SIGNING AND DESIGNING WITH DATA RECOVERY FOR SECURED CLOUD STORAGE

S. Arshiya Kausar, S. Karthik

***Abstract*—Using cloud data services, it is commonplace for data to be not only stored in the cloud, but also shared several users across the world. By any chance to the integrity of cloud data is subject to skepticism due to any failure (like hardware/software) and day to day errors. There are several mechanisms have been designed to permit the data owners and users to capable examine cloud data uprightness without recover the entire data form the cloud server. We use the technique Signing and Designing for Data Recovery (SDDR) However, public auditing on the examine of shared data with these existing mechanisms will naturally reveal securable information identity privacy to public onlookers. In this paper, we use elliptic curve cryptographic algorithm, we exploit ring signatures to compute verification metadata needed to audit the correctness of shared data. With using our mechanism, the identity of the signer on each block in shared data is kept private from public onlookers, who are free to efficiently verify shared data integrity without retrieving the entire file. In addition our mechanism is free to perform multiple auditing tasks simultaneously instead of verifying them one by one. Our mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one.**

***Index Terms*—Elliptic curve cryptographic algorithm; ECC; Cloud data; Pauditing, SDDR.**

I. INTRODUCTION

Cloud service providers offer users efficient and scalable data storage services with a much lower marginal cost than traditional approaches [1]. It is routine for users to leverage cloud storage services to share data with some in a group, as data sharing becomes a constant feature in most cloud storage provide, its contains Dropbox, iCloud and Google drive.

The integrity of data in cloud storage, whatever, is subject to doubt and scrutiny, as data load in the cloud can clearly be lost or corrupted due to the inevitable hardware/ software failures and human errors [2], [3]. To make this matter even worse, cloud service initiates may be reluctant to inform users about these data errors in order to maintain the reputation of their services and avoid losing profits [4]. Therefore, the integrity of cloud data should be verified before any data utilization, such as search or computation over cloud data [5].

***S Arshiya Kausar**, Krishnasamy College of Engineering and Technology, Cuddalore, Tamil Nadu, India.*
***S. Karthik**, Krishnasamy College of Engineering and Technology, Cuddalore, Tamil Nadu, India.*

In this model they are using three parties: the server, the public user and third party verification which checks the integrity of the data. The original user to initiate the shared data in cloud, and also to shares it with group users. The group contains original user and group users itself. All the group members is allowed to access and alter the shared data. Both shared and verification data stored in cloud server.

II. PUBLIC AUDITING MECHANISM

A. Overview

Using HARS and its properties we established in the previous section, we now construct Oruta, a privacy-preserving public auditing mechanism for shared data in the cloud. With Oruta, the public checker can check the integrity of shared data without retrieving the hole data. Meanwhile, the identity of the signer on each section in shared data is kept private from the public verifier during the auditing.

B. Reduce Signature Storage

Another important issue we should consider in the construction of Oruta is the size of storage used for ring signatures. To reduce the storage of ring signatures on shared data and still allow the public verifier to audit shared data efficiently, we exploit an aggregated approach from [6] to expand the size of each block in shared data into k _ jpj bits.

C. Support Dynamic Operations

To enable each user in the group to easily alter data in the cloud, Oruta should also support active operations on shared data. A active operation contains an insert, delete or *update* operation on a every single block [7]. However, since the computation of a ring signature contains an identifier of a block (as presented in HARS), established methods, which only use the index of a block as its identifier (i.e., the index of block $\mathbf{m}_j$ is j), are not suitable for supporting dynamic operations on shared data efficiently.

The reason is that, when a user modifies a single block in shared data by performing an insert or delete operation, the indices of blocks that after the modified block are all changed, and the changes of these indices require users, who are sharing the data, to re-compute the signatures of these blocks, even though the content of these blocks are not modified.

III. EXISTING PROBLEM STATEMENT

When the public verifier accept to check the integrity of shared data, it first send to auditing opponance to the cloud server. After receiving the auditing feedback, the cloud server to responds to the public verifier with feedback of auditing proof of the permission of

ISSN: 2278 – 1323

shared data. Then, the public verfier to check the correctness of the proof [8-15].

A. Computation Cost

During an auditing task, the public verifier first generates some random values to construct an examine challenge, which only introduces a small amout in computation. Then, challenge-and-response protocol between a public verifier and the cloud server.

B. Communication Cost

The communication amount of Oruta with SDDR is mostly introduced by two aspects: the auditing challenge and auditing proof.

IV. STUMBLING BLOCK

In this mechanism contains of some kinds of disadvantage related to the integrity of shared data. The cost of the Third Party Auditor(TPA) is very high. The TPA can itself hack the integrity of data. The performance will be reduced by the third party verification [16] [17].

V. PROPOSED SYSTEM

I the suggested system the data is encrypted by (ECC) algorithm with SDDR and gets spitted into n number of parts depending upon the threshold frequency. The back up of all the files stored in the single server with out any redundancy. The data will be integrated when it is requested by the user then gets decrypted.

In this proposed system ECC to provide the security in the cloud server. All the shared data is secured by the user and it does not depend upon any other one even the cloud itself. Unfortunately data will completely crashed, it can be recovered even if there is any loss in cloud data.

VI. METHODS

A. Data Encryption with ECC

ECC could be used the way that the data is encrypted with the public key instead of the random generated key. ECC can be case ECIES used the a symmetric encryption algorithm to actually encrypt the data, so even if you use ECC to encrypt all the data, you're still encrypting it with a random symmetric key. But if you're encrypting the data itself with SDDR you could use a simple XOR as the symmetric encryption algorithm, which is effectively a one-time-pad. This has a theoretical advantage in that, unlike other symmetric encryption algorithms, one-time-pads are information-theoretically secure.

B. Spitting Up of Data

The encrypted data is a single file. It split up into n number of parts with the encrypted format. The n value to denotes the number of cloud servers where each part of file will be stored. Each spliting data requires accurate information for integrating the files back. These information about splitting of data will be stored locally to the client system for security reasons.

C. Data Back Up

Backups have two distinct purposes. The primary purpose is to recover data after its loss, be it by data deletion

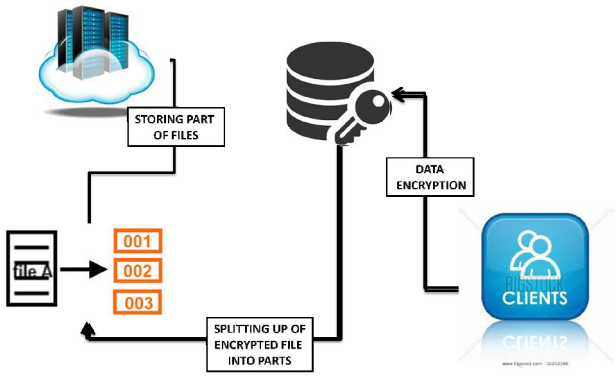

Fig. 1 SDDR data flow diagram.

or corruption. Data loss can be a common experience of computer users. A 2008 survey found that 66 % of respondents had lost files on their home PC. The secondary purpose of backups is to recover data from an earlier time, according to a user-defined data retention policy, typically configured within a backup application for how long copies of data are required [20]. Though backups popularly represent a simple form of disaster recovery, and should be part of a disaster recovery plan, by themselves, backups should not alone be considered disaster recovery. One reason for this is that not all backup systems or backup applications are able to reconstitute a computer system or other complex configurations such as a computer cluster, active directory servers, or a database server, by restoring only data from a backup [21] [22] [23].

Since a backup system contains at least one copy of all data worth saving, the data storage requirements can be significant. Organizing this storage space and managing the backup process can be a complicated undertaking. A data repository model can be used to provide structure to the storage. Nowadays, there are many different types of data storage devices that are useful for making backups. There are also many different ways in which these devices can be arranged to provide geographic redundancy, data security, and portability [24-31].

Before data are sent to their storage locations, they are selected, extracted, and manipulated. Many different techniques have been developed to optimize the backup procedure. These include optimizations for dealing with open files and live data sources as well as compression, encryption, and de-duplication, among others. Every backup scheme should include dry runs that validate the reliability of the data being backed up. It is important to recognize the limitations and human factors involved in any backup scheme [32] [33].

VII. CONCLUSION AND FUTURE WORK

Wang et al. leveraged homomorphic tokens to ensure the correctness of erasure codes-based data distributed on multiple servers. This mechanism is able not only to support dynamic data, but also to identify misbehaved servers. To minimize communication overhead in the phase of data repair, Chen et al. also introduced a mechanism for auditing the correctness of data under the multi-server sce-nario, where these data are encoded by network coding instead of using erasure codes. More recently, Cao et al. constructed an LT codes-based secure and reliable cloud storage mechanism. Compare to previous work [34] [35], this mechanism can avoid high decoding computation cost for data users and save computation resource for online data owners during data repair [36] .

The files which splits according to the number of servers will be copied in to k numbers. This back up data doesn't affect the security because only two different part of file which cannot be integrated with one another is stored in one particular server. If any server is crash or under attack then the data recovery will be done through this back up data.

REFERENCES

[1] A.I. Anton, J.B. Earp, Q. He, W. Stufflebeam, D. Bolchini, and C. Jensen, "Financial Privacy Policies and the Need for Standardization," IEEE Security and Privacy, vol. 2, no. 2, pp. 36-45, Mar./Apr. 2004.

[2] D. Balfanz, G. Durfee, D.K. Smetters, and R.E. Grinter, "In Search of Usable Security: Five Lessons from the Field," IEEE Security and Privacy, vol. 2, no. 5, pp. 19-24, Sept./Oct. 2004.

[3] R. Biddle, P.C. van Oorschot, A.S. Patrick, J. Sobey, and T. Whalen, "Browser Interfaces and Extended Validation SSL Certificates: An Empirical Study," Proc. ACM Workshop Cloud Computing Security, pp. 19-30, 2009.

[4] E. Chin, A.P. Felt, V. Sekar, and D. Wagner, "Measuring User Confidence in Smartphone Security and Privacy," Proc. Eighth Symp. Usable Privacy and Security (SOUPS '12), pp. 1-16, 2012.

[5] L.F. Cranor, M. Arjula, and P. Guduru, "Use of a P3P User Agent by Early Adopters," Proc. ACM Workshop Privacy in the Electronic Soc., pp. 1-10, 2002.

[6] L.F. Cranor, P. Guduru, and M. Arjula, "User Interfaces for Privacy Agents," ACM Trans. Computer-Human Interaction (TOCHI '06), vol. 13, no. 2, pp. 135-178, 2006.

[7] N. Dell, V. Vaidyanathan, I. Medhi, E. Cutrell, and W. Thies, "Yours is Better!: Participant Response Bias in HCI," Proc. Conf. Human Factors in Computing Systems, pp. 1321-1330, 2012.

[8] S. Egelman, L.F. Cranor, and A. Chowdhury, "An Analysis of P3P -Enabled Web Sites among Top-20 Search Results," Proc. Eighth Int'l Conf. Electronic Commerce, pp. 197-207, 2006.

[9] S. Egelman, J. Tsai, L.F. Cranor, and A. Acquisti, "Timing Is Everything?: The Effects of Timing and Placement of Online Privacy Indicators," Proc. 27th Int'l Conf. Human Factors in Computing Systems, pp. 319-328, 2009.

[10] B. Fathi, Engineering Windows 7 : User Account Control, MSDN blog on User Account Control, http://blogs.msdn.com/b/e7/archive/2008/10/08/user-account-control.aspx, Oct. 2008.

[11] A.P. Felt, K. Greenwood, and D. Wagner, "The Effectiveness of Application Permissions," Proc. Second USENIX Conf. Web Application Development (WebApps '11), 2011.

[12] A.P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android Permissions: User Attention, Comprehension, and Behavior," Proc. Eighth Symp. Usable Privacy and Security, 2012.

[13] M.L. Finucane, A. Alhakami, P. Slovic, and S.M. Johnson, "The Affect Heuristic in Judgments of Risks and Benefits," J. Behavioral Decision Making, vol. 13, no. 1, pp. 1-17, 2000.

[14] M. Gondan, C. G€otze, and M.W. Greenlee, "Redundancy Gains in Simple Responses and Go/no-Go Tasks," Attention, Perception, & Psychophysics, vol. 72, no. 6, pp. 1692-1709, 2010.

[15] K.A. Juang, S. Ranganayakulu, and J.S. Greenstein, "Using System-Generated Mnemonics to Improve the Usability and Security of Password Authentication," Proc. Human Factors and Ergonomics Soc. Ann. Meeting, vol. 56, no. 1, pp. 506-510, 2012.

[16] D. Kahneman, Thinking, Fast and Slow. Farrar, Straus and Giroux, 2011

[17] P.G. Kelley, S. Consolvo, L.F. Cranor, J. Jung, N. Sadeh, and D. Wetherall, "A Conundrum of Permissions: Installing Applications on an Android Smartphone," Proc. Workshop Usable Security (USEC '12), Feb. 2012.

[18] P.G. Kelley, L.F. Cranor, and N. Sadeh, "Privacy as Part of the App Decision-Making Process," Proc. Conf. Human Factors in Computing Systems (CHI '13), pp. 3393-3402, 2013.

[19] T. H.-J. Kim, P. Gupta, J. Han, E. Owusu, J. Hong, A. Perrig, and D. Gao, "OTO: Online Trust Oracle for User-Centric Trust Establishment," Proc. ACM Conf. Computer and Comm. Security, pp. 391-403, 2012.

[20] J. Lin, S. Amini, J.I. Hong, N. Sadeh, J. Lindqvist, and J. Zhang, "Expectation and Purpose: Understanding Users' Mental Models of Mobile App Privacy Through Crowdsourcing," Proc. ACM Conf. Ubiquitous Computing (UbiComp '12), pp. 501-510, 2012.

[21] R.D. Luce, Response Times: Their Role in Inferring Elementary Mental Organization. Oxford Univ. Press, 1986.

[22] S. Mishra, M. Gregson, and M.L. Lalumi_ere, "Framing Effects and Risk-Sensitive Decision Making," British J. Psychology, vol. 103, no. 1, pp. 83-97, Feb. 2012.

[23] S. Motiee, K. Hawkey, and K. Beznosov, "Do Windows Users Follow the Principle of Least Privilege?: Investigating User Account Control Practices," Proc. Sixth Symp. Usable Privacy and Security, 2010.

[24] H. Peng, C.S. Gates, B.P. Sarma, N. Li, Y. Qi, R. Potharaju, C. Nita-Rotaru, and I. Molloy, "Using Probabilistic Generative Models for Ranking Risks of Android Apps," Proc. ACM Conf. Computer and Comm. Security, pp. 241-252, 2012.

[25] E.E. Schultz, "Web Security, Privacy, and Usability," Handbook of Human Factors in Web Design, K.-P.L. Vu and R.W. Proctor, eds., pp. 663-677, CRC Press, 2011.

[26] J. Schwarz and M. Morris, "Augmenting Web Pages and Search Results to Support Credibility Assessment," Proc. SIGCHI Conf. Human Factors in Computing Systems, pp. 1245-1254, 2011.

[27] J. Staddon, D. Huffaker, L. Brown, and A. Sedley, "Are Privacy Concerns a Turn-Off?: Engagement and Privacy in Social Networks," Proc. Eighth Symp. Usable Privacy and Security (SOUPS '12), pp. 1-13, 2012.

[28] S. Sternberg, "Inferring Mental Operations from Reaction-Time Data: How We Compare Objects," An Invitation to Cognitive Science: Methods, Models and Conceptual Results, D. Scarborough and S. Sternberg, eds., pp. 703-863, MIT Press, 1998.

[29] J. Sun, P. Ahluwalia, and K.S. Koong, "The More Secure the Better? A Study of Information Security Readiness," Industrial Management and Data Systems, vol. 111, no. 4, pp. 570-588, 2011.

[30] W. Van Wassenhove, K. Dressel, A. Perazzini, and G. Ru, "A Comparative Study of Stakeholder Risk Perception and Risk Communication in Europe: A Bovine Spongiform

ISSN: 2278 – 1323

Encephalopathy Case Study," J. Risk Research, vol. 15, no. 6, pp. 565-582, 2012.
[31] K.-P.L. Vu, V. Chambers, B. Creekmur, D. Cho, and R.W. Proctor, "Influence of the Privacy Bird User Agent on User Trust of Different Web Sites," Computers in industry, vol. 61, no. 4, pp. 311-317, 2010.
[32] K.-P.L. Vu, R.W. Proctor, A. Bhargav-Spantzel, B. Tai, J. Cook, and E. Eugene Schultz, "Improving Password Security and Memorability to Protect Personal and Organizational Information," Int'l J. Human-Computer Studies, vol. 65, no. 8, pp. 744-757, 2007.
[33] S. Werner and C. Hoover, "Cognitive Approaches to Password Memorability—The Possible Role of Story-Based Passwords," Proc. Human Factors and Ergonomics Society Ann. Meeting, vol. 56, pp. 1243-1247, 2012.
[34] Diederich and J.R. Busemeyer, "Judgment and Decision Making," Experimental Psychology, A.F. Healy and R.W. Proctor, eds., second ed., pp. 295-319, John Wiley & Sons, 2013.
[35] XF. Xie, M. Wang, R. Zhang, J. Li, and QY. Yu, "The Role of Emotions in Risk Communication," Risk Analysis, vol. 31, no. 3, pp. 450-465, 2011.
[36] Tversky and D. Kahneman, "The Framing of Decisions and the Psychology of Choice," Science, vol. 211, no. 4481, pp. 453-458, 1981.

Arshiya Kausar S has received her B.E.(CSE) degree in THE YEAR 2013. At present she is pursuing M.E. (CSE) in Krishnasamy College of Engineering and Technology, Cuddalore, Tamil Nadu, India. Her research interests lies in the areas of BIG DATA, Data Mining, Cryptographic security in Cloud Computing ,wireless security and Distributed Computing.

S. Karthik, Completed his B.E. (CSE) degree in the year 2005, M. Tech (CSE) degree in the year 2007, MBA(HRM) in the year 2008, M. Phil (CSE) degree in the year 2009. Currently he is pursuing Ph.D in the area of BIG DATA. Currently he is working as a HOD/ Associate professor in Computer Science and Engineering at Krishnasamy College of Engineering & Technology, Cuddalore, Tamil Nadu, India. His research interests lies in the areas of BIG DATA, DBMS, Data Mining, Data warehousing, Cryptography & Network Security, and Cloud Computing. He has published 3 International Journals and 3 research papers in National/ International conferences. Also he is life member of Indian Society of Technical Education of India (ISTE). He attended many workshops & National seminars in various technologies and also attended Faculty Development Programme.

ISSN: 2278 – 1323