DOI: 10.3969/j. issn. 1673-5188. 2017. 02. 006
http://kns.cnki.net/kcms/detail/34.1294.TN.20170508.1055.002.html, published online May 8, 2017

A Survey on Cloud Security

WU Chunming, LIU Qianjun, LI Yuwei, CHENG Qiumei, and ZHOU Haifeng
(College of Computer Science and Technology,
Zhejiang University, Hangzhou 310058, China)

Abstract

Cloud computing system packages infrastructures, applications and other resources as services, and delivers the services to market in an elastic and fast way. The significant advantages of cloud computing, e.g., scalability, elasticity, and pay-per-use, bring it considerable commercial values. Nevertheless, owing to the new application scenario, e.g., multi-tenant, cloud computing is encountering potential security risks. This paper reviews the state-of-art research in cloud security. According to the attack levels, it analyzes four kinds of attacks in the cloud, i.e., network-based attacks, VM-based attacks, storage-based attacks, and application-based attacks. The countermeasures and corresponding techniques are then introduced. Furthermore, this paper also discusses an innovative and promising solution for cloud security by dynamically changing system configuration.

Keywords

cloud computing; security; virtualization; storage

1 Introduction

Cloud computing has recently been experiencing fast development as a distributed model for performing utility computing. The cloud environment combined with virtualization techniques provides on-demand service, i.e., pay-per-use service, which ensures timely effective resource scheduling and solves the problem of resource shortage for cloud users. Currently, the most widely accepted concepts and features related to cloud computing are defined by the National Institute of Standards and Technology (NIST). NIST makes the following statements: “Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources involving networks, servers, storage and applications that can be rapidly provisioned and released with minimal management effort or service provider interaction [1].” In simple terms, the word “cloud” refers to resources (both hardware and software) stored in the Internet infrastructures. These infrastructures, also named as “data centers”, are equipped with a large number of servers to store and compute user data. In 2016, Cisco predicted that traffic in data centers would enlarge three times from 2015 to 2010 and cloud traffic would account for more than 92% by 2020 [2]. These data reveal that IT industry is going to be heavily dependent on cloud computing.

Although it is easy to understand the advantages of cloud computing from a commercial view, its security issues are quite complex. As the promotion of cloud services, more and more enterprises start to adopt the cloud computing. Cloud Security Alliance (CSA) reported that outage is found more and more frequent in cloud computing area in recent years [3]. However, the cloud is encountering many security threats. The well-known American software company Symantec made a threat report in 2015 [4], in which a 91% increase of attacks targeted at certain victims was reported. Some research has been made to cope with the increasing security threats. The network-based attacks, e.g., botnet, is now able to be detected and prevented in time [5], [6]. To prevent the attacks targeting at data, the traditional techniques like encryption as well as authentication and authorization are utilized [7]–[9]. For precluding the attacks targeted at virtual machines (VMs) and hypervisors, a promising solution is proposed by setting access control policies [9]. Cloud computing inherits from the traditional network architecture to some extent, but it is more vulnerable to security compromise. Benefiting from the development of virtualization security techniques, trusted cloud computing, identity management and other key techniques, cloud security is improving gradually. However, potential users still hesitate to move their sensitive data off-premise. As a result, despite the efforts from the research community, the further development of cloud service also needs the assistance and progress from regulations and laws.

The rest of this paper is presented as follows. In Section 2, we analyzes four kinds of attacks in the cloud, i.e., network-based attacks, VM-based attacks, storage-based attacks, and application-based attacks. The countermeasures and the corresponding core techniques are then introduced in Section 3. This is followed by a discussion of an innovative solution of cloud security by dynamically changing system configuration

This work was supported by the National Key Research and Development Program of China under Grant 2016YFB0800102, the National High Technology Research Program of China under Grant 2015AA016103, the Fundamental Research Funds for the Central Universities, and the ZTE Industry-Academia-Research Cooperation Funds.

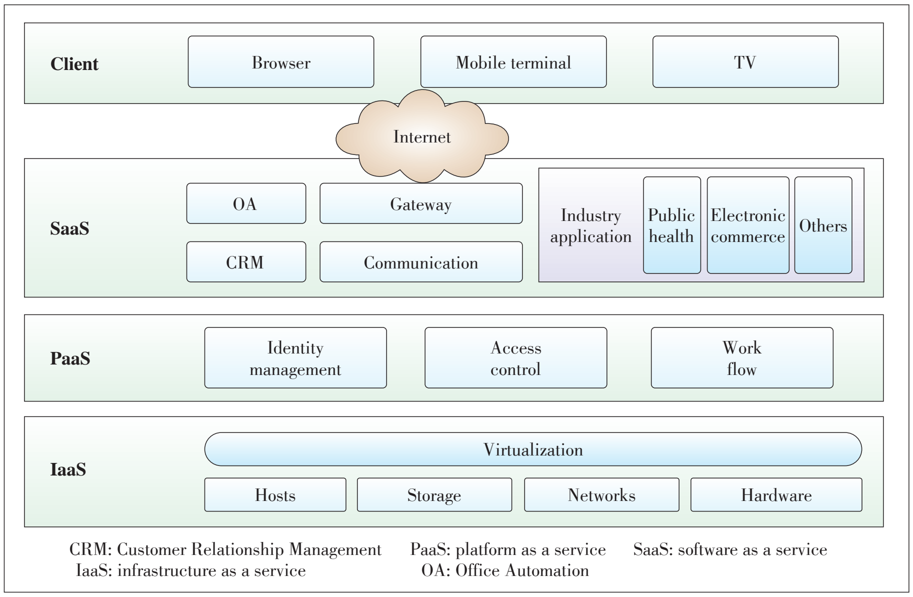
in Section 4. In Section 5, we conclude the paper.

2 Cloud Security Categorization

Current cloud computing services could be categorized in to three main types: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS), according to the system structure level. IaaS means that users can access services from well-constructed infrastructures through the Internet. PaaS packages the platform for software developing as a service and delivers it to the users in an SaaS model. SaaS enables users to rent web-based software from service providers.

As **Fig. 1** shows, these three different service models have different components. The IaaS model provides users with servers, storage, network, virtualization and other fundamental resources; The PaaS model provides identity management, access control, work flow and other support for operating systems, databases and web servers; The SaaS model supplies a variety of applications that can be accessed through the Internet and that are charged by time or resource. In the cloud framework, any component is possible to expose system loopholes that can be utilized by attackers to conduct attacks. For instance, attacks based on network loopholes could bring about communication latency or connection failure; attacks based on storage loopholes could cause data exposure or destroy; and attacks based on VM, hypervisor and application loopholes are able to compromise cloud security in many ways. Generally, the cloud platform mainly includes high-efficiency networks, high-speed storage devices, high-powered servers, and applications.

According to attack targets, we classify attacks in cloud into four categories, i.e., network-based attacks, storage-based attacks, VM-based attacks, and application-based attacks. The first category of attacks could bring about long communication latency or connection failure. The second one could induce data exposure or destroy. The third one is able to compromise cloud security in many ways. The last one is because of application vulnerabilities.



▲**Figure 1. Framework of cloud computing.**

2.1 Network-Based Attacks

Network-based attacks in cloud are similar to the same kind of attack in traditional networks, but they are more destructive. In a traditional network, the system boundary can be clearly determined, and the infrastructures can be well-protected through physical and logical security domains. While in the cloud environment, multi-tenancy with scattered data storage makes it extremely difficult to fully provide safeguard for all the uses. This kind of attack, e.g., port scanning, botnets, spoofing, Denial of Service (DoS), could lead to deteriorative Quality of Service (QoS) and steal user data in cloud. For instance, botnets, e.g., Zeus, is able to utilize Amazon´s Elastic Computing Cloud (EC2) to steal user passwords. Currently, some network-based attacks can be timely detected and prevented. Lin and Lee [5] proposed an approach to detect botnets by tracing the botmaster. This approach initially tries to find out the cryptographic keys used for botnet communication between bots and the botmaster. The attack traffic is first decrypted by identifying patterns of regions that may contain these keys. An entropy search is then performed to identify these keys. Subsequently, the communication between bots and the botmaster is decrypted. Finally, the botmaster´s location is found by acquiring its IP address. To solve the abovementioned instance of attacks, EC2 is enforced by configuring an inner firewall for each user [6]. This inner firewall denies traffic in any mode by default. As a result, the users need to configure a port to allow traffic in. However, the boundary threshold of connections allowed by the firewall is a new problem that needs to be solved.

2.2 VM-Based Attacks

In cloud computing, virtualization technique enables creation, operation, shutdown, destruction and other functions for VMs, which brings convenient management for the computing resource. However, the VM technique also brings new security risks. Having multiple VMs in one system can lead to several serious security issues, i.e., wiretap from a malicious VM neighbor. Many attacks arise in different phases of VM management. These attacks are able to be roughly divided into four types, i.e., cross VM side channel attacks, VM creation attacks, VM migration and rollback attacks, VM scheduler-based attacks. The virtualization system in cloud computing and its security threats are shown in **Fig. 2**.

1) Cross VM side channel attacks: Because of weak isolation mechanisms between VMs in the same physical machine, this type of attack is from a malicious VM, and aims to steal, falsify or destroy user data from neighbor VMs on the same machine by bypassing isolation mechanisms. It first tries to infer the functionality and activity of software by observing a variety of system hardware behavior. It then tries to obtain the physical machine’s information, e.g., resource usage, secret keys, and other information [10]. This kind of attack happens in various hardware levels, e.g., CPU cache, memory, and access driver, which makes it hard to detect and defend. Moreover, potential security risks brought by this kind of attack are disconcerting, when considering that attackers can even control victim VMs by associating with other kinds of attacks.

2) VM creation attacks: An attacker that conducts such a kind of attack needs to inject malicious code, e.g., worms, into the VM image. As a result, the malicious code is proliferating in the VM creation and replication processes, which will induce serious problems. In addition, since VMs are copied and transferred as files, the attacker can copy a VM and get sensitive data from it in an easier way. Furthermore, since the survival time of a VM is usually very short, this VM may disappear before the malicious code is detected. What’s worse, a virus infects a VM in the same way of infecting a file, while the antivirus in a VM needs to traverse each part of the guest operating system, which makes the detection very difficult.

3) VM migration and rollback attacks: Owing to the elastic and dynamic feature of cloud, VM is easy to migrate and roll back. Nevertheless, this makes sensitive data in VM exist for a relatively long time. When a VM image is copied during a VM migration, the data in this VM could be accessed by an attacker. For instance, in an S/key system, if the password has just been input for logging in and at the same time the VM is asked to roll back, attackers can easily get the password.

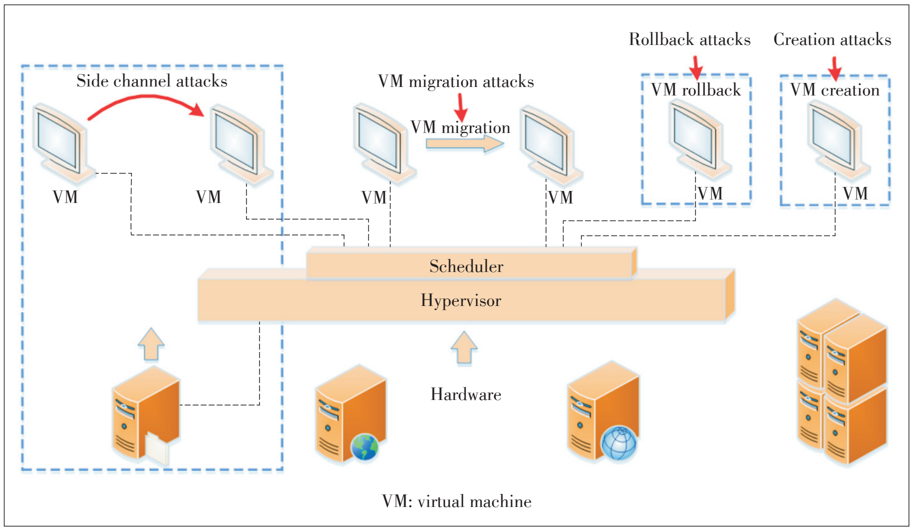
4) VM scheduler-based attacks: The time scheduling algorithm of VM that has some design loopholes can be utilized by attackers for initiating an attack. Given an unfair scheduler, an attacker is able to occupy a lot of other clients´ resources with a little cost [11]. Wei et al. [9] proposed a mechanism to share VM images in a secure manner, which uses a filter to remove private information or malicious code from the image and traces those operations on these VM images. After the image is published, the framework can also be used to scan and repair infected software.

VM-based attacks usually come along with the steal or destroy of user data. Consequently, storage security is another important research aspect of cloud security, as we will discuss in the next section.

2.3 Storage-Based Attacks

Cloud storage provides data storage and business access functions by gathering various types of storage devices. An external attacker usually steals privacy information from storage devices and attacks a series of vulnerabilities by manipulating the data. In the cloud, data need backing up, snapshot, or archiving, resulting in a significant increase in resource occupation and cost of cloud storage. In order to remove redundant and ineffective information, efficient data erasing technology and data deduplication technology are extremely important. However, due to multi-user data stored in a shared cloud environment, the manipulation of data is likely to cause information leakage or loss. Storage-based attacks thus can be divided mainly into two cases, i.e., data erase and data deduplication.

1) Data erase: When deleting data from storage devices, the file system in cloud will not remove them completely. Consequently, the remaining data can be found and utilized by attackers. In elastic clouds, the data erasing usually occurs in the resource reallocation process. Since the data of previous users may still remain in the storage devices, it is possible that these data could be accessed by the new user or by an attacker.



▲**Figure 2. VM-based security threats in cloud.**

2) Data deduplication: Data deduplication is used to keep a single copy of data, but it can also be utilized to identify files and file content. Currently, some attackers are even able to create a hidden channel to perform communication between the malicious software and the command server through data deduplication.

Several techniques, e.g., data encryption and identity management, are used to ensure data security and privacy to a certain extent. Kaaniche and Laurent [7] proposed an approach to use data deduplication for sharing data in public cloud. This approach encrypts data and encapsulates permissions in a single file, which is allowed to be decrypted only by authenticated users. Sanchez et al. [8] described an identity management system using the Security Assertion Markup Language (SAML), to provide users with access to cloud resources while protecting their privacy. The VM image access control mechanism is also proposed to ensure data cleanup security [9]. Wang et al. [12] introduced a privacy-preserving cloud data storage system which also enables public auditing/verification.

2.4 Application-Based Attacks

Applications running on cloud are also vulnerable to attacks, especially in the related protocols that serve these applications. We generally consider three types of application-based attacks, i.e., malware injection and steganography attacks, shared infrastructure based attacks, and network and protocol based attacks.

1) Malware injection and steganography attacks: Since common software usually has millions of lines of code and the code is usually written by numerous people, it is actually impossible to have fully reliable software. That is to say, the PaaS or SaaS provider is not always reliable. Moreover, if the cloud platform involves insecure interfaces, malicious code is possibly inserted into applications. Through a steganography attack [13], the attacker is able to add secret data within seemingly innocent carriers. Those secret data will be embedded in regular data. The secret data usually include malicious code that brings about unpredictable security risks.

2) Shared infrastructure based attacks: Multi-tenants' VMs are isolated by VM isolation mechanisms in the circumstance of shared infrastructures. Utilizing application loopholes or injecting malicious code into a SaaS system, an attacker is possibly able to break the isolation mechanisms. Further, the attacker can launch code injection or Cross-Site Scripting (XSS) to trace the victim application's execution path and activities [14].

3) Network and protocol based attacks: Network services involve a variety of protocols, e.g., Simple Object Access Protocol (SOAP). The packet header defined in SOAP can be replaced with an invalid request for conducting an attack [15]. If the related security policies and validation mechanisms fail to check the header, relevant services will not work normally.

3 Countermeasures and Key Techniques

To cope with the aforementioned security threats in cloud, many security countermeasures and key techniques for cloud computing have been proposed recently. We introduce four key techniques in this section.

3.1 Virtualization Security

The cloud employs virtualization techniques to achieve flexible dynamic management of physical resources. The virtualization technique also enables the isolation of multi-tenant. The security of VMs and hypervisors directly determine the security of the whole cloud platform. IBM proposed a secure hypervisor architecture named as sHype [16]. It enforces access control for traffic between different VMs, which is capable of guaranteeing isolation. Wei et al. [17] put forward the image file management system to achieve access control, source tracking, filtering and scanning of VM images. Their method could ensure the integrity of VM image files.

3.2 Trusted Computing

Trusted computing in cloud is able to provide a safe and trusted execution environment, and to ensure the integrity of data and computing. Eguro and Venkatesan [18] proposed the idea of Field Programmable Gate Arrays (FPGAs), which can identify the computation implemented in the logic fabric. A symmetric encryption key is stored in FPGA memory. The FPGA is installed in a cloud server. A trusted authority in cloud can encrypt and sign applications with the keys of FPGAs. Consequently, the application can process data in a secure manner. Sadeghi et al. [19] designed a trustful software token and bound it with security verification module. Owing to their approaches, the leakage of sensitive outsourcing data can be largely avoided.

3.3 Data Security and Privacy Protection

Under the cloud computing architecture, data are usually stored in the data center which is usually away from users [20], [21]. As a result, users have no specific idea of where their data are stored and how their data are managed. Avoiding data loss, protecting data privacy and ensuring data isolation are important security requirements for cloud storage. Therefore, it is necessary to take effective measures to protect data, e.g., multiple copies, storage encryption, and trust mechanisms. To achieve reliable data storage, real-time data backup is essential. Maintaining a copy both in the cloud and in the enterprise is a considerable way. Jensen et al. [22] designed an encryption mechanism based on ring and group to achieve anonymous storage of user data. Mowbray et al. [23] proposed a client-based tool for privacy management while storing and using data. This tool provides a user-centric trust model to help users control their sensitive data stored and used in cloud.

3.4 Identification and Access Control

In a multi-tenant cloud environment, how to realize user identity management and access control and how to ensure the separation of data between different users are the key problems in cloud security. Yan et al. [24] combined federal identity management and hierarchical cryptography in their identification system, which made the distribution and authentication easier and more safe. Yu et al. [25] defines and enforces access policies based on data attributes by exploiting and uniquely combining techniques of Attribute-Based Encryption (ABE), proxy re-encryption, and lazy re-encryption.

4 Dynamic Proactive Defense in Cloud

Current data centers usually adopt traditional security defense mechanisms, e.g., traditional firewall, Intrusion Detection System (IDS), and monitor. However, theses defense mechanisms are increasingly becoming passive in cloud when encountering more and more advanced attacks, e.g., advanced persistent threat (APT). As a result, it is critical to explore completely new defense mechanisms to guard cloud in a more proactive way for coping with those potential threats.

Recently, some proactive defense mechanisms are proposed to enforce cloud security through dynamically changing the configuration of cloud system, e.g., IP addresses, network routing algorithms, communication encryption algorithms, and authentication methods. Evolving Defense Mechanism (EDM) [26] is such a new mechanism, which is designed to dynamically change the configuration of a network system to proactively defend potential attacks. Dynamic certificate mechanisms [27] are also proposed to remove the main obstruct for the further application of cloud, i.e., trustworthiness of cloud service providers. Traditional authentication methods, e.g., Cloud Service Certifications (CSCs), fail to guarantee a certificate valid all the time. The dynamic certificate mechanism uses a third-party authority to authenticate cloud services constantly in order to avoid illegal certificates or security vulnerabilities.

Such new research is able to solve some of cloud security issues. For instance, by dynamically changing VM IP addresses, internal and external malicious scanning can be largely avoided; by changing encryption algorithms, communication between VMs becomes more reliable; by changing authentication methods, the reliability of authentication between the users and administrators is able to be enforced. In practical applications, software defined networks (SDN) [28] is favorable for achieving dynamical configuration changes owing to its centralized control and programmable logic. Current SDN controllers, e.g., OpenDaylight, and ONOS, also provide network management services for cloud by opening its northbound interfaces for OpenStack.

5 Conclusions

As the cloud industry plays an increasingly important role in the information arena, it is encountering more and more security threats. This paper discusses several main issues and key techniques of cloud security associated with the existing research from both the academic and industry. Meanwhile, a safe and reliable cloud environment relies not only on technological progress, but also on legal regulations. We look forward that the cloud industry community, academia community and government can work together to achieve a safer cloud environment.

References

[1] P. Mell and T. Grance. (2011, Sept.). *The NIST definition of cloud computing* [Online]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[2] Cisco. (2016). *Cisco global cloud index: forecast and methodology, 2015−2020* [online]. Available: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns1175/Cloud_Index_White_Paper.pdf

[3] R. Ko, S. Lee, and V. Rajan. (2013, Mar.). *Cloud computing vulnerability incidents: a statistical overview* [Online]. Available: https://cloudsecurityalliance.org/download/cloud-computing-vulnerability-incidents-a-statistical-overview.March

[4] Symantec. (2015). *Internet security threat report* [Online]. Available: https://www.symantec.com/security_response/publications/monthlythreatreport.jsp

[5] W. Lin and D. Lee , "Traceback attacks in cloud—pebbletrace botnet," in *IEEE International Conference on Distributed Computing Systems Worksho*ps, 2014, pp. 417−426.

[6] A. Web, S. Overview, and S. P. May. (2009, Jun.). *Amazon web services: overview of security processes* [Online]. Available: https://fenix.tecnico.ulisboa.pt/downloadFile/3779573805259/AWS_Security_Whitepaper.pdf

[7] N. Kaaniche and M. Laurent , "A secure client side deduplication scheme in cloud storage environments," in *6th International Conference on New Technologies, Mobility and Security*, Dubai, United Arab Emirates, 2014, pp. 1−7. doi: 10.1109/NTMS.2014.6814002.

[8] R. Sanchez, F. Almenares, P. Arias, et al., "Enhancing privacy and dynamic federation in IdM for consumer cloud computing," *IEEE Transactions on Consumer Electronics*, vol. 58, no. 58, pp. 95−103, 2012.

[9] J. Wei, X. Zhang, G. Ammons, et al., "Managing security of virtual machine images in a cloud environment," in *ACM Cloud Computing Security Workshop*, 2009, pp. 91−96.

[10] Y. Zhang, A. Juels, M. K. Reiter, et al., "Cross-VM side channels and their use to extract private keys," in *ACM Conference on Computer and Communications Security*, Chicago, USA, 2012, pp. 91−96. doi: 10.1145/1655008.1655021.

[11] F. Zhou, M. Goel, P. Desnoyers, et al. ,"Scheduler vulnerabilities and coordinated attacks in cloud computing," in *IEEE International Symposium on Network Computing and Applications*, Cambridge, USA, 2011, pp. 123−130. doi: 10.1109/NCA.2011.24.

[12] Q. Wang, C. Wang, J. Li, et al., "Enabling public verifiability and data dynamics for storage security in cloud computing," in *14th European Conference on Research in Computer Security*, Saint-Malo, France, 2009, pp. 335−370.

[13] J. Sen, "Security and privacy issues in cloud computing," in *Architectures and Protocols for Secure Information Technology Infrastructures*, Hershey, USA: IGI Global, 2013.

[14] Y. Zhang, A. Juels, M. K. Reiter, et al., "Cross-tenant side-channel attacks in PaaS clouds," in *ACM SIGSAC Conference on Computer and Communications Security*, Scottsdale, USA, 2014, pp. 990−1003. doi: 10.1145/2660267.2660356.

[15] N. Gruschka and L . L. Iacono, "Vulnerable cloud: SOAP message security validation revisited," in *IEEE International Conference on Web Services*, Los Angeles, USA, 2009, pp. 625−631. doi: 10.1109/ICWS.2009.70.

[16] R. Sailer, E. Valdez, and T. Jaeger, "sHype: secure hypervisor approach to trusted virtualized systems," IBM, Yorktown Heights, USA, Research Report RC23511, 2005.

[17] J. Wei, X. Zhang, G. Ammons, et al., "Managing security of virtual machine images in a cloud environment," in *ACM Workshop on Cloud Computing Security*, Chicago, USA, 2009, pp. 91−96. doi: 10.1145/1655008.1655021.

[18] K. Eguro and R. Venkatesan, "FPGAs for trusted cloud computing," in *IEEE International Conference on Field Programmable Logic and Applications (FPL)*, Oslo, Norway, 2012 , pp. 63−70.

[19] A. R. Sadeghi, T. Schneider, and M. Winandy, "Token-based cloud computing: secure outsourcing of data and arbitrary computations with lower latency," in *International Conference on Trust and Trustworthy Computing*, Berlin, Germany, 2010, pp. 417−429.

[20] J. Tang, "Ensuring security and privacy preservation for cloud data services," *ACM Computing Surveys (CSUR)*, vol. 49, no. 1, article 13, Jul. 2016. doi: 10.1145/2906153.

[21] C. Wang, K. Ren,W. Lou, et al., "Toward publicly auditable secure cloud data storage services," *IEEE Network* , vol. 24, no. 4, pp. 19–24, Jul./Aug. 2010.

[22] M. Jensen, S. Schäge, and J. Schwenk ,"Towards an anonymous access control and accountability scheme for cloud computing," in *IEEE International Conference on Cloud Computing*, Miami, USA, 2010, pp. 540-541. doi: 10.1109/CLOUD.2010.61.

[23] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of retrievability: theory and implementation," in *ACM Workshop on Cloud Computing Security*, Chicago, USA, 2009, pp. 43–54. doi: 10.1145/1655008.1655015.

[24] L. Yan, C. Rong, and G. Zhao ,"Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography," in *International Conference on Cloud Computing*, Bangalore, India, 2009, pp. 167–177 .

[25] S. Yu, C. Wang, K. Ren, et al., "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *Proc. IEEE INFOCOM*, San Diego, USA, 2010, pp. 534–542. doi: 10.1109/INFCOM.2010.5462174.

[26] H. Zhou, C. Wu, M. Jiang, et al., "Evolving defense mechanism for future network security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 45-51, 2015. doi: 10.1109/MCOM.2015.7081074.

[27] S. Lins, P. Grochol, S. Schneider, et al., "Dynamic certification of cloud services: trust, but verify," *IEEE Security & Privacy Magazine*, vol. 14, no. 2, pp. 66–71, 2016. doi: 10.1109/MSP.2016.26.

[28] Open Networking Foundation. (2012, Apr. 13). *Software - defined networking: the new norm for net*works [Online]. Available: https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf

Manuscript received: 2016-10-24

Biographies

WU Chunming (wuchunming@zju.edu.cn) received the Ph.D. degree in computer science from Zhejiang University in 1995. He is currently a professor with the College of Computer Science and Technology of Zhejiang University, and the Associate Director of the Research Institute of Computer System Architecture and Network Security. His research fields include Software-Defined Network, reconfigurable networks, proactive network defense, cloud security, network virtualization, and intelligent networks.

LIU Qianjun (liuqj0522@163.com) is now a Ph.D. candidate at the College of Computer Science, Zhejiang University, Hangzhou, China. Her research interests involve cloud security, big data security and smart security analytics.

LI Yuwei (liyuwei@zju.edu.cn) is now a Ph.D. candidate at the College of Computer Science, Zhejiang University, Hangzhou, China. Her research interests involve system security, code security and smart security.

CHENG Qiumei (chengqiumei@zju.edu.cn) is currently pusuing the Ph.D. degree with the College of Computer Science and Technology, Zhejiang University, Hangzhou, China. Her research interests include cloud security, software-defined security, network virtualization, software-defined networks, and proactive network defense.

ZHOU Haifeng (zhouhaifeng@zju.edu.cn) is currently pursuing the Ph.D. degree with the College of Computer Science and Technology, Zhejiang University, Hangzhou, China. His research interests include software-defined networks, software-defined network security, cloud security, proactive network defense, intelligent networks and security systems, network traffic engineering, and innovative network and security technologies.

Roundup

Introduction to *ZTE Communications*

An international ICT R&D Journal Sponsored by ZTE Corporation
ZTE COMMUNICATIONS
ISSN 1673-5188
CN 34-1294/ TN
CODEN ZCTOAK
tech.zte.com.cn
April 2017, Vol. 15 No. 2
SPECIAL TOPIC: Edge Computing

ZTE Communications is a quarterly, peer-reviewed international technical journal (ISSN 1673-5188 and CODEN ZCTOAK) sponsored by ZTE Corporation, a major international provider of telecommunications, enterprise and consumer technology solutions for the Mobile Internet. The journal publishes original academic papers and research findings on the whole range of communications topics, including communications and information system design, optical fiber and electro-optical engineering, microwave technology, radio wave propagation, antenna engineering, electromagnetics, signal and image processing, and power engineering. The journal is designed to be an integrated forum for university academics and industry researchers from around the world. *ZTE Communications* was founded in 2003 and has a readership of 5500. The English version is distributed to universities, colleges, and research institutes in more than 140 countries. It is listed in Inspec, Cambridge Scientific Abstracts (CSA), Index of Copernicus (IC), Ulrich's Periodicals Directory, Abstract Journal, Norwegian Social Science Data Services (NSD), Chinese Journal Fulltext Databases, Wanfang Data — Digital Periodicals, and China Science and Technology Journal Database. Each issue of *ZTE Communications* is based around a Special Topic, and past issues have attracted contributions from leading international experts in their fields.