IEEE International Conference on PKI and Its Applications (PKIA-2017)

November 14-15, 2017

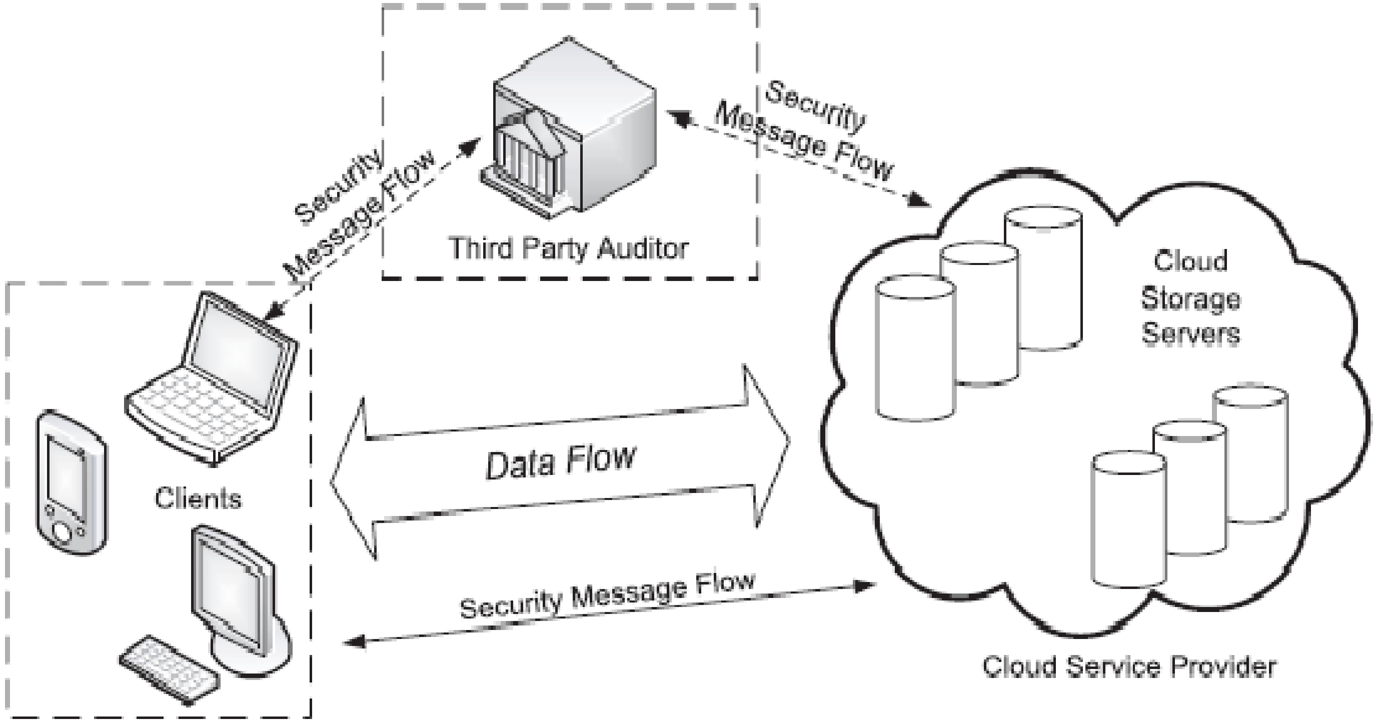
Hotel Chancery Pavilion, Bangalore

A Study on Remote Data Integrity Checking Techniques in Cloud

C. Sasikala
JNTUA, Anantapuramu, A.P.
Prof. C. Shoba Bindu, Dept.of CSE
JNTUACE, Anantapuramu,A.P.

Cloud Storage

- Storing data in the remotely located cloud servers
- Cloud Storage Architecture



The security issues in Cloud

These security issues arise due to the following reasons:

- Loss of Control
- Lack of Trust
- Multi tenancy

The security issues related to cloud data are:

- Confidentiality
- Integrity
- Availability

Data Integrity Checking Techniques

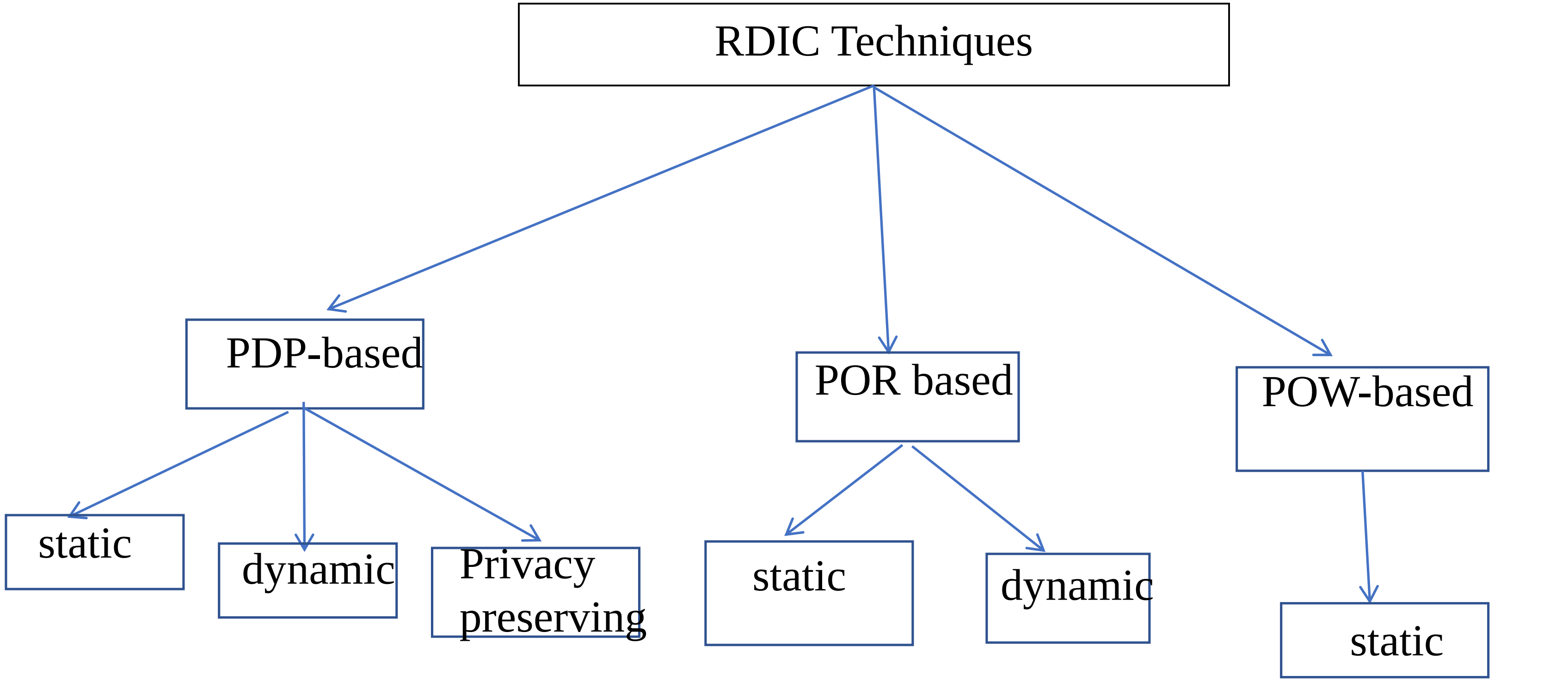
Traditional Data Integrity Checking Techniques:

- Hash Functions
- Signatures

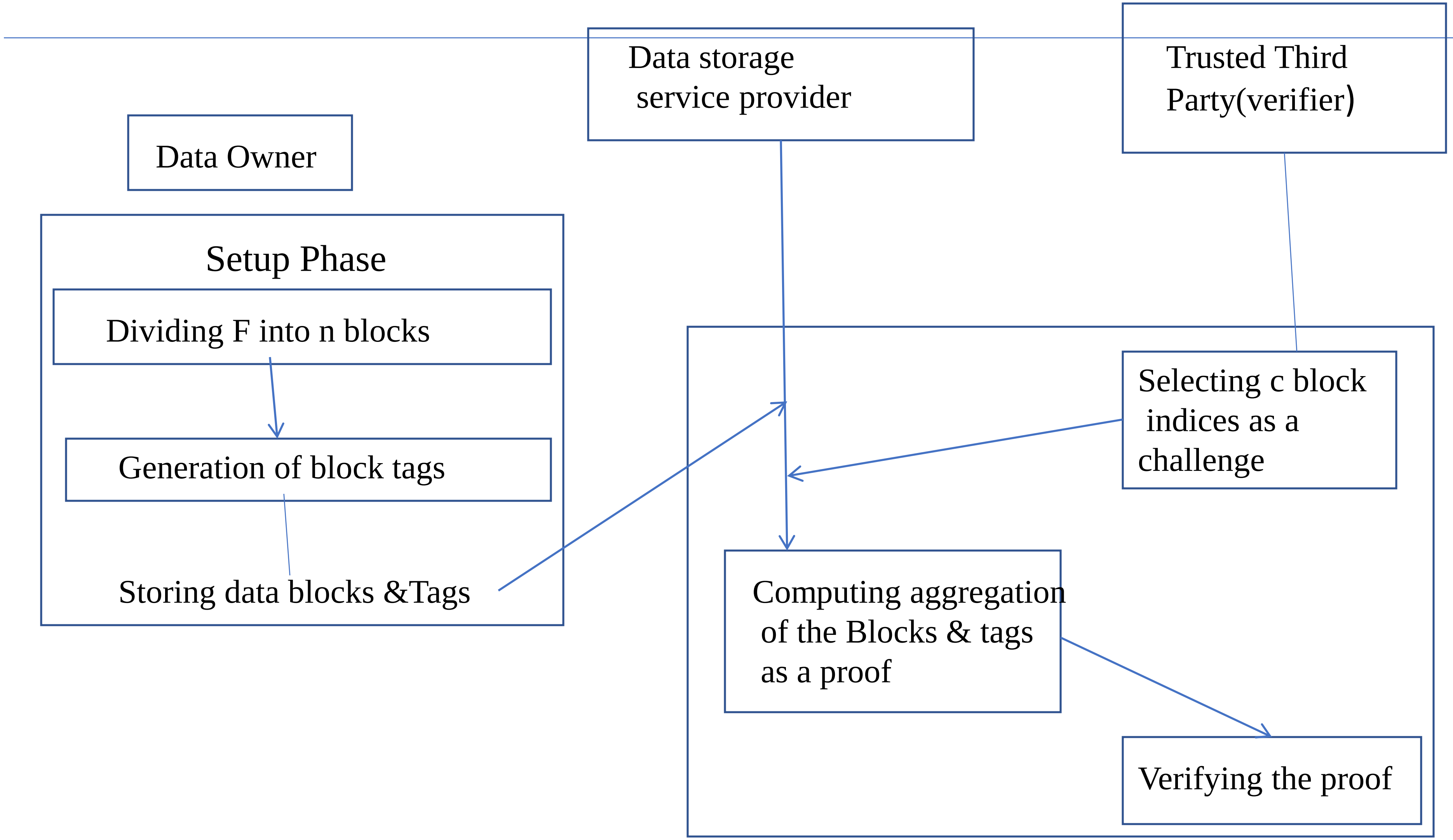
Remote Data Integrity Checking(RDIC)

Refers to a group of protocols to securely, frequently& efficiently verify the correctness of the data over a cloud managed by untrustworthy provider without having to retrieve the data

Taxonomy of RDIC Techniques

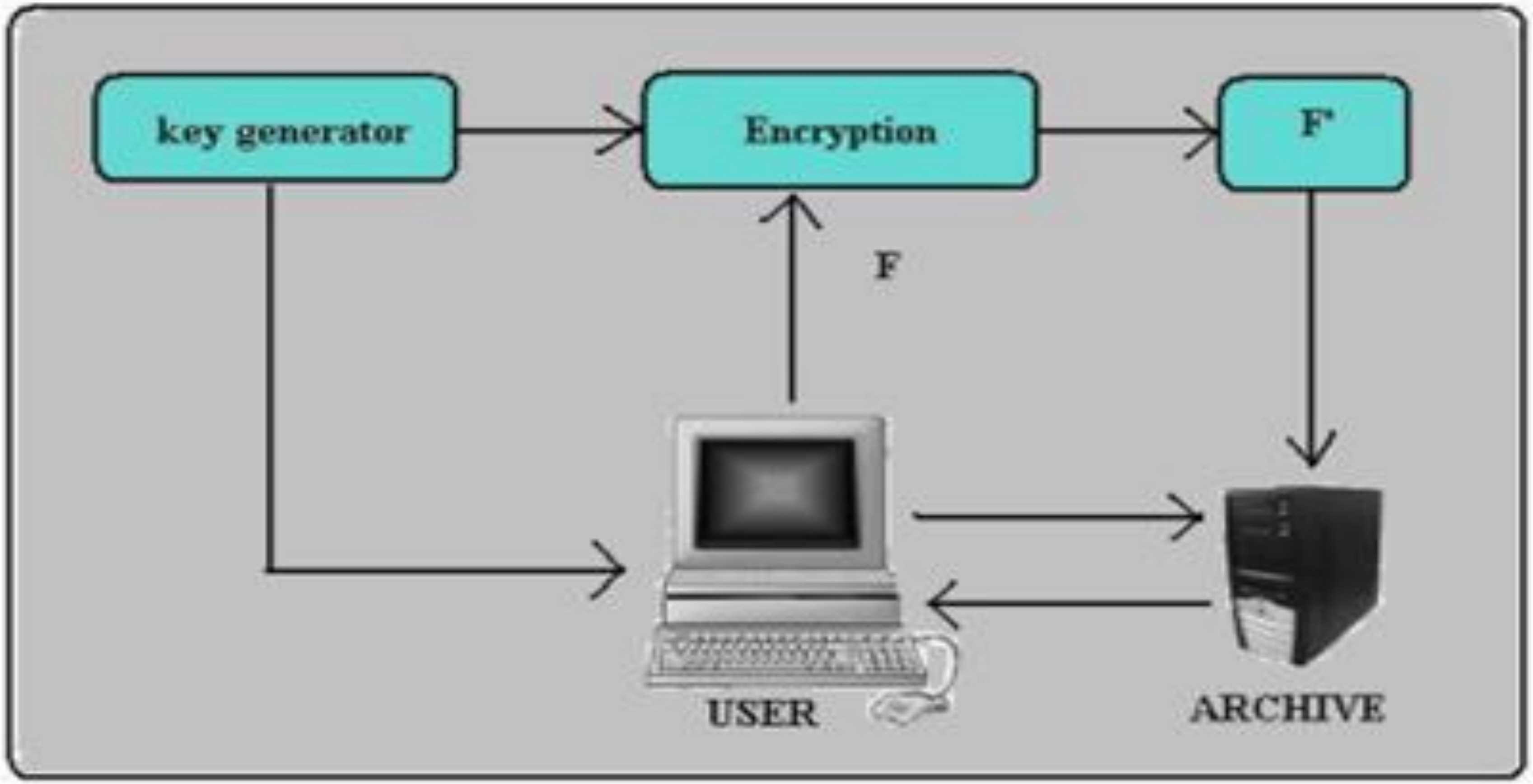


Structure of PDP method


Data storage service provider
Trusted Third Party(verifier)
Data Owner
Setup Phase
Dividing F into n blocks
Generation of block tags
Storing data blocks &Tags
Selecting c block indices as a challenge
Computing aggregation of the Blocks & tags as a proof
Verifying the proof

Proof of Retrievability Model

A. Juels and B. Kaliski.(2007) “Proofs of retrivability for large files” CCS’07 Proceedings of the 14th ACM conference on comupetr and Communication Security” ACM,2007



Proof of Ownership (POW)based models

Halevi et.al.(2011) " A Proof of Ownership in remote Storage System"

- It is constructed on the basis of Merkle Hash Tree(MHT) and Collision-Resistant Hash(CRH) functions.

- It is vulnerable against security attacks because any one who gets hash value is permitted to access the file

Public Auditing Protocols

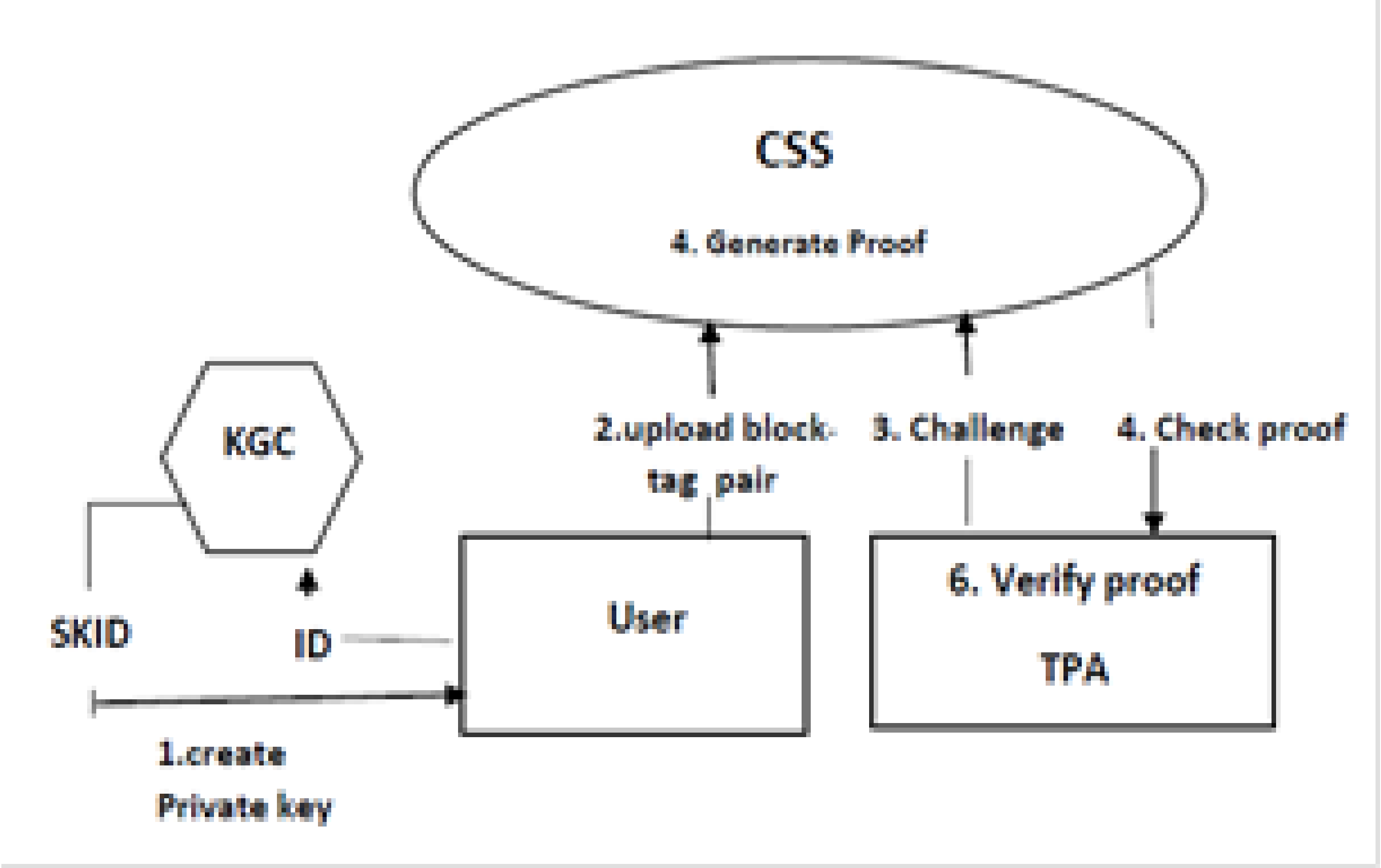
- 1.K.Zeng “ **Public verifiable remote data integrity”** International conference on information and communication security” ICICS2008,pp-419-438.
- **2**.Q.wang,C.Wang et.al. “**Enabiling public auditability and data dynamics for storage security in cloud computing**” in 14th European Sympoism on Research in Computer Security,pp.355-370,Springer,2009.
- 3.Q.wang et.al. **“Privacy-Preserving public auditing for data storage security in cloud computing”** in InfoCom2010 IEEE,/march 2010.
- 4.C.Wang,K.Ren et.al. “**Toward public auditable secure cloud data storage services**” IEEE Network: The Magazine of Global Internetworking, Volume 24 Issue 4, July-August 2010, Pages 19-24.
- 5.Y.Zhu et.al.“ **Cooperative provable data possession for integrity verification in multi cloud storage**” IEEE Transaction on parallel and distributed systems, pp 1-14,2012.
- 6. C.wang et.al. **“Privacy-Preserving public auditing for secure cloud storage”,** IEEE transaction on Computers,vol.62,n0.2,pp.362-375,2013.

- These protocols mainly focused on performance optimization, privacy protection and support for dynamic operations

Limitations of PKI based RDIC Ptotocols

- It supports one key for one file.
- If the data user loose the keys ,he might no longer execute any integrity
- So, for the source constrained cloud user, the key management of PKI based data integrity checking scheme become a difficult problem .
- It also brings burden on auditor in terms of computation and communication cost.

ID-Based RDIC Protocol Model



ID-Based RDIC protocol Definition

1.**Setup**(1^{k})→(params ,mpk, msk) It is run by PKG,it takes k as input security parameter and outputs system public params, the master public key and master secrete key of PKG.

2.**KeyExtrack**$(1^{k}$,params,mpk,msk,id)→(sk $_{ID}$) It outputs private key sk $_{ID}$ corresponding to the User with identity ID.

3.**TagGen(M, sk** $_{ID}$)→ $^{\delta}$ It takes outsourced data file M and Private key as inputs ,for each data block m $_{i}$, it computes a data authentication tag $^{\delta}$i. Finally it outputs a set of data authentication tag $^{\delta}$= ($^{\delta}$1, $^{\delta}$2,..., $^{\delta}$n).

ID-Based RDIC protocol Definition Contd..

4.Challenging(M_{info})→C It takes the the abstract information of the data (e.g.,data file name, total no.of data blocks, the challenged index set.) as input and outputs a challenging information C.

5.ProofGen(M, δ ,C)→P .This algorithm takes the data file M, the authentication tags δ,and the challenge information C from the auditor as inputs, and outputs a proof information.

6.Proofcheck(params, ID,C,P, M_n)→1/0. to indicate whether the file is intact or not

PKIA-2017

ID-Based RDIC Protocols

- Yong Yu et.al. “Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage “IEEE Transactions onInformation Forensics and Security, Volume 12, Issue 4,2017. pages 767-778.
- Zhang and Dong , ”Efficient ID based public auditingfor the outsourced data in cloud storage” International Journal of information sciences volumes 343-344 20-May-2016.pages1-14.
- Jianhong Zhang, Pengyan Li1 ,Jian Mao” IPad: ID-based public auditing for the outsourced data in the standard model” International journal of Cluster Computing March 2016, Volume 19, Issue 1, pages 127–138.

Limitations

- Key escrows problem:

Comparison of Existing RDIC Protocols:

- IEEEconference\comparetable.docx

Research Challenges and Possible Solutions to Design RDIC protocol in Cloud

- Certificateless Cryptography: In this model, the private keys are generated by combining the partial private key generated by Key Generation Center(KGC) and users secrete information, so that we can solve the key escrow problem in IBS and compared to the ID based RDIC protocols it may provide better security.
- Dynamic Data update: We may solve this problem using Merkle HashTrees (MHT).

Contd...

- Batch Auditing:In multi-cloud storage, the auditor can handle multiple auditing tasks simultaneously from various users. Therefore, it can reduce the computation cost of auditing on both auditor and cloud server.
- Data Computational Integrity: To address this issue, migrate the computational functions along with data into the cloud and to check the integrity of both computation and data using a challenge-response protocol.

References

1.G. Ateniese , RD. Pietro , LV. Mancini, T. Sudik .”Scalable and efficient Provable data possession”. In: Proceedings of the 4th international Conference on security and privacy in communication Networks. Istanbul, Turkey: ACM; 2008.p.1-10.

2. A. Juels and B.S. Kaliski “Proofs of Retrievability for Large Files,” Proc.14th ACMConf. Computer andComm. Security (CCS'07) 2007. p.584-597.

3. S. Halevi , D. Harnik , B.Pinkas , P. Shulman , “A .Proof of ownership in remore storage systems”.In proceedings of the 18th ACM conference on computer and communications security”. Chicago, Illinois, USA: ACM ; 2011.p.491-500

4. M Sookhak , H Talebian , E ,AbdullahGani ,M KhurramKhan “A review on remote data auditing in single cloud server:Taxonomy and open issues” international Journal of Network and Computer Applications 43(2014)121–141.

5. S. Halevi , D. Harnik , B.Pinkas , P. Shulman , “A .Proof of ownership in remore storage systems”.In proceedings of the 18th ACM conference on computer and communications security”. Chicago, Illinois, USA: ACM ; 2011.p.491-500

6. C. Wang, Q. Wang, K. Ren , Lou WJ. ”Privacy –preserving public auditing for data storage security in Cloud Computing”. In: Proceedings IEEE INFOCOM., San Diego, CA: 2010.P.1-9

References

- 7. H.Wang,Q.Wu,B.Qin,J.Domingo-Ferrer, "Identity-based remote data possession checking in public clouds".IETInf.Secur.8(2)(2014)114-121.
- 8. J. N. Zhao, C. X. Xu, F. G. Li, and W. Z. Zhang, "Identity-Based Public Verification with Privacy-Preserving for Data Storage Security in Cloud Computing", IEICE Transactions, 96-A(12), 2709-2716, 2013.
- 9. H. Wang "Identity-based distributed provable data possession in multi cloudstorage" IEEE Trans. on Service Computing, 8(2), 328–340,2015.
- 10. Zhang J, Dong Q. "Efficient id-based public auditing for the outsourced data in cloud storage". Information Sciences 2016;343:1–14.
- 11. Mihiri B, Chanathip N,Gregory N. "Security Proofs for Identity-Based Identification and Signature Schemes". Published in Advances in Cryptology – EUROCRYPT 2004, volume3027 of Lecture Notes in ComputerScience,Springer,2004.

CCA

IEEE

PKIA-2017

सी-डैक

CDAC

Thank You

www.pkiindia.in www.facebook.com/pkiindia PKIIndia @pkiindia