Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2013, Article ID 871430, 6 pages
http://dx.doi.org/10.1155/2013/871430

Research Article

A Novel Cloud Computing Algorithm of Security and Privacy

Chih-Yung Chen[1] and Jih-Fu Tu[2]

[1] *Department of Information Management, St. John's University, 499 Section 4, Tam King Road, Tamsui District, New Taipei City 25135, Taiwan*
[2] *Department of Electronic Engineering, St. John's University, 499 Section 4, Tam King Road, Tamsui District, New Taipei City 25135, Taiwan*

Correspondence should be addressed to Chih-Yung Chen; yung@mail.sju.edu.tw

Received 12 September 2013; Accepted 12 October 2013

Academic Editor: Teen-Hang Meen

The emergence of cloud computing has simplified the flow of large-scale deployment distributed system of software suppliers; when issuing respective application programs in a sharing clouds service to different user, the management of material becomes more complex. Therefore, in multitype clouds service of trust environment, when enterprises face cloud computing, what most worries is the issue of security, but individual users are worried whether the privacy material will have an outflow risk. This research has mainly analyzed several different construction patterns of cloud computing, and quite relevant case in the deployment construction security of cloud computing by fit and unfit quality, and proposed finally an optimization safe deployment construction of cloud computing and security mechanism of material protection calculating method, namely, Global Authentication Register System (GARS), to reduce cloud material outflow risk. We implemented a system simulation to test the GARS algorithm of availability, security and performance. By experimental data analysis, the solutions of cloud computing security, and privacy derived from the research can be effective protection in cloud information security. Moreover, we have proposed cloud computing in the information security-related proposals that would provide related units for the development of cloud computing security practice.

1. Introduction

Cloud computing provides service of several different service types, namely, software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) [1]. Each pattern in risk of control and benefit will differ from each other, the protection right of privacy in cloud computing is an important subject [2], and the traditional encryption solution was unable to provide effective privacy protection mechanism of the cloud environment [3]. For example, the user of cloud service response pays close attention to individual or company related information, whether under the condition that possibly the material owner does not know the circumstances of the matter provided to other people usages [4]. The right of privacy in traditional software development is not a main issue but in the protection right of privacy regarding the cloud computing is a big challenge at present, because these materials usually in unencrypted form are deposited on a machine, but the owner of the material possibly contains the different organization operators, enhancement divulging commercial sensitive information, and possible loss in privacy material [5]; therefore, protection of individual secret and sensitive information stores up in the clouds is very important. When establishing the cloud computing service system carries on the information security risk control, one must consider all type factors and promotes user the level of trust in the laws condition, needs to analyze and take the gauge of the system in principle of design of each stage [6].

Clouds computing on the Internet is an important development application; the cloud serves the user without hardware master control power [7], the user by the application service that the cloud service provides, processing and depositing material, for example, credit card, account dense, and personal preference profile, picture conduct calendar, finance and health, and other materials. Characteristics of cloud computing are to provide the service of data storage, processing, and platform use flow to global users, but the result of this material set will be material privacy protection, causing the common reason for the enterprise or individual not being willing to use the cloud service solution package.

Furthermore, the security of cloud computing material still has many problems not yet solved, at present there is not a good and effective test method for cloud computing material of privacy right system [2], and different types of cloud computing service need a different data safety protection solution. The objective of this research is mainly the hope to establish a research model of cloud computing to discuss the fit and unfit quality relations of material protection and to analyze which application of cloud computing service needs to be protected, including the following several parts: (1) establishing a research model for cloud arithmetic system construction privacy material protection; (2) discussing fit and unfit quality relations of cloud service material protection and traditional material protection; (3) discussing some applications of cloud computing service type. Which type of news needs to be protected? (4) Analysis result provides relevant unit to referring to, in order to help it in the future research, and contribute to the practical realm.

2. Related Works

2.1. The Operation Principle of Clouds Computing. The cloud computing system is mainly comprised of the software service supplier (SaaS), the platform service supplier (PaaS), and the network infrastructure construction supplier (IaaS) [8]; the typical operation principle is shown in Figure 1.

By Google Cloud Computing Trends analysis chart (Figure 2) it can be seen that in the trend of cloud computing the well-respected degree has grown year by year, the products of the database manufacturer are joining the function of the cloud computing to support the database (e.g. Oracle now operates a cloud computing platform (EC2) service directly in Amazon) [9], therefore, deposits along with more and more materials in the clouds service, expansion that the issue of data safety will also continue, because these materials usually contain the company or individual related important sensitive news.

2.2. Management Style of Cloud Computing. The hardware device of cloud computing can be provided by internal cloud or the exterior third party organization entrusted with the clouds (TTP Cloud), the cloud computing is possibly limited in sole organizations and agencies Private Cloud (private cloud) or many organizations and agencies share the public cloud (Public Cloud) [11, 12].

2.3. Privacy Right Issues

2.3.1. What Is Privacy Right? The private right of privacy is a fundamental human right, coming from the current UN Universal Declaration of Human Rights and European human rights convention, including various types of privacy rights, for example, May control with right of own relevant information [13]. Regarding how to protect the personal privacy not to be encroached upon and harmed became important discussion of privacy right on safe presented [14–16].

2.3.2. Privacy Right Risk of Cloud Computing. As shown in an investigation that was done by Pew Internet in 2008 [4], 69% of Internet users use the online mail service in US, stores up material in the network, or uses homepage application program, such as the copy clerk distributed processing. These users are using the clouds to operate an actual emerging construction; the user through the equipment (PC, NB ...) connects to Internet downloading application program processing material and deposit material in cyberspace, Table 1 explains various cloud application services for the proportion that Internet user uses, and may understand why the clouds computing will issue the right of privacy risk.

In this section, we explain the concrete right of privacy issues in cloud computing, analyze the different clouds service case to explain that the request degree of each right of privacy under the different conditions was possibly different, and provide the comprehensive appraisal of the privacy risk of cloud computing. The main right of privacy risk is as follows [6]: (1) Individual user of cloud service: Runs counter to individual wish, was forced or convinced to provide the personal data, or makes them feel uncomfortable in other ways. (2) Enterprise or organization user in cloud service: Does not observe the policy and legislation of enterprise, loses prestige. (3) Clouds platform implementer: exposition of Sensitive information in storage platform (possibly for cheating goal), the faith of legal liability, influence goodwill and deficient user. (4) Clouds ASP: Does not abide by the law, loses prestige, uses the background program to store up personal data in the clouds, that is, the material is used in the non-clouds service. (5) Material level: Revelation personal data.

2.4. The Security Requirements of Different Levels. We need to consider the security problem level classification as follows [7]: (1) server deposit security, (2) Internet deposit security, (3) database deposit security, (4) material privacy security, and (5) program deposit security.

3. Research Methodology

3.1. Research Supposition. This research of the nature of cloud computing and challenge concept of privacy rights proposes that the research supposition of several possibilities in cloud computing services needs protected material type as follows. (1) Individual identification information can be used to distinguish or find individual material. (2) Sensitive information: health, tendency, religious belief or race material, union members, or others are considered as the personal information. (3) To be considered as sensitive information, for example, the biological information or the image data that the public places monitoring device are filmed. (4) User preference uses computer ancillary equipment collection material—like printer, behavior material—such as viewing habit, the digital content, and the user had visited recently the historic information of websites or products. (5) Unique identification equipment, using the only characteristics of hardware, may correspond to trace the equipment of user, for example, IP address, RFID label type material. (6) Transaction material, for example, electronic commerce material contains the order material of the user. These materials possibly have the sensitive information, for example, user

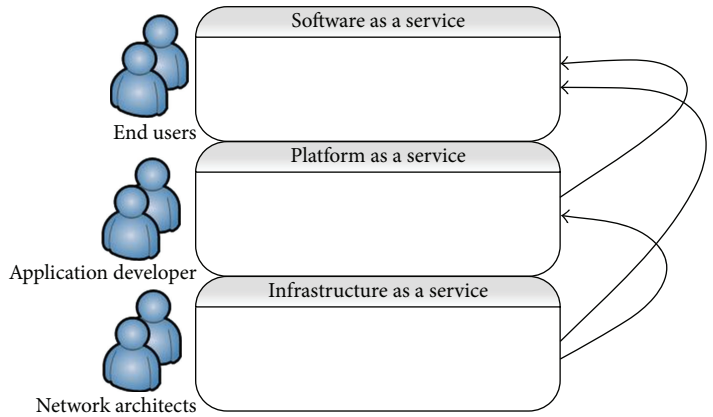

Figure 1: Composition and operation principle of clouds computing.

Table 1: The Internet network user uses the cloud service of questionnaire of all kinds of application offered.

All kinds of application clouds service—the Internet network user uses service of all kinds of application (%)	
Use Webmail service, for example, Hotmail, Gmail, or Yahoo! Mail	56%
Online to store the personal photo	34%
Use the Online application program, for example, Google Documents or Adobe Photoshop Express	29%
Online to store the personal film	7%
Online to pay and store the computer file	5%
Online to back up the hard disk	5%

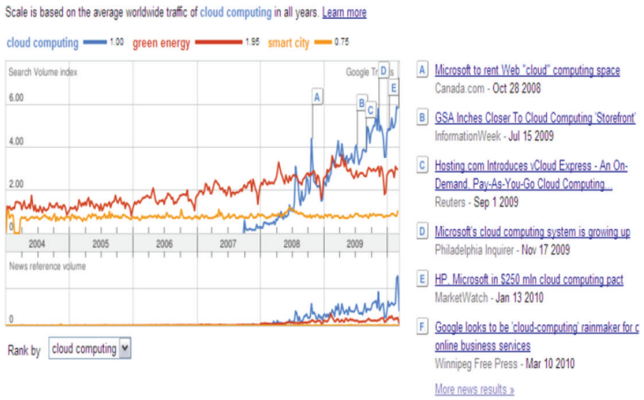

Figure 2: Cloud Computing Trends [10].

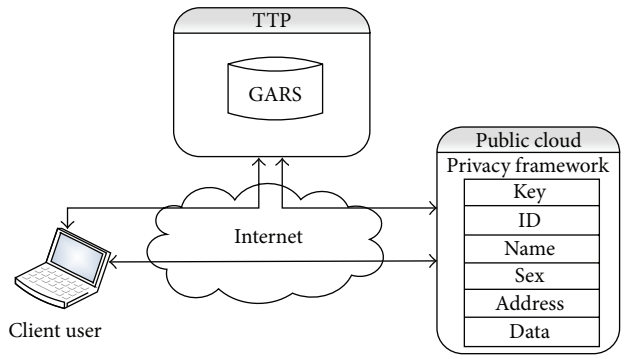

Figure 3: Optimization model of cloud computing.

material or credit card number and any latent, or increase the infringement privacy of the security loophole.

3.2. Range of Research. This research's main discussion and analysis issue of data safety and privacy right of cloud computing service, through comparative analysis proposes a suggestion of cloud computing optimization model. The usability and test relevant question of cloud computing service are not in this range of study.

3.3. Optimization Model. This research proposes a cloud computing optimization model according to the comparison analysis method as shown in Figure 3 in the processing of the solution of privacy protection and in the security issue. This research suggests to establish Global Authentication Register System (GARS) on third party clouds of trust (TTP), provides the subscriber's premises and clouds both sides separately carries out a disposable registration certification service, but Public Cloud part establishes right of privacy frame and model in the public cloud, and the encryption mechanism uses the GARS calculating method of this research and makes processing and protection on the privacy material and security.

3.4. Data Transmission Flow. Figures 4 and 5 are subscriber's premise/clouds and TTP proof procedure data transmission flow chart.

The Calculating Method Parameter Definitions.

C: Client.

S: Server.

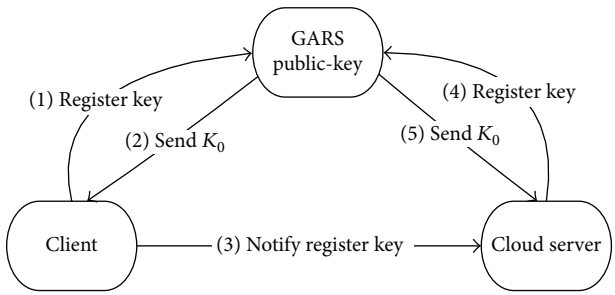

Figure 4: Optimization model of cloud computing (initialization).

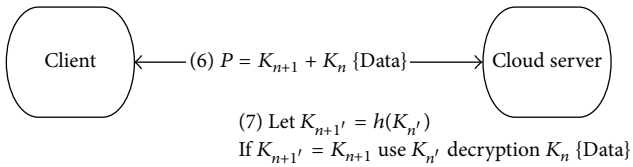

Figure 5: Optimization model of cloud computing (after TTP authorizes).

K_n: Authentication basis code. (K_0 obtains initial authentication basis code by GARS).

H: Hash Function.

$K_{n+1} = h(K_n)$: Encryption key (transmission end).

$K_{n+1'} = h(K_{n'})$: Encryption key (receiving end).

$P = K_{n+1} + K_n$ {Data}: Encryption seal material (Package).

The GARS Calculating Method. GARS calculating method steps are as follows.

Step 1. The client sends out Request Register Key to GARS. C-TTP: Request Register Key.

Step 2. GARS transmits one group of Key: K_0 to give Client. TTP-c: Send Public Key: K_0.

Step 3. Client informs Cloud Server Register Key. C-s: Notify Register Key.

Step 4. Cloud Server sends out Request Register Key to GARS. S-ttp Request Register Key.

Step 5. GARS transmits the same group Key: K_0 to give Cloud Server. TTP-s: Send Register Key.

Step 6. The subscriber's premise uses K_0 to produce one group of authentication encryption Key: K_1 ($K_1 = h(K_0)$) transmission encryption material ($P = K_1 + K_0$ {Data}) to Cloud Server. $C \rightarrow S : K_{n+1} = h(K_n)$, $P = K_{n+1} + K_n$ {Data} (Initial Value: 0).

Step 7. Cloud Server receives the encryption material and uses original $K_{n'}$ Hash Function to obtain $K_{n+1'}$, confirmation comparison Step 6 K_{n+1} weather is equal to Step 7 $K_{n+1'}$; if equal, then it uses K_n to decipher the material. S: use K_n Create $K_{n+1'}$ ($K_{n+1'} = h(K_n)$). If $K_{n+1'} = K_{n+1} \Longrightarrow$ Identify C then use K_n decryption K_n {Data} S-c: $K_{n+1} = h(K_n)$, $P = K_{n+1} + K_n$ {Data}.

Note. (1) If the Server end must transmit material to return to the Client end, then similarly use Steps 6 and 7, Server and Client role exchange.

(2) If material authentication mistake, by the subscriber's premise were decided whether needs to duplicate the Step 1 to Step 5 to authenticate. And the GARS calculating method flow is shown in Figure 6.

4. Results and Discussion

The previous section introduced the research method of the main system function operation and GARS calculating flow in detail. To confirm that research of the present paper is feasible and effective, therefore in this section, we simulate to make the reality of GARS flow and analyze to discuss different flows by the empirical datum and result. In the system environment test, and experiment, the implementation of the present paper contains three flow function of main operation in the GARS flow and uses the testing tool record flow operation time needing comparative data.

Figure 7 is Client/Server both sides authenticate Http Response Time after authentication; we may see that it takes approximately 7 seconds to carry out the analog transmission material 50 times response time to complete.

Figure 8 is the general three parties authenticate Http Response Time; we may see that it takes 33 seconds to carry out the analog transmission material 50 times response time to complete.

Figure 9 is GARS one time authenticates Http Response Time; we may see that it takes 22 seconds to carry out the analog transmission material 50 times response time to complete.

4.1. Experimental Data Analysis. Through the above experimental data, we may see one time authentication of GARS flow simplified flow time of TTP authentication each time. Obviously we may see the result of simplified authentication flow, the condition of abbreviated execution step, and the execution time reduced relatively. From this we may confirm the design of GARS to have good execution efficiency. By way of the above results analysis of experimental data is stated as follows. (1) Client/Server/TTP one time authentication flow (5 steps): data are made by the simulation implementation in carrying out 50 times Client/Server to TTP authentication flow in which the finish time is 22 seconds, and authentication time on average is 0.44 second each time. (2) Client/Server both sides authentication flow (2 steps): after carrying out TTP authentication, Client/Server does not need to make the authentication with TTP again so long as carries out Client/Server both sides authentication flow in carrying out 50 times Client/Server both sides authentication flow in which the finish time is 8 seconds, and authentication time on average is 0.16 second each time. (3) Client/Server/TTP tripartite authentication flow (7 steps): this empirical datum

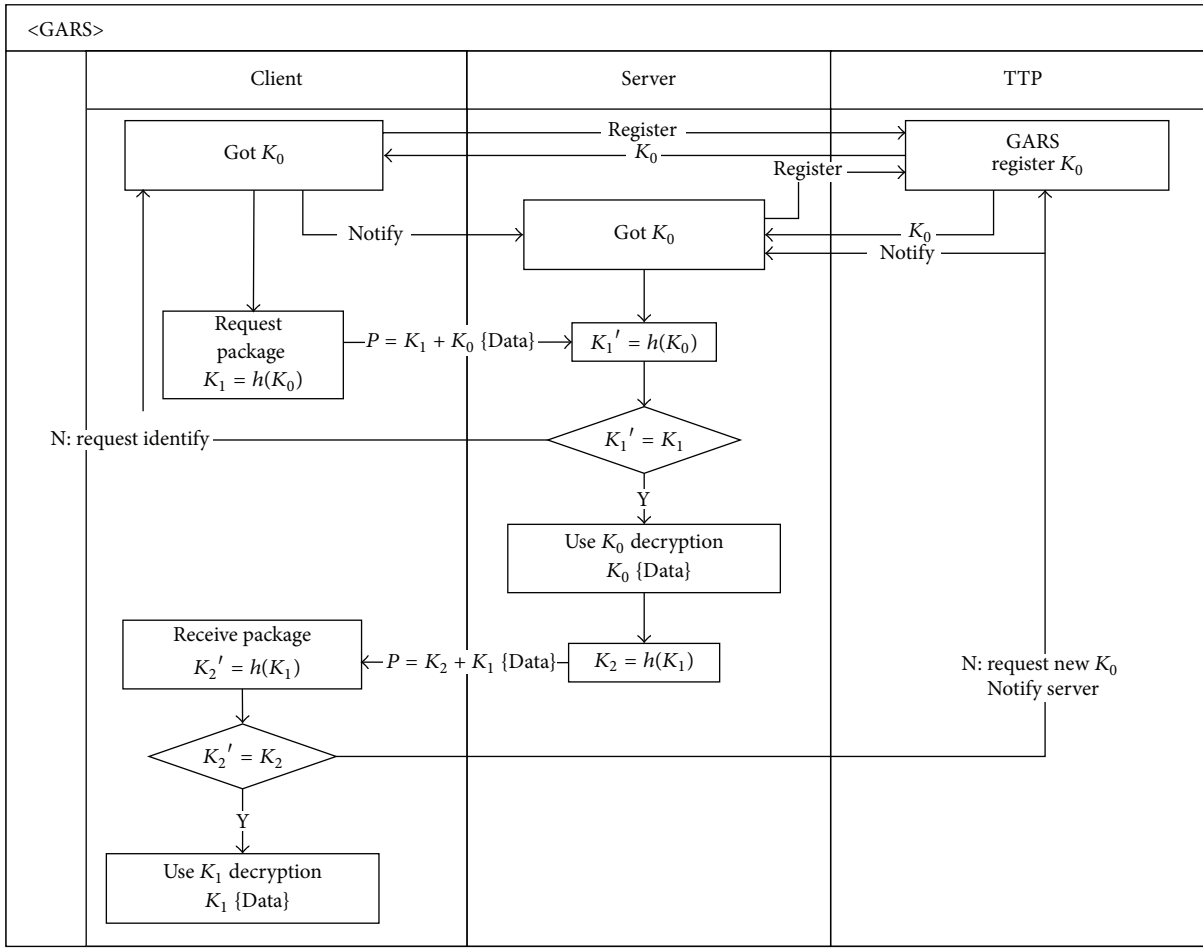

Figure 6: GARS algorithm flow diagram.

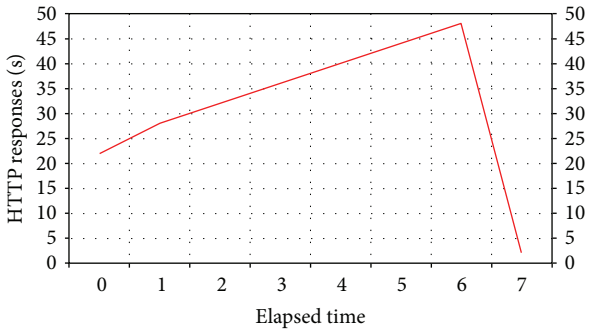

Figure 7: Both sides authenticate Http Response Time.

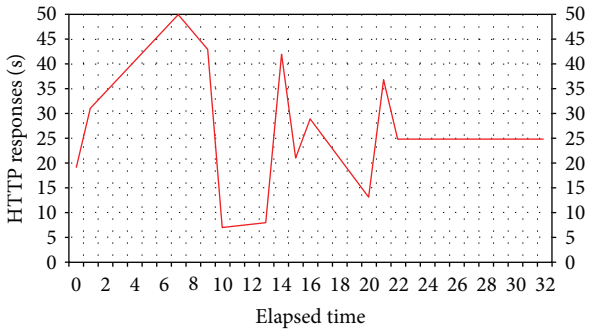

Figure 8: The three parties authenticate Http Response Time.

needs to carry out the time needed of tripartite authentication for the simulation in which each time is 33 seconds, and authentication time on average is 0.66 second each time.

4.2. Experimental Data Comparison. By the above data analysis results, the present procedure is to take tripartite authentication flow, and each time authentication must authenticate to TTP; this research takes one time authentication procedure to transmit data in carrying out both sides authentication flow. By the data it was shown that the latter (present research) surpasses the former (present general procedure) in carrying out the potency. Therefore, by assessment of experimental data analysis, if authentication flow needs the tripartite authentication way of TTP authentication by each time, execution time is longer after being compared with the GARS one time authentication. Therefore, it can have fast potency performance in carrying out both sides authentication flow.

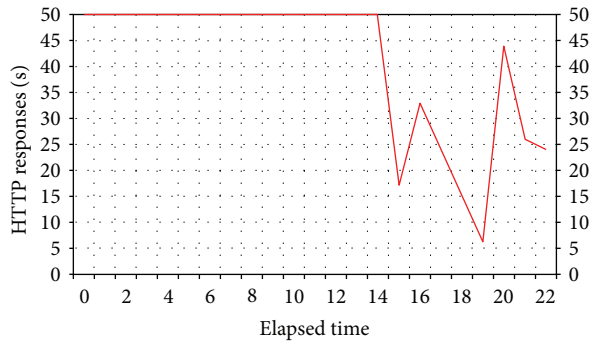

Figure 9: Authenticates Http Response Time one time.

5. Conclusions

In this research we proposed an effective feasible cloud material protection algorithm (GARS) which takes the technical theory of symmetrical encryption as the foundation, applies GARS in the information security of cloud computing. GARS has used the third party authentication mechanism trust, contains using Hash function and AES/DES data encryption technology characteristics, and coordinates the completed GARS flow to effectively protect security of cloud material and readability of stolen material. This research promotes and improves privacy right and security capital issue in cloud computing and provides in capital security procedure of relevant unit when develops cloud computing for reference. By the experiment it was shown that the data encryption way of GARS utilization can protect the material security, in potency, because after GARS carrying out one time authentication, only needs user and cloud make both sides authentication flow; it has the obvious performance in the potency with currently general procedure of the authentication flow. By way of the result of analysis discussion, we may know usability of this algorithm, and in cloud service security issue, it improves and strengthens cloud security relevant question using GARS.

References

[1] M. Armbrust, A. Fox, R. Griffith et al., *Above the Clouds: A Berkeley View of Cloud Computing*, 2011.

[2] L. Gu and S.-C. Cheung, "Constructing and testing privacy-aware services in a cloud computing environment—challenges and opportunities," in *Proceedings of the 1st Asia-Pacific Symposium on Internetware (Internetware '09)*, October 2009.

[3] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "On technical security issues in cloud computing," in *Proceedings of the IEEE International Conference on Cloud Computing (CLOUD '09)*, pp. 109–116, September 2009.

[4] J. B. Horrigan, "Use of cloud computing applications and services," Pew Internet & American Life Project Memo, 2008.

[5] M. Mowbray and S. Pearson, "A client-based privacy manager for cloud computing," in *Proceedings of the 4th International ICST Conference on Communication System Software and Middleware (COMSWARE '09)*, Dublin, Ireland, June 2009.

[6] S. Pearson, "Taking account of privacy when designing cloud computing services," in *Proceedings of the ICSE Workshop on Software Engineering Challenges of Cloud Computing (CLOUD '09)*, pp. 44–52, Vancouver, Canada, May 2009.

[7] B. R. Kandukuri, P. V. Ramakrishna, and A. Rakshit, "Cloud security issues," in *Proceedings of the IEEE International Conference on Services Computing (SCC '09)*, pp. 517–520, September 2009.

[8] L.-J. Zhang and Q. Zhou, "CCOA: cloud computing open architecture," in *Proceedings of the IEEE International Conference on Web Services (ICWS '09)*, pp. 607–616, Los Angeles, Calif, USA, July 2009.

[9] Amazon Elastic Compute Cloud—EC2, http://aws.amazon.com/ec2/.

[10] Cloud Computing Trends, http://trends.google.com/trends.

[11] L. Robert and G. Yunhong, *On the Varieties of Clouds for Data Intensive Computing*, 2009.

[12] Wikipedia, CloudComputing, http://en.wikipedia.org/wiki/Cloud_computing#cite_note-idc-28.

[13] The Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change*, 2007.

[14] D. J. Solove, "A taxonomy of privacy," *University of Pennsylvania Law Review*, vol. 154, no. 3, pp. 477–564, 2006.

[15] E. Bertino, *Privacy-Preserving, Digital Identity Management for Cloud Computing*, 2010.

[16] M. Mowbray and S. Pearson, "A client-based privacy manager for cloud computing," in *Proceedings of the 4th International ICST Conference on Communication System Software and Middleware (COMSWARE '09)*, Dublin, Ireland, June 2009.