I J C T A, 9(14) 2016, pp. 6701-6709

A Survey on CIA Triad for Cloud Storage Services

F. Sammy[1] and S. Maria Celestin Vigila[2]

ABSTRACT

Now a day's cloud computing shows proliferation in the area of computing because of its provision of services and storage of data in the Internet. Remote servers are used to store the data in the cloud maintained by a third party. Cloud storage is suitable and flexibility endeavor than physical storage but security of data becomes the challenging issue. In this research work, we conduct an in-depth survey on recent research activities of cloud storage security in terms of CIA triad, i.e., data confidentiality, data integrity, and availability. For each of these three terms, we discuss about the challenges faced by the cloud storage services and new mechanisms proposed to meet those challenges. The ultimate aim of our research work is to provide a modern and recent knowledge to new researchers in the field of cloud storage security.

Key Words: Cloud Storage, Data integrity, Confidentiality, Access control, Cryptography, Data availability.

1. INTRODUCTION

Interest in the cloud is growing because cloud solutions provide users to access applications and files hosted on the cloud consisting of thousands of computers related components and servers, all associated together and accessible with the help of the Internet. More vitally, these results can be acquired on demand; the network becomes the supercomputer in the cloud where users can buy what they need when they need it. Using Internet technologies, the customers utilize the IT resources from the cloud. Processes, applications and services can be available on demand, regardless of the user location or device. The cloud provider is answerable for the framework, so organizations can make use of services for short periods of time without having to maintain the framework when it is not being used. The cloud computing model consists of five essential characteristics (ie.,Broad network access, On demand Self Service, Rapid elasticity, Resource Pooling , Measured Service), three delivery models (ie., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS)) and four deployment models (ie., Public Cloud, Private Cloud. Hybrid Cloud, Community Cloud) explained by National Institution of Standards and Technology [1], [2].

While cloud computing models are attractive because of their flexibility and cost effectiveness, certain difficult task must be addressed in order to provide security. Security in cloud computing is a complicated task spanning across many aspects including physical security, infrastructure security, data security, network security, and software security. Besides, it involves distributed responsibilities and agreement among the components of the cloud service. Security implementation would not be successful without agreement, confidence, rules, and involvementbetween service providers and cloud users.

Since storage is one of the necessary core frameworks in clouds, security of data which is stored in the cloud storage becomes one of the highlighting concerns in cloud computing services. The consequences of security rifts in cloud storage could be seriously damaging to both service providers and users. Without

[1] Research Scholar, Department of Information Technology, Noorul Islam University, Kumaracoil, Tamil Nadu, India.
[2] Associate Professor, Department of Information Technology, Noorul Islam University, Kumaracoil, Tamil Nadu, India.
E-mails: fvr.sammy@gmail.com, celesleon@yahoo.com

trust from users, the service provider could lose their customers. On the other hand, users whose valuable information lost or hacked could experience irretrievable loss or damage. There have been many situations reported as threats of cloud storage security. Many notorious service providers come across disconnections of their web-based cloud services due to different reasons such as power failure, hardware failure, and software failures. In spite of the fact that security claim for cloud storage varies with different services and users, they come across with three criteriaof any information systems: confidentiality, integrity, and availability. Numerous different techniques have been evolved to achieve these criteria, such as authentication, access control, encryption, certification, audition, and digital signature. This paper aims at providing a thorough study on recent data security mechanisms developed for the cloud storage. Based on the results of the study, we give our insights and suggestions on the future research directions in achieving each security objectives. The remaining part of this paper is set as follow: In Section II, a cloud storage system model is proposed to address security issues in different layers. In Section III, recent research on data confidentiality such as access control and cryptographic techniques were discussed. In Section IV, recent researches on data integrity protection such as Provable Data Possession (PDP) and Proofs of Retrievability (POR) are reviewed and compared. In Section V, we probe methods for ensuring data availability in distributed cloud storage systemswere explained. At last, conclusions are given in Section VI.

2. PROPOSED CLOUD STORAGE SYSTEM

The proposed cloud storage system consists of three-levels, based on the logical function boundaries as shown in (Fig 1).

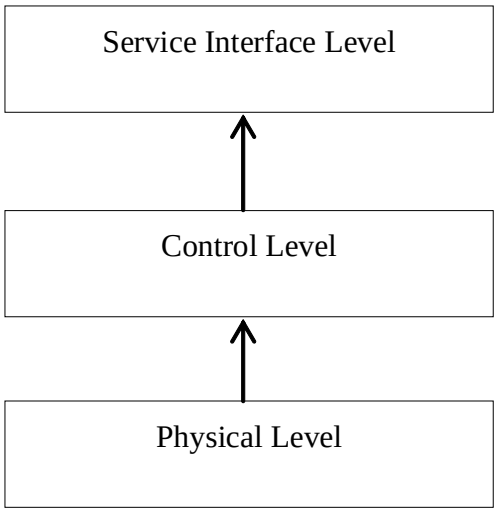

Figure 1: Cloud Storage System

The Physical level consists of wired and wireless networks tying together the wide range of distributed storage device network. The second part of the cloud storage system is the Control level, which performs certainactivitieson the data which is stored in the first level. This level hides the complexity of the bottom level by the concept of virtualization.Service interface level provide a platform to access the data which is stored in the cloud storage by the users.Mostly service interface level uses two types of interfaces to access the cloud data. They are either user-side software or a web browser interface, or sometimes both. The interface which has to be installed on the user's devices to access the data is called user-side software, whereas a web browser interface allows the user's to access of data from any place without local installations. The physical level deals with hardware security. The Control level should efficiently control the resource allocation and reliably perform data management. In the service interface level, how to avoid the encroachment on rights of both clients and service providers using secure interfaces.

3. DATA CONFIDENTIALITY

Data Confidentiality refers to the prevention of private informationleak out to the unauthorized person. Access control and Cryptography have been generally deployed to protect data confidentiality in the cloud computing. In this section, we discuss new objection faced by access control and cryptographic techniques, as well as recent developments to meet those challenges of data confidentiality protection in cloud computing.

3.1. Access Control

Access control provides a wide variety of mechanism to limit or prevent the unauthorized person utilizing the resources through the network. In the following, we examine recent research on more efficient access control techniques developed for cloud storage systems.

3.1.1. Discretionary Access Control (DAC)

This is the classicaccess controlpolicy which states, access control is given to the userbased on proprietor circumspection. Before accessing those resources each individual user request has to be checked carefully. In this access control techniquealmost all the authorization is stated explicitly and also authorizations of individual user are closed. When the authorizations are open then it is called as open policies DAC and it consists of access rules and access attributes .The access rules provide the path to prevent unauthorized users accessing to the private information and the access attributes permits the system to statethe possible different level of authorization. The information can be use flexibly in DAC model. In this model, the numbers of authorized users are maintained in the authorization database. In DAC there is no stability on the flow of information and limitation on the use of information. These consput a way to steal the copy of original message withoutproprietor permission. [3], [4].

3.1.2. Mandatory Access Control (MAC)

In this model, proprietorhas no rights of deciding who can access their resources and it is handling bythe operating system (OS). Allthe resources are classified and assigned with different security level. These classifications consist of confidential, secret and top secret. Each individual user and device is assigned by a same classification and security level. When a person or device attempts to access a specific resource, the OS will check the entity's information and provide the permission to access that information. [3], [4].

In MAC the flow of information is controlled because of the different security levels. All user in lower security level can read those information only when the permission is given by higher security level .The cons in MAC is that once the security level is defined we cannot able to modify it[5].

3.1.3. Attribute-based Access control (ABAC)

Attribute-based Access control (ABAC) uses attributes that defines an access control rules to permit the users to access the information.The rules can use different type of attributes. In this model, a user's keys and cipher texts are named with sets of descriptive attributes. A particular key can decrypt a particular cipher text only if there is a match between the attributes of the cipher text and the user's key.

The ABE was launched by Waters and Sahai [6]. Here when the number of over lied attributes between a cipher text and a private key exceeds a specified threshold k then only the access control allowed for decryption. Two well-known and important ABE schemes with more general tree-access structures, namely, Key-Policy Attribute-Based Encryption (KP-ABE) [7] and Cipher text-Policy Attribute Based Encryption (CP-ABE) [8], were explained respectively. In KP-ABE, each cipher-text was named with a set of attributes during encryption, while the users' private keys were associated with an access tree specifying which

cipher-texts the key can decrypt. Whereas, in CP-ABE, users' private keys were based on a set of their attributes while cipher-texts are associated with an access tree over the attributes during encryption. As a result, in KP-ABE scheme, it is the key distributor (usually the service provider), who decides the access policy, while in CP-ABE scheme; it is the encryptor (usually the data owner) who controls the access over the encrypted data. Goyal et al.[9]provided a new mechanism to transform a KP-ABE scheme into a CP-ABE one. Malek and Miri combined the two ABE schemes into one system, and proposed a balanced access control that allows both service providers setting up system wide access policies and data owner setting up access structure to their own data [10]. Further research on ABE is also discussed in [11]. When using the ABE in a system where there is a large number of attributes, assessing the qualification of users and generating decryption keys by a central authority becomes impractical. Multi-Authority Attribute-Based Encryption (MA-ABE) was first proposed [12]. In a MA-ABE scheme, attributes are divided into different sets, and each set can be managed by an independent attribute authority. Corresponding attribute keys for decryption are issued by multiple attribute authorities, and encryptors can specify an access policy that requires a user to obtain decryption keys for appropriate attributes from different authorities in order to decrypt a message.

3.1.4. Role-based Access Control (RBAC)

In this model the access to a resource is permitted based on the role that the user holds within an organization. The user does not have any rights to change the role that he will be assigned. The components of RBAC such as role-permissions, user-role and role-role relationships make it simple to do user assignments. By separation the tasks of role assignment and permission assignment, RBAC is much more efficient and scalable compared to other access control based on individual users, because the number of roles are usually significantly less than the number of users. Furthermore, it makes dynamic access control easier. The authors of [13] suggested including RBAC in a new access control model for the health care system that can provide flexible access rights, because it can be modified dynamically while the task changed. However, one of the major cons of this model is its complex process when fixing the role structure. This model becomes more efficient, if the roles can be structured hierarchically so that some roles inherit permissions from others.

To enforce RBAC policies, one approach is to transform the access control problem into a key management problem. In the literature, there exist many hierarchical access control models [14], [15], [16] which have been designed based on hierarchical key management (HKM) model. Because of the resemblance in structures between hierarchical access control and RBAC, a hierarchical access control scheme can be easily used to enforce RBAC access policies in cloud environment. A role-based encryption (RBE) scheme [17] was built directly on RBAC access policies. The security of the RBE is based on the use of various cryptographic algorithms.

3.2. Cryptography

Cryptography is used to secure the data while transmitting across the network. The encryption algorithm uses the combination of public and private keys to protect the sensitive data. By suitably choosing the encryption keys and implementing the digital signature we can minimize the network security issues. There are many cryptographic algorithms available and widely used for network security.

Cryptography can be divided into two types- symmetric and asymmetric. Symmetric encryption uses only one key for encryption and decryption eg. Data Encryption Standard (DES), Advanced Encryption Standard (AES), Ron's Code (RCn), and Triple DES etc. and asymmetric encryption use two keys- public and private, one for encryption and other for decryption eg. Rivest, Shamir, &Adleman (RSA), Elliptic Curve(EC), Diffi-Hillman(DH) etc.

This classic technique does not afford expected output as it support one to one encryption type communication. Public Key Encryption is not highly acceptable. This leads to the development of some advanced encryption methods which is shown below.

3.2.1. Searchable Encryption

A searchable encryption scheme is applied at high level in order to encrypt the content that is available in search list so that it can hidden from others except the party that provide the authorized tokens. A collection of files which consists of full-text list otherwise keyword list considered to generate a search list. The list is encrypted based on searchable encryption scheme in such a way (i) The pointers to the encrypted files can be retrieved based on the tokens given for the keyword. (ii) If the token is not provided then the contents are hidden for the list. However, with the complete understanding of secret key, the tokens are generated. The retrieval procedure does not reveal the content of the files or the keywords apart from the files that comprise the keyword in common. The previous statement is worth taking about since it is difficult to understand the searchable encryption that is applicable for security. After many searches the researchers identified the file containing the common keyword may have a probability to deliver the information to the third party. Based on the repeated search from the client search pattern, the server automatically guesses some assumption of required keywords that is being searched. While searching, some information is leaked and this information is similar to the appropriate file that is being returned to the customer by the server. This information that is leaked and based on leaked information the server retrieved the file is learned by the provider. (i.e. file may contain repeated keywords). We can also say the data leaked to the provider is based on the service is being used whereas it is not disclosed by the cryptographic primitives, (i.e., Exact keyword matches is used to fetch files).

This leakage seems almost essential for both efficient and reliable service in cloud storage, At worst case; the data leaked from the public cloud storage service is having very less information. Depending on different scenarios, there exist various types of searchable encryption schemes that can be applied. For example, Symmetric Searchable Encryption (SSE) is implemented for data processing in small enterprise architectures, whereas Asymmetric Searchable Encryption (ASE) is implemented for large enterprise architecture. In the subsequent topics, we explain each type of encryption scheme in detail.

3.2.1.1. Symmetric searchable encryption

In this scheme the party who is searching the data and the one who generate it are the same.This scenario is referred as Single Writer/Single Reader (SWSR). SSE schemes were presented in [18],[19]. Two major prosof SSEare its security and efficiency. Functionality and tradeoff efficiency are its cons SSE schemes are suitable for the party who perform the encryption and also for the party who searches with a keyword from the cloud storage system. They use the concept of pseudo-random functions and block ciphers for encryption this makes the SSE schemes to be efficient mostly.

Goh et al. [20] proposed the index can be upgraded effectively in the server but the search period is not optimal. ButCurtmola *et al.* [21] explained the duration of search period is optimal for the server but the index are inefficient during upgrades. The above mentioned scheme doesn't not focus on the search based on conjunctions or disjunction of terms.

3.2.1.2. Asymmetric Searchable Encryption (ASE)

In this scheme the party who is searching the data is totally different from the one who generates it. This scenario is referred as Many Writer/Single Reader (MWSR). Numerous works have been performed to show how to achieve more difficult queries in public-key setting like conjunctive searches and range queries [22], [23], [24]. In [25], the complete privacy of queries is guarantee in ASE. The major advantage of this

scheme is its functionality and its disadvantage is weaker security. But while compared with SSE scheme, the ASE is suitable for large amount of setting due to the multiple writer and reader. The concept of pairings on elliptic curves makes the ASE to become inefficient. This concept will make the operation slow when compared to hash functions or block ciphers.

3.2.2. Homomorphic encryption

Homomorphic encryption allows particular algebraic operations to be manipulated on a ciphertext, so it can produce the same encrypted result as the ciphertext of the result of the same (or different but known) operations performed on the plaintext. Homomorphic encryption can be categorized into two types: partially homomorphic encryption(PHE) and Fully homomorphic encryption(FHE). PHE allows only one homomorphic operation, either addition (e.g. Paillier [26]) or multiplication (e.g.,unpadded RSA), while FHE supports both addition and multiplication operations. Limited security applications such as electronic voting systems uses PHE algorithms. On the other hand, since the first FHE algorithm was announced [27], it has been recognized as animportant paradigm shift in the computing security field. Practical application of FHE cryptosystems will potentially enable development of computing programs, which runs on encrypted input data to generate encrypted output. These programs can thus be run by untrusted entities without revealing any sensitive information during the computing process.

4. DATA INTEGRITY

Data Integrity refers to protecting data from being modified or destroyed by unauthorized parties. Data integrity can also be threatened by environmental hazards, such as heat, dust, and electrical surges. There are three basic requirements for data integrity verification process, namely, unbounded-use, self-protect mechanism and efficiency. Unbounded-use states that the verification process should support enormous number of queries without any limit. Self-protect mechanism means the process itself should be secure against malicious server that passes the integrity test without accessing the data.Efficiency implies minimal network bandwidth and client storage capacity are needed for the verification process. The client does not need to access the entire data for verification purpose.

A number of different techniques and mechanisms have been proposed and designed for cloud data integrity verification process. The main branch of this research belongs to Provable Data Possession (PDP) and Proof of Retrievability (POR), both were designed to the above three requirements.

4.1. Provable Data Possession (PDP)

Provable Data Possession is the mechanism to protect the integrity of the data, when the data is being outsourced to a untrusted cloud storage servers. The users can check the integrity of their uploaded data without obtaining the entire stored data from the server. It was introduced as an alternate for the traditional signatures and Hash functions.

The PDP came out simultaneously with Juels–Kaliski's scheme. It was proposed by Ateniese et al. [28] and constructed based on symmetric key cryptography. PDP primarily choose Rivest- Shamir- Aaleman (RSA) -based homomorphic verifiable tags [29] to combine multiple file blocks into a single value. A similar approach was also adopted later by Shacham and Waters [30] POR scheme. PDP scheme also provides data format independence, and it puts no restriction on the format of data. In other words, PDP allows any verifier (not only client) to query the server.

4.2. Proof of Retrievability (POR)

Proofs of Retrievability (POR) is a cryptographic technique for checking the integrity of files which are stored remotely in the cloud, without having a copy of the user's original files in local storage. In this

mechanism, userstores his data together with some authentication codeto an untrusted cloud storage server. The integrity of the stored data can be check by the user alongwith CSPs(Cloud Service Providers) using the authentication code, without getting back the data from cloud. It provides the proof that a file is Intact and not modified by any attack .This helps more in defining the existence of data than that of Integrity (i.e.) Helps more in Checking the full Existence of Data .Hence it is gives the proof of Existence. They consume less bandwidth than the file itself and hence can be used in remote environment. The main feature that occurs in this Scheme is that they can correct any Data Corruptions that is found by using Error Correction codes.

The first POR scheme introduced by Juels and Kaliski employed a sentinel scheme [31]. POR protocol encrypts File and installsunsystematicallymany sentinels into the other file data blocks after encryption. These sentinels play a crucial role for verification. The verifier can challenge the person by indicating the positions of a group of sentinels, and the person should return the values of the sentinels. If the values are different from the verifier's data, then it shows that person has deleted or modified File. POR also includes error-correcting code to recover a small portion File if corrupted. Nevertheless, this mechanismonly store the File into the data storage after pre-processing and encoding of File, and it is bounded use – within a limited queries it is possible for the number of sentinels to use. Therefore, Juels and Kaliski proposed another technique from Lillibridge et al.[32], Naor and Rothblum [33]. It stores the unessential encoded data blocks with message authentication code (MAC) to substitute sentinels, and the MACs are stored jointly with data blocks. In this case, verification algorithm can examine the data integrity and ensures retrievability by requesting random number of block positions with their MACs. This approach resolves bounded use problem of the previous scheme, but at the cost of higher communication complexity of the audit. The main difference between both initial POR and PDP is that POR protects not only data integrity at the server side but also retrievability, whereas PDP assures only data integrity at cloud data storage. However, PDP is more effective when compared to Juels–Kaliski's POR, since it does not require any mass encryption, and PDP requires lesser storage space on the client side and very minimum bandwidths for utilization. However, both schemes work on static data only, even though Ateniese et al.[34]proposed a dynamic version later, but it is restricted by number of queries and basic block operations.

Future research directions include further improvements on efficiency and fully dynamic data support. To improve efficiency of those schemes, reducing communication cost and storage overhead are rightful considerations. However, fully dynamic data support is a demanding criteria, because it enlarge complication but minimizeupgrade information on server side.

5. AVAILABILITY

Availability of information refers to ensuring that authorized parties are able to access the information when needed. Availability was one of the major security concern due to the reliable infrastructure in an earlier stage of cloud computing.It also has multiple security areas need to be identified to ensure availability on the cloud, such as network vulnerability, multisite redundancy and storage failure. The most straightforward solution is to keep backup copies of data in multiple physical locations. However, this approach is not efficient in terms of storage resource utilization.

Incremental backup and data deduplication are the storage management scheme that has been developed to improve the storage utilization. Proactive approach is to forecast future availability frustration happening so that effort could be taken advance to avoid interruption of service. Guanet al. proposed two learning approaches to predict failure dynamics in cloud computing systems by using Bayesian methods and decision trees [35]. An initial stage is required for monitoring data, and then an ensemble Bayesian methods labels data that have anomalous behaviors. After all the anomalies are identified, the model can predict future failure occurrences based on decision tree classifiers. Once the failure has occurred, data recovery schemes are necessary to reduce or eliminate the loss. Zhang et al. [36] presented a mechanism toinspect the destruction

in fine-grained cloud database storage and allows the Cloud database owner to know and identify the damage for the recovery purpose by using data recovery method. Information dispersal algorithm [37] is used to empower prominent availability of data when come across physical and network interruption.

Chi-won Song et al. proposed Parity Cloud Service(PCS) framework to achieve data recovery [38]. It generates virtual disk in user system for private backup and makes parity group of multiple users. The same data among those users in the parity group are stored at the server-end. Therefore, when users find out that original file requires recovery, they can request data from the server-end without violating privacy since private backup is stored at each user's virtual disk. This approach is simple and secure, but each user has to build up virtual disk, which costs additional overhead for users. The basic and primary requirement in cloud storage is to ensuring availability of users' data whenever users demand the data. The main challenge arises when taking other performance and security concerns into consideration.

6. CONCLUSION

With the tremendous growth of cloud storage and computing nowadays, it is very needful for the cloud storage systems to be built with security solutions proven to be reliable and trustworthy. In this research work, we conducted an in-depth survey on the most critical security measurements, namely, data integrity, data confidentiality, and availability, for the cloud storage systems. For each aspect, we identified the new challenges that are faced in the cloud storage systems and provided an insight for the future directions of research.

REFERENCES

[1] Guttman, B., Roback, E.A.: An introduction to computer security: the NIST handbook. Technical Report, Gaithersburg, MD, USA, 1995,Sp 800-12

[2] (NIST), http://www.nist.gov/itl/cloud/, Accessed in May-2011, Takabi, H., Joshi,J. B. D.,and Ahn, G.:Security and Privacy Challenges in Cloud Computing Environments, Security & Privacy, IEEE, 8 (2010), pp. 24-31

[3] Younis A. Younis.,Kashif Kifayat.,Madjid Merabti,: An Access Control Model for Cloud Computing. Journal of Information Security and Applications, Vol:19, No.1, 2014, 45-60

[4] Xiaohui Li., Jingsha he., Ting Zhang.:Negative Authorization in Access Control for Cloud Computing. International Journal of security and its Applications, Vol. 6, No.2 April 2012,307-312

[5] Ravi ,S., Sandhu., and Pierangela Samarati.: Access Control: Principles and Practice. IEEE Communications Magazine, September 1994, 40-48

[6] Sahai, A., Waters, B.: Fuzzy identity-based encryption. In Advances in Cryptology – EUROCRYPT 2005, 24th Annu. International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22–26, Lecture Notes in Computer Science, Vol:3494 , Springer, 2005, 457–473

[7] Goyal, V., Pandey, O., Sahai, A.: Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. InProc. 13th ACM Conference on Computer and Communications Security, CCS '06, New York, NY, USA, 2006, 89–98

[8] Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute based encryption. In Proc. 2007 IEEE Symp. on Security and Privacy, SP '07, Washington, DC, USA, 2007, 321–334.

[9] Goyal, V., Jain, A., Pandey, O., Sahai, A.: Bounded ciphertext policy attribute based encryption. In35th Int. Colloq. Automata, Languages and Programming, 2008, Lecture Notes in Computer Science, Vol. 5126, Springer, 2008, 579–591.

[10] Malek, B., Miri, A.: Combining attribute-based and access systems. InInt.Conf. on Computational Science and Engineering, 2009.CSE '09, volume 3, August 2009, 305–312.

[11] Chase, M.: Multi-authority attribute based encryption. In 4thTheory of Cryptography Conference., Lecture Notes in Computer Science, Vol. 4392, Springer, 2007, 515–534.

[12] Chase, M., Chow, S.S.M.: Improving privacy and security in multi authority attribute-based encryption. In Proc. 2009 ACM Conference on Computer and Communications Security, 2009, 121–130.

[13] Narayanan, H.A.J., Gunes, M.H.: Ensuring access control in cloud provisioned healthcare systems. In2011 IEEE Consumer Communications and Networking Conf. (CCNC), January 2011, 247–251.

[14] Atallah, M.J, Blanton, M., Fazio, N., Frikken, K.B.: Dynamic and efficient key management for access hierarchies. ACM Trans. Inf. Syst. Secur.,12(3) (2009), 18:1–18:43.

[15] De Capitani di Vimercati, S., Foresti, S., Jajodia, S.,Paraboschi, S., Samarati, P.: Encryption policies for regulating access to outsourced data. ACM Transaction on Database System,35(2) (2010), 12:1–12:46.

[16] Samarati, P., De Capitani di Vimercati, S.: Data protection in outsourcing scenarios: issues and directions. InProc.5th ACM Symposium on Information, Computer and Communications Security, 2010,2010, 1–14.

[17] Zhu,Y., Ahn,G.J., Hu, H., Wang, H.: Crypto graphic role-based security mechanisms based on role-key hierarchy. InProc.5th ACM Symposium on Information, Computer and Communications Security, 2010, 2010, 314–319.

[18] Wagner, D., Song ,D., Perrig, A.: Practical techniques for searching on encrypted data. IEEE Symposium on Research in Security and Privacy, IEEE Computer Society. 2000; 44–55.

[19] Chang, Y., Mitzenmacher, M.:Privacy preserving keyword searches on remote encrypted data. In: Ioannidis, J., Keromytis, A., Yung, M.: editors. Applied Cryptography and Network Security (ACNS '05), Lecture Notes in Computer Science. Springer. 2005; 3531:442–55.

[20] Goh, E-J.: Technical Report 2003/216, IACR ePrint Cryptography Archive, 2003. Available from: http://eprint. iacr.org/ 2003/216.

[21] Curtmola, R.,Garay, J., Kamara, S., Ostrovsky, R.: Searchable symmetric encryption: Improved definitions and efficient constructions. In: Juels, A., Wright, R., De Capitani di Vimercati, S.: editors. ACM Conference on Computer and Communications Security (CCS '06), ACM. 2006. p. 79–88.

[22] Park, D., Kim, K., Lee, P.:Public key encryption with conjunctive field keyword search. In: Lim, CH., Yung,M.: editors. Workshop on Information Security Applications (WISA '04), Lecture Notes in Computer Science, Springer. 2004; 3325:73–86.

[23] Boneh, D., Waters, B.: Conjunctive, subset, and range queries on encrypted data. In Theory of Cryptography Conference (TCC '07), Lecture Notes in Computer Science, Springer. 2007; 4392:535–54.

[24] Shi, E., Bethencourt, J., Chan, T., Song, D.; Perrig, A.; Multidimensional range query over encrypted data. IEEE Symp. on Security and Privacy, IEEE Computer Society, Washington, DC, USA. 2007; 350–64.

[25] Boneh, D., Kushilevitz, E., Ostrovsky, R., Skeith, W.:Public-key encryption that allowsPIR queries. In: Menezes A, editor.Advances in Cryptology, CRYPTO '07, Lecture Notes in Computer Science, Springer. 2007; 4622:50–67.

[26] Paillier, P.: Public-key cryptosystems based on composite degree residuosity classes. In Advances in Cryptology EUROCRYPT 99, volume 1592 of Lecture Notes in Computer Science,Springer Berlin/Heidelberg, 1999, 223–238.

[27] Gentry, C.: Fully homomorphic encryption using ideal lattices. In Proc. 41st Annu. ACM Symp. on Theory of Computing, STOC'09, New York, NY, USA, 2009, 169–178.

[28] Ateniese, G.: Provable data possession at untrusted stores. In Proc. 14th ACM Conf. on Computerand Communications Security, CCS '07, New York, NY, USA, 2007, 598–609.

[29] Johnson, R., Molnar, D., Song, D., Wagner, D.: Homomorphic signature schemes. InTopics in Cryptology CT-RSA 2002, volume 2271 of Lecture Notes in Computer Science, Springer Berlin/Heidelberg, 2002, 204–245.

[30] Shacham, H., Waters, B.: Compact proofs of retrievability. InProc. 14th Int. Conf. on Theory and Application of Cryptology and Information Security: Advances in Cryptology, ASIACRYPT '08, Springer-Verlag, Berlin, Heidelberg, 2008, 90–107.

[31] Juels, A., Kaliski, B.S. Jr.: Pors: proofs of retrievability for large files. InProc. 14th ACM Conf. on Computer and Communications Security, CCS '07, New York, NY, USA,2007, 584–597.

[32] Lillibridge, M., Elnikety, S., Birrell, A., Burrows, M., Isard, M.: Acooperative Internet backup scheme. In Proc. USENIX AnnualTechnical Conf., ATEC '03, USENIX Association, Berkeley, CA, USA, 2003, 3–3.

[33] Naor, M., Rothblum, G.: The complexity of online memory checking. Cryptology ePrint Archive, Report 2006/091, 2006.

[34] Ateniese, G., Di Pietro, R., Mancini, L.V., Tsudik, G.: Scalable and efficient provable data possession. InProc. 4thInt. Conf. on Security and Privacy in Communication Networks, Secure Comm '08,ACM, New York,NY,USA,2008, 9:1–9:10.

[35] Guan, Q., Zhang, Z., Fu, S.: Proactive failure management by integrated unsupervised and semi-supervised learning for dependable cloud systems. InProc.20116thInt.Conf.onAvailability,Reliability and Security, ARES '11, Washington, DC, USA, 2011, 83–90.

[36] Zhang, M., Cai, K.., Feng, D.: Fine-grained cloud db damage examination based on bloom filters. In Proc. 11th Int. Conf. on Webage Information Management, WAIM'10, Springer-Verlag, Berlin, Heidelberg, 2010, 157–168.

[37] Rabin, M.O.: Efficient dispersal of information for security, load balancing, and fault tolerance. J. ACM, 36 (2) (1989), 335–348.

[38] Won Song, C., Park, S., Wook Kim, D., Kang, S.: Parity cloud service: A privacy-protected personal data recovery service. In2011 IEEE10thInt.Conf. Trust, Security and Privacy in Computing and Communications (TrustCom), November 2011, 812–817.