Computers and Electrical Engineering 39 (2013) 47–54

Contents lists available at SciVerse ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Beyond lightning: A survey on security challenges in cloud computing ☆

Chunming Rong [a], Son T. Nguyen [a,*], Martin Gilje Jaatun [b]

[a] *Department of Electrical Engineering and Computer Science, University of Stavanger, 4036 Stavanger, Norway*
[b] *Department of Software Engineering, Safety and Security, SINTEF ICT, 7465 Trondheim, Norway*

ARTICLE INFO

Article history:
Available online 19 May 2012

ABSTRACT

Cloud computing is a model to provide convenient, on-demand access to a shared pool configurable computing resources. In cloud computing, IT-related capabilities are provided as services, accessible without requiring detailed knowledge of the underlying technologies, and with minimal management effort. The great savings promised by the cloud are however offset by the perceived security threats feared by users. This paper gives an overview of cloud computing, and discusses related security challenges. We emphasize that although there are many technological approaches that can improve cloud security, there are currently no one-size-fits-all solutions, and future work has to tackle challenges such as service level agreements for security, as well as holistic mechanisms for ensuring accountability in the cloud.

1. Introduction

According to Google's Kevin Marks, the term "cloud computing" comes "from [the] early days in the Internet where we drew the network as a cloud. We didn't care where the message went… the cloud hid it from us" [1]. The National Institute of Standards and Technology (NIST) has defined cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources, e.g. networks, servers, storage, applications, and services, that can be rapidly provisioned and released with minimal management effort or service provider interaction [2].

In contrast to the conventional computing model, where end-user data and computing power are located in the users' computer systems, cloud computing resources are provided in massive, abstracted (virtualized) infrastructures managed by professional service providers [3]. The cloud model simplifies installation, operation and maintenance of information systems, and reduces costs while increasing system reliability and efficiency. A cloud system is also user friendly, in the respect that it requires less expertise to use. One can draw the analogy with current electricity and running-water systems, where end-users can use services from providers with ease, without being concerned with the technical complexity behind those systems.

Cloud computing can provide elastic resources with dynamic provisioning and scaling based on user demands. This approach is intended to deal with both resource over-provisioning, i.e., more resources than needed are allocated, and resource under-provisioning, i.e., fewer resources than required are allocated. The elastic management yields better overall system resource usage and hence increases system efficiency.

In previous work [4], we have discussed the MapReduce programming model and its impact on cloud computing, and we will not cover this further here. This paper gives an overview of cloud computing and related security challenges, and highlights some areas for further work. The rest of this paper is organized as follows: Section 2 introduces different classifications

☆ Reviews processed and proposed for publication to Editor-in-Chief by Associate Editor Dr. Taeshik Shon.
* Corresponding author.
E-mail addresses: chunming.rong@uis.no (C. Rong), sonnt@ux.uis.no (S.T. Nguyen), martin.g.jaatun@sintef.no (M.G. Jaatun).

0045-7906/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.compeleceng.2012.04.015

of cloud computing. In Section 3, we review security challenges that cloud computing needs to address. Section 4 briefly discusses how Service Level Agreements (SLAs) in cloud computing could be extended to also cover security aspects. Section 5 presents a solution to provide trusted data sharing over public cloud storage. Section 6 briefly sketches some important issues regarding accountability in the cloud. Finally, Section 7 concludes the paper.

2. Cloud computing classification

Although "cloud computing" is a relatively new and emerging term, many believe that other forms of "cloud" existed long before the term was introduced. Though referred to by different names, other technologies and concepts have been developed and used to form the current cloud computing technology.

The first cloud-like technology ("Cloud 1.0") resulted from the abstraction of TCP/IP layers, where network devices communicate with one another by complying with TCP/IP protocol specifications without knowing exactly where and who the other one is. The abstraction of World Wide Web data, where documents can be published and retrieved from the web without users on beforehand knowing exactly where they are located or who published them can be considered the next cloud technology ("Cloud 2.0"). The current brand of cloud computing ("Cloud 3.0") is the abstraction of infrastructure complexities of servers, applications, data, and heterogeneous platforms where the infrastructure, servers, or applications can be used without knowing exactly where they are located. Note that this development of the internet can also be plotted along other axes, for instance the semantic web, which among other things facilitates semantic search [5], is one such aspect which is not directly related to cloud computing, but may still be seen as something which is *enabled* by the cloud computing paradigm [6]. Cloud-like structures are also emerging in other domains such as process control systems [7] and smart grid constellations [8]; in the latter case, the Advanced Metering Infrastructure [9] is physically bringing this "always-on" aspect into people's homes. Eventually, we expect to see a merger of all such domain-specific networks into a single global cloud, as has long been a vision of telecom operators [10].

Cloud computing is typically classified based on either their deployment or service models. Fig. 1 represents cloud models based on the NIST definition framework [1]. Cloud deployment models can be classified as private, public, community, and hybrid cloud.

- A **Private cloud** is owned or rented by an organization. The whole cloud resource is dedicated to that organization for its private use. An example of this model is a cloud built by an enterprise to serve their business critical applications.
- A **Public cloud** is owned by a service provider and its resources are sold to the public. End-users can rent parts of the resources and can typically scale their resource consumption up (or down) to their requirements. Amazon, Google, Rackspace, Salesforce, and Microsoft are examples of public cloud providers.
- A **Community cloud** is similar to a private cloud, but where the cloud resource is shared among members of a closed community with similar interests. An example of a community cloud is the Media Cloud set up by Siemens IT Solutions and Services for the media industry [11]. A community cloud may be operated by a third party (as in the Siemens case), or may be controlled and operated in a collaborative fashion as in the Grid Computing paradigm.
- A **Hybrid cloud** is the combination of two or more cloud infrastructures; these can be either private, public, or community clouds. The main purpose of a hybrid cloud is usually to provide extra resources in cases of high demand, for instance enabling migrating some computation tasks from a private cloud to a public cloud.

Cloud service models are typically classified as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), though slightly different classifications also exist.

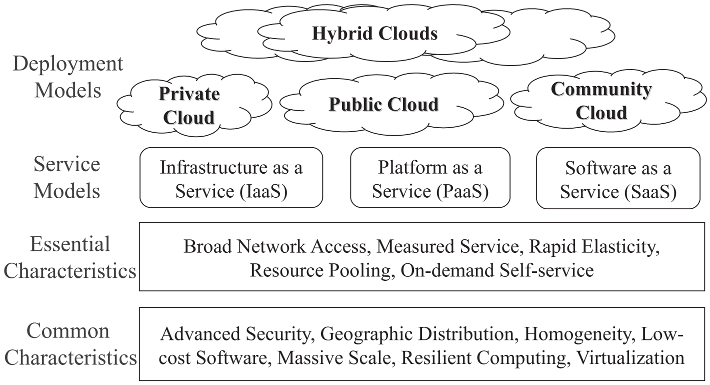
Hybrid Clouds
Deployment Models
Private Cloud
Public Cloud
Community Cloud
Service Models
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)
Essential Characteristics
Broad Network Access, Measured Service, Rapid Elasticity, Resource Pooling, On-demand Self-service
Common Characteristics
Advanced Security, Geographic Distribution, Homogeneity, Low-cost Software, Massive Scale, Resilient Computing, Virtualization

Fig. 1. The NIST cloud definition framework [1].

- Cloud **SaaS** is the use of applications running on a cloud infrastructure to provide services to end-users. SaaS can deliver business applications such as customer relationship management (CRM), enterprise resource planning (ERP), and accounting. Examples of cloud SaaS are Google Apps [12] and Salesforce CRM [13]. The consumer does not control underlying infrastructure.
- Cloud **PaaS** is the use of tools and resources running on a cloud infrastructure to provide services to end-users. The applications are developed and/or acquired by end-users on top of the tools provided. Microsoft Windows Azure [14] and Google App Engine [15] are examples of cloud PaaS. The consumer does not control the underlying infrastructure or operating systems, but does control deployment of individual applications.
- Cloud **IaaS** is the use of fundamental computing resources, e.g. storage, networks, servers, to provide services to end-users. The end-users can deploy and run arbitrary software including both applications and operating systems. An example of IaaS is Amazon EC2 [16]. The consumer does not control the underlying infrastructure, but can typically launch virtual machines with chosen operating systems which in turn are managed by the consumer.

With its many advantages, cloud computing is currently being used in large corporations such as Google, Yahoo, Amazon and Facebook. It is also beneficial for startups, as it saves their initial investment cost. Dropbox [17] and Groupon [18] are examples of startups that utilize cloud computing for their daily operations. It is a trend that other companies are moving their applications to the cloud to reduce investment and operation costs and to increase their business efficiency [19].

3. Cloud computing security challenges

The benefits introduced by cloud computing are legion. According to IDC [20], the most beneficial aspects of using cloud include fast and easy deployment, the pay-per-use model, and reduction of in-house IT costs. However, they also point out that security is the most important issue to be addressed in order to promote the widespread use of cloud computing.

Cloud computing providers need to solve the common security challenges of traditional communication systems. At the same time, they also have to deal with other issues inherently introduced by the cloud computing paradigm itself. In this section, we have categorized the main cloud security issues as *traditional* and *new cloud* security challenges.

3.1. Traditional security challenges

Although the security concerns in traditional communication systems also apply to the cloud, the use of cloud computing introduces new attack vectors that will make attacks either possible or simply easier to carry out.

The authentication and authorization applications for enterprise environments may need to be changed to work with a cloud environment. Forensics tasks may become much more difficult since the investigators may not be able to access system hardware physically. The availability of cloud service providers is also a big concern, since if the cloud service is disrupted, it affects more customers than in the traditional model. For example, the recent disruption of the Amazon cloud service took down a number of websites including Reddit, Foursquare, and Quora. Last but not least, virtual machine security is also a problem. The hypervisor and virtual machines used in cloud providers may also have vulnerabilities, as exemplified by Xen [21]. Such vulnerabilities represent an even more serious problem in multi-tenant environments, where the compromise of a virtual machine can affect all users on the same physical server.

Cloud providers, therefore, might need to reconsider traditional security concerns from different angles.

3.2. Cloud security challenges

As end-users utilize the cloud services and store their data in the provider's infrastructure, the most critical security concern is about privacy and user data confidentiality. End-users want to know where their information is stored, and who is in control of that information in addition to the owners. They also want to be guaranteed that the critical information is not accessed and used illegally, even by the cloud providers. Section 5 in this paper is dedicated to discuss a solution for data leakage prevention and privacy when storing data in the cloud. This section discusses other important security challenges when using cloud services, including:

- *Resource location*: end-users use the services provided by the cloud providers without knowing exactly where the resources for such services are located, possibly in other legislative domains. This poses a potential problem when disputes happen, which is sometimes beyond the control of cloud providers.

  Data stored at the cloud service providers is not only affected by the provider policies but also by the legislation of countries where the providers reside. When using such services, users have to agree to the "Terms of Service" which grant the providers the right to disclose user information in compliance with laws and law enforcement requests, for example, as noted in the recent Dropbox's Terms of Service [22]. The European Union has issued Directive 95/46/EC [23] to protect user privacy. The directive prohibits transfers of personal data to countries which do not ensure an adequate level of protection.[1] The transfer of personal data outside EU countries is legally possible if it is done with the owner's consent or if it is

[1] Articles 25 and 26 in the directive.

done to a country having "safe harbor principle"[2] agreements with EU, or under some other special cases as mentioned in article 26 of the directive. However, implementation and enforcement of this directive beyond the EU border in the general case remains an open challenge.

- *Multi-tenancy issue*: this issue poses a challenge to protect user data against unauthorized access from other users running processes on the same physical servers. This is in fact not a new issue taking into consideration the current concern with web hosting services. However, with the widespread use of cloud computing and with the fact that users store more important data in the cloud, this issue needs to be reconsidered seriously.
- *Authentication and trust of acquired information*: as the critical data is located in the cloud provider infrastructure, the data may be altered without the owner's consent. The modified data may then be retrieved and processed by the owner to make critical decisions. The authenticity of the data in this case is very important, and therefore needs to be guaranteed. However, common standards to ensure data integrity do not exist.
- *System monitoring and logs*: as more business critical applications are migrated to the cloud, customers may request that cloud providers provide more monitoring and log data for the customers' personnel. As the results of monitoring and logs may contain sensitive infrastructure information, and are traditionally used internally by the providers, sharing parts of such data to either customers or third-party examiners is not something all cloud providers are willing to do. It will require a lot of negotiation between cloud providers and customers to come up with appropriate monitoring and log information as part of any service agreement.
- *Cloud standards*: standards are needed across different standard developing organizations to achieve interoperability among clouds and to increase their stability and security. For example, the current storage services by a cloud provider may be incompatible with those of other provider. In order to keep their customers, cloud providers may introduce so-called "sticky services" which create difficulty for the users if they want to migrate from one provider to the other, e.g., Amazon's S3 is incompatible with IBM's Blue Cloud or Google storage.

  There are currently a large number of standards bodies with different interests, e.g. IEEE Cloud Computing Standard Study Group (IEEE CCSSG) [24], ITU Cloud Computing Focus Group [25], Cloud Security Alliance (CSA) [26], Distributed Management Task Force (DMTF) [27], Storage Networking Industry Association (SNIA) [28], Open Grid Forum (OGF) [29], Open Cloud Consortium (OCC) [30], and Organization for the Advancement of Structured Information Standards (OASIS) [31], and so forth. To promote the wide use of cloud computing, those standards bodies need to sit down and work together for establishing common standards. Possible "Intercloud" standards in the following domains are needed to increase cloud interoperability and free data movement among clouds:

  - network architecture,
  - data format,
  - metering and billing,
  - Quality of Service,
  - resource provisioning,
  - security, identity management and privacy.

Clearly, there are many general computing standards that may be reused in the cloud, but for the moment, there are to our knowledge no dedicated cloud standards. This may add to the confusion for cloud users [32], and is something which must be addressed in the future.

There are currently many open problems in cloud computing security that should be addressed by cloud providers in order to convince end-users to use the technology. The most important concerns, in our view, is to guarantee that user data integrity and confidentiality is attained while they are stored in the cloud systems. In a long, non-transparent provider chain, it is difficult for an end-user to even determine what security mechanisms are applied to data in the Cloud. Section 4 presents recent work on extending Service Level Agreements with security elements to enable negotiation of security levels in the cloud. In Section 5, we present a scheme to prevent user data leakage in cloud storage systems. The scheme gives end-users strong control of their data, independently of the security solutions provided by the cloud providers. In Section 6 we present an alternative approach based on ensuring accountability of cloud providers.

4. Service level agreements for cloud security

In many respects, cloud computing represents outsourcing of computation and storage to an external service provider. Such outsourcing has been governed by Service Level Agreements (SLAs) that specify minimum levels of performance that the customer can expect, e.g., 99.999% system availability per year. Traditionally, however, SLAs have not covered security aspects such as confidentiality and integrity.

In a cloud computing marketplace, it is reasonable to expect that not all providers will be able, or willing, to provide the same level of security to their customers. Furthermore, a given cloud provider may offer services with varying levels of

[2] Safe harbor in this context can be understood as a foreign location where the data stored in that location is not affected by the local law of the foreign country. The US and EU member countries have signed a safe harbor agreement to protect personal data though there is still criticism about the agreement's effectiveness.

security depending on how much the customer is willing to pay for the service. Bernsmed et al. [33,34] have outlined how a cloud SLA could be extended to cover security aspects, allowing composition of cloud services from several service providers with a defined security level.

Security SLAs will typically follow a lifecycle where they are first published generically by a provider, and when a user wishes to use a cloud service, she will then negotiate a specific SLA to which the provider will commit, and the service will be provisioned. The user may want to monitor the service to ensure that the negotiated SLA is being adhered to by the provider. At any time during the commitment, provisioning and monitoring phases, the cycle may return to the negotiation phase, e.g., if the provider after all cannot commit to the previously negotiated SLA. In federated cloud services, these negotiations will have to be performed at multiple levels.

Fig. 2 illustrates suggested security mechanisms that can be specified in a cloud SLA. The specific mechanisms used will depend on the application. Bernsmed et al. offer examples of how this could be applied for a cloud CRM application [34] and a cloud Unified Communication application [33].

5. Trusted data sharing over untrusted cloud storage providers

Cloud computing shifts most of the IT infrastructure and data storage to off-premises third-party providers, with two important consequences [4]: (*a*) Data owners have only limited control over the IT infrastructure, therefore data owners must establish a mechanism to mandate the enforcement of their security policies to ensure data confidentiality and integrity; (*b*) Cloud service providers have excessive privileges, allowing them extensive control and ability to modify users' IT systems and data.

These lead to a low trust level when keeping and sharing data on a cloud, especially in a business model which requires strict secure data processing in order to safeguard business interests. Hence, a secure system is essential to enable trusted data sharing through untrusted cloud providers. The system should furthermore impose access control policies of data owners, preventing the cloud storage providers or other unauthorized users from illegally accessing the data. Fig. 3 is a simple representation of this requirement.

The specific security requirements for securing data storage in the cloud can be summarized as follows:

1. Data stored on the cloud should be kept private and the cloud storage provider should not be able to compromise the data confidentiality by any means.
2. The data owner has full control over authorization of data sharing. With authorization given by the owner, the designated user can then access the data kept on the cloud. Nevertheless, the process should not give the cloud provider any right to access the data.
3. Data access authorization is designated to the intended user only. Other users, who are not the permission holder, should not be able to exercise the permissions to access the data.

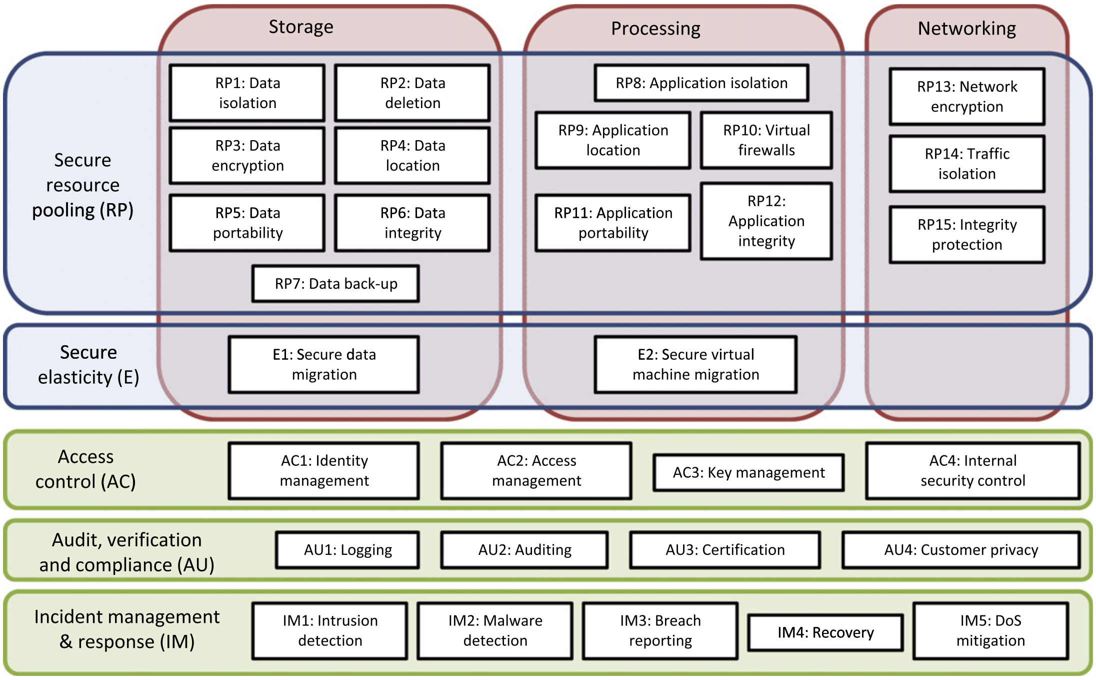

Fig. 2. A framework for security mechanisms for cloud SLAs [33].

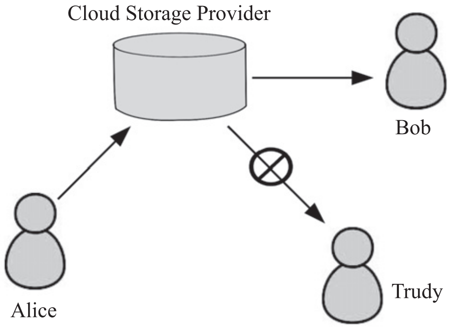

Fig. 3. Secure sharing on a cloud [4].

The above requirements of secure data sharing must be achieved via an untrusted cloud storage provider. It is necessary that the cloud storage provider helps to enforce the authorization policy for data access, but the enforcement should not reveal any information to the cloud storage provider or enable the cloud storage provider have excessive privileges to allow unauthorized access. The requirements can be achieved by using either homomorphic encryption or incremental encryption.

Homomorphic encryption [35] is a cryptography scheme where algebraic operations applied on the ciphertext are directly reflected in the corresponding plaintext. Simply put, this allows a third party to compute the sum of two encrypted numbers, and when this encrypted result is returned to the user, it can be decrypted with the original key, and the result is the same as the sum of the two numbers in plaintext form. This allows multiple parties to cooperatively generate a piece of ciphertext without knowing the plaintext that others work on.

Incremental encryption [36,37] allows the computation of the final ciphertext based on the initial ciphertext and the change of the plaintext. Rong et al. [38,39] propose an incremental encryption scheme based on elliptic curve cryptography which is different than that presented by Bellare et al. [36,37]. The mechanism allows users to have trusted data storage and sharing over untrusted cloud storage providers. Being able to implement trusted services on untrusted cloud storage providers allows users to manage their data on any cloud storage provider, eliminating the required trust on the providers. Fig. 4 illustrates this data leakage prevention scheme. The general idea is to encrypt the data before storing it in the cloud. On sharing the data, the encrypted data will be re-encrypted without being decrypted first. The re-encrypted data will then be cryptographically accessible only to the authorized user with the corresponding token.

The whole process does not reveal the cleartext data to the cloud provider at any stage, preventing the data being shared without the permission from the data owner. During the sharing, the data is always in its encrypted form, though at different stages it may be encrypted with different keys. There is no single stage that the data is decrypted into its clear form before it is delivered to the authorized users. This ensures that the whole sharing process will not disclose the information of the data to any parties.

6. Accountability in the cloud

While bulletproof confidentiality-preserving solutions for the cloud remain a desirable goal, it is clear that as long as "big data" needs to be processed in the cloud, there are currently no sufficiently efficient mechanisms that can do this without

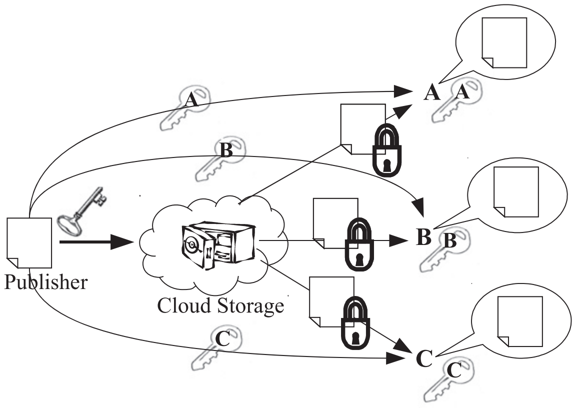

Fig. 4. A cloud data leakage prevention solution [4].

letting the cloud providers have access to cleartext data. Thus, there is a need for other mechanisms that can allay the fears of users that otherwise might be scared away from using the cloud.

Pearson et al. [40,41] highlight that the current lack of transparency is preventing many users from reaping the benefits of the cloud. Even though many cloud services currently work smoothly in daily use, it seems that little thought has been given to what happens when things go wrong; cloud providers may go bankrupt, local authorities may seize equipment with stored data, and so forth. Furthermore, as already stated, current cloud services are offered in a manner which implies that the customer must place full trust on the provider; as long as there are fallible humans in the loop, such trust may not always be warranted.

The cross-border nature of cloud computing also introduces the challenge of complying with multiple, sometimes conflicting, legal codes, especially when data is of a personal sensitive nature. Pearson [41] states that central components of the notion of accountability are transparency, responsibility, assurance and remediation. She also argues that there is a need to move from only *retrospective* to also *prospective* accountability, extending mechanisms for implementing security policies to encompass both preemptive and reactive mechanisms, i.e., both preventing bad things from happening, and establishing that bad things *did* happen, if they could not be prevented.

Achieving accountability in the cloud will require re-engineering many services to incorporate legal mechanisms, procedures and technical measures to support such prospective and retrospective accountability mechanisms. One small component of this work can be the deployment of security SLA mechanisms as described in Section 4.

7. Conclusion

Cloud computing is a very promising technology that helps companies reduce operating costs while increasing efficiency. Even though cloud computing has been deployed and used in production environments, security in cloud computing is still in its infancy and needs more research attention. Our paper presents a survey regarding security in cloud computing and discusses a number of possible research topics to improve security in cloud.

We presented an overview of cloud computing, its benefits and classifications. We then discussed security challenges in the current cloud computing model, including both the conventional security challenges that can be applied to cloud computing and a number of new challenges that we think are inherently connected to the new cloud paradigm. Among the current security issues with cloud computing, we emphasized three areas of particular interest, namely SLAs, trusted data sharing, and accountability in the cloud. We have outlined ongoing work on security SLAs for cloud computing, and briefly presented a scheme to address the security and privacy issue in the cloud. As secure data storage in cloud environment is a significant concern which prevents many users from using the cloud, we presented a solution to provide security and privacy for user data when it is located in a public cloud. This secure storage solution does not always fit as there are still a number applications that rely on accessing "cleartext" data in the cloud. We have highlighted the need for further work on accountability mechanisms in public clouds, in order to provide transparent services that can be trusted by all users.

Acknowledgements

Thanks to Dr. Karin Bernsmed for the illustration of security mechanisms in cloud SLAs.

Parts of this work have been funded by the Telenor-SINTEF research agreement.

References

[1] Mell Peter, Grance Tim. Effectively and securely using the cloud computing paradigm; 2011. <http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v26.ppt> [retrieved 18.04.11].

[2] National Institute of Standards and Technology. The NIST definition of cloud computing; 2011. <http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf> [retrieved 14.04.11].

[3] Baek Sung-Jin, Park Sun-Mi, Yang Su-Hyun, Song Eun-Ha, Jeong Young-Sik. Efficient server virtualization using grid service infrastructure. J Inform Process Syst 2010;6(4):553–62.

[4] Rong Chunming, Nguyen Son T. Cloud trends and security challenges. In: Proceedings of the 3rd international workshop on security and computer networks (IWSCN 2011); 2011.

[5] Klyuev Vitaly, Oleshchuk Vladimir. Semantic retrieval: an approach to representing, searching and summarising text documents. Int J Inform Technol Commun Converg 2011;1(2):221–34.

[6] Nyre Åsmund Ahlmann, Jaatun Martin Gilje. A probabilistic approach to information control. J Internet Technol 2010;11(3):407–16.

[7] Wlodarczyk Tomasz, Rong Chunming, Thorsen Kari Anne. Industrial cloud: toward inter-enterprise integration. In: Jaatun M, Zhao G, Rong C, editors. Cloud computing. Lecture notes in computer science, vol. 5931. Berlin/Heidelberg: Springer; 2009. p. 460–71. 10.1007/978-3-642-10665-1_42. <http://dx.doi.org/10.1007/978-3-642-10665-1_42>.

[8] Ling Amy Poh Ai, Masao Mukaidono. Selection of model in developing information security criteria for smart grid security system. J Converg 2011;2(1):39–46.

[9] Hsu Ping-Hai, Tang Wenshiang, Tsai Chiakai, Cheng Bo-Chao. Two-layer security scheme for AMI system. J Converg 2011;2(1):47–52.

[10] Kryvinska Natalia, Thanh Do Van, Strauss Christine. Integrated management platform for seamless services provisioning in converged network. Int J Inform Technol Commun Converg 2010;1(1):77–91.

[11] Siemens IT Solutions and Services. Community clouds: supporting business ecosystems with cloud computing; 2011. <http://www.it-solutions.siemens.com/b2b/it/en/global/Documents/-Publications/Community-Clouds-Whitepaper_PDF_e.pdf> [retrieved 18.04.11].

[12] Google, Google Apps. <http://www.google.com/apps/>.

[13] Salesforce. Salesforce CRM applications and software solutions. <http://www.salesforce.com/eu/crm/products.jsp>.

[14] Microsoft. Microsoft Windows Azure. <http://www.microsoft.com/windowsazure/>.

[15] Google. Google App Engine. <http://code.google.com/appengine/>.
[16] Amazon. Amazon Elastic Compute Cloud (EC2). <http://aws.amazon.com/ec2/>.
[17] Dropbox, Where Are My Files Stored?; 2011. <http://www.dropbox.com/help/7> [retrieved 26.04.11].
[18] Salesforce. Groupon expands throughout the US and beyond with salesforce; 2011. <http://www.salesforce.com/showcase/stories/groupon.jsp> [retrieved 26.04.11].
[19] Lee Hong Joo. Analysis of business attributes in information technology environments. J Inform Process Syst 2011;7(2):385–96.
[20] IDC Blogs. IT cloud services user survey, pt.2: top benefits & challenges; 2011. <http://blogs.idc.com/ie/?p=210> [retrieved 20.04.11].
[21] Secunia. Xen multiple vulnerabilities; 2011. <http://secunia.com/advisories/26986/> [retrieved 20.04.11].
[22] Dropbox's Blog. Privacy, security & your dropbox; 2011. <http://blog.dropbox.com/?p=735> [retrieved 25.04.11].
[23] European Union. Directive 95/46/EC of the European parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; 1995.
[24] IEEE Cloud Computing Standard Study Group. <http://www.computer.org/portal/web/sab/cloud>.
[25] ITU Cloud Computing Focus Group. <http://www.itu.int/en/ITU-T/focusgroups/cloud/Pages/default.aspx>.
[26] Cloud Security Alliance. <http://www.cloudsecurityalliance.org/>.
[27] Distributed Management Task Force. <http://www.dmtf.org/>.
[28] Storage Networking Industry Association. <http://www.snia.org/>.
[29] Open Grid Forum. <http://www.gridforum.org/>.
[30] Open Cloud Consortium. <http://www.opencloudconsortium.org/>.
[31] Organization for the Advancement of Structured Information Standards. <http://www.oasis-open.org/>.
[32] Fogarty Kevin. Cloud computing standards: too many, doing too little; 2011. <http://www.cio.com/article/679067/Cloud_Computing_Standards_Too_Many_Doing_Too_Little> [retrieved 15.09.11].
[33] Bernsmed Karin, Jaatun Martin Gilje, Meland Per Håkon, Undheim Astrid. Security SLAs for federated cloud services. In: Proceedings of the 6th international conference on availability, reliability and security (AReS 2011); 2011.
[34] Bernsmed Karin, Jaatun Martin Gilje, Undheim Astrid. Security in service level agreements for cloud computing. In: Proceedings of the 1st international conference on cloud computing and services science (CLOSER 2011); 2011.
[35] Gentry Craig. A fully homomorphic encryption scheme. Ph.D. thesis, Stanford University; 2009. <http://crypto.stanford.edu/craig/craig-thesis.pdf> [retrieved 21.04.11].
[36] Bellare Mihir, Goldreich Oded, Goldwasser Shafi. Incremental cryptography: the case of hashing and signing. In: Advances in cryptology – CRYPTO'94. Springer; 1994. p. 216–33.
[37] Bellare Mihir, Goldreich Oded, Goldwasser Shafi. Incremental cryptography and application to virus protection. In: Proceedings of the 27th annual ACM symposium on theory of computing. ACM; 1995. p. 45–56.
[38] Zhao Gansen, Rong Chunming, Li Jin, Zhang Feng, Tang Yong. Trusted data sharing over untrusted cloud storage providers. In: Proceedings of the 2nd IEEE international conference on cloud computing technology and science (CloudCom 2010); 2010.
[39] Rong Chunming, Zhao Gansen. Incremental encryption. Norwegian Patent No. P3683NO00-DT (Pending).
[40] Pearson Siani, Charlesworth Andrew. Accountability as a way forward for privacy protection in the cloud. In: Jaatun M, Zhao G, Rong C, editors. Cloud computing. Lecture notes in computer science, vol. 5931. Berlin/Heidelberg: Springer; 2009. p. 131–44. 10.1007/978-3-642-10665-1_12. <http://dx.doi.org/10.1007/978-3-642-10665-1_12>.
[41] Pearson Siani. Toward accountability in the cloud. EEE Internet Comput 2011;15(4):64–9. http://dx.doi.org/10.1109/MIC.2011.98.

[41] Pearson Siani. Toward accountability in the cloud. EEE Internet Comput 2011;15(4):64–9. http://dx.doi.org/10.1109/MIC.2011.98.

Chunming Rong is a professor and head of the Center for IP-based Service Innovation at University of Stavanger in Norway. His research interests include cloud computing, big data analysis, security and privacy. He is co-founder and chairman of the Cloud Computing Association (CloudCom.org) and its associated conference and workshop series. He is a member of the IEEE Cloud Computing Initiative, and co-Editor-in-Chief of the Springer Journal of Cloud Computing.

Son T. Nguyen is a postdoctoral researcher at University of Stavanger. He obtained his PhD degree in Computer Engineering from the University of Stavanger in 2009 and his Master degree in Telecommunications from Asian Institute of Technology in 2002. He is interested in a broad range of research issues related to security in communications networks and cloud computing.

Martin Gilje Jaatun is a Senior Scientist at SINTEF ICT (Trondheim, Norway), where he has been employed since 2004. He received his MSc degree in Telematics from the Norwegian Institute of Technology (NTH) in 1992. His research interests include software security, security in cloud computing and security of critical information infrastructures. He is vice chairman of the Cloud Computing Association (cloudcom.org) and a Senior Member of the IEEE.