3rd International Conference on Recent Innovations in Science Engineering and Management
Sri Venkateswara College of Engineering and Technology,Srikakulam,Andhra Pradesh (ICRISEM-16)
27 February 2016, www.conferenceworld.in ISBN: 978-81-932074-1-3

# CLOUD COMPUTING ENVIRONMENT: A MULTI-LEVEL SECURITY FRAMEWORK

**Satinder**

*Assistant Prof.(Extn.), Department of Computer Science, Govt. College, Hisar, Haryana, (India)*

**ABSTRACT**

*Cloud Computing environment is a new emerging trend of information technology. There is an impressive change in computational power, storage and network communication technologies. These changes let human being to generate process and share huge sets of information and data/ services via the internet. Cloud computing is a completely internet dependent technology where client data is stored and maintain in the data center of a cloud service providers (CSP's). Limited control over the data may incur various security issues and threats which include data leakage, insecure interface, sharing of resources, data availability and inside attacks. There are various research challenges also there for adopting cloud computing such as well managed service level agreement, privacy, interoperability and reliability. The proposed work aims to enhance authorization and authentication process by using multilevel authentication to protect cloud from malicious user and unauthorized access, implement security measure to protect data of users stored in cloud environment. The multilevel security system for cloud storage is also support to avoid duplication and maintain unnecessary disk utilization to increase the cloud server performance.*

***Keywords: Cloud Computing, Crypto systems, Security, Multi-level framework.***

## I. INTRODUCTION

There is an impressive change in computational power, storage and network communication technologies, from last few years. These changes let human being to generate process and share huge sets of information and data. Cloud Computing is a new and emerging technology innovation that bring the concept of virtualization of data and information storage in local infrastructure. It gives permission to customers and businesses to use applications without installation and access their personal files, data and information at any corner of the world with the help of internet. It also provides the service of dynamic storage capacity, computing capacity, data and information exchanging capability using networking. The "cloud" is an allegory – it is abstraction hiding the complicated infrastructure of the Internet Technology. It is a low-cost usable option to the end users in which IT-related capabilities are given "pay-as-a-service", allowing users to access Internet technology, which supply and deliver to the users with Information Technology services according to their demands. Cloud computing is categorized into two main parts: Front End and Back End. Front End is customer or client or any application (i.e. web browser etc.) which is uses the cloud services and Back End is the network of servers with a computer programs and data storage system. The idea of cloud computing is based on a very fundamental principal of

"reusability of IT capabilities". The difference that cloud computing brings compared to traditional concepts of "grid computing", "distributed computing", "utility computing", or "autonomic computing" is to broaden horizons across organizational boundaries.

Although there are many benefits to adopting Cloud Computing, there are also some significant barriers to adoption. One of the most significant barriers to adoption is security, followed by issues regarding compliance, privacy and legal matters. Because Cloud Computing represents a relatively new computing model, there is a great deal of uncertainty about how security at all levels (e.g., network, host, application, and data levels) can be achieved and how applications security is moved to Cloud Computing. In this paper we attempt to demystify the multi-level security challenges introduced in a cloud environment and clarify issues from a security perspective. The notion of trust and security is investigated and specific security requirements are documented. The research methodology adopted towards achieving this goal, is based on software engineering and information systems design approaches.

### 1.1 Definition

Cloud computing is internet-based computing and latest trend in information technology (IT) world. The internet is frequently represented as a cloud and the term "cloud computing" arises from that analogy.

Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These property can be energetically reconfigured to adjust to a variable load (scale) allowing also for best possible resource utilization. This group of resources is typically demoralized by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized service level agreements.

According to Forrester, *"A pool of abstracted, highly scalable, and managed compute infrastructure capable of hosting end customer applications and billed by consumption."*

## II. RELEATED WORK

Different types of approaches are developed in the past decades by researchers for solving, cloud computing security problems. As users no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted. In particular, simply downloading all the data for its integrity verification is not practical solution due to the expensiveness in input and output transmission cost across the network. Besides, it is often insufficient to detect the data corruption only at the same time accessing the data, as it does not give users correctness assurance for those un accessed data and might be too late to recover the data loss or damage.

Merkle ,proposed a paper to describe a number of cryptographic protocols. Certainly, these are not only possible valuable tools to the system designer can be achieved and provide feasible solutions to problems of recurring interest. It gives only basic ideas and methods to implement public crypto systems. But it doesn't have an enhancement for the cloud security solution.

Boneh, proposed a short signature scheme based on the Computational Diffe-Hellman assumption on certain elliptic and hyper-elliptic curves. The signature length is half the size of a Digital Signature Algorithm for a similar level of security. This short signature scheme is designed for systems signatures are typed in by a human or signatures are sent over a low-bandwidth channel. It has a problem in Key generation on high bandwidth.

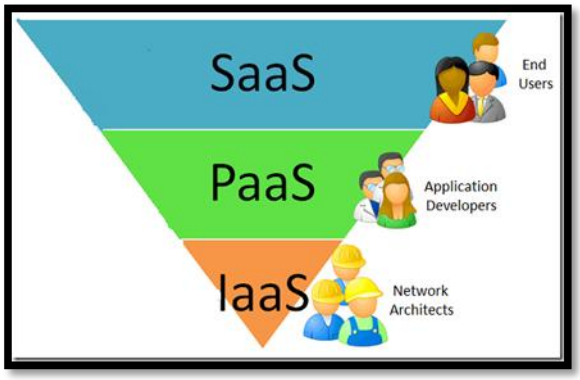
ISBN: 978-81-932074-1-3

Mary Michael, proposed the method of Delegating Log Management to the Cloud Using Secure Logging In this method investigate the tough challenges against the secure cloud management service. It provides a comprehensive solution for storing and maintains log records in a server operating in cloud-based environment. Also address security and integrity issues not only just during the log generation phase but also during other stage in the log management.

Ateniese and Kamara, provide a framework for building public-key Homomorphic Linear Authenticator from any identification protocol satisfying certain homomorphic properties. The research shows to turn any public-key Homomorphic Linear Authentication into a publicly verifiable Proofs of Storage with communication complexity independent of the file length and supporting an unbounded number of verifications. This research illustrate the use of our transformations by applying them to a variant of an identification protocol by Shoup, thus obtaining the first unbounded-use Proofs of Storage based on factoring.

## III. CLOUD COMPUTING DELIVERY MODEL

Cloud computing normally works on service-oriented architecture in nature. It can be easily integrated with other systems. Cloud computing architecture is based on three types of abstraction layer and each layer has its own services and responsibility of work.




### a. Software as a Service (Saas)

SaaS is based on pay-per-use basis costing model where software applications are leased out to contracted organizations by specialized SaaS sellers. SaaS giver may host the software either in their own data network center. Initially software has limited functionality, it can be easily customized based on demand which is billed accordingly Softwares are accessed using secured web browser over the Internet. Web services (WS) security, XML encryption, Secure Socket Layer (SSL) etc is used in enforcing data protection transmitted over the Internet.

### b. Platform as a Service (Paas)

PaaS cloud model layer is similar to IaaS model with an additional “rented” feature. Virtual machines are secured against unauthorized attacks such as cloud malware and hackers. PaaS model services are expensive than IaaS and SaaS. Cloud sellers and users need to maintain cloud computing network security at all interfaces. In a virtual platforms physical resources, infrastructures as well as business applications and middle wares environment are being consumed as services in the cloud models.

**c. Infrastructure as a Service (Iaas)**

IaaS is a single layer cloud model where cloud computing vendor's dedicated resources are only shared with contracted users at pay-per-use service. This model is also provides different degrees of financial and functional pliability which is not found in inside data servers or with co-location services, because computing resources can be added or released much more quickly and cost-effectively than in an internal data servers As a initial investment cost of computer servers, results, networking devices, processing power etc. are minimized.

## IV. DEPLOYMENT MODEL OF CLOUD COMPUTING

It is most primary to decide which type of cloud model is selected for secure cloud services. There are basically four types of deployment model in cloud computing.

**a. Public Cloud**

A network that is open and uses only for publicly purpose is called Public cloud. This model is based on pay-per-use method, same as prepaid electric meter technology. It is ideal for businesses seeking less complex Information technology hosting. Public cloud allows user's access to the cloud via interfaces using mainstream web browser. Applications run on it have either seasoned demand or unforeseeable traffic. It is less secure cloud models

**b. Private Cloud**

Private cloud model is designed with organization's internal enterprise data center. Here scalable resources and virtual services are provided by the cloud vendors are combine together and available for cloud users to share and use Only the organization people and designated stakeholders may have use to operate on a specific private cloud. Thus, private cloud model is much more secure than public cloud model. Just like Intranet, all there sources and applications are managed by organization itself.

**c. Hybrid Cloud**

Hybrid cloud is a combination of both public cloud model and private cloud model which is centrally circumscribed and managed by a secure network. It gives more secure control of the data and applications and provides various parties to access data and information over the Internet.

**d. Community Cloud**

Infrastructure shared by several organizations for a shared cause and may be managed by them or a third party service provider and rarely offered cloud model. These clouds are normally based on an agreement between related business organizations such as banking or educational organizations. A cloud environment operating according to this model may exist locally or remotely.

## V. SECURITY ISSUES WITH CLOUD COMPUTING

Cloud computing consists of applications, platforms and infrastructure segments. Each segment performs different operations and offers different products for businesses and individuals around the world. The business application includes Software as a Service (SaaS), Utility Computing, Web Services, Platform as a Service (PaaS), Managed Service Providers (MSP), Service Commerce and Internet Integration. There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency

control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. The given below are the various security concerns in a cloud computing environment.

a. **Access to Servers & Applications:** In traditional datacenters, administrative access to servers is controlled and restricted to direct or on-premise connections which are not the case of cloud data centers. In cloud computing administrative access must be conducted via the Internet, increasing exposure and risk. It is extremely important to restrict administrative access to data and monitor this access to maintain visibility of changes in system control. Data access issue is mainly related to security policies provided to the users while accessing the data. The security policies may entitle some considerations wherein some of the employees are not given access to certain amount of data.

b. **Data Transmission:** Encryption techniques are used for data in transmission. To provide the protection for data only goes where the customer wants it to go by using authentication and integrity and is not modified in transmission. SSL/TLS protocols are used here. In Cloud environment most of the data is not encrypted in the processing time, But to process data, for any application that data must be unencrypted. To provide the confidentiality and integrity of data-in-transmission to and from cloud provider by using access controls like authorization, authentication, auditing for using resources, and ensure the availability of the Internet-facing resources at cloud provider. Man-in-the-middle attacks is cryptographic attack is carried out when an attacker can place themselves in the communication's path between the users. Here, there is the possibility that they can interrupt and change communications.

c. **Virtual Machine Security:** Virtualization is one of the main components of a cloud. Virtual machines are dynamic i.e. it can quickly be reverted to previous instances, paused and restarted, relatively easily. Ensuring that different instances running on the same physical machine are isolated from each other is a major task of virtualization. They can also be readily cloned and seamlessly moved between physical servers. Vulnerabilities or configuration errors may be unknowingly propagated. Also, it is difficult to maintain an auditable record of the security state of a virtual machine at any given point in time.

d. **Network Security:** Networks are classified into many types like shared and non-shared, public or private, small area or large area networks and each of them have a number of security threats to deal with. Problems associated with the network level security comprise of DNS attacks, Sniffer attacks, issue of reused IP address, etc which are explained in details as follows. A Domain Name Server (DNS) server performs the translation of a domain name to an IP address. Since the domain names are much easier to remember. Hence, the DNS servers are needed. But there are cases when having called the server by name, the user has been routed to some other evil cloud instead of the one he asked for and hence using IP address is not always feasible. Although using DNS security measures like: Domain Name System Security Extensions (DNSSEC) reduces the effects of DNS threats but still there are cases when these security measures prove to be inadequate when the path between a sender and a receiver gets rerouted through some evil connection.

e. **Data security:** For general user, it is quite easy to find the possible storage on the side that offers the service of cloud computing. The most common utilized communication protocol is Hypertext Transfer Protocol (HTTP). In order to assure the information security and data integrity, Hypertext Transfer Protocol Secure (HTTPS) and Secure Shell (SSH) are the most common adoption. In cloud computing, the enterprise data is stored outside the enterprise boundary, at the Service provider end. Consequently, the service

provider must adopt additional security checks to ensure data security and prevent breaches due to security vulnerabilities in the application or through malicious employees.

f. **Data Privacy:** The data privacy is also one of the key concerns for Cloud computing. A privacy steering committee should also be created to help make decisions related to data privacy.

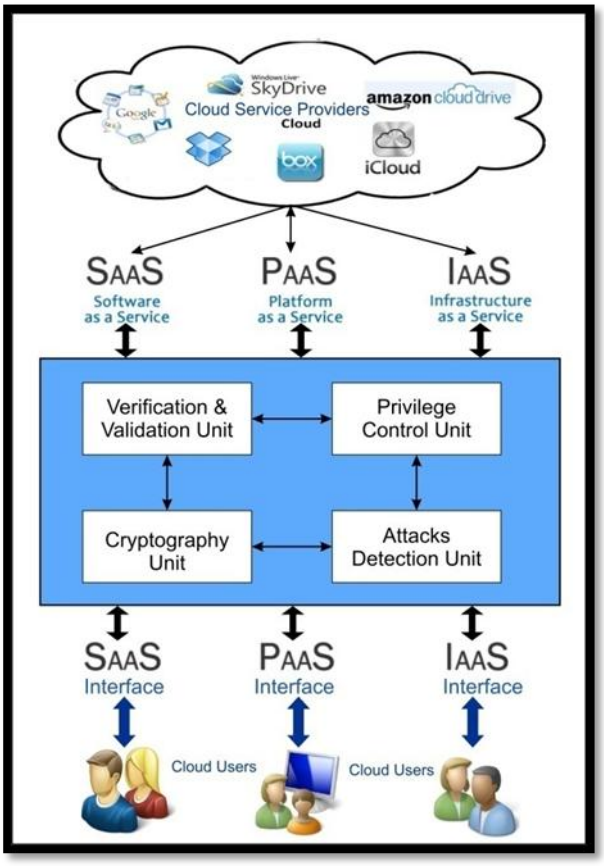
g. **Data Integrity:** Data corruption can happen at any level of storage and with any type of media, So Integrity monitoring is essential in cloud storage which is critical for any data center. Data integrity is easily achieved in a standalone system with a single database. Data integrity in such a system is maintained via database constraints and transactions.

h. **Insecure Interface and API:** The cloud providers deliver the cloud services via different interfaces and API where customers have freedom to choose interface and interact with cloud services. It's been observed that the security and availability of general cloud services is dependent on the security of interfaces and API [1]. Some time cloud users share their interface and API to access the cloud services and due to the week knowledge of security aspects, users will allow to such interfaces to store and use their personal information in the form of remember password, transaction history, scripts, cookies and additional plug inns. So its responsibility to cloud provider to invent an API and interface in such a way that interface need only meaningful information of users to provide access to cloud services and do not store user's personal information such as passwords, cookies, scripts, transaction history even user wishes to do it.

i. **Identity Management:** The proper identity of customer will help to manage the uniqueness of each user and to carry out such things the different levels of user authentication and validation schemes being implemented in cloud but still the access control will create a threat. Apart from authentication the identity management should have control over the user's privileges and access to required resources [5]. Cloud should have capability to formulate and maintain user privileges about its access and task that user will performs on cloud as a part of identity management.

j. **Shared Technology Issues:** IaaS deliver the service of sharable infrastructure between multiple users. The underlying components such as CPU and Memory were not designed to offer strong isolation properties. To address this gap a virtualization hyper visor between guest operating system and the physical compute resources [3]. Strong compartmentalization must be implemented to avoid the access and control over the sharable infrastructure and the individual customers should not impact on other customers operation.

## VI. MULTILEVEL SECURITY FRAMEWORK FOR CLOUD COMPUTING




Cloud Computing Security Model

***A. Verification and Validation Unit:***

The main task of any cloud security is to verify and validate the proper users and to ensure that the correctness of data and services on the cloud. Here the user authentication mechanism will identify the user and allocates privileges and authorization as per the prescribe norms. To maintain the authentication of user on cloud we can implements various techniques such as simple user name and password protection scheme, Graphical passwords protection scheme or bio information based user authentication as per the requirements of data and cloud services. Digital signature is one the era of user authentication and authorization where documents being verified on the basis of digital signature to maintain the secrecy.

*1) Provide Secure Interface*

During verification and validation of user most of the Interfaces and API are stored the user personal information such as remember password, transaction history, scripts, cookies and additional plug inns without concerning or with concern to users. This information some time will access by cloud service provider to track the client and maintain the web traffic records. Sometime it will reach to intruder and entire securities of user as well as service provider get leaked to the outside world. So its responsibility to cloud provider to invent an API and interface in such a way that they will need only important information of users to provide interaction with cloud services and do not store user personal information such as passwords, cookies, transaction history even user wishes to do it.

***B. Privileged Control Unit:***

On cloud there are millions and billions of users who are performing thousands of operation of same or different data element in a same or different area of computing. To manage the privacy and secrecy among these people is really a tedious job. Here privileged based separation will reduce the burden of mixing. This unit is essential because it protects users' privacy and security. It ensures that data integrity and confidentiality by applying a set of regulations and policies that govern the authorization process of cloud users [2]. Only authorized customers get access to data. Privileges set by cloud service provider as per the security norms fulfilled by services users. Privileges may verify time to time using public key encryption.

*1) Policy Approach:*

In this framework the cloud should make a decision about to enforce privacy protection mechanism publically or privately to the access of data stored on cloud server either concerning to user or automatically [6]. Every user should specify the private or public access to all its data. Every file, documents, or data unit should consist of these policy norms, and if any user forgets to specify security policy then automatically security norms being allocated to its all data elements on cloud server. If any other person want to access data preset on cloud but it belongs to other user then policy approach will take into consideration and as per the security approach if data is available publically then other user will get access to it otherwise access should denied to that documents or files. Important documents such as financial data or personal data may be protected by introducing the run time alert on user's mobile phone.

***C. Cryptography Approach***

Cryptography is a method to provide the data security in the cloud network. The original text is called as plain text and sometimes called as clear text. The plain text is covert in to cipher text format is called as Encryption. The cipher text is convert into plain text is called as Decryption. Encryption is performed in the source place and Decryption is performed by destination place. There are two types of algorithms used for cryptography method one is symmetric approach and another is asymmetric approach. In symmetric approach encryption and decryption is used same key for data security. The different symmetric algorithm comparison is presented in Table 1. The asymmetric approach encryption and decryption is used different keys it is suitable for shared network data transmission.

| PARAMETERS | DES | 3DES | AES |
|---|---|---|---|
| Block Size | 64 bits | 64 bits | 128 bits |
| Key length | 56 bits | 112,168 bits | 128,192,256 |
| Number of Rounds | 16 | 48 | 10,12,14 |
| Security level | Not enough | Adequate | Excellent |
| Execution time | Slow | Very slow | More fast |

**Table i. Symmetric algorithm comparison**

The comparison of symmetric algorithm Advanced Encryption Standard (AES) is the best algorithm for secure data storage in the cloud domain. AES algorithm used key size is 128 bits, 192 bits or 256 bits. The bits within such sequences will be numbered starting at zero and ending at one less than the sequence length. All byte values in the AES algorithm will be presented as the concatenation of its individual bit values 0 and1 between braces in the order {b7, b6, b5, b4, b3, b2, b1, b0}. The AES algorithm performs four functions in each round encryption and inverse function of four operations performed in the decryption.

**SubBytes:** The SubByte transformation is a non-linear byte substitution that operates independently based on the S- Box substitution table. In S-Box one byte is substituted for another based on substitution algorithm.

**ShiftRows:** The ShfitRows performs the bytes in the last three rows of the state are cyclically shifted over different number of bytes. Row zero of the state is not shifted, row one is shifted one byte, row two is shifted two bytes and row three is shifted three bytes.

**MixColumns:** The MixColumns provides by mixing data within columns. The four bytes of each column in the state are treated as a four byte number and transformed to another four byte number.

**AddRoundKey:** The actual encryption is performed in the AddRoundKey function, each byte in the state is XORed with the sub key.

***D. Attack Detection Unit:***

This unit is responsible to stop the unwanted operation carried out by intruder on physical or logical resources of the cloud. To stop the attacks first there is need to detect and identify the type of an attack. This unit is identify the software attack by introducing the software based solution such as log file information, history, web analytics, IP address, Mobile No, decryption key, Service provider and other things being implemented in the software security form.

## VII. CONCLUSION

In this paper, we first discussed various delivery models, deployment models of cloud computing and security issues in cloud computing environment. Data security is major issue for Cloud Computing. Users do not want to lose their confidential data and information as a result of malicious insiders in the cloud. There are several other security challenges including security aspects of network and virtualization. The research work is extending to focus on data security in the cloud computing. In this paper it's explained that if we implement the multilevel security framework on cloud then customer can enjoy the outcome without any worry. The file is successfully uploaded in the cloud storage after only the encryption is performed to implement the security in the cloud. The forthcoming work the data owner will encrypt the file using cryptography algorithm and store the virtual drive in the local system to upload the content to the cloud server. Apart from this it is responsibility of cloud users and cloud provider organizations should enforce some security and privacy policies to protect cloud. There is wide scope for researcher and developers to introduce the new era knowledge in the area of security and privacy of cloud and it will bind strong and secure relation between cloud users and their vendors.

## REFERENCES

[1.] Harish shah, Shrikant, Sharma Shankar Anadane, "Security Issues in Cloud Computing".

[2.] Ahmad Youssef, "A Framework for secure cloud computing", IJCSI international Journal of Computer Science, Issues, Vol 9, Issues4, N0 3 July 2012, ISSN(Online) 1694-0814, www.IJCSI.org

[3.] Ramasami S., Umamaheshwari P., Survey on data security issues and data security model in cloud computing, International Journal of Engineering and Technology (IJEIT), Volume 1, issue 3,March 2012.

[4.] Ayesha Malik, Muhammad Moshin Nazir, Security Framework for cloud computing environment : A review, Journal of engineering trends in computing and information sciences, vol. 3 No. 3 March 2012, ISSN 2079-8407.

[5.] Wayne A. Jansen, NIST, Cloud hooks: Security and Privacy in cloud computing, Proceeding of the Hawaii International conferences on System Sciences-2011.

[6.] Peter Mell, and Tim Grance, "The NIST Definition of Cloud Computing,"2009, http://www.wheresmyserver.co.nz/storage/media/faqfiles/clouddef-v15.pdf, Accessed April 2010.

[7.] F. Soleimanian, S. Hashemi, "Security Challenges in Cloud Computing with More Emphasis on Trust and Privacy", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, Vol. 1, ISSUE 6, pp. 49-54, 2012.

[8.] S. Qaisar, K.F. Khawaja, Cloud Computing: Network/Security Threats and Countermeasures, Interdisciplinary journal of con-temporary research in business, Vol.3, No 9, p. 1323-1329, 2012.

[9.] J.R. Winkler, Securing the Cloud: Cloud Computer Security Techniques and Tactics, Technical EditorBill Meine, Elsevier Publishing, 2011.

[10.] Satinder, Niharika, IMPACTS OF CLOUD COMPUTING ON E-COMMERCE BUSINESSES IN INDIA, International Journal of Advance Research In Science And Engineering IJARSE, Vol. No.4, Special Issue (01), April 2015

[11.] A Platform Computing Whitepaper. "Enterprise Cloud Computing: Transforming IT." Platform Computing, pp6, 2010.

[12.] S. Subashini and V. Kavitha. (2010) "A survey on security issues in service delivery models of cloud computing." J Network Comput Appl doi:10.1016/j.jnca.2010.07.006. Jul.,2010.

[13.] J. Brodkin. (2008, Jun.). "Gartner: Seven cloud-computing security risks." Infoworld,Available: http://www.infoworld.com/d/securitycentral/gartner-seven-cloudcomputingsecurity-risks-853?page=0,1 [Mar. 13, 2009].

[14.] New IDC IT Cloud Services Survey: Top Benefits and Challenges. Retrieved April 8, 2011 from http://blogs.idc.com/ie/?p=730.

[15.] C. Wang, Q. Wang, K. Ren, and W. Lou (2010), „Privacy-Preserving Public Auditing for Storage Security in Cloud Computing", Proc.IEEE INFOCOM "10.

[16.] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia (2009), „Above the Clouds: A Berkeley View of Cloud Computing", Technical Report UCB-EECS-2009-28, Univ. of California, Berkeley.

[17.] Cloud Security Alliance (2010), „Top Threats to Cloud Computing", http://www.cloudsecurityalliance.org.

[18.] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li(2011), „Enabling Public Auditability and Data Dynamics for Storage Security in Cloud mputing", IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859.

[19.] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song(2007), „Provable Data Possession at Untrusted Stores",Proc. 14th ACM Conf. Computer and Comm. Security (CCS "07), pp. 598-609.

[20.] M.A. Shah, R. Swaminathan, and M. Baker (2008), „Privacy-Preserving Audit and Extraction of Digital Contents", Cryptology ePrint Archive, Report 2008/186.

[21.] A. Juels and J. Burton, S. Kaliski (2007), „PORs: Proofs of Retrievability for Large Files", Proc. ACM Conf. Computer and Comm. Security (CCS "07), pp. 584-597.

ISBN: 978-81-932074-1-3

[22.] Cloud Security Alliance(2009), „Security Guidance for Critical Areas of Focus in Cloud Computing", http://www.cloudsecurityalliance.org.

[23.] H. Shacham and B. Waters(2008), „Compact Proofs of Retrievability", Proc. Int"l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (Asiacrypt), vol. 5350, pp. 90-107.

[24.] C. Wang, K. Ren, W. Lou, and J. Li(2010), „Towards Publicly Auditable Secure Cloud Data Storage Services", IEEE Network Magazine, vol.24, no. 4, pp. 19-24.

[25.] R. Curtmola, O. Khan, and R. Burns(2008), „Robust Remote Data Checking", Proc. Fourth ACM Int"l Workshop Storage Security and Survivability (StorageSS "08), pp. 63-68.