Jie Liang CSE300

Professor Suver Nov 3rd 2016

Data Security issues in Cloud Computing

With emergence of various cloud services software, such as Dropbox, Google Drive, and Amazon products, it changes the fundamental idea of data storage in people's minds. Data is no longer files that sit in our local hard drive but running in the cloud which we can access remotely. However, what comes with the convenience is security risks. Cloud system faces several data security problems, like loss control of the data, accessibility vulnerability, and multi-tenancy issues. Data security concerns remain major issues and challenges in the field of cloud computing.

In Zhang, Cheng, and Boutaba's study, they talked about several advantages of cloud computing: no up-front investment, lowering operating cost, highly scalable, easy access and reducing maintenance expenses, which are the reasons why cloud computing is so popular nowadays. Since service providers typically don't have access to the physical security system of data centers, they must rely on the infrastructure providers to achieve full data security (Zhang, et al. 16). In the cloud computing model, cloud providers provide highly integrated storage space for consumers to manage their data for its own use, but users don't know where their data has been stored. They argued that data stored in cloud often faces more problems such as data loss, data disclosure and data manipulations. While in traditional data storage model, data is relatively very close to users because they often are stored in local disks and under users' control. They can implement the security measures based on their own needs. However, in a cloud system, the data are kept in a data base where beyond the user's reach, so the data needs more secure actions such as encryption, authentication and authorization. In Zhang, Cheng, and Boutaba's paper, they only focus on addressing the potential problems that can be created due to the characteristics of cloud computing, but there's much more aspects of data security issues and challenges that needs to be addressed.

Data security can be violated not only when storing data as Zhang, Cheng, and Boutaba stated, but also during the data transmission. Data flow over the network should also be protected from data leakage. As Subashini and Kavitha addressed in *A Survey on Security Issues in Service Delivery Models of Cloud Computing*, accessibility vulnerability is one of the most important data branches when we talk about security issues in cloud computing. Their paper is one of the significant journals that discussing data security during the transmission time. In the cloud computing model, the data travels through the network to the cloud provider for processing, it faces the main problem is how to ensure that the enterprise data transmission process in the network is not stolen or modified. In order not to leak Enterprise's useful information, Subashini and Kavitha proposed that we have to focus on validating network security via Network penetration and packet analysis, session management weakness, and insecure SSL trust configuration. Since malicious users may be unable to get the data by hacking into the cloud due to the security measure of the cloud providers, but they can access information by sniffing network packets during the data transmission, or hijacking active sessions in order to access user's credentials. Those three categories that they mentioned should be the important aspects of preventing data leakage during the transmission.

User authentication for data security has consistently been a major problem in software development field. The problem is more critical in the cloud computing environment since the control of data is out of users' hands. Subashini and Kavitha discussed data leakage during data transmission while Mazhar, Samee, and Athanasios paid more attention on user authentication during the data transmission. In their article, *Security in Cloud Computing: Opportunities and Challenges*, they suggested that user authentication is one of the most important aspect of securing data during the transmission. The cloud services are normally available to the customers through the Internet. Standard Internet protocols and mechanisms are used for communication between the customers and the cloud by validating user's identity. The communication process results in transmission of either data/information or applications between the customer and the cloud. They divide the cloud communication into two categories: communication external to the cloud (between customers and cloud) and communication internal to the cloud (Mazhar, et al. 5). Mazhar brings valuable idea into data security in cloud computing since these procedures could potentially be hijacked. Each user in a cloud system is identified with either a unique id or email address and other additional information to guarantee the validity of the client. If user information is obtained by others, that would result in user's data to be reached by other people other than the user.

Mazhar, Samee, and Athanasios also proposed data integrity can be violated due to lack of hierarchy of user's roles. Data security rises to another level when the data stored by specific user is for authorized purposes, such as government files or business files etc. disclosure of user's information would provide access of data to improper person and allow them to manipulate or spread data. Cloud system also demands highly organized user roles. A business's cloud account would involve organizing user roles. The boss of the business would have a higher authority than other employees within the company. If the cloud system does not specify the roles of users, then there would exists no hierarchy in accessing data. The result of such cloud system would be chaotic; users would have permission to grant data beyond their authority.

As Mazhar, Samee, and Athanasios mentioned, data communication within the cloud could potential problematic. Deyan and Hong systematically introduced multi-tenancy to summarize the potential problems we are facing on communication within the cloud. In their paper, *Data Security and Privacy Protection Issues in Cloud Computing*, they said due to the characteristics of cloud computing, it also brings many unique challenges to the table, especially data security. One of the biggest characteristics of cloud computing is multi-tenancy. Multi-tenancy is the property that enables the use of a single resource by multiple customers that may or may not belong to the same organization. Deyan discussed multi-tenancy where Mazhar didn't mention, and it brings a new perspective to us. For each cloud provider, they only need to take care of their own infrastructure, but it brings difficulties to manage resources and maintain data security among cloud providers. The key idea is about the isolation between tenants within the data center. It requires extra data encryption to secure data access and transfer so that cloud providers won't have the permission to each other's data.

In the cloud, however, in addition to external attacks, there are several other areas that will threat the data availability: such as Recovery of data and long term viability which are discussed in Aich, Sen, and Dash's paper. If the cloud services providers go bankrupted or some glitches within the data centers, will the data get lost? If not, how should the consumers retrieve their data and maintain the data integrity? If the cloud services companies do not provide some sort of off-site archiving, the availability of the data will be threatened. In this case, the data storage duration would be a big factor to play in data security on cloud computing, which makes Aich, Sen, and Dash's idea a valid argument.

Cloud computing are widely utilized among different fields of study, so it's very important that data security technique is up to date. In Zhang's, Mazhar's and Deyan's papers, they talked about the data leakage within the cloud due to loss control of the data and lack of hierarchy of user access as well as multi-tenancy issues. Subashini discussed potential problems during data transmission time, while Aich suggested data security challenges can be appeared in the long term. The fundamental challenges of data security in cloud computing is separation of sensitive data and access control. Further studies could be done with a focus in increasing transparency of data storage and data transmission to users in order to minimize loss of control in users' perspective as well as enhancing data encryption during exchanging data between users and cloud providers.

Works Cited

Zhang, Qi, Lu Cheng, and Raouf Boutaba. "Cloud Computing: State-of-the-art and Research Challenges." Journal of Internet Services and Applications 1.1 (2010): 7-18. Web.

Ali, Mazhar, Samee U. Khan, and Athanasios V. Vasilakos. "Security in Cloud Computing: Opportunities and Challenges." Information Sciences (2015): 1-27. Web. 18 Oct. 2016.

Chen, Deyan, and Hong Zhao. "Data Security and Privacy Protection Issues in Cloud Computing." International Conference on Computer Science and Electronics Engineering (2012): 1-5. Web. 18 Oct. 2016.

Subashini, S., and V. Kavitha. “A Survey on Security Issues in Service Delivery Models of Cloud Computing.” A Survey on Security Issues in Service Delivery Models of Cloud Computing, 2011, pp. 1–11.

Aich, Asish, Alo Sen, and Satya Ranjan Dash. "A Survey on Cloud Environment Security Risk and Remedy." International Conference on Computational Intelligence & Networks (2015): 1-2. Web. 18 Oct. 2016.