Review: The Secret Sharing Algorithms for Data Security in the Cloud

Rajshree Bose
DYPSOET
Savitribai Phule Pune University
Maharashtra, India

Subodh Chalak
DYPSOET
Savitribai Phule Pune University
Maharashtra, India

Amit Magdum
DYPSOET
Savitribai Phule Pune University
Maharashtra, India

Rajan More
DYPSOET
Savitribai Phule Pune University
Maharashtra, India

Roshani Raut (Ade)
DYPSOET
Savitribai Phule Pune University
Maharashtra, India

ABSTRACT
In this century all personal data are stored on cloud or on servers such as passwords, account numbers, notes, and other important information, but there is chance of misusing people's saved data by a competitor, a miscreant, a court of law. Confidentiality, Integrity and Availability (CIA) are the big challenges related with data storage management. Sometimes, the cloud service providers store or cache the personal information without user's authorization or permission and control. To prevent this, a self-destructing data system providing user's data security is used. In self-destructing data system, all the data stored on cloud or on servers are destructed automatically or transform into an unreadable state after the user specified time, without the user's intervention. In this paper, SeDas: self-destructing system for data security which is based on integration of cryptographic techniques is presented. Here a proof-of-concept of SeDas prototype is executed. Through the functionalities and properties of SeDas prototype, SeDas is proved to preserve all the data privacy and also it can be practically used. Output of downloading and uploading with SeDas system decreases and latency increases as compared to the system without self-destructing data mechanism. In this paper, different data security techniques are compared.

General Terms
Data privacy, Shamir's secret, Vanish, self-destructing data.

Keywords
Secret Sharing, Data Security, Symmetric encryption

1. INTRODUCTION
Cloud computing, mobile internet, cloud service is getting developed and getting popular day by day. They are much more important in our daily life. As the use of server and cloud are increasing, people are being asked to store their personal information on the cloud through internet. When people store their personal information on cloud, they expect that cloud service providers would guard and provide security to their data and providers will not violate their privacy. With the increasing use of internet, server storage etc. the risk of data leakage also increases. On the other side, when the data is being processed and stored in the system, the system takes the data and archive or copies it. These copies are important for system and networks. People might not have any idea or information about these copies, so there are chances of leakage of their privacy. If another side is considered, people's privacy can also be leaked by hacker intrusion or some legal actions or by some service providers.

2. DATA SECURITY TECHNIQUES
There are different data security techniques and each one has its advantages and limitations. Let's see these methods one by one.

2.1 Encryption and Decryption
Encryption is the process of converting plain text into cipher text. Plain text is unencrypted data. To access the cipher text, user must decrypt and retain in original form as a plain text. Sion[14] said that correctness, confidentiality and data access privacy ensures data privacy.

There are two types of data encryption algorithms, symmetric encryption and asymmetric encryption.

1. **Symmetric Encryption**
   Symmetric encryption uses the same key to decrypt the message or file. For the decryption of the data, recipient needs to use key which is send of sender during data encryption. Symmetric encryption is much faster than asymmetric encryption.

2.Asymmetric Encryption
It is also known as public key cryptography. It uses two different keys which are mathematically encrypted, one is public and other is private. The private key is kept secret and public is open to all. In asymmetric encryption, both the public and the private keys can encrypt a message. The opposite key which is used to encrypt the message by sender is used to decrypt it by the recipient and vice-versa. This method is slow but it provides confidentiality security.

2.2 Homomorphic Encryption
Homomorphic encryption [12] allows user do the complex mathematical operation or computations on data without decrypting it. It allows to-do computations only to authorized user and not to any other user. In cryptographic techniques, user needs to decrypt data while accessing it which makes it vulnerable. So, in Homomorphic encryption

there is no need to decrypt data while editing it and provides strong security. This method is computationally very expensive because it depends upon public cryptosystem and it is difficult and expensive to implement.

2.3 Vanish

Study of Vanish [1] provides a new technique for protecting and sharing privacy. Vanish system is based on a secret key, which is divided and stored in P2P system with distributed hash tables (DHTs). The system can maintain secret keys with existing and joining the P2P node. According to the features of P2P, DHT refreshes every node after about 8 hours. With Shamir's algorithm [2] one cannot decrypt the encrypted data if he does not have all the parts of the key. As a result the key will be destructed.

Some special challenges to the features of P2P are the challenges of Vanish [3], [4]. It is uncontrolled because one cannot know how long the key can survive. It is one of the disadvantages of Vanish.

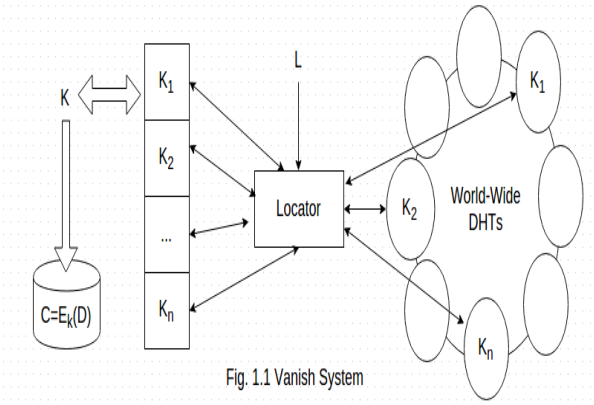

Fig. 1.1 Vanish System

In Vanish [1], after a period of time the message gets self-destructed automatically. It integrates cryptographic techniques with global-scale, P2P, distributed hash tables (DHTs). After certain period of time, data is deleted by DHTs. The key is permanently vanished, and the encrypted data is permanently unrecoverable after data lost. Vanish encrypts each message with a random key and store key shares in various large, public DHT. In Vanish system, the ttl (time to live) value is decided by DHT system and not by the user. In SeDas system, user can specify the ttl (time to live) value of distribution key.

2.4 Safe Vanish

Safe Vanish system is used to prevent hopping attacks. Hopping attack is one kind of the Sybil attacks. In VLAN hopping attack, the attacker connects to VLAN and tries to gain an access to traffic on other VLANs that would be unauthorized. There are two types of hopping attacks; switch spoofing and double tagging. In Sybil attack, a reputation system is subverted by attacker in peer-to peer network by forging identities. It extends the range of the key shares to increase attack cost gradually and makes some improvement in Vanish system.

2.5 FADE

Tang et al. [11] introduced a system, FADE, which uses standard cryptographic techniques and makes file unrecoverable to anyone by assuredly deleting them. Perlman et al. [13] presented three types to delete file: expiration time decide on file creation, deletion of individual files on request and custom keys for classes of data.

2.6 Tide

Tide is a key-storage system for self-destructing data. This system is used to maximize the advantages of ubiquity and easy deployment of Apache Web servers across the internet. Tide depends upon multiple, autonomous and distributed systems like Emphemerizer. Tide is a simple and lightweight system.

2.7 Completely Erase Bits of Encryption Key

Deleting files[12] is not enough because deleting files are still recoverable until the deleted portion of the disk is overwritten by new data. Several techniques are available to delete information from hard disk such as built–in ATA or SCSI commands and the software tools like HDDerase, SDelete etc. These software tools delete the data that reside on hard-disk by overwriting old data with new data by multiple times patters specifically designed to obscure any remnant data. This method works efficiently for platter based hard disks (HDDs). This way is not useful for Solid State Drives (SSDs) because of different designs.

The analog sanitization method is used to delete data on SSDs. It is a complex method. Several mechanisms are used in analog sanitization to imprint remnant data on the device. These mechanisms make analog sanitization more complex. There is not any complete method which works for each device type.

2.8 Shamir's SecretSharing Scheme

A secret sharing scheme means, dividing a message *m* in the number of parties *n* to carry shares and called as secrete, such that the whole set of secrete $n_1, n_2, n_3, \ldots\ldots, n_n$ of the parts determine the complete message *m*.

The data key should be very secure. If an intruder gets a key, then he can easily decrypt user's data. So in Shamir's Secrete Algorithm, the secret is divided is divided into a number of pieces and it is distributed among other administrators. Each administration needs to store secrete key piece. Knowing just only one piece of key is not enough to recover the original secret.

2.8.1 Properties of Shamir's Secret Sharing Scheme

a. Perfect:

Key shares does not leak any information

b. Ideal:

The size of each key share is same and works as a secret.

c. It is based upon all proven hypothesis. Other cryptosystems are based upon some well-known problems like discrete logarithmic problems, integer factorization etc. which makes them unreliable to provide security.

2.9 Private Information Retrieval

Private Information Retrieval is kind of protocol which hide the queries performed by the user on public databases, servers. PIR allowusers to perform queries on database with a guaranteed privacy. There is another advanced system called, Strong Private Information Retrieval (SPIR). SPIR comes with additional requirements over PIR that user can only deal with, the elements he is querying for and nothing about other elements. This way is very practically infeasible to implement single-server computational PIR protocol.

2.10 Information Dispersal Algorithm (IDA)

The IDA was proposed by Michael Rabin. Rabin stated that, divide the secret *S* into *n* number of pieces such that, the user can obtain secret only when he gets *k* number of pieces and $k<n$. Here, *k* is the threshold. In IDA, each secret is $S_i, i \leq n$, is of size |S|/k, where |*S*| is the size of the secret. Then the total size of all the secrets are $(n/k)*|S|$. Thus, IDA reduces the storage complexity. But, in IDA there are some security lapses. If the data exhibits some pattern frequently, and that the attacker gets $m<k$ pieces, then there are more chances that he may get secret *S*.

2.11 Cascade

Cascade is a mechanism for storing multiple keys in single self-destructing data mechanism. To hack the cascade system, the attacker must deal with all diverse components of the system. The new storage key storage components are added to cascade system to maximize the security of the data.

3. DISCUSSION AND CONCLUSION

In this paper, different methods of data security have been discussed. Data security algorithms have a wide range of applications across different domains. For Instance, data security over cloud which may contain a user's account number, password, personal images, videos, etc. Shamir's Secret Sharing algorithm, Rabin's Information Dispersal Algorithm (IDA) is computationally inexpensive than conventional cryptographic techniques.

These all techniques are not hardware dependent or do not require any special capability hardware. By considering the above points, one can say that,SeDas system which provides maximum security to user's data over the cloud by using Shamir's Secret Sharing Scheme Algorithm which is the most optimized algorithm.

4. ACKNOWLEDGEMENT

Here, we would like to thank our guide, Prof. Roshani Raut (Ade) for guiding us and we also like to thank NCAC-2015 for providing us big platform to present this paper.

5. REFERENCES

[1] R. Geambasu, T. Kohno, A. Levy, and H. M. Levy, "Vanish: Increasing data privacy with self-destructing data," in Proc. USENIX SecuritySymp., Montreal, Canada, Aug. 2009, pp. 299–315.

[2] A. Shamir, "How to share a secret," Commun.ACM, vol. 22, no. 11,pp. 612–613, 1979.

[3] S. Wolchok, O. S. Hofmann, N. Heninger, E. W. Felten, J. A. Hal-derman, C. J. Rossbach, B. Waters, and E. Witchel, "Defeating vanish with low-cost Sybil attacks against large DHEs," in Proc. Network and Distributed System Security Symp., 2010.

[4] L. Zeng, Z. Shi, S. Xu, and D. Feng, "Safevanish: An improved data self-destruction for protecting data privacy," in Proc. Second Int. Conf.Cloud Computing Technology and Science (CloudCom), Indianapolis,IN, USA, Dec. 2010, pp. 521–528.

[5] L. Qin and D. Feng, "Active storage framework for object-based storage device," in Proc. IEEE 20th Int. Conf. Advanced Information Networking and Applications (AINA), 2006.

[6] Y. Zhang and D. Feng, "An active storage system for high performance computing," in Proc. 22nd Int. Conf. Advanced Information Networking and Applications (AINA), 2008, pp. 644–651.

[7] T. M. John, A. T. Ramani, and J. A. Chandy, "Active storage using object-based devices," in Proc. IEEE Int. Conf. Cluster Computing,2008, pp. 472–478.

[8] A. Devulapalli, I. T. Murugandi, D. Xu, and P. Wyckoff, 2009,Design of an intelligent object-based storage device [Online].Available:http://www.osc.edu/research/network_file/projects/ob-ject/papers/istor-tr.pdf

[9] S. W. Son, S. Lang, P. Carns, R. Ross, R. Thakur, B. Ozisikyilmaz,W.-K. Liao, and A. Choudhary, "Enabling active storage on parallelI/O software stacks," in Proc. IEEE 26th Symp.Mass Storage Systems and Technologies (MSST), 2010.

[10] Y. Xie, K.-K.Muniswamy-Reddy, D. Feng, D. D. E. Long, Y. Kang,Z. Niu, and Z. Tan, "Design and evaluation of oasis: An active storageframework based on t10 osd standard," in Proc. 27th IEEE Symp. Mas-sive Storage Systems andTechnologies (MSST), 2011.

[11] S.JayaNirmala, S.MarySairaBhanu,AhteshamAkhtar Patel, "A Comparative Study Of The Secret Sharing Algorithms For Secure Data In The Cloud", International Journal on Cloud Computing: Services and architecture(IJCCSA),Vol.2, No.4, August 2012

[12] R. Perlman, "File system design with assured delete," in

[13] Proc.Third IEEE Int. Security Storage Workshop (SISW), 2005.

[14] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for storage security in cloud computing," in Proc. IEEE IN-FOCOM, 2010. Sion, R.: Secure data outsourcing. In: Proc. of the VLDBConf., pp. 1431–1432 (2007).