Deployment Models: Towards Eliminating Security Concerns From Cloud Computing

Gansen Zhao
School of Computer Science
South China Normal University, China
gzhao@scnu.edu.cn

Chunming Rong
Faculty of Science and Technology
University of Stavanger, Norway
chunming.rong.uis.no

Martin Gilje Jaatun
SINTEF ICT
Norway
Martin.G.Jaatun@sintef.no

Frode Eika Sandnes
Faculty of Engineering
Oslo University College, Norway
frodes@hio.no

ABSTRACT

Cloud computing has become a popular choice as an alternative to investing new IT systems. When making decisions on adopting cloud computing related solutions, security has always been a major concern. This article summarizes security concerns in cloud computing and proposes five service deployment models to ease these concerns. The proposed models provide different security related features to address different requirements and scenarios and can serve as reference models for deployment.

KEYWORDS: Cloud Computing, Deployment Models, Security Concerns, Cloud Security

1. INTRODUCTION

One of the identifying characters of cloud computing is that computing is delivered via the Internet as services. Computing and IT resources are encapsulated as services, hiding all the details of implementation, deployment, maintenance and administration. Computing will be shifted from on-premise systems to remote systems and users are connected to the IT infrastructure via the Internet. Individual organizations will lose their control of their IT systems to some extent, as the IT infrastructure is provided over the Internet and is likely leased from cloud operators.

With cloud computing, deployment of IT systems and data storage is changed from on-premises user-owned IT infrastructures to off-premises third-party IT infrastructures. Having the whole IT systems and data on infrastructures with limited controls creates an obstacle for migrating traditional IT systems and data into clouds, as users have the following concerns,

- Limited control over the IT infrastructure may incur security issues.
- Having the whole IT system and data on a single cloud may give the cloud operator excessive power for controlling and modifying users' IT system and data.

This article aims to develop deployment models for cloud computing based applications for addressing the security related concerns in cloud computing. We propose five different deployment models, which present the architecture for deploying IT systems based on cloud computing across multiple cloud providers. The proposed deployment models can address different issues that users are concerned about when deploying IT systems over cloud computing.

This article is organized is as follows. Section 2 identifies the security concerns that users have when adopting cloud computing. Section 3 surveys the related work. Section 4 presents five different deployment models to address the security concerns. Section 5 summarizes the security features provided by the models. Section 6 concludes the article and suggests possible future research.

978-1-4244-6830-0/10/$26.00 ©2010 IEEE

2. CLOUD SECURITY CONCERNS

Security concerns have been raised due to the new computing model introduced by cloud computing, which is characterized by off-premises computing, lost control of IT infrastructure, service-oriented computing, and virtualization, and so on. Security concerns from users can be briefly summarized as follows.

- Fault tolerance and service availability. When keeping data at remote systems owned by others, data owners may suffer from system failures of the service provider, as system failures will mean that data will become unavailable if the data depends on a single service provider. Similarly, when deploying IT systems over a single cloud, services may be unavailable if the cloud goes out of operation.
- Data migration. Users that adopt cloud computing may subject to the risk that their data cannot be migrated to other clouds. Without the capability of migrating data to other clouds, users may be forced to stay with a cloud if they have considerable dependence on the data.
- Data confidentiality and integrity. Data generated by cloud computing services are normally kept in the clouds as well. Keeping data in the clouds means users may lose control of their data and rely on cloud operators to enforce access control [23, 2], thus they may not be able to prevent unauthorized disclosure or malicious modification of their data.

These concerns have been identified in several earlier works [16, 2]. Armbrust et al. [2]. considered these concerns as the top three obstacles to growth of cloud computing, listed as Availability of Services, Data Lock-In, and Data Confidentiality and Auditability.

3. RELATED WORK

Extensive research efforts have been put into cloud computing and its related technologies, resulting in several well acknowledged cloud computing theories and technologies, including MapReduce [10] and its implementation Apache Hadoop [1], Microsoft Dryad [15], Condor DAGman [8], Eucalyptus [18], Nimbus [17], Reservoir [3], and CARMEN [6].

Various security related issues and concerns in cloud computing have been identified and are studied, including data privacy [19, 20, 16], data protection [9], access control [13, 7, 16], availability [24], authentication [25], scalability [27].

Armbrust et al. [2] identified ten obstacles to growth of cloud computing. The top three obstacles are actually very close to the concerns identified in Section 2, which are the issues that our proposed deployment models try to address.

Research in security patterns has established a structural way and a proven practice for secure system designs and implementations. They provide guidelines as well as knowledge that is proven and standardized [22, 12, 11, 5].

Domain security is a method developed by Qinetiq to develop architectural models for applications based on security requirements [14]. The architectures generated by the Domain Security method focus on the software engineering aspect of systems to implement, instead of security protocols, cryptographic operations, and so on.

4. REFERENCE DEPLOYMENT MODELS

In the following, we present five deployment models that address users' security concerns with cloud computing.

4.1. Separation Model

On the adoption of cloud computing, users are putting their applications and data onto a remote system that is not owned or controlled by them. The remote system operator has the complete power to control users' applications and data.

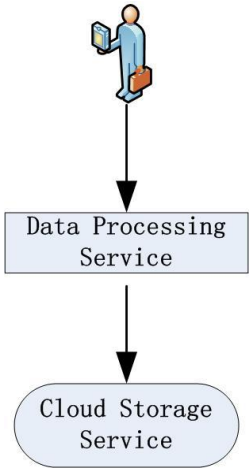

Figure 1. Separation Model

Figure 1 demonstrates a possible design based on the concept of separation of duty for cloud computing targeting a most basic case where data need to be processed and stored. The main idea is to have two independent services responsible for data processing and data storage. Data are presented to users and are processed by the Data Processing Service. When the data

need to be stored, they are handed over to the Cloud Storage Service, which will make the data persistent and ready for retrieval in the future.

To implement the separation model shown above, the following requirements must be met,

- At least two independent service providers are involved.
- The services should be provided by different providers respectively.
- Each service should be responsible for only one of the critical processes involved in a transaction.

The Separation Model mandates at least two different cloud computing service providers be involved in a transaction. To some extent, this prevents some frauds and errors by preventing any single service provider from having excessive control over the transactions.

4.2. Availability Model

Cloud computing users are normally concerned with service availability. Service providers may go out of service unexpectedly. If a single service provider going out of service could jeopardize the services users depend on, users will be seriously concerned about the availability of the services they need.

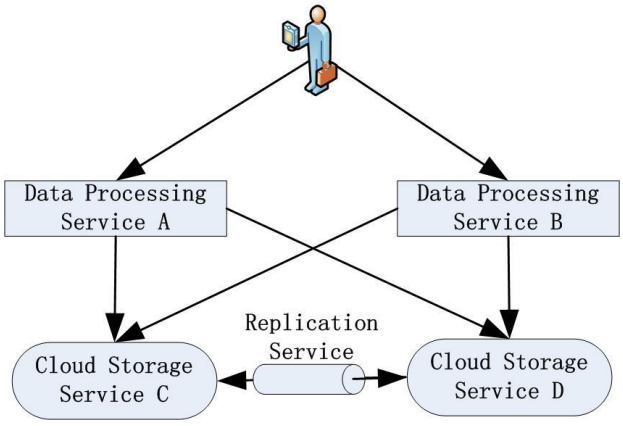

Figure 2. The Availability Model

Figure 2 illustrates the availability model built on top of a cloud infrastructure. With the availability model, a user can work on her data via a data processing service, and the data will be kept on a cloud storage service. To ensure the availability of the services, there are at least two independent data processing services, Data Processing Service A and Data Processing Service B respectively, and two independent data storage services, Cloud Storage Service C and Cloud Storage Service D respectively. Either one of the data processing services can have access to the data on either one of the cloud storage services. Data are replicated and synchronized via a Replication Service.

The Availability model imposes redundancy on both data processing and cloud storage. Hence there is no single point of failure with respect to data access. When a data processing service or a cloud storage service experiences failure, there is always a backup service present to ensure the availability of the data.

4.3. Migration Model

When data on clouds can only stay on the clouds where they are kept, users will be forced to stay with the clouds unless they decide to give up their data. This is not an acceptable situation.

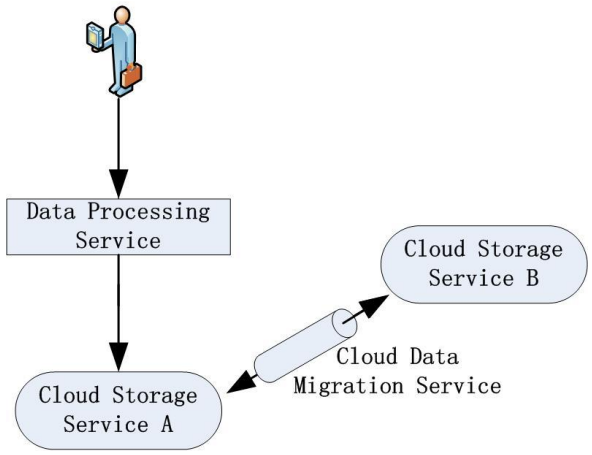

Figure 3. Migration Model

Figure 3 demonstrates the Migration model where the migration of data is guaranteed. Users process their data via a Data Processing Service, where the data are kept on Cloud Storage Service A. The Cloud Data Migration Service can interact with Cloud Storage Service A and another cloud storage service, namely Cloud Storage Service B. The Cloud Data Migration Service can move data from Cloud Storage Service A to Cloud Storage Service B, and vice versa. By being able to move data from Cloud Storage Service A to Cloud Storage Service B, users need not worry about their data being excessively controlled by a cloud provider, knowing that they can switch to another service provider by moving the data out from the current cloud storage service provider to another.

4.4. Tunnel Model

It is necessary to isolate the two service providers of the Separation Model by cutting all the direct communication

between them. Neither of the service providers should be able to identify each other. In this case, collusion can be prevented and filtering can be imposed on the communication between the two service providers.

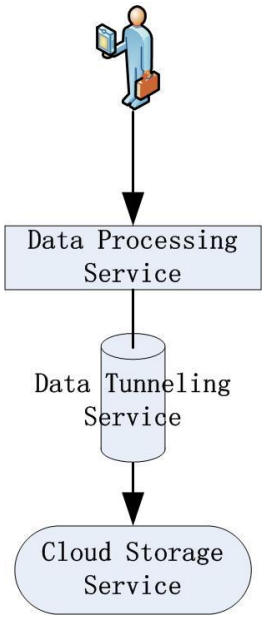

Figure 4. Tunnel Model

Figure 4 demonstrates the Tunnel Model. The Tunnel model introduces a tunnel service located between the Data Processing Service and the Data Storage Service. The tunnel servers as a communication channel between the Data Processing Service and the Cloud Storage Service. It is responsible for providing an interface for the two services to interact with each other, for manipulating and retrieving data. The tunnel can in fact be implemented as a service as well.

With the Tunnel Model, the Data Processing Service manipulates data based on the interface provided by the Data Tunneling Service. The Cloud Storage Service will not be able to relate the data it keeps with a specific data processing service. The Tunnel Model makes it extremely difficult for the Data Processing Service to collude with the Cloud Storage service for fraud.

4.5. Cryptography Model

For critical applications, the security of data, especially confidentiality and integrity, are key requirements. Data confidentiality and integrity are in most cases dependent on cryptography support.

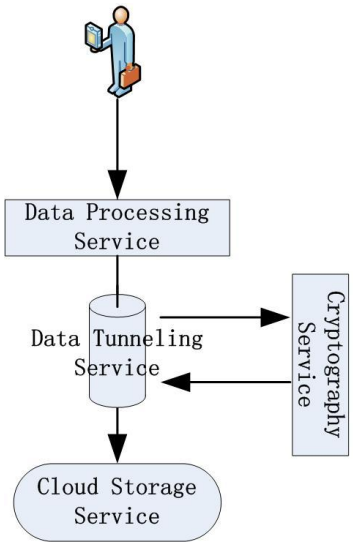

Figure 5. Cryptography Model

The Cryptography Model, as illustrated by Figure 5, augments the Tunnel Model with a Cryptography Service, which provides support for cryptographic operations on data. The Data Processing Service feeds data to the Data Tunneling Service for persistence. The Data Tunneling Service will invoke the Cryptography Service to perform a cryptographic operation on the data before handing the data over to the Cloud Storage Service. Thus the data kept by the Cloud Storage Service are cryptographically processed, meaning that they could be ciphertext that can only be read by those who have the decryption key, or they could be data augmented with digital signatures or message authentication codes, and so on, depending on the security requirements.

With the Cryptography Model, data can be stored in their cryptographically processed form. As the Data Tunneling Service hides the Cryptography Service from the Data Processing Service and the Cloud Storage Service, the cryptographic operations are transparent to the Data Processing Service and the Cloud Storage Service. The Data Processing Service and the Cloud Storage Service will not have access to the data without the cryptography key. Data access, such as reading and modifying the data, could be well protected by the cryptography key. In the case of encrypted data, the decryption key will be required. While in the case of digital signed data, all modification will need to be validated by producing new signatures with the needed keys.

5. MODEL ANALYSIS

Figure 6 shows the relationship between the models discussed in Section 4. The relations can be summarized as follows.

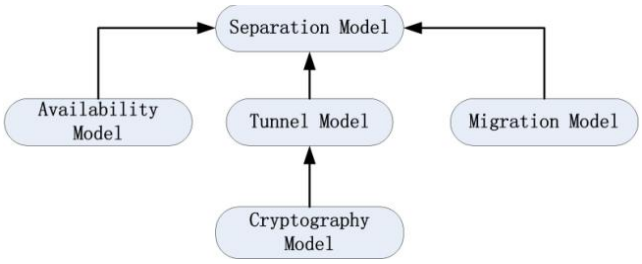

Figure 6. Relations between the Security Models

The Separation Model is the base model for all the other four models. It separates data storage from data processing, requiring at least two independent cloud computing providers to process data and to store data respectively. This can help ease users' concerns on having a single provider to have complete control over the data and the services they use.

The Availability Model introduces redundancy into the Separation Model, in both the data processing and the data storage, enabling the tolerance of a single service provider.

The Tunnel Model enhances the Separation Model by using a Tunnel Service to impose an isolation between the Data Processing Service and the Cloud Storage Service. The Tunnel Service prevents collusion by cutting the direct communications between the Data Processing Service and the Cloud Storage Service.

The Cryptography Model augments the Tunnel Model with cryptography support, such as data encryption, decryption, and digital signing. The Cryptography Model allows secure data storage transparent to Date Processing Service.

Note that, in Table 1, SM, AM, MM, TM, CM stand for Separation Model, Availability Model, Migration Model, Tunnel Model, and Cryptography Model respectively. Each of the five proposed models focus on different aspects of the security requirements, where the Separation Model serves as the base model for the other four models.

The proposed deployment models are different from existing work in the following aspects. Firstly, the techniques employed are mostly on the deployment level. Most of the previous work focus on implementation levels, such as cryptography protocols and algorithms [25, 23], design patterns for system design and implementation [12, 11], and internal control mechanisms [7, 9].

Secondly, the proposed models rely on inter-cloud interaction and require multiple clouds to cooperate. While existing work mostly investigate the techniques that can be used within a single system, such as the architecture for a network [21, 26], or techniques for building middleware or services [4, 11].

Table 1. Feature Summary

	Separation of Duty	Cross-clouds Service and Data Availability	Cross-clouds Fault Tolerance	Data Migration	Anti-collusion	Data Confidentiality	Data Integrity
SM	X						
AM	X	X	X				
MM	X			X			
TM	X				X		
CM	X				X	X	X

Thirdly, the proposed models are user oriented. Design and implementation techniques and methods are development oriented and are opaque for users. The deployment models require the cooperation of multiple clouds and create user awareness on it. By doing this, users' trust in deploying IT systems on cloud computing would be increased.

6. CONCLUSION

This article identifies the security concerns that users may have when adopting cloud computing, including fault tolerance and service availability, data migration, and data confidentiality and integrity. To eliminate these security concerns, five deployment models are proposed and described in detail, showing various architecture of deploying IT systems on cloud computing infrastructure. These deployment models are developed to address the security issues raised by the identified security concerns.

The proposed models are not without limitations. As the proposed models are at deployment architecture level, they do not include specific protocols and algorithms that can provide supports for confidentiality and integrity at cryptography level. Corresponding design patterns and interfaces should also be developed to allow cloud based

applications be deployed on clouds in the manners specified by the proposed models.

The contribution of this article is as follows. Firstly, This article identifies the three most important user concerns with respect to adopting cloud computing. We argue that these concerns are the major obstacles for users to adopt cloud computing. Secondly, this article proposes to eliminate the user concerns by using specific architecture for the deployment of IT systems on cloud computing. Thirdly, this article proposes five deployment models, each of which is developed to tackle specific issues raised by the users.

Future research on this work will include the development of corresponding design patterns and interfaces for cloud based applications to fit into the proposed deployment models and the investigation on integrating security protocols and algorithms with the proposed models to provide security supports at cryptography level.

REFERENCES

[1] Apache Hadoop, 2009. http://hadoop.apache.org/.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. “Above the clouds: A berkeley view of cloud computing”. Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley, Feb 2009.

[3] S. Beco, A. Maraschini, and F. Pacini. “Cloud computing and RESERVOIR project”. NUOVO CIMENTO DELLA SOCIETA ITALIANA DI FISICA C-COLLOQUIA ON PHYSICS, 32(2), Mar-Apr 2009.

[4] D. Bellebia and J.-M. Douin. “Applying patterns to build a lightweight middleware for embedded systems”. In PLoP ’06: Proceedings of the 2006 conference on Pattern languages of programs, pages 1–13, New York, NY, USA, 2006. ACM.

[5] B. Blakley and C. Heath. SECURITY DESIGN PATTERNS, 2004. The Open Group Security Forum.

[6] CARMEN, 2009. http://www.carmen.org.uk/.

[7] D. Chen, X. Huang, and X. Ren. “Access control of cloud service based on ucon”. In The First International Conference on Cloud Computing, pages 559–564, 2009.

[8] Condor DAGman, 2009. http://www.cs.wisc.edu/condor/dagman/.

[9] S. Creese, P. Hopkins, S. Pearson, and Y. Shen. “Data protection-aware design for cloud services”. In The First International Conference on Cloud Computing, pages 119–130, 2009.

[10] J. Dean and S. Ghemawat. “Mapreduce: simplified data processing on large clusters”. *Commun. ACM*, 51(1):107–113, 2008.

[11] E. B. Fernandez, J. Wu, M. M. Larrondo-Petrie, and Y. Shao. On building secure scada systems using security patterns. In CSIIRW ’09: Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research, pages 1–4, New York, NY, USA, 2009. ACM.

[12] T. Heyman, K. Yskout, R. Scandariato, and W. Joosen. “An analysis of the security patterns landscape”. In SESS ’07: Proceedings of the Third International Workshop on Software Engineering for Secure Systems, page 3, Washington, DC, USA, 2007. IEEE Computer Society.

[13] L. Hu, S. Ying, X. Jia, and K. Zhao. “Towards an approach of semantic access control for cloud computing”. In The First International Conference on Cloud Computing, pages 145–156, 2009.

[14] K. J. Hughes. “Domain Based Security: enabling security at the level of applications and business processes”, 2002. www.qinetiq.com.

[15] M. Isard, M. Budiu, Y. Yu, A. Birrell, and D. Fetterly. “Dryad: distributed data-parallel programs from sequential building blocks”. In EuroSys ’07: Proceedings of the 2nd ACM SIGOPS/EuroSys European Conference on Computer Systems 2007, pages 59–72, New York, NY, USA, 2007. ACM.

[16] L. Kaufman. “Data security in the world of cloud computing”. IEEE SECURITY & PRIVACY, 7(4), July-August 2009.

[17] Nimbus. “Introduction to nimbus”, 2009. http://workspace.globus.org/clouds/nimbus.html.

[18] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov. “The eucalyptus open-source cloud-computing system”. In Proceedings of Cloud Computing and Its Applications, October 2008.

[19] Å. A. Nyre and M. G. Jaatun. “Privacy in a semantic cloud: What’s trust got to do with it?”. In The First International Conference on Cloud Computing, pages 107–118, 2009.

[20] S. Pearson, Y. Shen, and M. Mowbray. “A privacy manager for cloud computing”. In The First International Conference on Cloud Computing, pages 90–106, 2009.

[21] K. Plobl, T. Nowey, and C. Mletzko. “Towards a security architecture for vehicular ad hoc networks”. In ARES ’06: Proceedings of the First International Conference on Availability, Reliability and Security, pages 374–381, Washington, DC, USA, 2006. IEEE Computer Society.

[22] M. Schumacher, E. Fernandez, D. Hybertson, and F. Buschmann. SECURITY PATTERNS:

INTEGRATING SECURITY AND SYSTEMS ENGINEERING. John Wiley & Sons, 2005.

[23] A. Singh, M. Srivatsa, and L. Liu. “Search-as-a-Service: Outsourced Search over Outsourced Storage”. *ACM TRANSACTIONS ON THE WEB*, 3(4), September 2009.

[24] T. Uemura, T. Dohi, and N. Kaio. “Availability analysis of a scalable intrusion tolerant architecture with two detection modes”. In The First International Conference on Cloud Computing, pages 178–189, 2009.

[25] L. Yan, C. Rong, and G. Zhao. “Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography”. In The First International Conference on Cloud Computing, pages 167–177, 2009.

[26] S. M. Youssef, A. B. Mohamed, and M. A. Mikhail. “An enhanced security architecture for wireless sensor network”. In DNCOCO’09: Proceedings of the 8th WSEAS international conference on Data networks, communications, computers, pages 216–224, Stevens Point, Wisconsin, USA, 2009. World Scientific and Engineering Academy and Society (WSEAS).

[27] G. Zhao, J. Liu, Y. Tang, W. Sun, F. Zhang, X. ping Ye, and N. Tang. “Cloud computing: A statistics aspect of users”. In The First International Conference on Cloud Computing, pages 347–358. Springer, 2009.