Journal of Supercomputing manuscript No.
(will be inserted by the editor)

Reference Deployment Models for Eliminating User Concerns on Cloud Security

Gansen Zhao · Chunming Rong · Martin Gilje Jaatun · Frode Eika Sandnes

Received: February 1, 2010 / Accepted: May 25, 2010

Abstract Cloud computing has become a hot topic both in research and in industry, and when making decisions on deploying/adopting cloud computing related solutions, security has always been a major concern. This article summarizes security related issues in cloud computing and proposes five service deployment models to address these issues. 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 · Cloud Security · Reference Deployment Model · Security Concerns

1 Introduction

Extensive research efforts have been put on cloud computing and its related technologies, resulting in several well acknowledged cloud computing theories and technologies.

Cloud computing is a collection of technologies that allow IT resources to be virtualized, used on an on-demand basis and delivered via the Internet as services.

Gansen Zhao, Ph.D., Associate Professor
School of Computer Science, South China Normal University
Guangzhou, China
E-mail: gzhao@scnu.edu.cn

Chunming Rong, Ph.D., Professor
Faculty of Science and Technology, University of Stavanger
Stavanger, Norway

Martin Gilje Jaatun
Department of Software Engineering, Safety and Security, SINTEF ICT
Trondheim, Norway

Frode Eika Sandnes, Ph.D., Professor
Faculty of Engineering, Oslo University College
Oslo, Norway

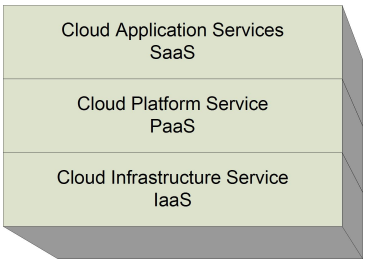

Fig. 1 Cloud Technology Stack

Hence, virtualization, utility computing, and service oriented computing are three of the most important underlying technologies.

Cloud computing is typically described as a three layer stack, with each layer providing its own services, as illustrated in Figure 1. The Cloud Infrastructure Service or the Infrastructure as a Service (IaaS) provides IT infrastructures as a service over computer networks. The Cloud Platform Service or the Platform as a Service (PaaS) delivers computing platforms as a service to sustain the cloud applications. The Cloud Application Services or Software as a Service (SaaS) delivers software as a service over the network, allowing users to use applications without having to install and run software on their own computers. The deployment models proposed in the rest of this article illustrate how applications can be deployed on the Cloud Platform and the way applications interact with each other.

One of the identifying characters of cloud computing is that computing is delivered via the Internet as services. This has the following implications.

- Computing and IT resource 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. Users are connected to the IT infrastructure via the Internet.
- Individual organizations will lose 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 an infrastructure 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, such as service availability due to failure of a single cloud operator, data confidentiality and integrity, and so on.
- 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. To be

specific, this article proposes five different deployment models, which present the architecture for deploying IT systems based on cloud computing across multiple cloud providers. This article argues that the proposed deployment models can address different issues that users are concerned about when deploying IT systems over cloud computing. The techniques used in addressing the user concerns include separating the duties across multiple cloud operators, providing redundancy across multiple clouds, mandating interaction between clouds, isolating different involved parties from each other for anti-collusion, and implementing cryptographic operations.

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.

2 Cloud Security Challenges

It has been suggested that cloud computing related security can be classified into three categories: cloud computing security, security for cloud computing, and cloud computing for security [12].

Cloud computing security refers to the security of a cloud computing system's infrastructure that guarantees system confidentiality, integrity and availability.

Security for cloud computing refers to the trust on the services that users enjoy when the users work with the services delivered using cloud computing technology.

Cloud computing for security involves using cloud computing technologies to develop and deliver security solutions for IT systems.

2.1 Security Threats

Several security threats towards cloud computing have been discussed. The security threats can be summarized as follows.

- Security threats from IT systems. Cloud computing systems are built on top of cloud computing providers' IT systems. It is inevitable that there are potential security weaknesses in these IT systems. These weaknesses will weaken the cloud computing services that are built on top.
- Security threats from external services. Users work on applications provided by cloud computing service providers. Details of the applications and the underlying services are not known to the users. Hence users cannot adopt any security protection on their own accord, and they will have to rely on the cloud computing service providers to ensure security.
- Security threats incurred by concentrated resources. Cloud computing concentrates various IT resources to provide extreme capacity beyond any individual IT systems. The large amount of concentrated resources will attract the attentions of malicious users and become attractive targets for attacks.

2.2 Users' 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, 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 be 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 [40, 6], 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 [24, 6]. Armbrust et al. [6]. 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 [15] and its implementation Apache Hadoop [5], Microsoft Dryad [23], Microsoft DryadLINQ [46], and Condor DAGman [13].

A few cloud platforms and cloud infrastructures have been reported, including Eucalyptus [16, 32], Nimbus [31], Kupa [27], Wispy [42], CARMEN [10]. The industry is providing services based on cloud computing technologies, such as Amazon EC2 [1], Amazon Simple Storage Service [2], Microsoft Live Mesh [29], Salesforce [37], Google File System [18], and Google App Engine [19], and so on.

3.1 Security Concerns

Armbrust et al. [6] identified ten obstacles to growth of cloud computing, arguing that these were the most ten important obstacles. The identified obstacles include availability of service, data lock-in, data confidentiality and auditability, data transfer bottlenecks, performance upredictability, scalable storage, bugs in large distributed systems, scaling quickly, reputation fate sharing, and software licensing. The top three

obstacles are actually very close to the concerns identified in Section 2.2, which are the issues that our proposed deployment models try to address.

Various security related issues and concerns in cloud computing have been identified and are under study, including data privacy [33,34,24], data protection [14], access control [21,11,24], availability [41], authentication [43,28], scalability [47], and so on.

3.2 Cloud Security

Several banks have experience with security infrastructure provided as cloud computing services. Boiling Springs Savings Bank and Ulster Savings Bank relied on a security-on-demand provider's security services to maintain their internal networks' security compliance with related regulation [3,4]. Both banks reported that a higher level of security had been achieved with lower cost.

Cloud storage, which is in fact a form of data storage outsourcing, incurs concerns on data security, such as data integrity and data confidentiality. Singh et al. [40] proposed an indexing scheme that can build indices with access control information for searching encrypting data, to implement access control on the searching of encrypted outsourced data kept on a cloud.

3.3 Security Patterns

Security patterns have been accepted as a structural way and an established practice for secure system designs and implementations. They provide guidelines as well as knowledge that is proven and standardized [39,20].

Existing security patterns include the ROLE pattern [44], the ASSET VALUATION pattern [38], the ROLE BASED ACCESS pattern [26], the REPLICATED SYSTEM pattern [9], and others [30,9]. Successful cases have been reported on applying security patterns in building critical infrastructures and secure systems, such as [17] and [8].

3.4 Architectural Models

Domain security is a method developed by Qinetiq to develop architectural models for applications based on security requirements [22,36]. 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.

The study reported in [45] presents architecture for the provision of basic properties of data secrecy, authentication, and replay protection for ad hoc networks. The architecture relies on cryptography techniques to implement the properties.

The RESERVOIR project [7] aims to develop architecture for multiple cloud providers to dynamically federate with each other to construct a seemingly infinite pool of IT resources with the autonomy of technological and business management decisions preserved.

Keahey et al. [25] suggests that with the emergence of cloud computing, virtual sites can be constructed over distributed resources spanning several clouds.

In a priliminary work [48], we have proposed to address cloud computing security concerns at architecture levels, by using specifically designed architectures.

4 Reference Deployment Models for Cloud Computing Security

We have devised five reference deployment models for cloud computing that progressively address user security concerns; the separation model, availability model, migration model, tunnel model, and encryption model. In the following, we describe a typical scenario and the details of each model.

4.1 Separation

4.1.1 Scenario

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 users will rely heavily on the remote system. This means that the remote system operator can potentially abuse its power by modifying the data at will and by refusing service requests from the users, and so on. This concern could reduce users' trust in cloud computing to a level where they will not put any critical applications or data onto the cloud.

4.1.2 Separation Model

One of the key internal control mechanisms, separation of duty, is a very important method to prevent fraud, errors, and abuse of privileges. To implement separation of duty, it is required that at least two or more principals are involved in any single transaction. Each principal is responsible for only part of the transaction. The basic principle is to split the duties among the principals such that none of the principals would have excessive control over critical processes.

Figure 2 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 by the Data Processing 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.

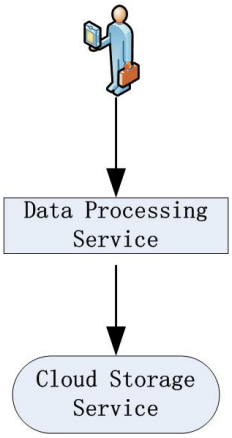

Fig. 2 Separation Model

The Separation Model mandates that 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

4.2.1 Scenario

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

4.2.2 Availability Model

An availability model similar to the banking system for cloud computing can be developed to ensure the availability of users' data. Figure 3 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. Either one of the data processing services can have access to the data on either one of the cloud storage service. Data are replicated and synchronized via a Replication Service.

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

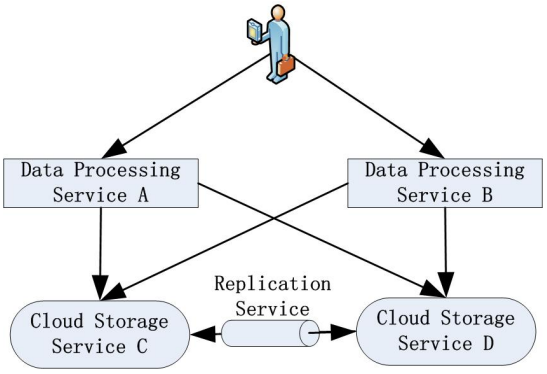

Fig. 3 The Availability Model

- There exist at least two independent cloud computing providers that provide equivalent Data Processing Services, and two independent cloud computing providers that provide equivalent Data Storage Services.
- Replication of data between the two cloud storage services should be bi-directional as well as transparent to users.
- Data from either of the cloud storage services are available to all the Data Processing services, provided that the required credentials are presented.

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

4.3.1 Scenario

When data on clouds are forced to stay on the cloud platforms where they are kept, users will be forced to stay with the cloud providers unless they decide to give up their data. Cloud providers can then ask for premium fees for their services, which could be far beyond reasonable. This is not an acceptable situation when the users heavily depend on the data or the data otherwise are critical.

As a result, these users will adopt cloud computing only when they are assured that their data can be freely migrated to other clouds. Therefore, a model that can ensure the capability of migrating data from one cloud to another is imperative in this case.

4.3.2 Migration Model

Figure 4 demonstrates a 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

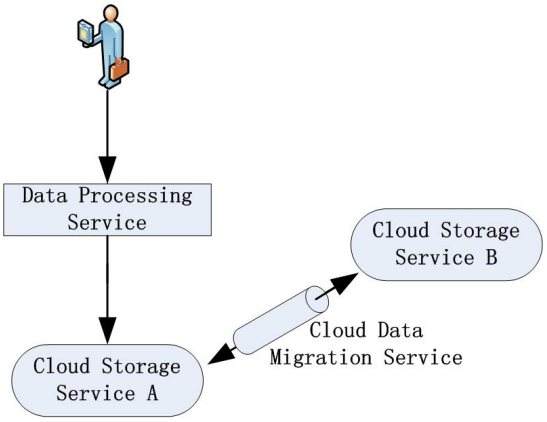

Fig. 4 Migration Model

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. In this way, 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.

To implement the Migration Model, the following requirements must be met.

- There is a Cloud Data Migration Service that can interact with the Cloud Storage Service that keeps users' data for exporting users' data.
- There is a second Cloud Storage Service that allows users to import data and export data.
- The two Cloud Storage Services should be provided by two independent cloud providers.

4.4 Tunnel

4.4.1 Scenario

The Separation model described in Section 4.1 separates the processing from the storing of data for the purpose of preventing frauds and errors. It is effective with the assumption that the two service providers will not collude with each other. To ensure the assumption, it is necessary to isolate the two service providers by cutting all the direct communication between them. In this case, neither of the service providers will be able to identify each other, and filtering can be imposed on the communication between the two service providers.

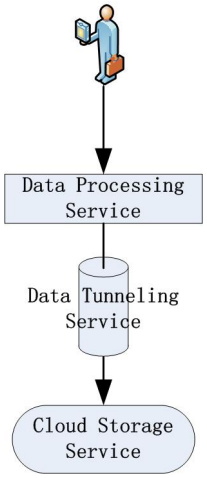

Fig. 5 Tunnel Model

4.4.2 Tunnel Model

Figure 5 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 Data Processing Service does not need to care about details of the Cloud Storage Service, such as location, identity, etc. On the other hand, the Cloud Storage Service will not be able to relate the data it keeps with a specific data processing service. This achieves a complete isolation between data processing and data storage, as well as the two service providers. It will be extremely difficult for the Data Processing Service to collude with the Cloud Storage service for fraud.

4.5 Cryptography

4.5.1 Scenario

Both the Separation Model and the Tunnel Model isolates the service provider responsible for storing data from the service provider responsible for processing data, preventing the Data Processing service from arbitrary manipulation of the data. But they are incapable of preventing unauthorized data disclosure or unauthorized modification on the data by the Cloud Storage Service. The confidentiality and integrity cannot be ensured.

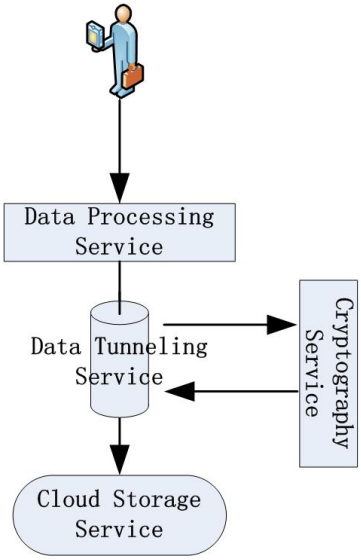

Fig. 6 Cryptography Model

4.5.2 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.

The Cryptography Model, as illustrated by Figure 6, 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.

On accessing the data, the Data Tunneling Service will first retrieve the encrypted data from the Cloud Storage Service. The retrieved data are then decrypted by the Cryptography Service if they are encrypted, or are verified by the Cryptography Service if they are associated with digital signatures or message authentication codes, etc. The decrypted data would then be sent to the Data Processing Service for processing.

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

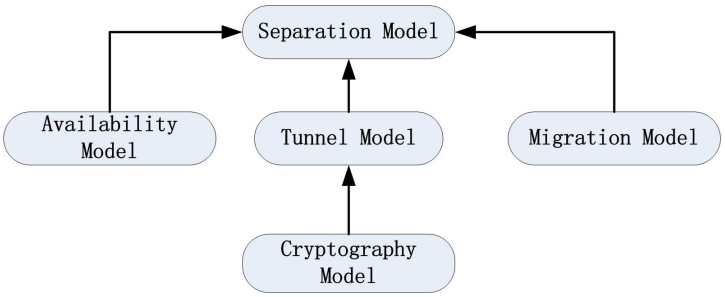

Fig. 7 Relations between the Security Models

data without the cryptographc key. Data access, such as reading and modifying the data, is well protected by cryptography. 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 7 shows the relationship between the models discussed in Section 4. The relations can be summarized as follows.

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. With the redundancy in the Availability Model, failures of one data processing service and one data storage service can be tolerated.

The Tunnel Model further 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, assuming that it is very unlikely for two isolated providers to collude. The Tunnel Service can also be used to impose filtering on the communications between the Data Processing Service and the Cloud Storage Service to enforce security policies.

The Cryptography Model augments the Tunnel Model with cryptography support, such as data encryption, decryption, and digital signing. The Cryptography Model allows transparent secure data storage by encrypting the data before storing and decrypting the data on access, and it can also prevent unauthorized modification by associating digital signatures with the data. Depending on the security requirements, cryptography support can be adjusted differently to fit into the application scenarios.

Note that, in Table 1, SM, AM, MM, TM, CM stand for Separation Model, Availability Model, Migration Model, Tunnel Model, and Cryptography Model respec-

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

Table 1 Feature Summary

tively. 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.

Note also that, the proposed models can be combined together to implement more security features than a single model. For example, the Migration Model can be combined with the Cryptography Model, in which case the combined model can provide data migration, anti-collusion, data confidentiality, and data integrity.

5.1 Model Comparison

The proposed deployment models are different from existing work in the following aspects.

- The techniques employed are mostly on the deployment level. Most of the previous work focuses on implementation levels, such as cryptography protocols and algorithms [28,43,40], design patterns and for system design and implementation [20,30,38,26,8,17], and internal control mechanisms [21,11,14], and so on. These techniques and research relate to the internal implementation, instead of the deployment architecture.
- The proposed models rely on inter-cloud interaction and require multiple clouds to cooperate. All five proposed deployment models require the involvement of at least two clouds, while existing work mostly investigate the techniques that can be used within a single system, such as the architecture for a network [35, 45,44], or techniques for building middleware or services [8,17] . The scope of the security provided by these existing techniques is confined to the domain of homogeneous systems.
- The proposed models are user oriented. Design and implementation techniques/methods are development oriented and are opaque for users. Most users will not see the difference between two systems built on different design and implementation techniques, unless the techniques are user interface related. The deployment models require the cooperation of multiple clouds and create user awareness with respect to this concept. By doing this, users' trust in deploying IT systems on cloud computing would be increased.

5.2 Compatibility

The proposed deployment models assume that the cloud services involved are compatible with each other. The compatibility could be guaranteed by defining standardized interaction interfaces between the cloud services. This will include the following.

- Data Access Interface (DAI). DAI should be implemented by the Cloud Storage Service and used by the Data Processing Services to access data on the Cloud Storage Service.
- Data Replication Interface (DRI). DRI should be implemented by the Cloud Storage Service and used by the Data Replication Service to synchronize data between two Cloud Storage Services.
- Data Migration Interface (DMI). DMI should be implemented by the Cloud Storage Service and used by Cloud Data Migration Service to export data from and import data into Cloud Storage Services.
- Data Tunneling Interface (DTI). DTI should be implemented by the Data Tunneling Service and used by the Data Processing Service tunnel DAI interactions.

Once these interfaces are defined and implemented by the corresponding services, the services will be able to interoperate with each other as expected by the proposed deployment models.

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 their limitations. As the proposed models are at deployment architecture level, they do not include specific protocols and algorithms that can provide supports on confidentiality and integrity at cryptography level. Corresponding design patterns and interfaces should also be developed to allow cloud based applications can be deployed on clouds in the manners specified by the proposed models.

6.1 Contributions

The contribution of this article is five fold.

- This article has presented a review on related research, providing a clear overview of the current progress of related work.
- 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.

- This article proposes to eliminate the user concerns by using specific architecture for the deployment of IT systems on cloud computing.
- This article proposes five deployment models, each of which is developed to tackle specific issues raised by the users.
- This article, to the best knowledge of the authors, is the first article that proposes user oriented methods to increase users' trust on cloud computing.

6.2 Future Research

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 support at cryptography level. We also find providing support for these deployment models at platform level interesting. In this case, by federating one or more clouds, they can cooperate to allow user applications be deployed in the proposed way in a transparent manner.

To a large extent, our deployment models solve the challenges regarding privacy and confidentiality of data at rest, but there still remains the issue of users having to trust the cloud data processing provider and/or the cloud cryptography service provider with their data. A fundamental area of further work on the technology side is thus to devise cloud data processing services that function without having access to a customer's complete data in clear text. A possible approach to this would be to extend the availability model to let each data processing provider only process parts of the customer's data, returning the complete results (via the encrypted tunnel model) only to the customer.

Acknowledgements The work is partially supported by the National Natural Science Foundation of China (Grant No.60970044, Grant No.60940033), the National Key Technology R&D Program (Grant No.2008BAH24B03), the China Postdoctoral Science Foundation (Grant No. 20080440121), and by Telenor through the SINTEF-Telenor research agreement.

References

1. Amazon Elastic Compute Cloud (EC2), 2009. http://www.amazon.com/ec2/.
2. Amazon Simple Storage Service, 2009. http://aws.amazon.com/s3.
3. Anonymous. Bank outsources security to the cloud. *COMMUNICATIONS NEWS*, 42(12), December 2005.
4. Anonymous. Bank trusts security to 'the cloud'. *COMMUNICATIONS NEWS*, 43(9), September 2006.
5. Apache Hadoop, 2009. http://hadoop.apache.org/.
6. Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia. Above the clouds: A berkeley view of cloud computing. Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley, Feb 2009.
7. 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.

8. 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.
9. B. Blakley and C. Heath. Security design patterns, 2004. The Open Group Security Forum.
10. CARMEN, 2009. http://www.carmen.org.uk/.
11. Danwei Chen, Xiuli Huang, and Xunyi Ren. Access control of cloud service based on ucon. In *The First International Conference on Cloud Computing*, pages 559–564, 2009.
12. CIE Cloud Computing Expert Committee. Cloud computing white paper. Technical report, Chinese Institute of Electronics, 2010.
13. Condor DAGman, 2009. http://www.cs.wisc.edu/condor/dagman/.
14. Sadie Creese, Paul Hopkins, Siani Pearson, and Yun Shen. Data protection-aware design for cloud services. In *The First International Conference on Cloud Computing*, pages 119–130, 2009.
15. Jeffrey Dean and Sanjay Ghemawat. MapReduce: simplified data processing on large clusters. *Commun. ACM*, 51(1):107–113, 2008.
16. Eucalyptus, 2009. http://eucalyptus.cs.ucsb.edu/.
17. Eduardo B. Fernandez, Jie Wu, M. M. Larrondo-Petrie, and Yifeng 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.
18. Sanjay Ghemawat, Howard Gobioff, and Shun-Tak Leung. The Google File System. *SIGOPS Oper. Syst. Rev.*, 37(5):29–43, 2003.
19. Google App Engine, 2009. http://appengine.google.com.
20. Thomas Heyman, Koen Yskout, Riccardo Scandariato, and Wouter 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.
21. Luokai Hu, Shi Ying, Xiangyang Jia, and Kai Zhao. Towards an approach of semantic access control for cloud computing. In *The First International Conference on Cloud Computing*, pages 145–156, 2009.
22. K J Hughes. Domain based security: enabling security at the level of applications and business processes, 2002. www.qinetiq.com.
23. Michael Isard, Mihai Budiu, Yuan Yu, Andrew Birrell, and Dennis 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.
24. LM. Kaufman. Data security in the world of cloud computing. *IEEE SECURITY & PRIVACY*, 7(4), July-August 2009.
25. K. Keahey, M. Tsugawa, and A. Matsunaga. Sky computing. *IEEE INTERNET COMPUTING*, 13(5), Sep-Oct 2009.
26. S.R. Kodituwakku, P. Bertok, and L. Zhao. Aplrac: A pattern language for designing and implementing role-based access control. In *EuroPLoP'01*, 2001.
27. Kupa, 2009. http://meta.cesnet.cz/cms/opencms/en/docs/clouds/.
28. Hongwei Li, Yuanshun Dai, Ling Tian, and Haomiao Yang. Identity-based authentication for cloud computing. In *The First International Conference on Cloud Computing*, pages 157–166, 2009.
29. Microsoft Live Mesh, 2009. http://www.mesh.com/.
30. K. Maruyama N. Yoshioka, H. Washizaki. A survey on security patterns. *Progress in Informatics*, pages 35–47, 2008.
31. Nimbus, 2009. http://workspace.globus.org/.
32. Daniel Nurmi, Rich Wolski, Chris Grzegorczyk, Graziano Obertelli, Sunil Soman, Lamia Youseff, and Dmitrii Zagorodnov. The eucalyptus open-source cloud-computing system. In *Proceedings of Cloud Computing and Its Applications*, October 2008.
33. Åsmund Ahlmann Nyre and Martin Gilje 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.
34. Siani Pearson, Yun Shen, and Miranda Mowbray. A privacy manager for cloud computing. In *The First International Conference on Cloud Computing*, pages 90–106, 2009.
35. Klaus Plobl, Thomas Nowey, and Christian 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.
36. Qinetiq. Domain Based Security - User Guide No 2: Introduction to Infosec Architecture Models, November 2003. www.qinetiq.com.

37. Salesforce, 2009. http://www.salesforce.com/.
38. M. Schumacher, E. Fernandez-Buglioni, D. Hybertson, F. Buschmann, and P. Sommerlad. *Security Patterns*. Wiley, 2006.
39. Markus Schumacher, Eduardo Fernandez, Duane Hybertson, and Frank Buschmann. *Security Patterns: Integrating Security and Systems Engineering*. John Wiley & Sons, 2005.
40. 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.
41. Toshikazu Uemura, Tadashi Dohi, and Naoto 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.
42. Wispy. A cloud computing testbed, 2009. http://www.rcac.purdue.edu/teragrid/resources/#wispy.
43. Liang Yan, Chunming Rong, and Gansen 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.
44. Joseph Yoder and Jeffrey Barcalow. Architectural patterns for enabling application security. In *PLoP*, 1997.
45. Sherin M. Youssef, A. Baith Mohamed, and Mark 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).
46. Yuan Yu, Michael Isard, Dennis Fetterly, Mihai Budiu, úlfar Erlingsson, Pradeep K. Gunda, and Jon Currey. DryadLINQ: A System for General-Purpose Distributed Data-Parallel Computing Using a High-Level Language. In *Proceedings of the 8th Symposium on Operating Systems Design and Implementation (OSDI '08)*, San Diego, CA, December 2008.
47. Gansen Zhao, Jiale Liu, Yong Tang, Wei Sun, Feng Zhang, Xiao ping Ye, and Na Tang. Cloud computing: A statistics aspect of users. In Martin Gilje Jaatun, Gansen Zhao, and Chunming Rong, editors, *The First International Conference on Cloud Computing*, volume 5931 of *Lecture Notes in Computer Science*, pages 347–358. Springer, 2009.
48. Gansen Zhao, Chunming Rong, Martin Gilje Jaatun, and Frode Eika Sandnes. Deployment Models: Towards Eliminating Security Concerns From Cloud Computing. In *The First International Workshop on Cloud Computing Interoperability and Services*, June 2010.