for the client.

3.1.3 TPA

The TPA plays two important roles: the first is to audit the data files stored in cloud for the client; the second is to update the encrypted secret keys of the client in each time period.

4. CONCLUSION

The proposed system can be helpful to create multiple copies of sensitive data in different server. Also, it verifies integrity where CSP prove all copies are intact. In addition it identifies corrupted copies and reconstruct before dynamic operation performs. It also discussed to share access authority by providing security and privacy. Outsourcing data to remote servers has become a growing trend for many organizations to alleviate the burden of local data storage and maintenance. In this work it has studied the problem of creating multiple copies of dynamic data file and verifying those copies stored on untrusted cloud servers. It proposed a new PDP scheme (referred to as MB-PMDDP), which supports outsourcing of multi-copy dynamic data, where the data owner is capable of not only archiving and accessing the data copies stored by the CSP, but also updating and scaling these copies on the remote servers. To the best of the knowledge, the proposed scheme is the first to address *multiple* copies of *dynamic* data. The interaction between the authorized users and the CSP is considered in our scheme, where the authorized users can seamlessly access a data copy received from the CSP using a single secret key shared with the data owner. Moreover, the proposed scheme supports public verifiability, enables arbitrary number of auditing, and allows *possession-free* verification where the verifier has the ability to verify the data integrity even though he neither possesses nor retrieves the file blocks from the server.

FUTURE WORK

Through performance analysis and experimental results, it demonstrated that the proposed MB-PMDDP scheme outperforms the TB-PMDDP approach derived from a class of dynamic single-copy PDP models. The TB-PMDDP leads to high storage overhead on the remote servers and high computations on both the CSP and the verifier sides. The MB-PMDDP scheme significantly reduces the computation time during the challenge-response phase which makes it more practical for applications where a large number of verifiers are connected to the CSP causing a

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

huge computation overhead on the servers. Besides, it has lower storage overhead on the CSP, and thus reduces the fees paid by the cloud customers. The dynamic block operations of the map-based approach are done with less communication cost than that of the tree-based approach. A slight modification can be done on the proposed scheme to support the feature of identifying the indices of corrupted copies. The corrupted data copy can be reconstructed even from a complete damage using duplicated copies on other servers. Through security analysis, it is shown that the proposed scheme is provably secure.

REFERENCE

[1]. R. Buyya, C.S. Yeo, S.Venugopal, J. Broberg , and I. Brandic, "Cloud computing and emerging IT platforms", Future generation computer system, vol. 25, no. 6, pp. 599-616, 2009.

[2]. Giuseppe Ateniese, Randal Burns,RezaCurtmola, Joseph Herring, LeaKissner, Zachary Peterson, and Dawn Song, "Provable data possession at untrusted stores", in Proceedings of the 14th ACM Conference on Computer and communications security, Oct 2007.

[3]. F. Sebé, J. Domingo- Ferrer, A. Martinez-Balleste, Y. Deswarte and J.-J. Quisquater,"Efficient remote data

possession checking in critical information infrastructures," IEEE Trans. Knowl. Data Eng. vol. 20, no. 8, pp. 1034–1038, Aug. 2008

[4]. Giuseppe Ateniese, Roberto Di Pietro, Luigi V.Mancini and Gene Tsudik, "Scalable and Efficient Provable Data Possession", in Proceedings of the 4th international conference on Security and privacy in communication, 2008.

[5]. C. Wang, Q. Wang, K. Ren, and W.Lou.(2009)."Ensuring data security in cloud computing", http:// eprint.jacr. org/

[6]. Christo Ananth, M.Danya Priyadharshini, "A Secure Hash Message Authentication Code to avoid Certificate Revocation list Checking in Vehicular Adhoc networks", International Journal of Applied Engineering Research (IJAER), Volume 10, Special Issue 2, 2015,(1250-1254)

[7]. Decio Luiz Gazzoni Filho and Paulo Sergio Licciardi Messeder Barreto, "Demonstrating data possession and uncheated data transfer", 2006

[8]. Ayad F. Barsoum and M. Anwar HAsan "Provable Multi- Copy Dynamic Data Possession in Cloud Computing Systems" IEEE trans. On information foraensics and security VOL10, NO. 3, March 2015.

[9]. Giuseppe Ateniese, Roberto Di Pietro, Luigi V.Mancini and Gene Tsudik, "Scalable and Efficient Provable Data Possession", in Proceedings of the 4th international conference on Security and privacy in communication,2008.