ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 3, March 2013

Enhancing Data Storage Integrity in Cloud Environment by mitigating Repudiation using CS-MPNR

Meena S, Esther Daniel, Dr. N.A. Vasanthi

***Abstract* – Cloud computing is envisioned as the next generation architecture of IT organisation. It makes the users need of their data to be available wherever they are. Although recent emerging technology Cloud has many striking features, it also has some security dreads. So the users find it difficult to trust the providers who store their data. The vulnerabilities in Cloud storage lead to some loopholes for the attackers to snatch the data and modify or delete it. Data to be secure such as medical reports, industrial files, and other personal and important data should be protected enough from the repudiation problems to maintain Data integrity. To overcome these challenges, a novel new CS-MPNR [Chaining Signature-Multi Party Non Repudiation] protocol is proposed, which is a method that uses Chaining Signature [CS] acting as a link of signature to have a follow up of the chained users and lessens the Disputation. For the need of challenging the providers and also to have fairness during the transaction of data, TTP (Trusted Third Party) is allowed, which reduces the users work of checking the data completeness. Not only it reduces repudiation problem, it also maintains and upholds Data Integrity. Performance evaluation shows that the computational time is reduced with provable security**

***Index Terms*--Cloud Storage, Storage security, Chaining Signature, Non repudiation, Data Integrity.**

I. INTRODUCTION

Cloud is one of the recent technology that has grown tremendously and became famous among the users because of its various services offered like Iaas, Paas, Saas, SECaas, STaas and etc., [1-2]. It obtained its popularity in all areas like industries, medical organisation, military, academic institution and general usage of individual users.

Today mostly all the organisations depends on Cloud computing. They move towards this modern way of computing, where their financial deposits decreases by utilizing the large number of Cloud resources offered as Pay-as-per-use manner. Services are rendered based on demand and the necessary of the whole organization or the individual user [1].

Manuscript received Mar, 2013.

***Meena S**, PG Scholar – Information Technology, Karunya University, Coimbatore, India.*

***Esther Daniel**, Assistant Professor - IT, Karunya University, Coimbatore, India,*

***Dr. N.A. Vasanthi**, Professor and Dean, Nehru Institute of Engineering and Technology, Coimbatore, India.*

Many Cloud providers are there to offer those services. Currently Cloud storage is in a modern and emerging way, where the days are outsourced daily by the data users and the cloud provider take the responsibility over it for its availability and reliability. Those data should be monitored and maintained by them.

The most profitable application in the Cloud is storage of data potentially. Cloud storage providers attempt to persuade their users for storing their important and sensitive data in the Cloud by often advertising the new business model. Potential users are left to wonder whether the confidentiality, integrity, and the availability of their data are guaranteed in Cloud Storage [1]. Just as no one would want to put his valued possessions in a house without a secure lock, users are reluctant to move important and sensitive data to Cloud until these challenges have been well addressed. Therefore, to date this potentially valuable service model is still not widely accepted. In addition, some user concerns cannot be alleviated by simply developing new technologies. There is naturally some psychological anxiety when a user is faced with the decision to store sensitive data in a location that is out of his control. In fact, some problems require more than conventional cyber security mechanisms and introduce new security challenges. Research in Cloud storage security is far from mature, and traditional cyber security solutions cannot provide enough protection in the Cloud for other reasons. In the meantime, the uniqueness of secure Cloud storage still has not been fully understood [1-2]. One characteristic of Cloud Storage is mass storage in which data is communicated through the Internet.

Still there exists some vulnerability that can potentially lead to disputation. To correct such weakness, we propose a novel CS-Multi Party Non-repudiation Protocol (CS-MPNR) scheme by utilizing the chaining signature for secure Cloud storage systems. We focus on how to ensure integrity with fair non-repudiation, not just how to maintain integrity itself since current integrity algorithms are sufficient. The idea of integrity checks and non-repudiation is not new [2]. Using traditional non-repudiation protocols, the receivers can decrypt the received data. This is not preferable for cloud storage. So in this paper we describe about the basic MPNR protocol and the proposed CS-MPNR protocol for overcoming the repudiation and integrity problems.

The paper is structured as follows where Section 1 gives an intro about cloud computing and its services.

Section 2 depicts the review of various recent approaches which aim to achieve secure data storage through cryptographic primitives. Section 3 illustrates the proposed model and the steps performed. Section 4 evaluates the performance of CS-MPNR. We conclude in section 5 followed by list of references.

II. Related works

The main issue that prevails in the storage performances processing is integrity of the data [2] and the security mechanisms like repudiation, fairness, confidentiality, and different attacks like Rollback attack, Data leakage, Tag forgery attack, Replay attack, Timeliness attack and byzantine failure of the server.

Many schemes were proposed related to securing the data integrity and the data possession. Proof of Retrievability (POR) model is described by Juels *et.al* [3] for ensuring the data integrity in remote areas. Ateniese *et.al* [4], *"Provable Data Possession"* (PDP) scheme is introduced, which checks the intact and possession of users data in remote servers or untrusted storages. Here public key is used based on homographic tags for data file auditing. Instead of using the public key, symmetric key cryptography method [5] [10] are proposed, which allows block updating, deletion and appending.

Yun Zhu *et.al* [6] proposed a scheme called Cooperative PDP (CPDP). The data to be stored are considered to be stored on different and multiple Cloud storage providers for the support of scalability of service and data redundancy. NR protocol is proposed by Jun Feng.*et.al* [7], where the storage correctness and integrity vulnerabilities has been overcome. The integrity of the data is checked in both the uploading and downloading sessions. The evidence is encrypted by recipient's public key by the sender for data confidentiality.

Even though Q.Wang.*et.al* [8] proposed a scheme for roll-back attack, it is not compatible for cloud storage process. So J.Feng.*et.al* [15] [17] proposed a scheme, where Repudiation and Rollback event in cloud is prevented by using Merkle Hash tree method. The main idea behind this method is that the trust over the root counter is transferred to its children by checking the integrity of the tag and the data blocks as well. Bowers.*et.al* [9] proposed a cryptographic system HAIL. This High availability and Integrity Layer protocol proves that the client data is stored intact and securely retrievable from a set of servers. This is robust against data loss, but it only focuses on static data.

From the above work, it is clear that the need of data integrity is most important for a better storage in Cloud environment. But repudiation along with data integrity is not explained properly. The basic MPNR protocol is proposed by J.Feng.et.al [17], where they dealt with repudiation. But the security can be still more provided for a robust storage of data in the cloud environment.

Hence there is a need of better and resilient model, where all the security metrics are maintained and users have the confident to store their data in the remote servers. The next section explains about the model for performing those mechanisms by implementing the new MPNR protocol, known as CP-MPNR, which is resilient in nature against security dreads.

III. Proposed system

The proposed system deals with main issue of cloud storage, Data Integrity and the repudiation problem. We explain about the basic MPNR and the CS-MPNR, after the description of some basic definitions used throughout the paper for a better understanding.

Definition 1: Data Integrity

The Data Integrity, in general term is defined as the data intact (i.e.,) no modification of the data without users knowledge [2]. Clients will loss trust in a service provider when any corruption happens to their data. So it is a provider's duty to take responsibility over the information. Protecting private and important details, such as credit card information or a patient's medical records detail from attackers or malicious insiders is of critical importance. Security for the information stored by the user should be well provided [11 - 12].

Definition 2: Repudiation

If a user gets data through cloud service provider and the user claims that the data is tampered. The innocent entity needs evidence to defend against false accusations. And it is desired to find the peer who is responsible for the fault. In the proposed system, we overcome this issue by using a Non-Repudiation Protocol

Definition 3: Non-Repudiation

Non-repudiation evidences [19] are based on digital signatures which act as the evidence. A digital signature that can be used as non-repudiation evidence provides a link between a message and a public verification key. In this paper we focus on the protocols distributing the evidences among the peers. The aim of a non-repudiation protocol is to provide with the evidences like non-repudiation of origin (evidence form the originator) and non-repudiation of receipt (evidence from the recipient), with respect to a given message.

Definition 4: Fairness

During the data transmission procedure, in order to gain certain advantages, [17] malicious party may refuse to response after receiving the evidence from other peers.

Definition 4: Confidentiality

The service provider is assumed to be an untrustworthy third party, and the owner does not want to reveal the data to the provider [20].

Definition 5: Rollback

By supposing that data owner uploads with 1 MB of data, and a user, downloads it. After sometime, the data owner updates 50 KB, and the user wants to download the updated 50 KB of data. At this time, the user needs certain evidence to help ensure that the data is updated and that the downloaded

50 KB of data is up-to-date. If a malicious cloud service provider deletes the updated content and delivers out-dated data, the user should be able to detect the inconsistency based on the evidence. This is also defined as "user's freshness" [20]

Fair non-repudiation protocols are the one traditionally studied in the previous work. Throughout the remaining of the paper, we assume that CS-MPNR protocol is fair and free from attacks by maintaining the integrity of the data.

A. Basic MPNR protocol:

The Multi Party Non-repudiation protocol is the extended protocol of TPNR, Two Party Non repudiation Protocol.

The first phase is between the data owner and the Cloud provider. The second phase is between the data owner and the data user, where the third phase is between the data user and the cloud provider. The two modes of process are also described, normal mode and the resolve mode. In case of any repudiation, the repudiation mode is initialized, where the arbitrator comes into play. This protocol alleviates the repudiation problem. But while considering, the security can be little bit improved. Generally the steps needed for the doing this process takes place in four steps.

- With evidence NRO, Transmitter/sender forwards the encoded data to the receiver/recipient.
- With NRR, the receiver responds back.
- When the sender gets the NRR, he sender will send the NRO along with the key to the recipient.
- Recipient replies with NRR.

If there is any problem like repudiation, then the resolve mode will be initiated. The Table 1 gives the notations and the abbreviation used in this paper.

Table 1: Notations

CS	Chaining Signature
MPNR	Multi Party Nonrepudiation Protocol
TTP	Trusted Third Party
NRO	Non Repudiation of the Origin
NRR	Non-Repudiation of the Recipient
Seq	Sequence Number
L	Label
O	Owner
C	Cloud Provider
TTP	Trusted Third Party
Ts	Timestamp

A.1 Normal Mode

It is when the owner, the originator of transaction sends his/her data to the cloud provider. So the owner encrypts the data with the key and generates two evidences. They are NROoc [Non Repudiation of Origin -for cloud provider] and NROou [Non Repudiation of Origin - for the data user].

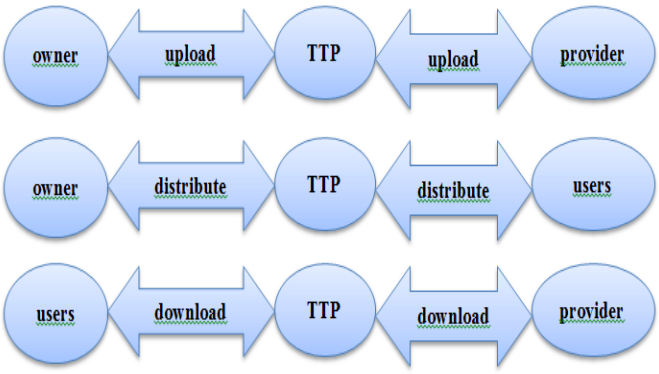

Fig 1: MPNR framework for cloud

Access control is applied for different users and according to the list; the data is deciphered by different users. Figure 1 shows the general framework of the MPNR protocol.

Step 1: sends NRO along with data

NRO = Sign{H(upload), Seq1, L, Ts}

Step2: provider responds with NRR

NRR = Sign{H(store), Seq2, Ts, NRO}

Fig 2: Evidences between Owner and Providers

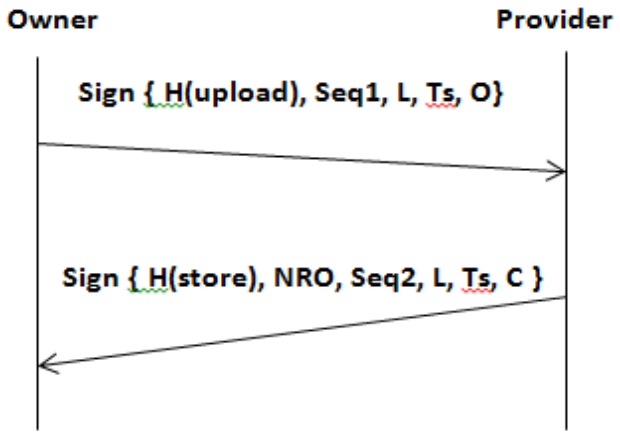

Fig 3: Normal Mode (Owner - Provider)

The step taken place between the owner and the provider is shown in the figure 3. The owner sends the evidence to the provider while uploading the data to them. In return, the provider responds with the evidence of the recipient to the owner. By doing so, the disputation among the owner and the provider will be avoided.

Step 3: the owner sends NRO to user

NRO = Sign{H(upload), Seq3, L, Ts, O, C, TTP, EGu{NROou}, }

Step 4: the user responds with NRR to owner

NRR = Sign {H(upload), NRR, Seq4, L, Ts, C}

Fig 4: Evidences between Owner and Providers

When the user gets the NRO along with the encrypted data, they decipher it with the key for which they are eligible to use. This is maintained through the Access Control mechanism, (i.e.) for which user which data should be accessed with. Figure 3 show the transaction taken place between the owner and the user.

Step 5: the users send NRO to the provider

NRO = Sign {L, O, U, C, Seq5, Ts}

Step 6: the provider responds with NRR to the user

NRR = Sign {H(upload), L,O<C, Seq6, Ts, EGu {NROou}}

Fig 5: Evidences between Owner and Providers

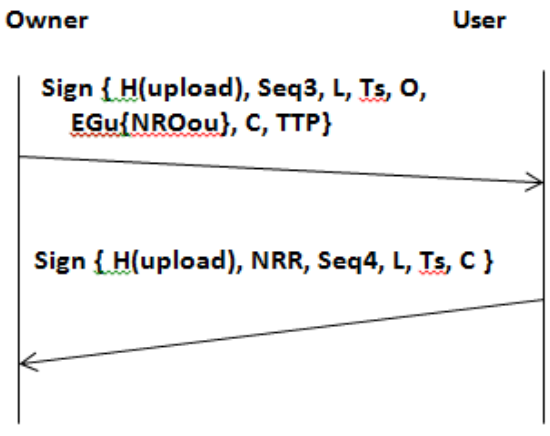

Fig 6: Normal mode (Owner - User)

A.2 Resolve Mode

This is initialized when any one of the peer refuses to respond back. By providing the evidence, the originator of the process request TTP to start the resolve mode to get the process to finish. The TTP will set a time limit for the recipient to respond back. If the recipient does not respond back within the time limit, then the process will abort.

A.3 Disputation mode:

In case if any disputation occurs among the peers, then the arbitrator is used to solve the issue. The arbitrator is provided with the enough evidence of the transaction made. The poor entity which is innocent has to be freed. The arbitrator takes care of it with the evidence provided.

B. Proposed CS-MPNR

In this session we describe our proposed model, a novel CS-MPNR protocol, which uses the method called *Chaining Signature* in Cloud Storage - which acts as a link, through which the Repudiation problem can be avoided. In the previous section, the basic MPNR protocol for enhancing the storage security is described [15 -17], where the protocol takes place in three phases. The proposed model extends the MPNR protocol [17] by using Chaining Signature [18] between users to avoid the repudiation issue further and also it enhances the Integrity of the Data. In our model, mainly three roles are assigned like Data owner, Cloud Provider and the Data Users. First the Data Owner uploads his data to the Cloud Storage, which is maintained by Cloud Provider. The Trusted Third Party is included for the purpose of checking the security and the integrity of the data uploaded, through which the Fairness is preserved.

We assume that the communication channel is secure enough between the Trusted Third Party and the transmitting entity as robust and the communication between the Data owner and the Data user is trustworthy.

In the remainder of the session, we label the details of our proposed model. Till now the basic MPNR protocol is explained. But the security can be still more added where there are many possible ways for the intruder the grab the data. Hence to enhance the non-repudiation, Chaining Signature [18] is used.

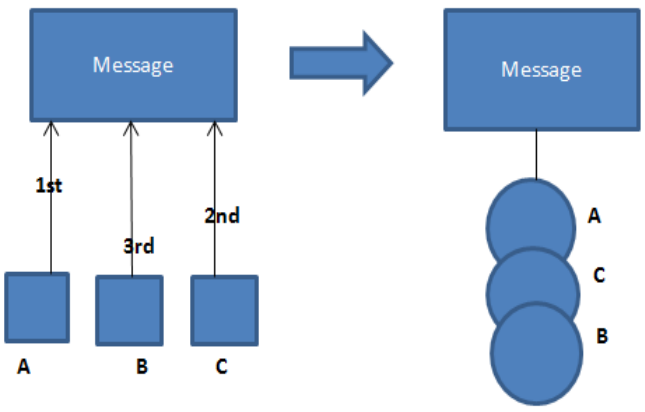

Fig 7: Model of Signing Signature

From the figure 7, the model of the Chaining Signature is clear that the message contains the signature of the users who registered in first. The path of the users is noted. In case if any disputation among users occurs, then the TTP or the Cloud provider can check the evidence of the logged in time and the user's id. Their identification is stored in the Cloud provider's database.

The Figure 8 shows the signing formation, where the sign of the users follows up next by next. From the figure, the *Mn* indicates the Message, *TN* indicates the Timestamp required, *Ln* is the Label used and the *S (Un)* indicates the signature of the n-users.

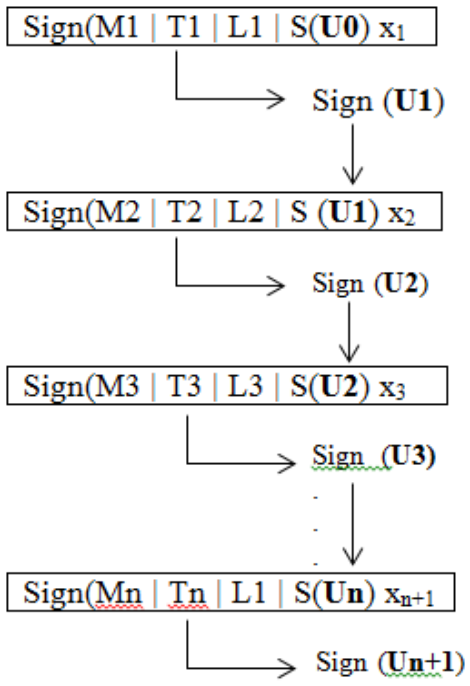

Fig 8: Signing Formation

The Chaining Signature is the method of generating a chain of signature on the message by different users. Each signature acts as a LINK of chain. Considering that chained signatures enable us to correctly validate the path of any received message and provide non-repudiation. This encrypted with the key of the user. The key generation algorithm generates two key pairs (x1, y1). Then the chain sign algorithm intakes the value of the key pair along with data. The procedure is formulated in the equation (Eq.1) as

$$Sign\ (\ M_n \mid H(S'_{n-1}) \mid L_x\ )q_w \qquad (1)$$

The value M_n indicates the message that is updated. If the data is not updated, then the value of M_n remains same. The $H(S'_{n-1})$ is the hash value of the signature generated. The L_x is the label, which is useful for the identification purpose. The label indicates the purpose of the step, which may contain the version number or upload request from the peer. The process is continued for which the users of the group are logged in. The timestamp is used for avoiding timeliness attack and to identify at which time the user sends and receives a request.

IV. Performance Evaluation

Here, the features needed for the proposed model is listed. This CS-MPNR scheme extends the original MPNR [17] for the support of Non-Repudiation. Therefore we call it CS-MPNR for using the Chaining signature to enhance the security of the data. This protocol is implemented in one of the version of Microsoft's Windows 7 which uses 64 bit operating system. The experiment is built using the Java language on a system with Intel Core i3 processor running at 2.40 GHz with 4.00 GB RAMS. Since the Integrity checking alone is not an issue, the algorithms used for digest generation is MD5. This is used where the computational cost is reduced. The security package from the Java is used for the implementation. The result generated is the result of 15 trails with different sized data by considering the probability detection of the computational time.

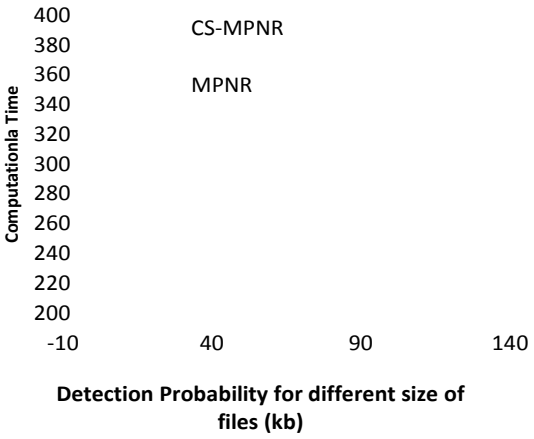

Fig 9: Detection Probability of different sized data against the Computational Time

By considering the performance evaluation of the method, Figure 9 gives the detail about the detection probability for different sized data against the Computational time it took for processing. The evaluation is made between MPNR protocol and proposed protocol CS-MPNR (Chaining Signature – Multi Party Nonrepudiation Protocol). From the Figure 2, it is clear that the efficiency is high and the computational cost is greatly reduced. For the given data file of size 40, CS-MPNR took 220-250 computational time, while for basic MPNR, it took around 280 computational time.

From the Figure 10, the evaluation made is clearly visible that the security is highly provable. The figure is evaluated by

considering the mechanisms like fairness, write-serializability, confidentiality, data integrity and repudiation.

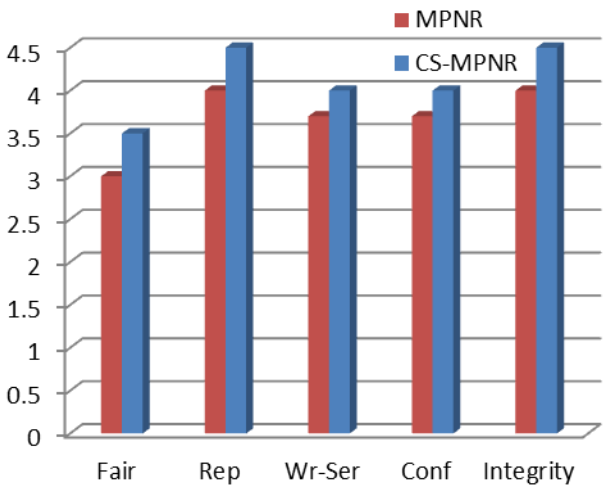

Fig 10: Probability of different security mechanisms for both the MPNR protocol and CS-MPNR protocol

The data integrity is intact without any modification when compared with the existing method. The nonrepudiation is maintained by the strong CS-MPNR protocol. The evidences are securely transferred among the peers for the purpose of avoiding disputation. Fairness is achieved through the use of TTP (Trusted Third party). Write-serializabaility avoided through the chain of attestation. The data is maintained to be up-to-date by which the Freshness is achieved and it is safe from the attacks like man-in-the-middle attack, roll-back attack and timeliness attack.

V. Conclusion

Even though Cloud has many useful features through which it greatly reduces the users' work of maintaining their data, it also has some security dreads. The low security in Cloud storage leads to some loopholes for the attackers to modify the data. Data which should be protected should be secure enough against the attacks and the dreads like integrity issue and repudiation problem. To overcome these challenges, a novel CS-MPNR [Multi Party Non Repudiation] protocol is proposed, which uses Chaining Signature [CS] acting as a link of sign to have a follow up of the chained users and lessens the Repudiation. It upholds Data Integrity in a better manner. The evaluation results show that there is reduced computational cost. The security mechanisms of the protocol are robust enough. Therefore it is clear that the evaluated result is within reasonable limits and resilient. .

Acknowledgment

The authors wish to thank Karunya University for providing infrastructure for carrying out the simulation and financial support. The authors thank the senior professors and the technical experts for providing valuable suggestions to improve the quality of the research paper.

References

[1] Rajkumar Buyya, James Broberg and Abdrzej Goscinski, "Cloud Computing Principles and Paradigm", John Wiley and Sons, Inc. publication, 2011

[2] R.Sravan Kumar and A. Saxena, "Data integrity proofs in cloud storage," in Third International Conference on Communication Systems and Networks (COMSNETS), 2011, pp.1-4.

[3] A. Juels and J. Burton S. Kaliski, "Pors: Proofs of retrievability for large files," in *Proc. of CCS'07*, Alexandria, VA, October 2007, pp.584–59

[4] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in *Proc. of CCS'07*, Alexandria, VA, October 2007, pp. 598–609

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

[6] Y. Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative provable data possession for integrity verification in multi-cloud storage," IEEE Transactions on Parallel and Distributed Systems, no. 99, 2012

[7] J. Feng, Y. Chen, W.-S. Ku and P. Liu, "Analysis of Integrity Vulnerabilities and a Non-repudiation Protocol for Cloud Data Storage Platforms," 2nd International Workshop on Security in Cloud Computing (SCC 2010), San Diego, California, USA, Sep. 14, 2010

[8] C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Service Computing (TSC), 2012

[9] K.D. Bowers, A. Juels, and A. Oprea, "HAIL: A High-Availability and Integrity Layer for Cloud Storage," Proc. ACM Conf. Computer and Comm. Security (CCS '09), pp. 187-198, 2009

[10] H.-Y. Lin and W.-G. Tzeng, "A secure erasure code-based cloud storage system with secure data forwarding," IEEE Trans. on Parallel and Distributed Systems, vol. 23, no. 6, pp. 995–1003, 2012

[11] A. Yun, C. Shi, and Y. Kim, "On Protecting Integrity and Confidentiality of Cryptographic File System for Outsourced Storage" , in ACM Cloud Computing Security Workshop (CCSW), Nov 2009

[12] Brian Hay, Kara Nance and Matt Bishop, "Storm Clouds Rising: Security Challenges for IaaS Cloud Computing", In., Proc., of Hawaii International Conference, IEEE – 2011

[13] Bowers, K.D., Juels, A., Oprea, A. Hail: A high-availability and integrity layer for cloud storage.Cryptology ePrint Archive, Report 2008/489 (2008)

[14] 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 '09), pp. 355-370, 2009

[15] Jun Feng , Yu Chen , Douglas H. Summerville , and Kai Hwang" Fair Non-repudiation Framework for

Cloud Storage: Part II" in *Cloud Computing for Enterprise Architectures*, Springer – 2011, pp. 283-300.

[16] R. Popa, J. Lorch, D. Molnar, H. Wang, and L. Zhuang. Enabling Security in Cloud Storage SLAs with CloudProof. Microsoft Tech Report MSR-TR-2010-46, May, 2010.

[17] J. Feng, Y. Chen, D. Summerville, W.S. Ku, and Z.Su "Enhancing Cloud Storage Security against Roll-back Attacks with A New Fair Multi-Party Non-Repudiation Protocol", in The 8th IEEE Consumer Communications & Networking Conference, 2010.

[18] Saxena, Amitabh, and Ben Soh. *One-way signature chaining: A new paradigm for group cryptosystems and e-commerce*. Cryptology ePrint Archive, Report 2005/335, 2005.

[19] The Non Repudiation Concept http://searchsecurity.techtarget.com/definition/nonrepudiation.

[20] J.Feng , Yu Chen , Douglas H. Summerville, and Kai Hwang, "Fair Non-repudiation Framework for Cloud Storage: Part I" in *Cloud Computing for Enterprise*