Data Security and Privacy in Cloud Storage
Xinhua Dong, Ruixuan Li, Wanwan Zhou, Dongjie Liao, and Shuoyi Zhao

DOI: 10.3969/j.issn.1673-5188.2013.02.003
http://www.cnki.net/kcms/detail/34.1294.TN.20130627.1101.001.html, published online June 27, 2013

Data Security and Privacy in Cloud Storage

Xinhua Dong, Ruixuan Li, Wanwan Zhou, Dongjie Liao, and Shuoyi Zhao
(School of Computer Science and Technology, HuaZhong University of Science and Technology, Wuhan 430074, China)

Abstract

In this paper, we survey data security and privacy problems created by cloud storage applications and propose a cloud storage security architecture. We discuss state-of-the-art techniques for ensuring the privacy and security of data stored in the cloud. We discuss policies for access control and data integrity, availability, and privacy. We also discuss several key solutions proposed in current literature and point out future research directions.

Keywords

cloud storage; cloud computing; data security; privacy-preserving

1 Introduction

With the recent development of information technology, various types of cloud storage platforms have appeared. These platforms are often convenient, scalable, and cost-effective, so cloud computing services are widely used. Amazon's EC2/S3, Google's MapReduce/AppEngine, Microsoft's Azure, IBM's Blue Cloud and Salesforce's CRM are well-known cloud service platforms. In China, the cloud platforms of Sinochem Group and Wuxi and Dongying municipal governments have appeared. At the same time, the national strategy for cloud storage and utility computing has been developing. Utility computing service models based on cloud storage have many new characteristics. New models based on cloud storage use a variety of techniques designed to tightly manage resources and provide users with flexible services. These new service models are likely to have a knock-on effect and cause significant changes within the industry. They will give rise to many new security issues that need to be addressed. At present, cloud storage is only really applied in scenarios where a high level of security is not required. Privacy and security are significant obstacles in the development of utility computing based on cloud storage. Security vulnerabilities of cloud service providers such as Amazon, Google, and Microsoft are widely publicized, and much attention has been drawn to these vulnerabilities. In [1], cloud security and privacy issues are detailed. The Cloud Security Alliance (CSA) has made recommendations for solving problems in cloud computing applications. In [2], the European Network and Information Security Agency (ENISA) detailed the risks to data and benefits of data security in cloud computing applications. In [3], EMC Corporation's RSA Security Division analyzed the most basic security issues in the cloud infrastructure. Domestic Chinese counterparts have also widely discussed the issue of cloud security [4]. Satisfactory solutions to cloud security and privacy problems will be a strong driving force for the overall development of cloud storage services. Solving these problems is also theoretically and practically important to vigorously promote the national digital infrastructure and national information security.

This work is supported by National Natural Science Foundation of China under grants 61173170 and 60873225, National High Technology Research and Development Program of China under grant 2007AA01Z403, and Innovation Fund of Huazhong University of Science and Technology under grants 2013QN120, 2012TS052 and 2012TS053.

2 Cloud Storage: Concepts, Applications and Security

2.1 Concepts

Cloud computing involves the development of distributed processing, parallel processing, and grid computing. With cloud computing, huge computing programs are automatically split into smaller subroutines via the network. Processing and analysis is referred to multiple servers in a large system, and results are returned to the user. The network service provider can process massive amounts of information in seconds—a capability that is equal to that of powerful supercomputer networks.

Cloud storage is an extension of cloud computing and is one of a large variety of storage devices found in networks. Through the use of application software and clustering, grid technology, distributed file system, or other functions, cloud

storage works with other storage devices to provide a service access function and a whole data-storage system. When the cloud processing core requires large-scale data storage and management, a large number of storage devices need to be configured, and a cloud storage system needs to be set up. Thus, cloud storage is a cloud computing system in which data storage and management is at the core.

Cloud storage systems differ from traditional storage systems in that they are designed for multiple types of online storage services. Traditional storage systems are designed for specific applications, such as high-performance computing or transaction processing. In terms of performance indexing, cloud storage services are primarily indexed according to data security, reliability, and efficiency. Cloud storage systems are suitable for large-scale applications, a wide range of services, and complex network environments. In terms of data management, cloud storage systems provide traditional file access similar to POSIX, but cloud storage also supports mass data management and public services.

2.2 Applications

Cloud storage is effective, flexible, low-cost, and easy to manage. Cloud storage can be used in either enterprise applications or personal applications, depending on the type of service and user orientation.

In enterprises, cloud storage is used for storage space leasing, remote data backup, disaster recovery, and video surveillance. With an IDC data center, operators can lease storage space to enterprises and institutions that do not wish to purchase mass-storage devices. A high-performance, high-capacity cloud storage system and remote data backup software also allows an operator to help enterprises and institutions build their own remote-backup and disaster-recovery systems as well as remote real-time video surveillance and playback systems.

Cloud storage applications for individuals include network disks, online document editing, and online games. Network disks are used to upload and download files when a user is storing and backing up personal data over the internet. With online document editing, a user can simply access a web page, such as Google Docs, to edit, manage, and transmit documentation. Cloud computing and storage can also be used to build a huge game server cluster so that all players are managed as a game server group, and gaming becomes more exciting.

2.3 Security

Because cloud storage is large-scale, complex, and dynamic, it creates many new security and privacy problems. These problems include unauthorized access to data, threats to confidentiality, threats to data integrity, unavailability of data, and lack of privacy.

To prevent unauthorized access to the storage system, a provider needs to confirm the user's identity and verify whether that user has the permission to access resources or perform certain operations. The user submits an access request to the cloud storage provider through storage access interfaces.

When using a cloud storage service, a user uploads their local data to the storage server and downloads the data when they need it. In this process, data passes through a public cloud, private cloud, and internet transmission line. Data may be stolen or altered when stored in the server. In this case, the confidentiality of the user's data is compromised.

In a both traditional and cloud storage environments, data integrity is remotely verified to prevent data tampering and counterfeiting. However, in a cloud environment, users do not have absolute control over their data, and there is a greater need to verify the integrity of the data. When the user updates their data in the cloud, the server must promptly update the data. Therefore, real-time verification of integrity is essential.

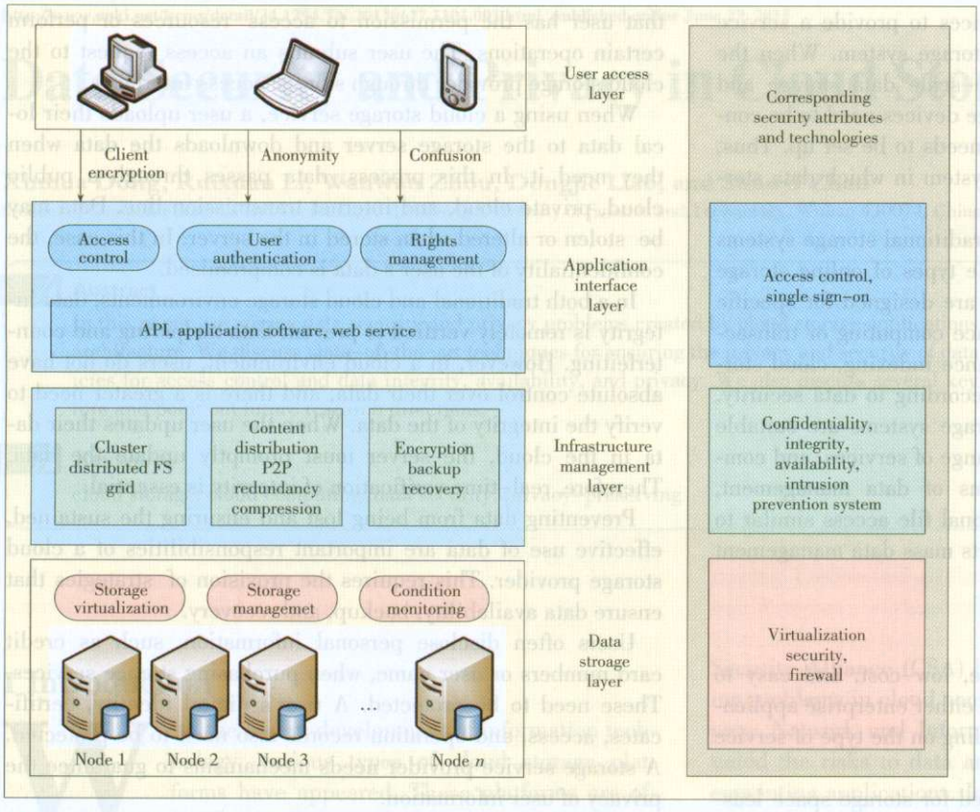
Preventing data from being lost and ensuring the sustained, effective use of data are important responsibilities of a cloud storage provider. This requires the provision of strategies that ensure data availability, backup, and recovery.

Users often disclose personal information, such as credit card numbers or user name, when purchasing storage services. These need to be protected. A user's digital identity, certificates, access, and operation records also need to be protected. A storage service provider needs mechanisms to guarantee the privacy of user information.

3 Architecture for Ensuring Security and Privacy in a Cloud Storage System

In [5], a secure cloud storage architecture is proposed. This architecture comprises business application layer, application interface layer, platform software layer, and infrastructure layer (Fig. 1). These layers provide information service management, statistical analysis, and a variety of safety measures.

In the access layer, an authorized user can log on to the cloud storage system via a standard public application interface to use cloud storage services. Different cloud storage providers have different types of access methods. The application interface layer is the SaaS layer of cloud computing services. Different cloud storage providers can develop different application interfaces and provide different application services based on the type of business. However, security problems may arise in access control and single sign on (SSO). The infrastructure management layer is the core of the cloud. It includes clusters, distributed file systems, and grid computing and allows cooperation between storage devices in the cloud. Content distribution systems and encryption of stored data ensures that data in the cloud is not accessed by unauthorized users. Various data-backup and disaster-recovery measures ensure that data stored in the cloud is not lost. In this layer, there may be problems with data confidentiality, integrity, availability, and intrusion. The data-storage layer is the fundamental part of cloud



▲Figure 1. Architecture for ensuring security and privacy in a cloud storage system.

storage. In the data-storage layer, huge amounts of data are managed in a unified way. The data-storage is also used for virtual management of storage, monitoring hardware, and fixing faults. In this layer, security problems arise in virtualization and in the firewall.

For a user uploading their data to a cloud storage system, privacy mainly depends on whether the cloud storage provider supports encryption, differential privacy protection, compulsory destruction of agreement, or data privacy management. However, cloud storage providers may also snoop on a user's data or analyze the privacy preferences of users. To fully protect user privacy, data needs to be encrypted, anonymized, or scrambled before being uploaded to the cloud.

4 Data Security in Cloud Storage

Existing technologies for controlling access to data, encrypting data, and ensuring data integrity and availability have been transplanted to cloud storage. Experts have proposed different models for ensuring data security in different cloud systems. The key technologies in these models relate to access control, data confidentiality, data integrity authentication, and data availability.

To control access to encrypted data, the owner of the data maintains encryption keys and manually sends them to users who want access to the data. This has become a bottleneck in the cloud storage environment. In [6], a new cryptographic access control scheme, called attribute-based access control for cloud storage (AB-ACCS), was proposed. Each user's private key is labeled with a set of attributes, and data is encrypted with an attribute condition so that the user can only decrypt the data if their attributes satisfy the data's condition. In [7], the authors consider the complexity of fine-grained access control for a large number of users in the cloud and propose a secure and efficient revocation scheme based on a modified ciphertext-policy attribute-based encryption (CP-ABE) algorithm. This algorithm is used to establish fine-grained access control in which users are revoked according to Shamir's theory of secret sharing. With a single sign-on (SSO), any authorized user can log in to the cloud storage system through a standard common application interface.

In a cloud storage environment, internal administrator's privileged mode is potentially a serious threat to user privacy data. To guarantee data privacy when administrator privileged mode is used, a variety of protection methods have been proposed. Attribute-based encryption (ABE) includes key-policy attribute-based encryption (KP-ABE) [8] as well as CP-ABE [9]. In ABE, decryption rules are contained in the encryption algorithm, and frequent distribution of keys in the access-control-based ciphertext is unnecessary. When the access control policy is changed, the data owner encrypts the data again. In [10], a method based on proxy re-encryption is proposed. A semi-trusted agent with proxy key can re-encrypt a ciphertext; however, the agent cannot gain the corresponding plaintext or compute the decryption key of either party in the authorization process [11]. In [12], a fully homomorphic encryption (FHE) mechanism is proposed. FHE permits a specific algebraic operation based on ciphertext, and the result is still encrypted. That is to say, retrieval and comparison of the encrypted data ends with the correct results, but the data is not decrypted throughout the whole process. The FHE scheme requires a huge amount of computation and is not always easy to implement with existing technology.

In [13], proofs of retrievability (POR) are proposed. A POR scheme allows an archive or backup service (prover) to pro-

duce a concise proof that a user (verifier) can retrieve a target file. The POR model verifies data integrity without the user having to download files themselves. A drawback of our proposed POR scheme is that the target file requires processing prior to being stored with the prover. This step creates computational overhead and increases the storage requirements on the prover. In addition, the POR scheme is based on static files, so the scope of its application is smaller. In [14], a flexible distributed scheme based on POR is proposed. This scheme assumes that operations are dynamic and data integrity is publicly verified. With Merkle Harsh Tree (MHT), the new scheme supports secure, efficient update, deleting, and appending of data blocks. The improved scheme supports public data-integrity verification and authorized third-party integrity verification.

A variety of data backup and disaster recovery measures guarantee that data stored in cloud is not be lost. These measures ensure that cloud storage is secure and stable. To counter theft of legacy data, the United States Department of Defense proposes reset and special processing [15]. In [16], a new scheme called Safe Vanish is proposed. This scheme prevents hopping attacks by extending the length of key shares and significantly increasing the cost of mounting an attack. The authors of [16] also propose using the public key cryptosystem to protect against sniffing.

Access control technology is more suited to a fine-grained cloud storage environment, and this creates large overhead. Data confidentiality is ensured by a variety of encryption methods, and confidentiality is considered in relation to access control. A data integrity verification scheme eliminates user concern throughout the data storage process. Researchers have paid attention to availability but are now also paying attention to security throughout the storage process. Security mechanisms create efficiency problems, and the trade-off between security and efficiency need to be further researched.

5 Ensuring Privacy in Cloud Storage

In a cloud storage system, privacy can be lost because of data outsourcing and service leasing. User data is stored in the cloud environment and is managed by the cloud storage provider. The security of this data depends on the level of technology used by the service providers.

In [17], a system called Arivat is proposed. This system is based on MapReduce and is designed to provide strong security and privacy for distributed computations on sensitive data. Mandatory access control and differential privacy are integrated in a novel way. In [18], the author proposes privacy management across the whole data lifecycle and uses a mandatory data destruction protocol to control user data. Dissolver is a prototype system based on Xen virtual machine monitor and CHAOS system [18]. It ensures that the user's text data only exists in a private operating space and the user's key only exists in the memory space of the virtual machine monitor. Data in the memory and the user's key are destroyed at a time specified by the user.

The system ensures the server-side privacy of user data throughout the data's lifecycle. In [19], a cloud storage framework is proposed to ensure data privacy and security. This framework has a multitree structure for indexing. An extirpation-based key derivation algorithm (EKDA) is used for key management, and discrete algorithm-based search on encrypted keyword (DLSEK) is used for data sharing and ciphertext retrieval. Lazy revocation is incorporated into the framework to deal with changes in user access rights and dynamic data operations. In [20], a mechanism with differential privacy is incorporated in the Map-Reduce computation model to analyze service efficiency and security of the mass data. A decision-tree generation algorithm is also incorporated into the computational model. Together, these measures satisfy ε-differential privacy.

Generally speaking, users distrust or only partly trust the cloud storage environment because as storage "tenants," they lack complete control over their data. A service provider has the potential to violate the privacy of user data, so the data needs to be processed before being uploaded to the cloud. Typically, data is encrypted, obfuscated, or anonymized before being uploaded.

Encrypting data negatively affects the processing of the data. Improving the speed and efficiency of ciphertext processing and retrieval is the focus of current research. In [21]-[23], the authors have done extended research on privacy preservation in the cloud and propose ciphertext retrieval solutions. In [24], a computable encryption scheme based on vector and matrix calculations (CESVMC) is proposed. In this scheme, cloud data is divided into two main categories: string and numeric. Encrypted strings can be retrieved using fuzzy retrieval, and the four basic arithmetic operations can be performed on numeric data.

Anonymous technology includes k-anonymity, L-diversity anonymous, and T-closeness anonymous. K-anonymity guarantees that each sensitive attribute is hidden in the scale of k groups [25]. This means that the probability of recognizing the individual does not exceed 1/k. The level of privacy depends on the size of k. The statistical characteristics of the data are retained as much as possible; however, k-anonymity is not only applicable to sensitive data. An attacker could mount a consistency attack or background-knowledge attack to confirm a link between sensitive data and personal data. This would constitute a breach of privacy. L-diversity anonymous ensures that each group's sensitive attributes have at least L different values [26]. This means that an attack has a maximum probability of 1/L of recognizing a user's sensitive information. T-closeness anonymous is based on L-diversity anonymous [27]. In T-closeness anonymous, the distribution of the sensitive attribute is taken into account, and the distribution differ-

ences between sensitive properties and values in groups does not exceed T. Anonymous technology is mainly used for database privacy, location privacy, and trajectory privacy, but we propose applying it cloud storage privacy.

In [28], a privacy manager that scrambles user data in the client is proposed. The privacy manager protects and monitors privacy according to the user's preferences. The privacy-preserving method in [24] supports data dyeing based on the normal cloud model in [10]. This method can be used to protect documents, images, videos, software, and other types of data. It also involves much less computation than traditional encryption or decryption. In [29], a novel privacy-preserving data-perturbation algorithm NETPA is proposed for clustering. The primitive data set can be perturbed by changing the value of neighboring main attributes, which is found in each data object, with the average attribute value of data objects in the data set's k-nearest neighborhood. This perturbation strategy is used to maintain stable k-nearest neighbor relations in primitive data. NETPA effectively stops privacy breaches. In [30], a novel data privacy protection mechanism based on partitioning and classification was proposed. The mechanism partitions the original data into a small, locally deployed block and a large, remotely deployed block. Then, data dyeing and data encryption are used according to the different security requirements of the data. This safeguards the privacy of data in the cloud, increases flexibility, and reduces overhead.

Much attention has been focused on safeguarding data at the storage provider's side; however, dynamic privacy needs at the user side have largely been ignored. Encryption, access control strategies, and other security mechanisms generally safeguard the privacy of data. There are many factors that allow privacy breaches, and user privacy requirements vary widely. Traditional authentication and security management strategies are insufficient for data stored in the cloud.

6 Conclusion

In this paper, we have described an architecture that ensures data privacy and security in cloud storage. We have also discussed access control and data integrity, confidentiality, availability, and privacy technologies. Cloud storage systems are moving towards unlimited bandwidth, capacity, and processing power, and data must be securely accessible anytime and anywhere. Because of changing demands, existing technology cannot ensure the privacy and security of data stored in the cloud. Further research needs to be done on scalability of secure storage and secure storage management in a large, complex cloud.

Storage devices are provided by a number of different service providers and shared by a large number of users. Frequent equipment deployment, data operations, and data access make the cloud a dynamic environment. Cloud data storage and management therefore needs to be safe but also highly scalable.

Intentional breaches of privacy call for dynamic countermeasures in a real-time cloud storage system. With frequent changes in computer technology, the means of breaching data privacy are constantly changing; consequently, security requirements are also changing. Privacy-preservation strategies need to be constantly devised for cloud storage systems.

An optimal balance must also be struck between security and availability in a cloud storage system. Security and availability exist in a contradictory relationship, and increasing safety often decreases availability. The foremost requirement of the data owner is security, and access limitations need to be imposed on applications. Further research is needed into the effects of security on data availability.

References

[1] T. Mather, S. Kumaraswamy, S. Latif, "Cloud Security and Privacy," USA: O'Reilly Media, 2009.
[2] D. Catteddu, G. Hogben, "Cloud Computing: Benefits, Risks and Recommendations for Information Security," Europe: European Network and Information Security Agency (ENISA), 2009.
[3] S. Curry, J. Darbyshire, D. W. Fisher, et al, "Infrastructure Security: Getting to the Bottom of Compliance in the Cloud," *The Security Division of EMC*, March 2010.
[4] D. G. Feng, M. Zhang, Y. Zhang, et al, "Study on Cloud Computing Security," *Journal of Software*, vol.22 no.1, pp. 71-83, 2011.
[5] J. Y. Liu, C. Wang, X. D. Xue, "Cloud Storage Security," *ZTE Technology Journal*, vol.18 no.6, pp. 30-33, 2012.
[6] C. Hong, M. Zhang, D. G. Feng, "AB-ACCS: A Cryptographic Access Control Scheme for Cloud Storage," *Journal of Computer Research and Development*, vol.47, pp. 259-265, 2010.
[7] Z. Q. Lv, H. Cheng, M. Zhang, et al, "A secure and efficient revocation scheme for fine-grained access control in cloud storage," in *Proc. of 4th IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, Taipei, 2012, pp. 545-550.
[8] S. C. Yu, C. Wang, K. Ren, et al, "Attribute based data sharing with attribute revocation ," in *proc. of the 5th ACM Symp. on Information*, Comput. and Commun. Security, Beijing, 2010, pp. 261-270.
[9] J. Bethencourt, A. Sahai, B. Waters, "Ciphertext-Policy Attribute-Based Encryption," *IEEE Symp. on Security and Privacy*, California, 2007, pp. 321-334.
[10] J. Li, G. S. Zhao, X. F. Chen, et al, "Fine-Grained Data Access Control Systems with User Accountability in Cloud Computing," in *proc. of the 2th Int. Conference on Cloud Comput.*, Indiana, 2010, pp. 89-96.
[11] L. Wang, L. Wang, M. Mambo, et al, "New identity-based proxy re-encryption schemes to prevent collusion attacks," in *proc. of Pairing-Based Cryptograghy-Pairing*, Ishikawa, 2010, pp. 327-346.
[12] C. Centry, "A fully homorphic encryption scheme," Stanford University, California, September 2009.
[13] A. Juels, Burton S. Kaliski Jr, "Pors: proofs of retrievability for large files," in *proc. of the 2007 ACM Conf. on Compu. and Commun. Security*, Virginia, USA, 2007, pp. 584-597.
[14] C. Wang, Q. Wang, K. Ren, et al, "Ensuring Data Storage Security in Cloud Computing," IACR Cryptology ePrint Archive (IACR), 2009, 81.
[15] Y. M. Huo, H. Y. Wang, L. Hu, et al, "A Cloud Storage Architecture Model for Data-Intensive Applications," *Computer and Management (CAMAN)*, Wuhan, 2011, pp. 1-4.
[16] L. F. Zeng, Z. Shi, S. J. Xu, et al, "SafeVanish: An Improved Data Self-Destruction for Protecting Data Privacy," in *proc. of second IEEE ont. conf. on cloud compu. technology and science (CloudCom)*, Indiana, 2010, pp. 521-528.
[17] I. Roy, H. Ramadan, S. Setty, et al. Airavat: Security and privacy for map reduce, in *proc. of the 7th USENIX conf. on networked syst. design and implementation*, SanJose, 2010, pp. 297-312.
[18] F. Z. Zhang, J. Chen, H. B. Chen, et al, "Lifetime Privacy and Self-Destruction of Data in the Cloud," *Journal of Computer Research and Development*, vol.48

no.7,2011, pp. 1155-1167.
[19] R. W. Huang, X. L. Gui, S. Yu, et al, "Design of Cloud Storage Framework with Privacy-Preserving," *Journal of XI' AN Jiaotong University*, vol.45 no.10, 2011, pp. 1-6.
[20] S. Y. Yang, S. Q. Wang, "Research of Data Privacy & Security in Map-Reduce Model ," *Computer Science*, vol.39 no.12, 2012, pp. 153-157.
[21] S. Ananthi, M. S. Sendil, S. Karthik, "Privacy Preserving Keyword Search over Encrypted Cloud Data," *Advances in Computing and Communications*, 2011, pp. 480-487.
[22] H. Hu, J. Xu, C. Ren, et al, "Proc. Private Queries over Untrusted Data Cloud through Privacy Homomorphism," in *Proc. the 27th IEEE Int. Conf. on Data Engineering (ICDE)*, Hannover, Germany, 2011.
[23] N. Cao, C. Wang, M, Li, et al, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," in *2011 Proc. IEEE INFOCOM*, Shanghai, 2011, pp. 829-837.
[24] R. W. Huang, X. L. Gui, S. Yu, et al, "Privacy-Preserving Computable Encryption Scheme of Cloud Computing," *Chinese Journal of Computers*, vol.34 no.12, 2011, pp. 2391-2402.
[25] P. Samarati, L. Sweeney, "Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression," *International Journal on Uncertainty*, Fuzziness and Knowledge-based Systems, vol. 10 no. 5, 2002, pp. 557-570.
[26] A. Machanavajjhala, J. Gehrke, D. Kifer, et al, "L-diversity: Privacy beyond k-anonymity," *ACM Trans on Knowledge Discovery from Data (TKDD)*, vol. 1 no. 1, 2007, pp. 24-33.
[27] L. Ninghui, L. Tiancheng, S. Venkatasubramanian, "t-Closeness: Privacy beyond k-anonymity and l-diversity," in *Proc. of the 23rd Int. Conf. on Data Engineering (ICDE)*, Istanbul, Turkey, 2007, pp. 106-115.
[28] M. Mowbray, S. Pearson, "A client-based privacy manager for cloud computing,"in *Proc. of the 4th Int. ICST Conf. on Commu*, NewYork, USA, 2009.
[29] W. W. Ni, L. Z. Xu, Z.H. Chong, et al, "A Privacy-Preserving Data Perturbation Algorithm Based on Neighborhood Entropy," *Journal of Computer Research and Development*, vol.46 no.3, 2009, pp. 498-504.
[30] X. L. Xu, J. L. Zhou, G. Yang, "Data Privacy Protection Mechanism for Cloud Storage Based on Data Partition and Classification," *Computer Science*, vol.40 no.2, 2013, pp. 98-102.

Manuscript received: May 15,2013

Biographies

Xinhua Dong (xhDong@hust.edu.cn) is a PhD student in the School of Computer Science and Technology, Huazhong University of Science and Technology, Whuan, China. He received his MS degree in computer science from HUST in 2008. His research interests include information retrieval, cloud security, and big data management. He is a student member of the CCF.

Ruixuan Li (rxli@hust.edu.cn) received his PhD in computer science from Huazhong University of Science and Technology, Whuan, China, in 2004. He is currently a professor in the School of Computer Science and Technology, HUST, and an adjunct associate professor at Concordia University, Canada. From 2009-2010, he was a visiting researcher at the University of Toronto. His research interests include cloud computing, big data management, social networking, and distributed system security. He has published more than 100 papers in refereed journals and conference proceedings. He has also co-authored two books and hold 14 China patents of invention. He is a member of IEEE and ACM and a senior member of the CCF.

Wanwan Zhou (zhoumila_wanwan@163.com) is an MS student in the School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan, China. She received her BS degree in computer science from Wuhan University of Science and Technology, China, in 2012. Her research interests include cloud computing and big data security.

Dongjie Liao (sxxj0301@163.com) is an MS student in the School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan, China. He received his BS degree from HUST in 2007. His research interests include cloud computing, Hadoop, and information retrieval. He has participated in many projects, and in 2010, was awarded second prize for outstanding software for engineering design (Hubei). In 2010, he also won first prize of for software for engineering design (Wuhan).

Shuoyi Zhao (zhaoshuoyi0508@vip.qq.com) is an MS student in the School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan, China. He received his BS degree in computer science from Hunan Normal University, China, in 2011. His research interests include cloud computing, big data security, and information retrieval.

ZTE Makes Industry Breakthrough with 1 Gbps LTE-Advanced

ZTE Corporation achieved a wireless data transmission rate of 1 Gbps in a live demonstration at Mobile Asia Expo in Shanghai. This represents a global breakthrough in the development of next-generation LTE-A networks.

In the demonstration, ZTE used carrier aggregation technology with four carrier frequencies on the F band and D band. With carrier aggregation, two or more carrier frequencies sharing the same or different bands are aggregated into one channel. This increases peak transmission speed of TD-LTE cells. ZTE used three carrier frequencies in the 2.6 G band and one carrier in the 1.9 G band to complete the 1 Gbps demonstration.

ZTE leads the global telecommunications industry in TD-LTE 4G networks. In February, ZTE demonstrated the first F+D cross-band CA transmission, achieving speeds of 430 Mbps. In January, ZTE and China Mobile completed D-band carrier aggregation testing in a trial network in Guangzhou. An outdoor transmission speed of 223 Mbps was achieved.

Carrier aggregation counters signal interference between neighboring cells that share the same band. By balancing the load between the primary carrier and secondary carrier, network capacity can be increased, and operators can provide customers with higher network speeds and richer user experience. Carrier aggregation is helping the telecommunications industry meet the challenges associated with surging data traffic and is making operator TD-LTE networks more competitive.

(ZTE Corporation)