ISSN:0975-9646
Niti Jain et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (5) , 2016, 2250-2255

An Robust Approach for Secure Sharing Using Cloud Computing

Niti Jain, Prof. Rahul Anjana
Dept. of Information Technology
Shree Vaishnav Institute of Technology and Science
Indore, India

Abstract*— Cloud computing is the intelligent framework that offers viable and minimal effort computation on demand as a support of end users. It is made possible by utilizing network computation and outsourced storage easily of share and process utilizing some third party infrastructural resources. Security is critical element of any cloud based application and plays vital role in picking up the trust of its consumer towards safe access of services. It covers all beginning with authentication, access control, privileges taking care of, integrity, confidentiality and malicious use protection. Data sharing is getting exponential prominence for extensive user groups, organizations and businesses towards getting bigger profits and lessened managerial difficult. into another developmental designs and wonders. One of such system is cloud computing who had demonstrated huge enthusiasm of users. Alongside advantages there are a few issues connected with it additionally and had rouses researchers to build up the solution for them. Starting now the computing difficult and the time based computing is changing along these lines to have finish and trusted solution these issues should be understood so as the causes which hinders the cloud development can be expelled. Let us begins with the model hence in cloud we have no less than three actors: user who uploads the data, user who brings the data securely and the storage server who produces and holds temporary files. This work proposes a novel security communication process for cloud environment utilizing authentication, encryption, integrity and self destruction or auto removal of temporary files. The recommended system will likewise controls on temporary file era and removal so if there should be an occurrence of unintentional data releases the system is equipped for ensuring the sensitive information of the users. Our work of proposed cryptosystem is simple and having high efficiency guided by integrity verifications, self destruction and key management.

***Keywords*— Include at least 5 keywords or phrases**

I. INTRODUCTION

Cloud computing is the logical framework that offers effective and low cost computation on demand as a service to end users. It is made feasible by using network computation and outsourced storage with ease of share and compute using some third party infrastructural resources. All of these services are countable and measureable so as to achieve cost effective pay per use modelling. All of these interactions requires high end management of multiple instances for different users using virtual machines and provides isolated services and their settings for user. It serve the purpose of demanded computation as cost effective services. Apart from the benefits the cloud suffers some of the problems associated with migration of security constrains from formal to informal computation using different service models. It is a layered multi-tenant model that offers dynamic scalability in virtualized environment.

Cloud also offers data storage at third party servers and data centers using service providers. They will pay a important role in managing and storing the data and their respective policies. As it was facilitative for user as someone is taking care for your data and controls but somewhere it is high risk that your data is open to even provider itself and he can take a look over any sensitive information you have placed in your account. Thus to make the system more reliable client needs to make some security trusted deals with its data. The actual deployment of cloud computing services is not reliable as they claim because the existing security model doesn‘t work after migration of services to clouds.

Security is another dimension in cloud which needs to be looked and handled according to the arisen situations. Entire service stack of cloud must be monitored to get secure solution deliverables before making it open to all. Many different organizations may be involved in providing infrastructure and application services, which increases the risk of misalignment. Any sort of malfunctioning of cloud service stack included network modelling and exchanges causes high security breaches with open control can completely destroys the applications and their data. Thus to reduces its negative impact the customers should evaluate how their service provider operates and understand the underlying infrastructure and platforms of the service as well as the actual applications.

Requirements for Security

Security is very important feature of any cloud based application and plays vital role in gaining the trust of its consumer towards safe access of services. It covers all starting with authentication, access control, privileges handling, integrity, confidentiality and malicious use protection. For formally counting the requirements the major player of security will take following things into account.

- **Privacy:** This construct deals with protection of users personal profiling and other sensitive information along with its account protection. Here the privacy keeps in concern about the user, owner and the retriever.

- **Data Confidentiality & Integrity:** It deals with protecting the data of users and serves the trustworthiness of the system. The outsider will only store their crucial and sensitive files at third party location when they feels assured of having high protection then local machines. Similarly, concerns about *confidentiality* (who can see the data) and *integrity* (who can modify the data) are important to include in any evaluation. Generally, the more access points to the data, the more complicated the risk profile creation process. Although many regulatory frameworks focus on confidentiality, others, such as Sarbanes-Oxley focus almost exclusively on the integrity of data that is used to produce reports financial statements. To satisfy these requirements cryptographic standards are the well known phenomenon. The main challenges for cryptographic methods include simultaneously achieving system scalability and fine- grained data access control, efficient key/user management, user accountability and etc.
- **Secure data destruction or erasure:** Many organizations have policies that require data to be deleted when it is no longer needed any more, or after a fixed interval. At times, these policies mandate that data deletion be attested to, which may take the form of a statement that the data has been destroyed in a manner that prevents its reconstruction?
- **User Revocation:** When a user is revoked access rights to data, that user should not be able to gain access to the data at any given time. Ideally, user revocation should not affect other authorized users in the group for efficiency purposes.
- **Scalable and Efficient:** Since the number of Cloud users tends to be extremely large and at times unpredictable as users join and leave, it is imperative that the system maintain efficiency as well as be scalability.
- **Collusion between entities:** When considering data sharing methodologies in the Cloud, it is vital that even when certain entities collude, they should still not be able to access any of the data without the data owner's permission. Earlier works of literature on data sharing did not consider this problem, however collusion between entities can never be written off as an unlikely event.

This Paper deals with developing a novel approach for robust security in cloud computing by achieving high data confidentiality, integrity, access control and secure deletion. Later section of this paper covers background, literature, problem definition, proposed solution, benefits and conclusion.

II. BACKGROUND

Data sharing is getting exponential popularity for large user groups, organizations and businesses towards getting larger profits and reduced managerial burdensome. One of such platform which offers high end support and optimized cost is cloud computing. Significantly the cloud offers all the features that are provided by any traditional computing and gives value added benefits to its consumer. It is now of high demand that more and more peoples are going for cloud based data sharing. Along with optimized cost, reduced burden and less management problems associated with cloud computing, security is the major benefits. It increases productivity, ease of access, professional feel and deliberative support for runtime issues. Data sharing in cloud requires some of the preliminary understanding to serve better towards fulfilling its objectives. The user must be assured about its benefitted actors form his sharing and feels confident about data security. The data and its ownership is non transferable but its privileges can be modified dynamically according to its owner. Even the providers have no access over the data of user followed by privacy policies. All it aims to stop unauthorized access of data at any given time. It should also cover the privacy, confidentiality, access control and integrity rules and assures complete and secure deletion of temporary residues.

Development of security solution requires clear understanding of possible attack interfaces. Thus cloud should also provides protection against various attacks such as CSS, XSS, DOS, Law enforcement, Data Theft, Modifications, Flooding etc. Cloud computing offers abstracted service using virtualized and scalable environment through chain of providers which is more vulnerable to attackers. Sharing for data in such untrusted network may also causes attacker to change the data or affects it in some manner hence it should also kept in mind. In last few years various security services and controls had been suggested for web based solution and services but are they capable of serving same objective with cloud environment is the major question today. Let us have a look over role of different security standard over cloud and will understand how to use them for developing a robust approach.

Role of Security Primitives

1) **Access Control and Authentication Using Hash Function:** As this primitive will work as first interaction of user to the system. By providing genuine credential the users gets authenticated for using the cloud service. In some cases the malicious users may get the access information of genuine user and hence gets malicious access to the system then the solution must be capable of removing such users. Hash function is one of the most important primitive which was dealing with these problems using their one way property. Majorly the hash algorithms include Message Authentication Codes (MAC) and Message Digest (MD) algorithms. We can also apply here the fine grained access control mechanism for further improving the security and gives the users privileges based on their behavioral characteristics.
2) **Data Confidentiality Using Cryptographic Standard:** Confidentiality deals with the protection and security of user's important data and let them convert it into certain format which is unreadable to user during the exchange or in unprotected environment it derives no informative relations.

Majorly it covers the way or rules to define who can see the data and its sustaining information. It is achieved using cryptosystems which convert the open text into some unreadable symbols or text. Majorly they are parted into symmetric or asymmetric. But considering the cloud scenarios asymmetric algorithms will proves as better option.

3) **Integrity Using Message Digest Standard:** While the integrity constraints show that the data must be in its original state before and after transmission. Thus if someone intentionally changes the data then the integrity measurement digest is totally distorted and we get which value is corrupted. Mainly it covers that which users can apply modification to the copy of data.
4) **Secure Deletion Using Vanish or Zero Residue Protocol:** All it needs data to be processed by various nodes, has to traverse through various networks, stored on different devices, work simultaneously on multiple copies of data. After the usage period of data is over along with its lifecycle, it should be removed from each and every entity. Normally the lifecycle management includes the production, transfer, use, share, and archive and deleted. The information which is mainly used and public will stays for longer phase and the data with fewer use will detached more recurrently. But in contemporary scenarios there are no such guidelines obtainable for effective data demolition. It could be named in several ways by different authors like destruction, deletion, removal, decommissioning, sanitizing, vanishing, disposal etc.

III. LITERATURE SURVEY

During the last few decades the computing paradigm had changed into a new evolutionary designs and phenomenon. One of such mechanism is cloud computing who had shown massive interest of users. Along with benefits there are some problems associated with it also and had motivates researchers to develop the solution for them. One of such area is cloud security.

In the paper [8] a study is presented that give an inside view to cloud security evolution with high infancy. It puts a statistical analysis of last two decades in involving the cloud phenomenon. Researchers are paying high attention to get better security primitives with cloud computing so as the aim of with study. With literature we have shown some papers and articles that had direct this work to be completed efficiently. The organizations that are moving their business and services towards cloud feel more cost benefits and elastic offerings. The paper also gives some of the security concerns of cloud like confidentiality, integrity and data availability. The study is somewhere guiding us in designing new secure services over cloud.

The paper [9] specifically considers the issues of outsourced data environments along with its current security solutions. Outsourcing the data always reduces the operational and management cost but increase the risk associated with data theft. The paper presents a new construct FADE for enhanced security though fine grained policy based data access control and secure deletion. The FADE is designed with taking the new cryptographic constraints and independent key management consoles for third party services. An implemented solution of FADE is given with Amazon S3 to get empirical analysis of the suggested directions. The result shows minimal performance and monetary cost overhead. The work provides insights of how to incorporate value-added security features into today's cloud storage services.

The paper [10] gives layered construct of security model applied at stagnant situations with different privileges iteratively. It emphasizes mainly on fine grained data access control and flexibility to assure better services. It makes the current access control more robust and relies on high end computation with data confidentiality algorithms. The paper proposes a model named as F2AC as fine-grained, flexible and lightweight model for file storage in cloud computing. IT depends on the tailored policies and dynamically changing users groups according to their security support. The approach covers the privileges transitions and revocations with directed tree and linked leaf model of data structure for implementing the real situations and extensive analysis.

Security not deals with secure sharing but also keeps a record of users file left temporary on different working host which may mis-leaded or informally used by the attacker to affect the system. Thus some of the researchers had worked in tracking a removing these files through some secure deletion approach. The paper [11] proposes a new approach Vanish for secure deletion and maintaining the number of copy records to assure the integrity policies. The model covers the cryptographic key controls, for P2P network along with distributed hash tables to get the complete control of main and temporary files generated during sharing. The implemented proof of Vanish of VizDHT is benefitting several individuals and organization in maintaining their data and files over third party cloud storage nodes.

Carrying forward the above approach the paper [12] puts a light on virtual implementation of these approaches on real cloud. As of now the problem is to erase the complete residues of file exchange and interaction from networked storage and cloud resources. But it is quite difficult to track such data. The paper suggested a model which is based on different policy classes and protection classes guided by deletion attributes. The implementation constructs are presented with secure deletion policies in a modular way to have tightly encrypted deletion. The model and the construction unify and generalize all previous encryption-based techniques for secure deletion. Finally, the paper describes a prototype implementation of a Linux file system with policy-based secure deletion.

In the paper [13] owners security constraints is analyzed with a specific situation to give a trivial solution. It says while exchanging the data if user applies encryption then the data remains information- theoretically secure against the malicious attackers and cloud providers. Whenever the user wants to share its file then he sends the key to other user who shows interest in getting access to that file. Thus any member of the group is interested in getting the complete access of that file must use its private key to decrypt that data. But the approach is

computationally puts burden on user's revocation each time when key needs to be processed. With this approach each user needs to manage a key register for accessing the data and key when he makes modifications with the data. When the data is re-encrypted, the primary user must distribute the new key to the remaining users in the group. In this article, we review existing literature on methods of achieving data sharing in the Cloud that is both secure and efficient

The paper [14] focuses on developing an efficient solution for serving the cryptographic control for network file system which is directing the solution for cloud logically. It makes an comparison with some of the existing approaches for developing the high confidentiality and integrity based random access solution. The paper proposes a novel design based on Message Authentication Control (MAC) using universal hash tables. It gives drastic performance improvements over existing approaches. The paper also defines various security notions for proving the applicability and results of the solution. It is service the needs of both confidentiality and integrity using coreFS, user network file system and proves their results on these notions.

IV. Problem Definition

After studying the evolution of clouds security approaches and linked direction for data confidentiality, integrity, access control and complete deletion we have found some of the issues which remains unaddressed. As of now the computing burdensome and the time based computing is changing thus to have complete and trusted solution these issues needs to be solved so as the causes which hinders the cloud growth can be removed. Let us starts with the model thus in cloud we have at least three actors: user who uploads the data, user who fetches the data securely and the storage server who generates and holds temporary files. Thus the points must be kept in serving these roles is to keep the track of privileges, their flexibility and lightweight nature towards resource consumption. All the above process must be efficiently monitored and with effective authentication control and key management concerns [15].

(i) The current solution is relying only on fulfilling the objective and will not assure the performance factors towards completing the task. As the number of users with exchanges increased then the performance is continuously degrading which affects the resources and cost associated with the secure sharing operations. Thus there must be some process which works in background and assures the performance by monitoring attributes and if their values are going below a certain limit then stops the unnecessary routines and blocks the users causing the problem.

(ii) The system must be capable of identifying the process which hinders the flow of cloud data and affects the security. It will also keeps the track of all integrity rules and policies followed and neglected by the information exchanges and tag the process as secure and unsecure so as to have clear view for user [16].

(iii) The cryptographic content should be handled separately than the normal file and hence the approaches must be of asymmetric nature. The overall process also be followed by some audit rules to get point in time assessment.

(iv) The approach also assures the complete deletion of all the metadata nd restudies of file after interaction so that the malicious users on third party storage or processing nodes may not be able to use it. Here the user must be provided with some control along with cryptographic process to restrict the boundaries of data shared securely using the designed tool.

While drafting the solution finally we could say that the approach must be capable of serving the access control, integrity, data confidentiality and secure deletion for complete security of data exchanges. The solution should also be capable of storing the temporary keys and integrity roots whoever worked on file for any time and keeps along record for that.

V. Proposed Solution

This work proposes a novel security interaction process for cloud environment using authentication, encryption, integrity and self destruction or auto removal of temporary files. The approach works as interface between the storage server cloud server and the user. Somehow the work is also having close grip on access control using its fine grained mechanism and robust key control. Here the key is stored in temporary server with its metadata file containing the file id for which the key stored is associated.

The design of approach must have policy based fine grained access control features in it because the cloud environment is open to all and if users have to face the uncertain situations then the trust over the system gets reduced.

With this development we are also suggesting the tool which works in compatible with the existing cloud tools. The suggested system will also controls on temporary file generation and removal so in case of unintentional data leaks the system is capable of protecting the sensitive information of the users.

Thus the situation is controlled even if the malicious user obtains the copy of data which is made persistent against or using the cryptographic primitives accordingly. It is not relied upon any new external services that need to be developed and deployed accordingly.

- **Components Required**

(i) CSP Server
(ii) Authentication Server (Hash)
(iii) Cryptosystem Server (RSA)
(iv) Integrity Server (MD5)
(v) Destruction Server (Triggers)
(vi) Key Register Server (Key Manager)
(vii) Storage Server

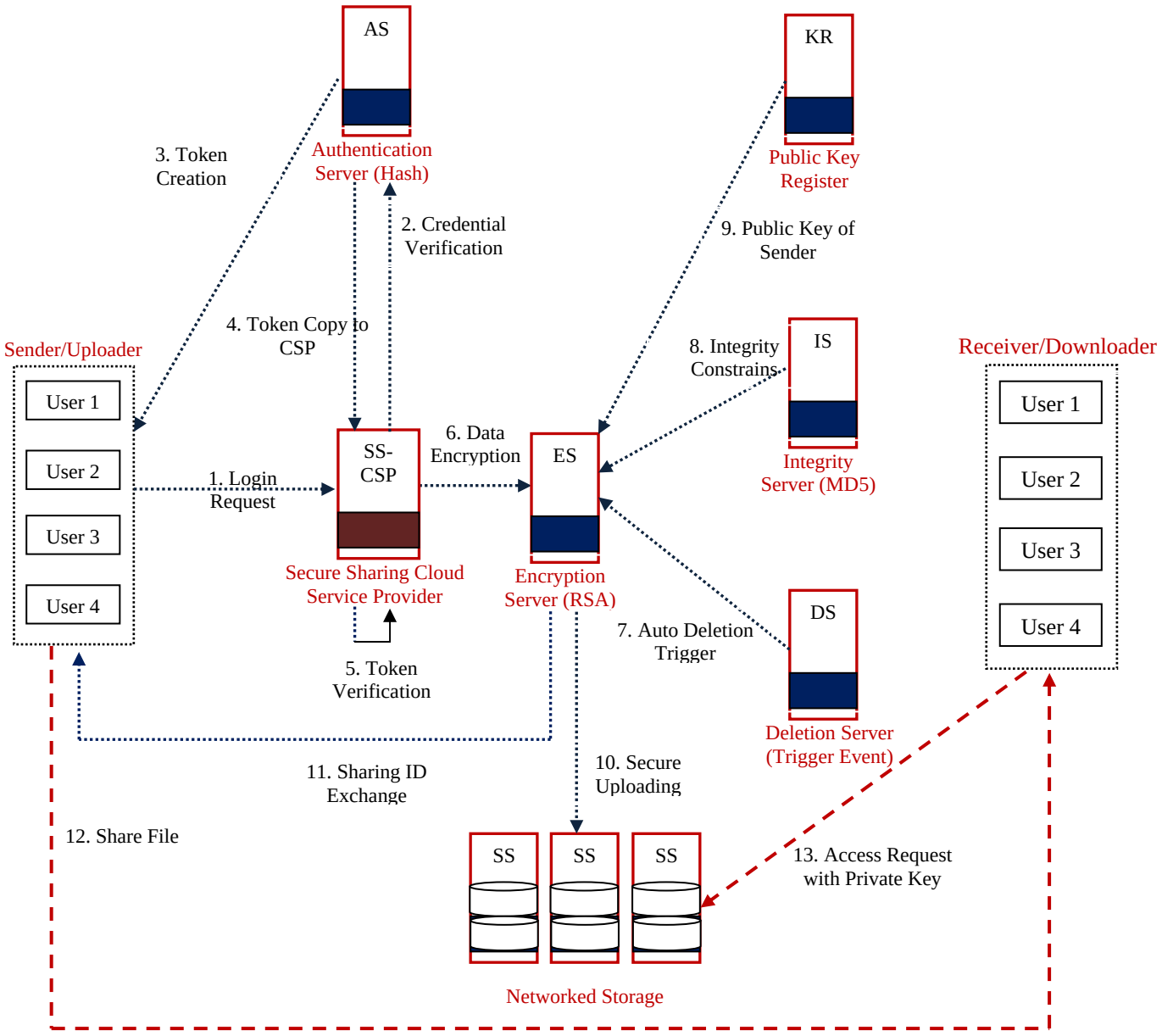

Figure 1: Proposed Architecture of Secure Sharing Using Cloud Computing

Description

The process starts with sending the access request to the system and verified using authentication approach. The user sends request to the service provider for getting the access to the system. The CSP server sends the credential request to authentication server for hash matching. Once the entered credentials are authenticated then the server will generates two copies of authentication tokens and sends the copy to user and the server. Once the credential gets verified the sender or up loader can upload the file which is passed directly to the encryption server. Here for achieving the high and robust confidentiality the system is using public key cryptography by implementing the cloud based solution of RSA cryptosystem.

This cryptosystem is easy and having high efficiency guided by integrity verifications, self destruction and key management. The integrity constraints applied here for checking the authenticity of data before and after transmission. If the data is modified or altered then it can only be detected by using digest based integrity checking process. For that this work is using MD5 algorithm as integrity checker phase. Before the data gets uploaded its digest is generated which is attached with the transmitted packets. For controlling the instances of data the wok is using self or auto deletion triggering phenomenon. It aims ion keeping the track of all intermediate data or files generated for secure or any sort of exchanges. Once the role or life of data gets finished then the associated triggers will automatically gets activated and performed their assigned actions. The system is also managing the records of several users and their files with key tracking so a separate key management server is also required to hold the metadata related to different sets of key for users and server. It works a public key register and the users participating

data exchanges will use this. Once all the above process is applied then the files gets stored securely to its storage servers. Now when the user like to share this uploaded file securely the he will allow sharing and the receiver have to go through all the phase in reverse direction. Before getting the access of shared files the user needs to presents its private key for decrypting the file. Later on the integrity is checked followed by destruction trigger. If all the constraints are ok then only the files gets viewed or downloaded by the receiver.

VI. BENEFITS OF APPROACH

(i) High end robust security based sharing
(ii) Hybrid approach for complete security
(iii) Supports the redistribution of the data to a non-trusted machine
(iv) Consistent operation and simultaneous read write into a single file.
(v) Better management of replicated copies their distribution and retrieval records, changes detection and monitoring
(vi) Self destruction and lifecycle based data sustainability for optimize storage
(vii) Fine Grained Access Control with Effective Authentication
(viii) Reduced vulnerability from attack planned to destruct the privacy and security of the systems.
(ix) Synchronous operations

VII. APPLICATIONS

- Sybil/False Identity Attack Detection/Removal
- Automatic Removal approach manages the memory utilizations.
- Improved privacy using message and chat removal based on lifecycle factors.
- Online file and change management
- ERP and BI (business intelligence) software's.
- E-commerce,
- Retail sector
- Transaction System
- Analytical Evaluations etc.

VIII. CONCLUSION

In spite of the fact that cloud computing has numerous focal points, there are still numerous genuine issues that need to be fathomed. The revenue estimation infers that cloud computing is a guaranteeing industry. Yet from another viewpoint, existing vulnerabilities in the cloud model will increase the threats from programmers. As per service conveyance models, organization models and key features of the cloud computing, data security and security protection issues are the essential issues that need to be eliminated as quickly as time permits. Data security and protection issues exist at all levels in SPI service conveyance models and in all phases of data life cycle. The capacity to control what information to reveal and who can get to that information over the Internet has turned into a developing concern. This work suggests a novel secure sharing phenomenon which covers complete aspect of cloud based sharing. Here the system starts operating with authentication followed by encryption, integrity verification, key handling and finally the sharing. The key to security protection in the cloud environment is the strict division of delicate data from non-touchy data took after by the encryption of touchy components. As per the investigation of data security and protection issues above, it is relied upon to have a coordinated and comprehensive security answer for addressing the needs of guard top to bottom. Regarding protection, security data recognizable proof and separation are the essential assignments.

REFERENCES

[1] Foster, I.; Yong Zhao; Raicu, I.; Shiyong Lu, "Cloud Computing and Grid Computing 360-Degree Compared", Grid Computing Environments Workshop, vol. 1, no. 10, doi: 10.1109/GCE.2008.4738445, Nov 2008
[2] Sudipto Das, "Scalable and Elastic Transactional Data Stores for Cloud Computing Platforms," PhD dissertation, December 2011.
[3] P. T. Jaeger, J. Lin, and J. M., "Grimes. Cloud computing and information policy: Computing in a policy cloud", Journal of Information Technology and politics, 5(3), 2009.
[4] Josiah Dykstra, "Seizing Electronic Evidence from Cloud Computing Enviornment", University of Maryland, Baltimore County, USA, IGI Global Journal, doi: 10.4018/978-1-4666-2662-1.ch007, 2013.
[5] R. Gellman, Privacy in the clouds: Risks to privacy and confidentiality from cloud computing. World Privacy Forum, 2009.
[6] Matthew Campagna, "Quantum Safe Cryptography and Security", in ETSI (European Telecommunications Standards Institute) White Paper, ISBN No. 979-10-92620-03-0, June 2015
[7] Arthur Rahumed, Henry C. H. Chen, Yang Tang, Patrick P. C. Lee, and John C. S. Lui, "A Secure Cloud Backup System with Assured Deletion and Version Control", Shun Hing Institute of Advanced Engineering, The Chinese University of Hong Kong.
[8] Noman Mazher and Imran Ashraf, "A Systematic Mapping Study on Cloud Computing Security", International Journal of Computer Application, ISSN:0975 – 8887, Volume 89 – No 16, March 2014
[9] Yang Tang, Patrick P. C. Lee, John C. S. Lui and Radia Perlman, "Secure Overlay Cloud Storage with Access Control and Assured Deletion",in Department of Computer Science and Engineering, The Chinese University of Hong Kong, Shatin.
[10] Wei Ren, Lingling Zeng, Ran Liu, and Chi Cheng, "F2AC: A Lightweight, Fine-Grained, and Flexible Access Control Scheme for File Storage in Mobile Cloud Computing", in Hindawi Publishing Corporation, Mobile Information Systems, doi: 10.1155/2016/5232846, 2016
[11] Roxana Geambasu, Tadayoshi Kohno, Amit A. Levy and Henry M. Levy, "Vanish: Increasing Data Privacy with Self-Destructing Data", in University of Washington.
[12] Christian Cachin, Kristiyan Haralambiev, Hsu-Chun Hsiao and Alessandro Sorniotti, "Policy-based Secure Deletion", in IBM Research – Zurich, August 2013
[13] Danan Thilakanathan, Shiping Chen, Surya Nepal and Rafael A. Calvo, "Secure Data Sharing in the Cloud", Springer-Verlag Berlin Heidelberg, DOI: 10.1007/978-3-642-38586-52, 2014
[14] Aaram Yun, Chunhui Shi and Yongdae Kim, "On Protecting Integrity and Confidentiality of Cryptographic File System for Outsourced Storage", in ACM, doi: 978-1-60558-784-4/09/11, November 13, 2009
[15] Tuomas Kekkonen, Teemu Kanstrén and Kimmo Hätönen, "Towards Trusted Environment in Cloud Monitoring", in ITNG IEEE Conference, 2014
[16] Farrukh Shahzad, "Safe Haven in the Cloud: Secure Access Controlled File Encryption (SAFE) System", in Science and Information Conference, London, UK, July 2015