National Conference on Recent Advances in Computer Science and IT (NCRACIT)
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 1 | ISSN : 2456-3307

Security Issues and Challenges in Cloud Computing: A Review

Prabal Verma[1], Aditya Gupta[2], Rakesh Singh Sambyal[3]

[1,2] Department of Computer Science and Engineering, BGBSU, Rajouri, Jammu & Kashmir, India
[3] Department of Information Technology Engineering, BGBSU, Rajouri, Jammu & Kashmir, India

ABSTRACT

Cloud computing provides a convenient access to a shared pool of configurable computing resources on demand. In cloud computing, the services are provided in the form of IT-related capabilities, which are accessible with minimal management effort and without requirement of the detailed knowledge of the technologies that are related to cloud computing. Because of the Security threats involved in Cloud Computing the users hesitate to use its services in spite of the great savings promised by Cloud. In this paper an overview of Cloud Computing and the security challenges related to Cloud are discussed. Although Cloud security can be improved with the help of many technological approaches available but currently there are no solutions that can provide all security features and the challenges such as service level agreements for security has to be tackled, also for ensuring accountability in the cloud certain holistic mechanisms should be implemented.

Keywords : Security, Cloud Computing

I. INTRODUCTION

The National Institute of Standards and Technology (NIST) has defined cloud computing as a technology that provides a convenient access to a shared pool of configurable computing resources (for e.g. networks, servers, storage, applications, and services) on demand , which can be released with minimum management effort or service provider interaction and can also rapidly provisioned [4]. According to Google's Kevin Marks, the term cloud computing has evolved from the starting days of the Internet where the network was drawn as a cloud. The cloud hided the message from us, therefore we didn't care where the message was....[6].

Based on user demands cloud computing also provide elastic resources with dynamic provisioning and scaling. This approach basically deals with the concepts of resource under-provisioning, i.e., fewer resources are allocated than needed and resource over-provisioning i.e., more resources are allocated than required. The elastic management increases system efficiency since it yields better overall system resource usage.

Cloud computing resources are managed by highly professional service providers which are provided in massive, abstraction (virtualization) based infrastructures, in contrast to the traditional computing model, where the computing power and the end-user data are located in the users' local machines [5].

The cloud model increases the system reliability and efficiency while simplifying installation, operation and maintenance of information systems and also reducing the costs. A cloud system requires less expertise to use therefore it is user friendly. We can co-relate the simplicity of the cloud usage with current running-water and electricity systems, where without being concerned with the technical complexity behind these systems; the end-users can easily use the services from providers.
This paper high-lights some areas for further work in cloud security, it also gives an overview of cloud computing and related security challenges.

The rest of this paper is organized as follows: Section 2 introduces different types of classifications of cloud computing. In Section 3, security challenges that cloud computing needs to address are reviewed. In Section 4 the brief discussion about how Service Level Agreements (SLAs) can be extended in cloud computing to cover security aspects also. Section 5 tries to provide a solution for providing trusted data sharing over public cloud storage. In Section 6, some important issues regarding accountability in the cloud are discussed. Finally, Section 7 provides the conclusion of the paper.

II. CLASSIFICATION OF CLOUD COMPUTING

In spite of "cloud computing" being a relatively new and emerging term, most of the people believe that other forms of "cloud" used to exist even before this term was introduced. Though it is being referred by many names, other technologies and concepts are being developed and used to form the current cloud computing technology.

The abstraction of infrastructure complexities of data, application, servers and heterogeneous platforms where the infrastructure, servers, or applications can be used without knowing their exact location is basically the current brand of cloud computing ("Cloud 3.0"). Note that this internet development can also be plotted along other verticals, such as the semantic web, which among other things facilitates semantic search [1], which is not related to cloud computing directly, but can still be viewed as something that is enabled by the cloud computing paradigm [2]. The cloud-like structures are also being emerged in other fields such as process control systems [9] and smart grid constellations [3]; the Advanced Metering Infrastructure [7] brings the "always-on" aspect physically into people's homes. Eventually, a merger of all such domain-specific networks into a single global cloud is expected, as has long been a vision of telecom operators [8].

Cloud computing is classified based on either there:-

a. Deployment models
b. Service models.

Figure 1 shows cloud models based on the NIST definition framework [6]. The four widely referenced deployment models are private, public, community, and hybrid cloud.

1. Private Cloud: - The cloud infrastructure is operated within a single organization, and managed by the organization or a third party regardless whether it is located premise or off premise. The cloud resources are used by the organization itself for its private use. The private clouds are built by an organization for serving its critical business applications.

2. Public Cloud: - This type of cloud is the dominant form of current cloud computing deployment model. The public cloud can be used by the general public cloud consumers for their own benefits and the public cloud service provider has got the complete ownership of the public cloud with their own policies, values, costing and charging models. Many popular public cloud service providers are Amazon EC2, Force.com, Microsoft and Google App Engine etc.

3. Community Cloud: - This type of cloud is jointly constructed by certain organizations and the same cloud infrastructure as well as policies, requirements, values and concerns is shared by them. The economic stability and democratic equilibrium is formed by the cloud community.

4. Hybrid Cloud: - This type of cloud infrastructure is basically a combination of two or more clouds, it can either be public, private or community. The hybrid cloud is used by the organizations for optimizing their resources to increase their core competency by margining out peripheral business functions onto the cloud while controlling core activities on premise through private cloud.

The cloud service models are classified as Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Data Storage as a Service (DaaS).

1. Software as a Service (SaaS):- In cloud SaaS the applications of the cloud consumers are released on a hosting environment which can be accessed from various clients (for e.g Web Browser, PDA etc.) through network by application users. Business applications like Enterprise Resource Management (ERP) , accounting , Customer Relationship Management (CRM) can be delivered by SaaS. Google Apps[14] and Salesforce CRM[16] are certain

examples of SaaS. The underlying infrastructure is not controlled by the consumers.

2. Platform as a Service (PaaS):- In cloud PaaS the tools and resources on cloud infrastructure are used to provide services to the end users. PaaS is basically a development platform with the help of which the cloud services and applications are directly developed by cloud consumers on PaaS cloud. The examples of PaaS are Microsoft Windows Azure [13] and Google App Engine [17]. The underlying infrastructure and operating Systems are not controlled by the consumers but the deployment of individual applications are controlled by consumers.

3. Infrastructure as a Service (IaaS):- In Cloud IaaS the fundamental computing resources such as storage, network, servers etc. are used to provide services to the end users. In IaaS cloud the concept of Virtualization is used extensively for integrating physical resources in an ad-hoc manner to meet the increasing and decreasing demand from cloud consumers. Amazon EC2[10] is an example of cloud IaaS. The underlying infrastructure is not controlled by the consumers but typically the virtual machines can be launched with chosen operating system, which in turn are managed by the consumers.

4. Data Storage as a Service (DaaS):- The cloud DaaS can seen as a special type of cloud IaaS in which on demand delivery of virtualized storage has become a separate cloud service – data storage service. Amazon S3 , Google BigTable are examples of cloud DaaS.

Many large organizations such as Google, Yahoo, Amazon, Facebook etc are currently using cloud computing since it has many disadvantages. Since it saves a lot of initial investment cost therefore it is very beneficial for start-ups also. Some examples of start-ups are Dropbox [19] and Groupon [15] etc. which utilize cloud computing for their daily operations. Now to reduce investment and operation costs various other companies are also moving their applications to cloud for increasing their business efficiency [11].

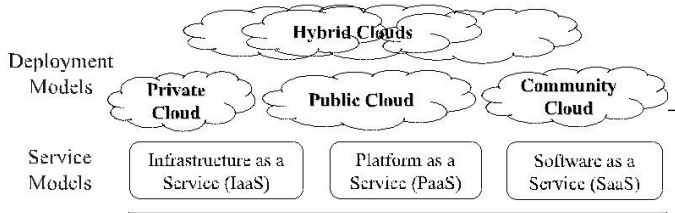

Figure 1. The NSIT Cloud Definition Framework [6]

III. SECURITY ISSUES IN CLOUD COMPUTING

There are various security threats that must be taken into consideration for getting full benefit from this new computing paradigm. Some of the security concerns are listed and discussed below:

1) Security concern 1: If the user decides to move from one cloud to the other cloud there can be the incompatibility issue with storage services provided by one cloud vendor with other cloud vendors services (e.g. Google cloud is incompatible with Microsoft cloud)[12].

2) Security concern 2: The data logs must be provided to security managers and regulators, in case of Payment Card Industry Data Security Standard (PCI DSS). [18][20][21]

3) Security concern 3: The control to physical security is lost with the cloud model since computing resources are shared with other companies. There is no knowledge or control of where the resources are running.

4) Security concern 4: It is difficult to maintain the consistency of security and ensure the auditability of records with the dynamic and fluid nature of virtual machines.

5) Security concern 5: There should be a common standard to ensure integrity of data.

6) Security concern 6: Company violates the law (i.e. risk of data seizure by (foreign) government).

7) Security concern 7: For the users to be sure that they are protected they must be regularly updated with application improvement.

8) Security concern 8: There are certain strict limits by some government regulations on what kind data about its citizens can be stored and for how long, and the customer's financial data should remain in their home country is the condition required by some banking regulators.

9) Security concern 9: Logically the encryption and decryption keys should be controlled by the customers.

There are various security issues that are associated with cloud computing and they can be grouped together into any number of dimensions.

In 2008 Gartner [22] said, the users should ask the vendors for seven specific security issues before they make a choice of cloud vendors and those seven security issues are: Privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support and long-term viability.

The security and privacy practices of some of the major cloud providers (such as Salesforce.com, Amazon, Google, and Microsoft) were evaluated by Forrester Research Inc. [23] in 2009 in three major aspects: Security and privacy, compliance, and legal and contractual issues. For information assurance in the cloud, Cloud Security Alliance (CSA) [24] is gathering non-profits, individuals and solution providers for getting into the discussion about the current and future best practices for clouds.

The thirteen domains of concerns on cloud computing security have been identified by CSA [25]. In 2011, investigations were made by S. Subashini and V. Kavitha on cloud computing security challenges from the cloud computing service delivery models (SPI model) and a detailed analysis and assessment method description for each security issue was given [26].

The cloud computing security issues were explored from different perspectives by Mohamed Al Morsy, John Grundy and Ingo Müller in 2010, which included security issues that associated with cloud computing architecture, service delivery models, cloud characteristics and cloud stakeholders [27].

Yanpei Chen, Vern Paxson and Randy H. Katz believed that the complexities of multi-party trust considerations and the ensuing need for mutual auditability are the two aspects that are to some degree new and essential to cloud. Some new opportunities in cloud computing security are also pointed out by them [28].

A large number of standard bodies with different interests currently exists and for promoting the wide use of cloud computing those bodies need to have a discussion and they should also work together for establishing common standards. In the below specified domains the possible "Inter-cloud" standards are needed to increase cloud interoperability and free data movement between clouds:

- Network Architecture,
- Data Format,
- Metering And Billing,
- Quality Of Service,
- Resource Provisioning,
- Security, Identity Management And Privacy

There are various general computing standards that may be reused in the cloud but there are no dedicated cloud standards to our knowledge. This is something that must be addressed in future and may add to the confusion for cloud users [29].
The user data integrity and confidentiality should be attained while the data is stored in the cloud systems and these two are the major concerns that should be guaranteed.

IV. SERVICE LEVEL AGREEMENTS (SLA) FOR ENHANCING CLOUD SECURITY

SLA is one of the most important protocols for ensuring transparency within cloud computing. It is the only legal agreement between the client and the service provider. SLA is the only means through which the cloud service provider can gain the trust of the client and its importance is discussed greatly in article titled "Cloud Security Issues" [30].

As the cloud computing marketplace is very competitive now days, it is quite expected that all providers will not be able to provide the similar level of security to their customers. Furthermore, varying levels of security may be provided by the cloud service providers depends upon the cost that customer pays to the service provider. However a cloud SLA could be extended to cover security aspects which have been outlined by Bernsmed et al. [31, 32], it allows composition of cloud services from several service providers with a defined security level.

A lifecycle will typically be followed by the Security SLA where the provider will generically publish them first, and the user, who wishes to use the cloud service, will then negotiate a specific SLA to which the provider will commit, and then the service will be provisioned. In order to ensure that the negotiated SLA is being adhered to by the provider, the user may want to the service. The cycle may return to the negotiation phase at any time during the commitment, provisioning and monitoring phases, for e.g., if the provider after all cannot commit to the previously negotiated SLA. In federated cloud services, these negotiations can be performed at multiple levels.

V. UNTRUSTED CLOUD STORAGE PROVIDERS

V/S TRUSTED DATA SHARING

Most of the IT infrastructure and data storage are shifted by cloud computing to off-premises third-party providers, with two important consequences (a) There is limited control of Data owners over the IT infrastructure, hence a mechanism should be established by the data owners to mandatorily enforce their security policies for ensuring data confidentiality and integrity; (b) The excessive privileges are given to clod providers, which allows them to have extensive control and ability to modify users' IT systems and data [33].

Because of these consequences a trust level is very low while keeping and sharing data on a cloud, especially in a business model where secure data processing is strictly required in order to safeguard business interests. Therefore, for enabling trusted data sharing through untrusted cloud providers a secure system is essentially required. The access control policies of data owners should furthermore be imposed by the system, which would prevent the illegal accessing of data by cloud storage providers or other unauthorized users. Figure 2 is a simple representation of this requirement.

For securing data storage in the cloud various security requirements can be summarized as follows:

1. The data confidentiality should not be compromised by the cloud service provider by any means and therefore the data stored on cloud should be kept private.
2. The authorization of data sharing is fully controlled by the data owner. The designated user can be able to access the data kept on the cloud only when the authorization is given by the data owner. Nevertheless, the cloud provider should not be given any right by the process to access the data.
3. Only the intended users are designated for data access authorization. The other users who don't have the data access authorization permission, the data accessing permissions should not be exercised by them.

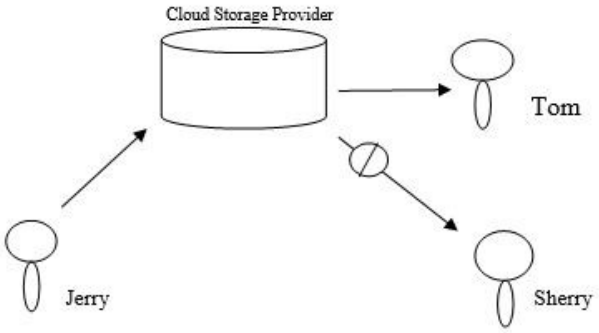

Figure 2. Secure Sharing On a Cloud

An untrusted cloud storage provider should achieve the above requirements of secure data sharing. The cloud storage provider should necessarily enforce the authorization policy for data access, but any information should not be revealed by this enforcement to the cloud storage provider or the cloud storage provider should not have excessive privileges to allow an unauthorized access. By using either incremental encryption or holomorphic encryption these requirements can be achieved.

The cryptography scheme where algebraic operations applied on the cipher-text are directly reflected in the corresponding plaintext is called the Holomorphic encryption [34]. A third party is able to compute the sum of two encrypted numbers, and when the user is given this encrypted result, then with the help of original key it can be decrypted, and we get the same result as the sum of the two numbers in plaintext form. This allows multiple parties to cooperatively generate a piece of cipher-text without knowing the plaintext that others work on.

In the Incremental encryption [35, 36] the initial cipher-text and the change of the plaintext helps in the computation of the final cipher-text. Rong et al. [37, 38] propose an incremental encryption scheme which is based on elliptic curve cryptography and is different than that presented by Bellare et al. [35, 36]. This mechanism provides the facility to the users to have trusted data storage and sharing over untrusted cloud storage providers. This facility of implementing trusted services on untrusted cloud storage providers allows managing the data of the users on any cloud storage provider, which eliminates the required trust on the providers. Figure 3 shows the scheme for preventing data leakage. The basic idea is that before the data is stored in the cloud, it is encrypted. While sharing the data, the encrypted data will be encrypted again without being decrypted first. The

again encrypted data will then be cryptographically accessible with the help of corresponding token only to the authorized user.

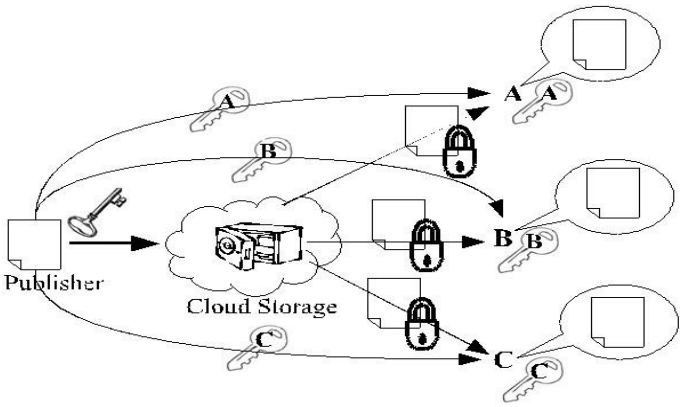

Figure 3. A Solution for preventing Cloud Data leakage

In this whole process the clear-text data is not revealed to the cloud provider at any stage, which prevents the data from being shared without the permission of the data owner. The data is always in its encrypted form during the sharing, though it may be encrypted with different keys at different stages. At not even a single stage the data is decrypted into its clear form before it is delivered to the authorized users. Therefore it is ensured that the information of the data will not be disclosed to any parties during the whole sharing process.

VI. CLOUD ACCOUNTABILITY

We know that for cloud the bulletproof confidentiality-preserving solutions will remain a desirable goal, it is quite clear that in the cloud as long as big data needs to be processed, currently there are no sufficiently efficient mechanisms that can make this happen without letting the cloud providers have access to clear-text data. Therefore, a need for other mechanisms is arising that can remove the fears of users that otherwise might be scared away from using the cloud.

The thing that is preventing many users from reaping the benefits of the cloud is the current lack of transparency which is highlighted by Pearson et al. [39, 40]. Various cloud services are currently working smoothly in daily use, but a little thought must be given to what would happen if the things go wrong; the local authorities can seize equipment with stored data, or the cloud providers may go bankrupt, and so forth. Furthermore, as it is already stated that the current cloud services are offered in a way that implies that the full trust of the customer must be placed on the provider; such trust may not always be warranted as long as there are fallible humans in the loop.

The challenge of complying with multiple, sometimes conflicting, legal codes, is also introduced by the cross-border nature of cloud computing especially when data is of a personal sensitive nature. In 2011 it was stated by Pearson [40] that transparency, responsibility, assurance and remediation are the central components of the notion of accountability. It is also argued by her that a move from only retrospective to also prospective accountability is needed, which extends mechanisms for implementing security policies to encompass both reactive and pre-emptive mechanisms, i.e., both prevents bad things from being happening, and establishes that bad things did happen, if they could not be prevented.

Re-engineering of many services will be required for achieving accountability in clouds for incorporating legal mechanisms, procedures and technical measures to support such prospective and retrospective accountability mechanisms. The deployment of security SLA mechanisms can be one small component of this work as described in Section 4.

VII. CONCLUSION

With the help of Cloud computing the companies reduce operating costs while increasing efficiency hence cloud computing is a very promising technology. Security in cloud computing is still in its infancy and needs more research attention, even though cloud computing has been deployed and used in production environments. Our paper presents a survey regarding cloud computing security and a number of possible research topics are also discussed to improve the security in cloud.

We have presented an overview of cloud computing, its advantages and classifications. After that the security issues in the current cloud computing model were discussed. From the current security issues with cloud computing, the three areas of particular interest were emphasized upon, which are SLAs, trusted data sharing, and cloud accountability. The ongoing work on SLAs cloud security is outlined by us, and a scheme to address the cloud security and privacy issue is also presented by us. We have also presented a solution to provide security and privacy for user data when it is located in a public cloud since secure data storage in cloud environment is a significant concern which prevents many users from using

the cloud. As there are still a number applications that rely on accessing "clear-text" data in the cloud, therefore this secure storage solution does not always fits. The need for further work on accountability mechanisms in public clouds, in order to provide transparent services that can be trusted by all users is also highlighted by us.

VIII.REFERENCES

[1] 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.

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

[3] 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.

[4] 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].

[5] 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.

[6] 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].

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

[8] 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.

[9] 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. <http://dx.doi.org/10.1007/978-3-642-10665-1_42>.

[10] Amazon. Amazon Elastic Compute Cloud (EC2). <http://aws.amazon.com/ec2/>.

[11] Lee Hong Joo. Analysis of business attributes in information technology environments. J Inform Process Syst 2011;7(2):385–96.

[12] M. Casassa-Mont, S. Pearson and P. Bramhall, "Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services", Proc. DEXA 2003, IEEE Computer Society, 2003, pp. 377-382.

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

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

[15] Salesforce. Groupon expands throughout the US and beyond with salesforce; 2011. <http://www.salesforce.com/showcase/stories/groupon.jsp>.

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

[17] Google. Google App Engine. <http://code.google.com/appengine/>.

[18] https://www.pcisecuritystandards.org/index.shtml.

[19] Dropbox, Where Are My Files Stored?; 2011. <http://www.dropbox.com/help/7> [retrieved 26.04.17].

[20] http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_ Security_Standard, 24 January 2010.

[21] J. Salmon, "Clouded in uncertainty – the legal pitfalls of cloud computing", Computing, 24 Sept 2008, http://www.computing.co.uk/computing/features/2226701/cl ouded-uncertainty-4229153.

[22] Gartner: Seven cloud-computing security risks. InfoWorld. 2008-07-02. http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputing-security-risks-853.

[23] Cloud Security Front and Center. Forrester Research. 2009-11-18. http://blogs.forrester.com/srm/2009/11/cloud-security-front-andcenter.html.

[24] Cloud Security Alliance. http://www.cloudsecurityalliance.org.

[25] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1,

http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf.

[26] S. Subashini, V.Kavitha. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications 34(2011)1-11.

[27] Mohamed Al Morsy, John Grundy, Ingo Müller, "An Analysis of The Cloud Computing Security Problem," in Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov 2010.

[28] Yanpei Chen, Vern Paxson, Randy H. Katz, "What's New About Cloud Computing Security?" Technical Report No. UCB/EECS-2010-5. http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html.

[29] 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 15.09.17].

[30] Balachandra R K, Ramakrishna P V, Dr. Rakshit A, 'Cloud Security Issues', 2009 IEEE International Conference on Services Computing, viewed 26 October 2009, pp 517-520.

[31] 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.

[32] 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.

[33] 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.

[34] 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].

[35] 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.

[36] 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.

[37] 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.

[38] Rong Chunming, Zhao Gansen. Incremental encryption. Norwegian Patent No. P3683NO00-DT (Pending).

[39] 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>.

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