Cloud Computing Security and Privacy

Li Yan*[1], Xiaowei Hao[1]
[1]Information Communication Branch Company, Shanxi Electric Power Company
No 71, Fudong Street, Xinghualing District, Taiyuan, Shanxi, PRC
*dianli54321@126.com

Zelei Cheng[2], Rui Zhou[3]
[2]School of Information and Communication Engineering, [3]International School
Beijing University of Posts and Telecommunications
No 10, Xitucheng Road, Haidian District, Beijing, PRC
chengzelei@bupt.edu.cn; zhourui.1997@bupt.edu.cn

ABSTRACT
Cloud computing is an emerging technology that can provide organizations, enterprises and governments with cheaper, more convenient and larger scale computing resources. However, cloud computing will bring potential risks and threats, especially on security and privacy. We make a survey on potential threats and risks and existing solutions on cloud security and privacy. We also put forward some problems to be addressed to provide a secure cloud computing environment.

CCS Concepts
• **Computer systems organization → Cloud computing Security and privacy→Security requirements**

Keywords
cloud computing; security; privacy; data security; standards

1. INTRODUCTION
Cloud computing is an emerging technology that can provide organizations, enterprises, and governments with cheaper, more convenient and larger scale computing resource. And the adoption of cloud computing is growing steadily in the past years. For example, more than 88 percent of organizations in India has already adopted cloud services[1].

Cloud computing has greatly changed our lives in the past years, changing the way we listen to music, share photos, and make business. However, the introduction of cloud computing will bring users potential risks, which are similar to other developing techniques. Security considerations are among the biggest obstacles for adoption of cloud computing. These security considerations include architecture security, platform security, application security, data security, and governance problems, etc. There are more than 20,000 types of cloud service in use today, but only 8.1 percent meets the strict data security and privacy requirements proposed by cloud security organizations, such as ENISA, cloud security alliance (CSA), NIST, and cloud service providers(CSPs) like IBM and Amazon[2] .

ICBDC '18, April 28–30, 2018, Shenzhen, China

ACM ISBN 978-1-4503-6426-3/18/04…$15.00
http://doi.org/10.1145/3220199.3220217

With the development of cloud computing, more and more governments, organizations and companies decide to adopt cloud computing. Cloud computing is critical for the further success of business and enterprises may need to adopt the technology ahead of their rivals. That it is, security is the key to the success of cloud computing and we should focus more on the security and privacy issues of cloud computing.

2. CLOUD COMPUTING
2.1 Definition of Cloud Computing
The US National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction" [3]. NIST cloud model is composed of five essential characteristics, three service models, and four deployment models.

2.2 Service Models
The three service models of cloud are software as a service(SaaS), platform as a service(PaaS), and infrastructure as a service(IaaS).

Consumers can use applications provided by CSPs through SaaS. The advantage of SaaS is that there is no need for consumers to install applications and applications can be accessed by different devices through interfaces such as a web browser. PaaS provides consumers with a cloud platform to have full control over the deployed applications and developing environment regardless of the underlying infrastructure, such as servers and operating systems. IaaS provides consumers with cloud infrastructures, such as storage, networks, and other fundamental computing resources.

2.3 Features of Cloud Computing
The most important features of cloud computing are on-demand service, broad network access, rapid elasticity, measured services, multi-tenant and virtualization.

Cloud computing can provide consumers with highly abstracted resources, near instant scalability and flexibility, near instantaneous provisioning, shared resources(hardware, database), service on demand, and programmatic management[3, 4]. Consumers purchase virtual machines, storage, services running on the same infrastructure owned by the CSPs. So multi-tenant and virtualization are two important features of cloud computing.

2.4 Benefits of Cloud Computing
Economical benefits[5]. The introduction of cloud computing can increase speed and flexibility and reduce costs[6,7]. Cloud computing can enable reduction of infrastructure, maintenance cost, and labor costs, increase the server and storage utilization, payback period. CSPs provide consumers with different kinds of computing resources, such as servers, storage. Cloud services

providers can provide more timely, effective and efficient updates for consumers, more secure and formal cloud services[8]. With features of low cost, on-demand, efficient and optimized services, businesses can benefit a lot from cloud computing.

Backup and Disaster recovery. Data stored in the cloud can be accessed at any time anywhere. Another advantage is data sharing between users[9]. Once cloud computing is adopted, data of the organization or enterprise will migrate to cloud. When natural disaster like earthquake happens, they can also use those service on the cloud. Even if the local data lost for some hardware errors, data on the cloud can also be accessed.

Easy access and dynamic resource provisioning. Compared to traditional model that provisions resources according to peak demand, dynamic resources model is based on the current demand, which can considerably lower the operating cost. Since resources can be allocated or deallocated on demand, service providers are empowered to manage their resource consumption according to their own needs. In this case, services providers can respond quickly to rapid changes in service demand, such as the flash crowed effect.

3. POTENTIAL THREATS AND RISKS

Cloud computing is an emerging technology and its infrastructure and architecture are different from existing computing architectures. The introduction of cloud computing must bring potential risks and threats, especially on security and privacy.

Services providers and consumers may have different security responsibilities in different service models. Take Amazon's AWS EC as an example, service provider should be responsible for physical security, environment security and virtualization security, while consumers are responsible for the IT system, such as operating system.

The nine top threats[10] in cloud computing are data breach, data loss, account or service hijacking, insecure interfaces and APIs, denial of service, malicious insiders, abuse of cloud service, insufficient due diligence and shared technology vulnerabilities. Other threats and risks include unauthorized access, communication security, storage security, etc..

Understanding the security and privacy risks in cloud computing and developing efficient and effective solutions are critical for its success[11].

3.1 Communication Security

Cloud computing provides users with cheap and flexible resources and services. While data between cloud and end users are transmitted on the Internet. Although security on the cloud is very important, the security of network and channel do matter. Malicious users may exploit vulnerabilities of the network configurations to probe the network, which will cause security risks, such as MIMT attacks and packet sniffing[12]. To make sure we can securely share data with others in the cloud, a trusted channel is needed for the data transmission. However, many company and organizations' network themselves are not secure. Without a trusted channel, data may be monitored and tampered.

3.2 Cloud Computing Resources Abuse

Cloud services providers provide services and resources to users and any users can purchase these services and resources for any purposes. In this case, cloud services may be abused for malicious use, launching attacks such as DDoS and DoS attacks for example. It means malicious users can launch a huge attack with a low cost using low-cost cloud services and resources. However, the use of cloud resources should be carefully monitored.

3.3 Virtualization and Multi-tenant

Multi-tenant[13] is an important feature of cloud computing and virtualization is the key technology. In the cloud, multiple virtual machines run on the same infrastructures which will cause some potential security risks. Cloud is such a shared environment and data in the cloud is not secure as it seems. Data on the cloud is stored where the owners do not know and CSPs may have access to these data without proper authorization. Virtual machines(VM) may access data on other virtual machines on the same infrastructure without proper isolation and configuration. As with VM hopping, attackers can access to data and resources on another VM, monitor resource usage, modify related configurations and delete stored data. What's worse, a virtual machine can exploit side channel timing information to extract private cryptographic keys used in other virtual machines on the same physical server[14]. It is two key features of cloud computing, virtualization and multi-tenant that will make cloud users in potential dangers.

3.4 Availability and Business Continuity

CSPs need to provide uninterruptible service to a large scale of users. However, attacks on the cloud will affect the performance of cloud system and cause financial losses both for the CSPs and consumers. Attacks like DoS and DDoS attacks prevent users from accessing their data and services relying on cloud services may be interrupted [15]. It is easier and cheaper to launch large scale attacks on cloud service, so it is needed to guarantee the availability and business continuity of cloud computing services.

3.5 Insecure Interface and APIs

In the cloud environment, consumers do not know where their data are stored, nor the infrastructure. Cloud services providers provide resources and services to consumers via services, such as API and. These APIs may be compromised if abused or not properly configured. Security mechanisms may be broken into from the resource to services and it will threaten consumers' data and system security.

3.6 Authentication and Authorization

Data owners or administrators need to assign privilege or access control to different users. There are compromised accounts problems in some companies and organizations [16]. Proper authentication and authorization should be used to guarantee data security and prevent unauthorized data access.

3.7 Malicious Insiders

Insider threats may be the most significant threat to organizations all over the world[17]. Most of data breach are blamed for human errors, insider attacks in particular[18]. The next attacker may be insiders and malicious insiders are difficult to prevent and will cause large loss for both consumers and organizations. It must be easier for insiders to steal confidential information than external attackers.

3.8 Data Security

Data security should be taken into consideration when migrating to cloud. Data security in cloud is composed of data integrity, data segregation, data access, data locality, data confidentiality and data breaches. From cloud consumers' perspective, data security should be guaranteed during entire data lifecycle. Data on cloud is sensitive to the organization or to the public, and may be stored

anywhere, consumers do not know whether it is coming under regulatory compliance and not violating any users' privacy. Migration to cloud may expose these sensitive data in danger, and threats can come from both internal side and external side. Once data was migrated to cloud, it is out of data owner's control. And it is why many organizations and companies are hesitated to take steps to cloud adoption. So data security and privacy is urgent to be addressed when migrating to cloud[6].

3.9 Cloud Auditing

Every operation may cause potential threats and auditing is necessary for cloud. Monitoring data is important for emergency response, data loss for example. Data monitoring may contain sensitive and significant information which may be accessed by malicious users both inside and outside. So cloud services providers may not provide rough monitoring data for consumers, which means cloud consumers must rely more on cloud service consumers to protect data security. Because they cannot do effective auditing without rough data. However, cloud services providers cannot guarantee cloud services they provide are secure.

3.10 Encryption and Key Loss

Encryption is commonly used to protect data, which can also be used to protect data in the cloud. Malicious users who can access the file cannot read it without keys. However, credentials and passwords are regularly reused, which increase the risks.

The most common way to protect sensitive and confidential information in the cloud is to use password. However, it is easy to be broken into by attackers. So password is not a good way to protect information on the cloud. What's worse, most cloud users are not aware of the importance of encrypting their data in the cloud. And keys may be extracted by malicious users in other ways, such as side channel attack [14].

4. EXISTING SOLUTIONS AND COUNTERMEASURES

Data owners cannot guarantee that their data on the cloud are under regulatory compliance and CSPs will not violate any users' privacy. Loganayagi.B[19] enhance the security of cloud by combining authentication and authorization with service policy monitoring and updating VMs periodically.

4.1 Standards

NIST, ENISA and CSA have released some guidelines and standards. For example, ENISA released cloud computing benefits, risks and recommendations for information security[20], which focuses in the area of personnel security and supply chain assurance. NIST guidelines on security and privacy in public cloud computing and definition of cloud computing give a broad category of standards and guidelines even though oriented for US government widely adopted by most IT industries.

4.2 Side Channel Resistant Algorithms

Side channel attacks are being a new attack trend. Some algorithms are resistant to side channel attacks, for example Montgomery ladder algorithm and a branchless algorithm. Modifying these algorithms and adapting to cloud computing virtualization environment can resist side channel attacks[21].

4.3 Deduplication

Encryption is a simple and efficient solution to weaken or stop deduplication[22]. Encrypting data with their own personal keys before performing deduplication at the client can stop deduplication. However, the personal keys should be changed regularly, because there will be identical files result with same encryption functions and key.

Cryptographic storage service can guarantee that data is controlled by the consumers and protect data against data breaches and electronic forensics. Seny Kamara and Kristin Lauter[23] propose a possible architecture for cryptographic storage, which is composed of data processor, data verifier and token generator. Data processor processes data before sent to cloud and data verifier checks whether cloud data was tampered with or not, and the token generator generates tokens that can be used to retrieve customer data, and a credential generator implements access control policies in the system.

4.4 Cloud Architecture

Michael Brock[13] proposed a cloud security framework to help design and implement effective cloud security infrastructures. The framework uses access control methods to protect cloud infrastructures, encryption to enhance communication and storage security, authentication and authorization to prevent unauthorized access to confidential information.

Cloudprotect[24] is a java HTTP proxy server which is adapted to work with cloud applications, such as Google calendar. The proxy server can modify HTTP requests from clients and HTTP response from servers to be suitable for the privacy middleware. CloudProtect can help cloud users find a balance between privacy requirements and good user-experience.

Twincloud[25] is composed of a trusted cloud and a commodity cloud, which can separate the underlying computations into their security and performance aspects. In the model, the client can communicate with the trusted cloud over a low bandwidth, secure channel. The trusted cloud and the commodity cloud are connected with an insecure, high bandwidth channel. The trusted cloud uses symmetric cryptography and authenticated encryption to guarantee the confidentiality and authenticity of data. Twin clouds are architectures for secure cloud computing, which combine the advantages of secure outsourcing of data and arbitrary combinations.

4.5 Access Control

Cloud storage increases the risk of unauthorized access to cloud data. Access control is a common and effective way against unauthorized access to data. However, traditional access control model is not applicable to cloud storage systems.

Joseph K. Liu[9] proposed a two factor data security protection mechanism for cloud storage systems. In the mechanism, one need his secret key stored in the computer and a unique personal security device to decrypt the ciphertext. Once stolen or lost, the security devices can be revoked. In this case, the cloud server only executes some algorithms, but not to read or decrypt the encrypted data, which can protect cloud data against unauthorized access by CSPs and malicious users.

Uriti Bhagya Latha[26] proposed an efficient multi-authority identity based signature schema for cloud storage and designed an access control framework for multi-authority systems. The signature schema does not require a global authority and can support all LSSS access structure. And the process of multi-authority can be revocated which can be against collusion attack. The identity based digital signature schema can be used to implement multi-authority of users in cloud and the key is generated by random code key.

Sheikh[27] proposed a multi-faceted Trust Management system architecture for cloud computing. The architecture can identify the trust cloud providers by assessing attributes from Service Level Agreements(SLAs), such as security, performance and compliance.

4.6 Identity Management (IDM)

Identity management (IDM) mechanism can help authenticate users and services based on credentials and characteristics. Identity based proxy encryption schemes are to manage files from the owner to proxy servers. However, it is mainly center oriented, impractical to implement, and vulnerable to collusion attacks. So it is not applicable to distributed cloud computing environment.

Han[28] proposed an identity based data storage scheme in the cloud environment which supports queries both from inter domain and outside. In the scheme, users can share files across co-existed multiple domains and the data owner compute the re-encryption key independently. The scheme is secure against collusion attacks and many other attacks.

To protect data on the cloud, Priyanka[29] proposed a new identity-based secure distributed data storage (IBSDDS) schemes. The schemes are composed of the private key generator(PKG), data owner, proxy server and the receiver. PKG is responsible for validating users' identity and issue secret keys. The data owner can encrypt data and outsource ciphertext to proxy servers. Proxy servers store the encrypted data and send cipher text to receiver, then the receiver can authenticate himself to the owner and decrypt the data.

4.7 Data Anonymization

Data anonymization is a technique which allows data to be analyzed and used in a more useful way while protecting data privacy. Formal data anonymization models include k-anonymity and l-diversity. K-anonymity makes that each record different from k other records if one want to identify the data. The larger the value k is, the more privacy the model provides. L-diversity model can provide more privacy protection than k-anonymity, which is against homogeneity and background knowledge attacks. Jeff[30] believes that data anonymization can be effective in enhancing security of cloud computing.

5. PROBLEMS TO BE ADDRESSED

5.1 Standards

NIST and ENISA both have their own standards on cloud and cloud security, such as NIST Cloud Computing Reference Architecture, and NIST Cloud Computing Security Reference Architecture (Draft). Different CSPs also have different standards when implementing cloud computing, such as Amazon's AWS CloudHSM API reference. However, there are no uniform standards on cloud security among different countries and fields. So it is urgent to standardize standards on cloud security and standardization can promote security. NIST, ENISA, CSA and companies like Google, Amazon may cooperate to propose best practices for secure cloud computing.

5.2 Cloud Resources Monitoring

CSPs can provide cloud services to any parties and malicious users may abuse cloud services for malicious purposes. So appropriate cloud resources monitoring is needed for CSPs. Artificial intelligence techniques, such as machine learning, can be introduced to monitor usage of cloud resources and prevent cloud abuse.

5.3 Communication Channel and APIs

Cloud clients communicate with servers with APIs, so continuous, secure Internet connection and secure APIs are necessary for clients to communicate with servers. It means that both the servers and clients should have uninterruptible Internet access and the network should be against common attacks. Secure APIs should also be considered because APIs are the only way that clients communicate with servers.

5.4 Identity Management and Access Control

Identity management and access control are necessary in the cloud environment, because cloud is a shared environment. In such a shared environment, some users may have access to other users' data. Identity management mechanism can be used to authenticate users and prevent unauthorized access to confidential data. There should be identity based management specific for cloud, like identity based storage model and identity based encryption model which can enhance cloud security and help to protect data privacy.

5.5 Reliable and Secure Services

CSPs should provide consumers with reliable and secure services, because the services consumers provided for others may depend on them. The quality of services CSP provided will be considered when cloud consumers try to choose potential CSP. Factors may be taken into consideration about the quality of services include uptime, response time, throughout, scalability, mean time to identify and mean time to contain when incident occurs. The design of virtual machine manager to avoid co-residency is important, because it can defend against side channel attacks.

5.6 Encryption

Encryption should be used to protect data during storing, transmitting and sharing in the cloud. A variety of techniques have been developed specifically for cloud storage, such as searchable encryption, attribute based encryption. However, keys may be lost or extracted by malicious users. So encryption is not enough to protect data in the cloud. So combination of encryption with other verification methods may be introduced to protect data security, such as two factor data protection mechanism. Executing the process of encryption and decryption in different servers or computers may be another choice.

6. CONCLUSION

Cloud computing brings potential risks and threats, especially on security and privacy. In the paper, we make a survey on potential threats and risks on cloud security and privacy, including communication security, abuse use of cloud computing resources, virtualization and multi-tenant, availability and business continuity, insecure interface and APIs, authentication and authorization, malicious insiders, data security and privacy, auditing, encryption and keys loss. Existing solutions on cloud computing security and privacy include standards, two factor data security protection mechanisms, cryptographic cloud storage, new cloud architectures, and identity based management schemes. Further problems to be addressed are on standards, cloud resources monitoring, secure communication channel and APIs, identity management and access control, reliable and secure services, and encryption.

7. REFERENCES

[1] CSA.https://downloads.cloudsecurityalliance.org/assets/survey/Cloud_Adoption_India_19Nov.pdf

[2] Gartner. 2016. Gartner Says Cloud Computing Will Become the Bulk of New IT Spend by 2016. http://www.gartner.com/newsroom/id/2613015

[3] Mell, P. M., & Grance, T. 2011. SP 800-145. The NIST Definition of Cloud Computing. National Institute of Standards & Technology.

[4] Ruan, K., & Carthy, J. (2012). Cloud Computing Reference Architecture and Its Forensic Implications: A Preliminary Analysis. Digital Forensics and Cyber Crime.

[5] IBM. A View Of Cloud Computing. https://cacm.acm.org/magazines/2010/4/81493-a-view-of-cloud-computing/fulltext

[6] Zhang, Q., Cheng, L., & Boutaba, R. 2010. Cloud computing: state-of-the-art and research challenges. Journal of Internet Services & Applications, 1(1), 7-18.

[7] Catteddu D. 2010 Cloud Computing: Benefits, Risks and Recommendations for Information Security. In: Serrão C., Aguilera Díaz V., Cerullo F. (eds) Web Application Security. Communications in Computer and Information Science, vol 72. Springer, Berlin, Heidelberg

[8] Zhilong Wang, Tao Zhang, Yu Yang, and Haipeng Qu. 2016. Comparison of Security Frameworks for Governmental Clouds between United States and European Union. In Proceedings of the 6th International Conference on Communication and Network Security (ICCNS '16). ACM, New York, NY, USA, 30-34. DOI: https://doi.org/10.1145/3017971.3017985

[9] Liu, J. K., Liang, K., Susilo, W., Liu, J., & Xiang, Y. 2016. Two-factor data security protection mechanism for cloud storage system. IEEE Transactions on Computers, 65(6), 1992-2004.

[10] CSA. The Notorious Nine Cloud Computing Top Threats in 2013. https://cloudsecurityalliance.org/download/the-notorious-nine-cloud-computing-top-threats-in-2013/

[11] IBM.http://public.dhe.ibm.com/common/ssi/ecm/en/xie12347usen/XIE12347USEN.pdf

[12] CSA. Defeating Insider Threats. https://downloads.cloudsecurityalliance.org/assets/survey/defeating-insider-threat-survey.pdf

[13] Rong, C., Nguyen, S.T., and Jaatun, M.G.2013. Beyond lightning: A survey on security challenges in cloud computing, Computers & Electrical Engineering, 2013, 39, (1), pp. 47-54

[14] Yinqian Zhang, Ari Juels, Michael K. Reiter, and Thomas Ristenpart. 2012. Cross-VM side channels and their use to extract private keys. In Proceedings of the 2012 ACM conference on Computer and communications security (CCS '12). ACM, New York, NY, USA, 305-316. DOI: http://dx.doi.org/10.1145/2382196.2382230

[15] Tsai, H. Y., Siebenhaar, M., Miede, A., Huang, Y., & Steinmetz, R. (2012). Threat as a service?: virtualization's impact on cloud security. It Professional, 14(1), 32-37.

[16] Takabi, H., Joshi, J. B. D., & Ahn, G. J. 2010. Security and privacy challenges in cloud computing environments. IEEE Security & Privacy, 8(6), 24-31.

[17] IBM.https://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03133usen/SEW03133USEN.PDF

[18] IBM. 2016. 2016 Cost of Data Breach Study: Global Analysis. https://www.ibm.com/security/data-breach

[19] Loganayagi, B., & Sujatha, S. (2012). Enhanced cloud security by combining virtualization and policy monitoring techniques. Procedia Engineering, 30, 654-661.

[20] Catteddu, D. 2010. Cloud Computing: Benefits, Risks and Recommendations for Information Security. Web Application Security. Springer Berlin Heidelberg.

[21] Brock, M., & Goscinski, A. 2010. Toward a Framework for Cloud Security. Algorithms and Architectures for Parallel Processing, International Conference, ICA3PP 2010, Busan, Korea, May 21-23, 2010. Proceedings (Vol.6082, pp.254-263).

[22] Harnik, D., Pinkas, B., & Shulmanpeleg, A. 2010. Side channels in cloud services: deduplication in cloud storage. IEEE Security & Privacy, 8(6), 40-47.

[23] Seny Kamara and Kristin Lauter. 2010. Cryptographic cloud storage. In Proceedings of the 14th international conference on Financial cryptograpy and data security (FC'10). Springer-Verlag, Berlin, Heidelberg, 136-149.

[24] Mamadou H. Diallo, Bijit Hore, Ee-Chien Chang, Sharad Mehrotra, and Nalini Venkatasubramanian. 2012. CloudProtect: Managing Data Privacy in Cloud Applications. In Proceedings of the 2012 IEEE Fifth International Conference on Cloud Computing. IEEE Computer Society, Washington, DC, USA, 303-310. DOI=http://dx.doi.org/10.1109/CLOUD.2012.122

[25] Bugiel, S., Nürnberger, S., Sadeghi, A. R., & Schneider, T. 2011. Twin clouds: an architecture for secure cloud computing.

[26] UB Latha, B Vineela. 2016. An Efficient Multi Authority Data Access Control using Identity Based Signature Schema in cloud computing", International Journal of Engineering Trends and Technology (IJETT), V31(5),240-244

[27] Habib, S. M., Ries, S., & Muhlhauser, M. 2011. Towards a Trust Management System for Cloud Computing. IEEE, International Conference on Trust, Security and Privacy in Computing and Communications (pp.933-939). IEEE.

[28] Jinguang Han, Willy Susilo, and Yi Mu. 2013. Identity-based data storage in cloud computing. Future Gener. Comput. Syst. 29, 3 (March 2013), 673-681. DOI=http://dx.doi.org/10.1016/j.future.2012.07.010

[29] A Novel Identity based Secure Distributed Data Storage System in Cloud Computing based on Database –as-a-Service.2014.http://www.advanceresearchlibrary.com/temp/downloads/jct/oct2014/v25.pdf

[30] Sedayao, J. 2012.Enhancing cloud security using data anonymization. Intel white paper on Cloud computing and information security