Multimedia Storage Security in Cloud Computing: An Overview

Chun-Ting Huang [#1], Zhongyuan Qin [*2], C.-C. Jay Kuo [#3]

[#] *Ming Hsieh Department of Electrical Engineering, University of Southern California, Los Angeles, CA 90089, USA*

[1] chuntinh@usc.edu

[3] cckuo@sipi.usc.edu

[*] *Information Science and Engineering School, Southeast University, Nanjing, Jiangsu 210096, China*

[2] zyqin@seu.edu.cn

***Abstract*— In this work, we conduct an in-depth survey on recent multimedia storage security research activities in association with cloud computing. After an overview of the cloud storage system and its security problem, we focus on four hot research topics. They are data integrity, data confidentiality, access control, and data manipulation in the encrypted domain. We describe several key ideas and solutions proposed in the current literature and point out possible extensions and futuristic research opportunities. Our research objective is to offer a state-of-the-art knowledge to new researchers who would like to enter this exciting new field.**

I. Introduction

Rapid advances in broadband communication and high speed package switching network systems as well as the growing demand on multimedia file sharing have made effective multimedia data transmission and storage increasingly important. Moreover, as a result of the fast development in cloud computing nowadays, multimedia mails, orchestrated presentations, high-quality audio and video, collaborative multimedia documents and other rich media applications can be stored in the cloud data storage server, and utilized by an increasing number of cloud users. However, a serious security issue arises in association with the expanding storage data center of the cloud server, which stores multimedia files of users such as personal photos and videos.

To enhance the security for multimedia data storage in a cloud center, known as cloud storage security, has become a popular research problem. There are various solutions proposed to ensure cloud storage security, including certification, authority, audit and encryption in last several years. As mentioned in X.800 [1], security services can be generally classified into five categories: 1) authentication, 2) access control, 3) data confidentiality, 4) data integrity, and 5) non-repudiation. The same classification scheme is applicable to cloud storage security problems. Since most recent research activities have emphasized more on data integrity and less on non-repudiation, we classify papers in the current literature into four categories only. They are data integrity, data confidentiality, authentication, and access control.

The rest of this paper is organized as follows. We first provide an overview on the cloud computing system and point out several key security problems in Section 2. Then, we review prior publications on data integrity, data confidentiality, and access control in Sections 3, 4 and 5, respectively. Since the authentication and the non-repudiation technologies do not differ significantly in the cloud storage context, we do not address them in this survey. We study the manipulation of encrypted data in the cloud storage system in Section 6. Finally, concluding remarks are given in Section 7.

II. Overview of Multimedia Storage and Its Security

The multimedia storage system in a cloud computing center is a cooperation storage service that contains multiple devices and application domains to reduce the operational cost at the client-end and boost overall system efficiency. The basic architecture of a cloud storage system is composed by a storage resource pool, including the distributed file system, the Service Level Agreements (SLA), and service interfaces [2]. Moreover, the architecture can be decomposed into five layers based on their logical function boundaries as shown in Fig. 1. This layered model shows the delivery flow of stored data in a cloud server.

Service Interface
Storage overlay
Metadata management
Storage management
Network and storage infrastructure

Fig. 1: Cloud storage layered model [2].

Many cloud computing and storage service providers are competing in the market, such as Amazon, IBM, Google, Sun Microsystems, Microsoft, EMC, HP, Symantec, etc. The cloud storage platforms developed by these companies are popular in the Internet such as SkyDrive, Amazon S3, HP Upline, Hitachi Content Platform, etc [3]. There are also many cloud storage platforms available in the market. A thorough performance comparison among these platforms is to be conducted. There are several performance metrics to be

978-1-4577-1434-4/11/$26.00 ©2011 IEEE

MMSP 2011

considered, including the cost-effectiveness in computing usage and storage usage. Clearly, security in data storage is one of the most important metrics in performance comparison of these cloud computing systems. If the provided cloud storage can be accessed or destroyed by malicious attackers, the service provider will lose trust from its users, and the leakage of personal data could cause great damage to each individual. Generally speaking, storage security consists of both physical storage security and data security. We will focus on data security issues in later sections since they can be attacked from the cyber space, which is of main concern in the modern information technology (IT) era.

III. Data Integrity

There are two popular solutions in data integrity; namely, the Third Party Auditor (TPA) and the Proofs of Retrievability (PORs). TPA introduces a mechanism that ensures clients' stored data integrity via a trustable third party while PORs guarantee that users can retrieve the intact stored data from the server with various algorithms. In the following, we will examine these two solutions in Sections III.A and III.B, respectively. Then, we examine other solutions in Section III.C.

A. *Third Part Auditor (TPA)*

The Third Party Auditor (TPA) is a mechanism used to gain the trust on a service provider from its users. The key issue here is the construction of a trustable mechanism. As depicted in Fig. 2, TPA audits the public data stored in the cloud server. By using the TPA to monitor the transaction between a cloud owner and stored data in the cloud server, the trust mechanism can be established [4].

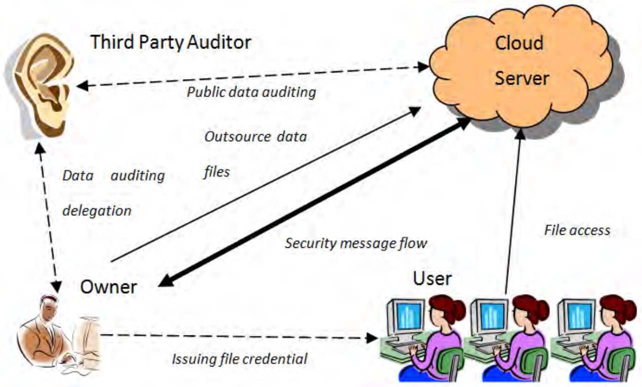

Fig. 2: Illustration of the *Third Party Auditor* (TPA) structure [4].

TPA can be built upon existing work or newly developed cryptographic primitives. Nowadays, a homomorphic solution is typically adopted by TPA to audit or check the integrated data in the cloud storage. The public-key-based homomorphic authenticator with random masking can perform traffic auditing without a local copy of the data for integrity check. This public audit system can be constructed from the setup stage, which allows a user to initialize his/her secret parameters of the system, send the verification metadata to TPA, and audit the corresponding result. In this process, TPA will issue an audit message to the server for checking user's data.

Basically, homomorphic authenticators are used to verify metadata generated from individual data blocks while the aggregated authenticators can verify a linear combination of data blocks. However, the linear combination of data blocks may potentially reveal user's privacy. With random masking, TPA cannot derive user's data content by building a correct group of linear equations. This is to ensure that TPA cannot learn further information about stored data content in the auditing process [5].

Furthermore, a protocol was proposed in [6] to integrate data dynamics and public auditability functionalities together. Basically, data dynamics is achieved by improving the classic Merkle Hash Tree (MHT) [7] construction for block tag authentication while public auditability is accomplished by TPA.

B. Proofs of Retrievability (PORs)

Another widely studied mechanism to ensure data integrity is known as Proofs of Retrievability (PORs). Under this framework, a system ensures the server (prover) to a client (verifier) that the stored data are intact during the storing and retrieving process of the client. PORs may be viewed as a kind of Proof of Knowledge (POK), yet with more emphasis on the file integrity. That is, PORs provide a guarantee to users that their stored data are not modified until they are retrieved by themselves [8].

Different prototypes of PORs have been proposed before, *e.g.* [9], [10], [11]. The POR system proposed in [11] has only one authentication value for the purpose of verification, which was built upon pseudorandom functions (PRFs) or the signature scheme of Boneh, Lynn and Shacham in a bilinear group [12]. The POR system proposed in [9] is constructed based on symmetric key cryptography, and it does not require any bulk encryption. More recently, a distributed cryptographic system, called HAIL (High-Availability and Integrity Layer), was proposed by Bowers *et al.* [10], which improves PORs by providing efficiently computable proofs with servers, and it can also verify and reallocate file shares. With the interleaving of different types of error-correcting layers, HAIL can enhance the file system availability greatly.

A theoretical framework of PORs was proposed by Bowers *et al.* [13]. Their model offers an improvement over the protocols of Juels-Kaliski [8] and Shacham-Waters [11] by proposing a new variant so that it can achieve lower storage overhead and tolerate higher error rates. Moreover, a POR scheme that deals with dynamic data was proposed with a new property in [14]; namely, fairness. It prevents dishonest clients from accusing an honest server about modifying their stored data.

Besides the study and development of various PORs, PORs provide a useful enhancement tool for other algorithms. For example, a manipulation of the MHT was proposed in [15] to achieve efficient data dynamics using the PORs model. This enhanced system can provide simultaneous public verifiability and data dynamics for remote data integrity check.

C. Other Data Integrity Methods

Research on trust dependence between cloud users and providers has grown significantly to ensure the security of data storage. Without the trust mechanism, the public will be reluctant to use the cloud storage service since people may be afraid of losing their privacy because of the leakage of personal data through the cloud server. As a result, some new requirements to achieve integrity based on users' requirements are studied by several researchers.

Gaining trust can be achieved by enhancing the storage security with the trusted cloud computing platform using the sealed storage capability [16]. With this approach, users can determine whether the environment is trustworthy or not and seal their cloud data based on their integrity requirement. This method relies on a careful design of the Virtual Machine Monitor (VMM), which is a host program that allows a single computer to support multiple, identical execution environments, in each cloud node.

Another data integrity scheme was proposed in [17], which allows customers to check the correctness of their data stored in the cloud server, and this proof can be agreed upon by both clients and the server via the Service Level Agreement (SLA). This scheme also minimizes the size of the proof of data integrity by storing only two functions at the client end. They are the bit generator function, *g,* and the data encryption function *h*.

Furthermore, there are several methods studied to address the storage security issue resulted from data insertion, modification and deletion at the block level. The first protocol that provides public verifiability without the help from the third party auditor was examined in [18]. It has been proved to be secure from an untrusted server. This protocol has functions "SetUp", "TagGen", "Challenge", "GenProof" and "CheckProof", and they are used in the verification process of checking data integrity.

The homomorphic algorithm has been applied to data integrity verification besides TPA. For example, one can use a homomorphic token with distributed verification to check the integrity of erasure-coded data. A scheme with explicit dynamic data support to ensure the correctness of data in the cloud storage was proposed in [19]. This scheme includes block update, delete and append operations. The erasure-correcting codes play an important role in preparing files for distribution so that the distributed files have redundancy parity vectors and the data dependability property.

IV. DATA CONFIDENTIALITY

By data confidentiality in the cloud storage system, we mean that the cloud system should protect the data from unauthorized disclosure. The development of new or improved techniques for data confidentiality is one of the major research topics in the field of cloud storage security. In this section, we give a brief survey on two of the research activities.

The application of cryptographic algorithms to data blocks in the cloud storage is a popular method used to ensure the confidentiality of stored data. A data confidentiality scheme in coreFS, which is a user-level network file system, was proposed in [20]. This scheme was constructed based on a new universal-hash stateful MAC. As compared with the MHT, it has smaller computational overhead of cryptographic operations. Besides, it allows better communication capability. Generally speaking, the choice of caching strategy, MAC tree update schedule, and the method to store the tree can affect the performance of this scheme.

Another data confidentiality scheme proposed in [21] exploits the newly proposed secure provenance (SP) model based on the bilinear pairing techniques. This scheme basically records the ownership and the process history of data objects in the cloud storage in order to increase the trust from public users. The SP model consists of the following modules: system setup, key generation, anonymous authentication, authorized access, and provenance tracking. The provable security technique has been tested on this scheme under the standard SP model. It demands some practical considerations in real-world applications and further improvement under the current framework.

Moreover, a new scheme of fully homomorphic encryption (FHE), was proposed by Craig Gentry [22]. Although the concept was first proposed by Rivest et al. [23] in the 70's, This algorithm was the first concrete proposal, which allows circuits evaluation over encrypted data without being able to decrypt. Thus, it offers a promising solution to multimedia storage security. With this too, the performance of data confidentiality methods discussed above can be enhanced greatly. Recently, Rothblum [24] showed how to transform any additively homomorphic private-key encryption scheme that is compact, into a public-key encryption scheme.

V. ACCESS CONTROL

One source of cloud security's leakage is caused by malicious service providers. For example, an estate company outsources its dataset such as properties information to a service provider for data storage and query processing. However, the service provider could sell the data to that company's competitor, or a malicious attacker can compromise the service provider and get unauthorized access to the data. Therefore, access control is used to allow only data owners to access their data. An access control scheme was proposed in [25], which transfers customer's data location before uploading their data to the cloud storage server. This transformation uses a spatial transformation that redistributes locations in space.

Another access control mechanism was proposed in [26] to achieve secure and efficient access to outsourced data in the owner-write-users-read application by using data block encryption. Using different keys to encrypt each data block, flexible cryptographic access control can be realized. The ideas of over-encryption and lazy-revocation were also discussed in [26] to prevent unauthorized users to access or update data blocks.

Without building a new mechanism to gain the trust, there are access control schemes that modify the existing design to improve the security of the cloud storage. One scheme proposed in [27] is to separate content and format for handling and storing in different locations as shown in Fig. 3, where a chosen optimized authorization method can help protect privacy by assigning the access right to authorized users only. This method prevents the data from being intercepted during transmission from the user client to the cloud.

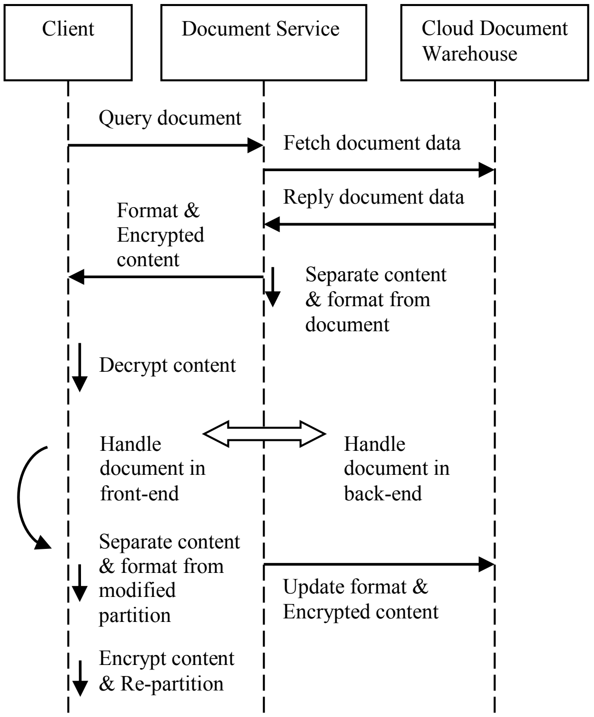
Client
Document Service
Cloud Document Warehouse
Query document
Fetch document data
Reply document data
Format & Encrypted content
Separate content & format from document
Decrypt content
Handle document in front-end
Handle document in back-end
Separate content & format from modified partition
Update format & Encrypted content
Encrypt content & Re-partition

Fig. 3: Operations in the scheme based on content and format separation [27].

Another mechanism called Role-Based Access Control (RBAC) was introduced in [28] to simplify the security management. It was motivated by the observation that the number of roles is significantly less, and users can be classified into those roles. In this work, Tsai and Shao adopted the RBAC model and used the role ontology with the Multi-Tenancy Architecture (MTA) in the cloud, where the ontology is used to build the role hierarchy in a certain domain.

Another data block encryption method was proposed in [26] for the purpose of access control, there is room left for improvement. For example, the design of dynamic mapping functions and index numbers of data blocks can enhance the reorganization of data blocks based on their access patterns.

VI. Data Manipulation in Encrypted Domain

Instead of focusing on cryptographic algorithms for the data storage security system, there are other research activities that examine the manipulation of encrypted data in a cloud storage system, including data search, computation, and recovery after corruption. We will examine their related issues in this section.

A. Data Search

Search in the database is an active research field which is studied in the context of improving data storage security. One approach was proposed in [29] to secure ranked keyword search in encrypted cloud data. This method utilized the order-preserving symmetric encryption, which achieves both security and privacy-preserving, although the guarantee to security could be weakened by the new crypto primitive called the Order-Preserving Symmetric Encryption (OPSE) [30],

Another approach, which was proposed in [31], offers search-as-a-service for the outsourced storage service. It performs indexing in the trusted enterprise domain, and utilizes the resulting indices systematically with the *Access Control Barrel* (ACB) primitives and concepts of user access hierarchy. This solution improves indexing efficiency and allows transferring to the *Storage Service Provider* (SSP) for hosting. The search-as-a-service for the outsourced storage can be developed based on the integrity of search results returned by the SSP in the future.

B. Data Recovery

The issue of data recovery has been studied by researchers. For example, the SCONEDB in [32] solves the general problem of the k-Nearest Neighbour (kNN) computation in an encrypted database. SCONEDB can incorporate other existing techniques, for example, OPES for the range query and homomorphic encryption for aggregate queries. Since attackers could be recognized by background knowledge in SCONEDB, one may extend attack models to cover other related issues such as the amount of computational power required for an attack. Moreover, one may set up another protection goal such as location privacy for SCONEDB to further protect the stored data in the system against attackers.

Another related work was presented in [33], which examines the damage in a fine-grained cloud database and allows the cloud database owner to know and locate the damage precisely for the recovery purpose.

C. Other Related Work

An architecture built with non-standard cryptographic primitives was described in [34], where the architecture employed a cryptographic storage system composed by three components: a data processor (DP), a data verifier (DV) and a token generator (TG). It integrates several individual components together to improve security to customers and service providers, which demonstrates the advance of cryptographic primitives in the cloud storage.

Sadeghi, Schneider and Winandy [35] presented a model to minimize computational latency by combining trusted hardware token with secure function evaluation (SFE), and three architectures were also discussed in association with this model. The first one is based on a tamper-proof hardware token, the second one is evaluated by a garbled circuit under fully homomorphic encryption, and the third one is the combination of the above two architectures.

The public key cryptosystem was applied to the *Patient Controlled Encryption* (PCE) scheme in [36], which enables patients to generate and store encryption keys so as to preserve patients' privacy in the electronic health record system. It compared three different PCE schemes: 1) the public key PCE, 2) the symmetric key PCE and 3) the flexible PCE. The pros and cons for each scheme are listed in Table 1 for comparison.

TABLE I
Properties comparison of three PCE schemes

Property	**Public Key PCE**	**Symmetric Key PCE**	**Flexible PCE**
Upload without Key Distribution	Yes	No	No
Flexible Hierarchies	No	No	Yes
High Efficiency	No	Yes	No
Easy to Add Categories	Yes	Yes	No

It was claimed in [37] that, although no cryptographic protocol, including FHE , can enforce privacy requested by common cloud services, this demand can be achieved by other enforcements such as through hardware implementation. Moreover, a new redefined architecture was discussed in [38]. It was composed by well established cryptographic algorithms so as to provide some advantages such as robustness and low latency. Thus, it is applicable to a real-world multimedia cloud storage system.

VII. Conclusion and Future Work

It is essential for the cloud storage to be equipped with storage security solutions so that the whole cloud storage system is reliable and trustworthy. In this work, we conducted a brief survey on a set of recently published papers and described some hot research topics in greater detail, including data integrity, data confidentiality, access control, data manipulation in the encrypted data domain, etc.

Overall, we feel that the multimedia cloud storage security is still in its infancy and expect to see more important breakthrough in the near future. For example, although the cloud storage security solutions have been developed rapidly in recent years, we have not yet seen a widely accepted model for the implementation. Besides the system design, the cloud storage security system should be flexible enough so that it can be improved by new cryptographic algorithms.

Acknowledgment

This work is supported by the Jiangsu Provincial Key Laboratory of Network and Information Security under Grants No. BM2003201, and the Key Lab of Information Network Security, the Ministry of Public Security.

References

[1] W. Stallings, Cryptography and network security: principles and practice: Prentice Hall, 2010.

[2] W. Zeng, Y. Zhao, K. Ou, and W. Song, "Research on cloud storage architecture and key technologies," in Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human, Seoul, Korea, 2009, pp. 1044-1048.

[3] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: a Berkeley view of cloud computing," Univ. of California, Berkeley, CA Technical Report No. UCB/EECS-2009-28, 2009.

[4] W. Cong, R. Kui, L. Wenjing, and L. Jin, "Toward publicly auditable secure cloud data storage services," IEEE Network, vol. 24, pp. 19-24, 2010.

[5] W. Cong, W. Qian, R. Kui, and L. Wenjing, "Privacy-preserving public auditing for data storage security in cloud computing," in 2010 Proceedings IEEE INFOCOM, 2010, pp. 1-9.

[6] W. Qian, W. Cong, R. Kui, L. Wenjing, and L. Jin, "Enabling public auditability and data dynamics for storage security in cloud computing," IEEE Transactions on Parallel and Distributed Systems, vol. 22, pp. 847-859, 2011.

[7] R. C. Merkle, "Protocols for public key cryptosystems," in Proc. of IEEE Symposium on Security and Privacy, 1980, pp. 122-133.

[8] A. Juels and J. Burton S. Kaliski, "Pors: proofs of retrievability for large files," in Proceedings of the 14th ACM conference on Computer and communications security, Alexandria, Virginia, USA, 2007, pp. 584-597.

[9] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proceedings of the 4th international conference on Security and privacy in communication netowrks, Istanbul, Turkey, 2008, pp. 1-10.

[10] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: a high-availability and integrity layer for cloud storage," in Proceedings of the 16th ACM conference on computer and communications security, Chicago, Illinois, USA, 2009, pp. 187-198.

[11] H. Shacham and B. Waters, "Compact proofs of retrievability," in Advances in Cryptology - ASIACRYPT 2008. vol. 5350, J. Pieprzyk, Ed., ed: Springer Berlin / Heidelberg, 2008, pp. 90-107.

[12] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," Journal of Cryptology, vol. 17, pp. 297-319, 2004.

[13] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of retrievability: theory and implementation," in Proceedings of the 2009 ACM workshop on Cloud computing security, Chicago, Illinois, USA, 2009, pp. 43-54.

[14] Q. Zheng and S. Xu, "Fair and dynamic proofs of retrievability," in Proceedings of the first ACM conference on Data and application security and privacy, San Antonio, TX, USA, 2011, pp. 237-248.

[15] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Computer Security – ESORICS 2009. vol. 5789, M. Backes and P. Ning, Eds., ed: Springer Berlin / Heidelberg, 2009, pp. 355-370.

[16] C. Ge and A. K. Ohoussou, "Sealed storage for trusted cloud computing," in 2010 International Conference on Computer Design and Applications (ICCDA), 2010, pp. V5-335-V5-339.

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

[18] Z. Hao, S. Zhong, and N. Yu, "A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability," IEEE Transactions on Knowledge and Data Engineering, vol. PP, pp. 1-1, 2011.

[19] W. Cong, W. Qian, R. Kui, and L. Wenjing, "Ensuring data storage security in cloud computing," in 17th International Workshop on Quality of Service (IWQoS), 2009, pp. 1-9.

[20] A. Yun, C. Shi, and Y. Kim, "On protecting integrity and confidentiality of cryptographic file system for outsourced storage," in Proceedings of the ACM workshop on Cloud computing security, Chicago, Illinois, USA, 2009, pp. 67-76.

[21] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure provenance: the essential of bread and butter of data forensics in cloud computing," in Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, Beijing, China, 2010, pp. 282-292.

[22] C. Gentry, "Fully homomorphic encryption using ideal lattices," presented at the Proceedings of the 41st annual ACM symposium on Theory of computing, Bethesda, MD, USA, 2009.

[23] R. L. Rivest, Adleman, L., Dertouzos, M.L., "On data banks and privacy homomorphisms," in Foundations of Secure Computation, ed London: Academic Press, 1978, pp. 169-180.

[24] R. Rothblum, "Homomorphic Encryption: From Private-Key to Public-Key " in 8th Theory of Cryptography Conference, TCC 2011, Providence, RI, USA, 2011, pp. 219-234.

[25] M. L. Yiu, G. Ghinita, C. S. Jensen, and P. Kalnis, "Enabling search services on outsourced private spatial data," The VLDB Journal, vol. 19, pp. 363-384, 2010.

[26] W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and efficient access to outsourced data," in Proceedings of the 2009 ACM workshop on Cloud Computing Security, Chicago, Illinois, USA, 2009, pp. 55-66.

[27] J.-S. Xu, R.-C. Huang, W.-M. Huang, and G. Yang, "Secure document service for cloud computing," in Cloud Computing. vol. 5931, M. Jaatun, G. Zhao, and C. Rong, Eds., ed: Springer Berlin / Heidelberg, 2009, pp. 541-546.

[28] W.-T. Tsai and Q. Shao, "Role-based access-control using reference ontology in clouds," in 2011 10th International Symposium on Autonomous Decentralized Systems (ISADS), 2011, pp. 121-128.

[29] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in 2010 IEEE 30th International Conference on Distributed Computing Systems (ICDCS), 2010, pp. 253-262.

[30] A. Boldyreva, N. Chenette, Y. Lee, and A. O'Neill, "Order-preserving symmetric encryption," in Proceedings of the 28th Annual International Conference on Advances in Cryptology: the Theory and Applications of Cryptographic Techniques, Cologne, Germany, 2009, pp. 224-241.

[31] A. Singh, M. Srivatsa, and L. Liu, "Search-as-a-service: outsourced search over outsourced storage," ACM Trans. Web, vol. 3, pp. 1-33, 2009.

[32] W. K. Wong, D. W.-l. Cheung, B. Kao, and N. Mamoulis, "Secure kNN computation on encrypted databases," in Proceedings of the 35th SIGMOD international conference on management of data, Providence, Rhode Island, USA, 2009, pp. 139-152.

[33] M. Zhang, K. Cai, and D. Feng, "Fine-grained cloud DB damage examination based on bloom filters," in Proceedings of the 11th international conference on Web-age information management, Jiuzhaigou, China, 2010, pp. 157-168.

[34] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Financial Cryptography and Data Security. vol. 6054, R. Sion, R. Curtmola, S. Dietrich, A. Kiayias, J. Miret, K. Sako, and F. Sebé, Eds., ed: Springer Berlin / Heidelberg, 2010, pp. 136-149.

[35] A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-based cloud computing: secure outsourcing of data and arbitrary computations with lower latency," in Proceedings of the 3rd international conference on Trust and trustworthy computing, Berlin, Germany, 2010, pp. 417-429.

[36] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in Proceedings of the 2009 ACM workshop on Cloud computing security, Chicago, Illinois, USA, 2009, pp. 103-114.

[37] M. V. Dijk and A. Juels, "On the impossibility of cryptography alone for privacy-preserving cloud computing," in Proceedings of the 5th USENIX conference on Hot topics in security, Washinton, DC, 2010, pp. 1-8.

[38] M. Yildiz, J. Abawajy, T. Ercan, and A. Bernoth, "A layered security approach for cloud computing infrastructure," in Proceedings of the 10th International Symposium on Pervasive Systems, Algorithms, and Networks, 2009, pp. 763-767.