A Case of Multilevel Security Application for Ensuring Data Integrity (Prevention and Detection) in Cloud Environment

Rajani Sharma
Graphic Era University

Rajender K Trivedi, Ph.D
Graphic Era University

ABSTRACT
Cloud computing is a collective, optimized usage of IT resources which can be accessed from anywhere and performs the task of providing IT resources and services through various platforms as a service for users. Cloud users use different services of Cloud service providers and eventually end up keeping their data (in various forms) in cloud multi tenant environment. Multi-tenancy in cloud environment makes data vulnerable though with times different forms of threats and corresponding securities are already implemented in cloud environment. Although many of these services provide key functionality such as uploading and retrieving files by a precise user, more on going to the side of advanced services it offer features such as shared folders, real-time collaboration, and minimization of data transfers or unlimited storage space. As data is placed publically it require to search ways to protect the data from unauthorized access, files are uploaded publically and need to retrieve them securely with token ensuring possession proofs. In this paper we have presented a case of multilevel security application for ensuring data integrity (prevention and detection) in cloud environment.

General Terms
Algorithm, Programming Language, Secure Retrieval, **[Cloud computing-Secure Data Retrieval]**: Data Security.

Keywords
Cloud Computing, Encryption, Decryption, Possession Proof, Security Token, Hash Code and UEC.

1. INTRODUCTION
Cloud computing is a collection of resources (hardware, software, services) that can be accessed over internet from anywhere at any time. Cloud computing is the way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. Recently it has emerged as a new way for hosting and delivering services over the internet. With the development of this technology, computing resources have become cheaper, more powerful and more ubiquitously available. This technological trend has enabled a new computing model called cloud computing, which provide the resources (H/W, S/W, and Storage.etc.) that can be taken as leased by user as an on demand services. It has several attractive features (no upfront investment, lowering operating cost, highly scalable, easy access) which make these services to be used by everyone [9].Cloud computing has generated significant interest in both academia and industry, but it's still an evolving paradigm. Essentially, its goal is to enhance the economic utility model with the improved development of many existing approaches and computing technologies, including distributed services, applications, and information infrastructures consisting of pools of computers, networks, and storage resources. Confusion exists in IT communities about how a cloud differs from existing models and how these differences affect its adoption. Some see a cloud as a novel technical revolution, while others consider it a natural evolution of technology, economy, and culture. Nevertheless, cloud computing is an important paradigm, with the potential to significantly reduce costs through optimization and increased operating and economic efficiencies. Furthermore, cloud computing could significantly enhance collaboration, agility, and scale, thus enabling a truly global computing model over the Internet infrastructure. However, without appropriate security and privacy solutions designed for clouds, this potentially revolutionizing computing paradigm could become a huge failure. Several surveys of potential cloud adopters indicate that security utilization techniques and the services model which are IAAS, PAAS and SAAS. It relies on the sharing and privacy is the primary concern hindering its adoption [3].Cloud computing based on the several of resources to achieve the coherency and Scalability for the utilization. Cloud computing relies on the network as an elementary service. Cloud computing is still in its infancy in spite of gaining tremendous momentum recently, high security is one of the major obstacles for opening up the new era of the long dreamed vision of computing as a utility.

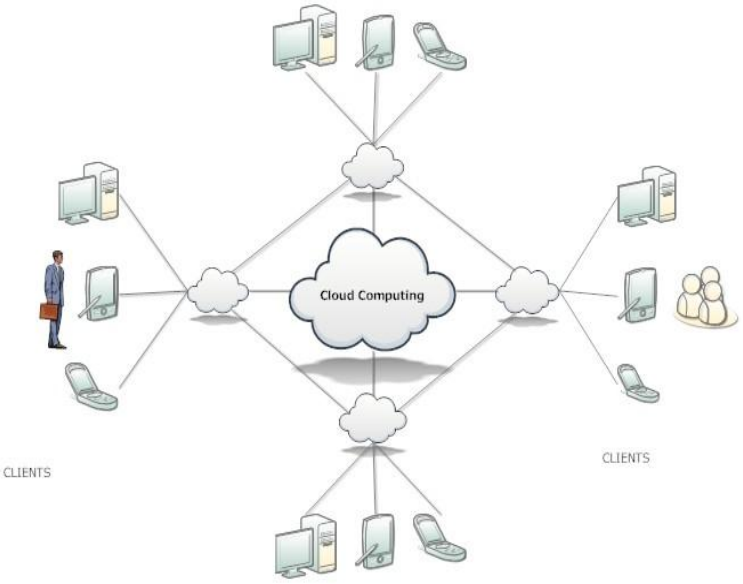

Figure 1: Cloud Environment

As the sensitive applications and data are moved into the cloud data centers, run on virtual computing resources in the form of virtual machine. This unique attributes, however, poses many novel tangible and intangible security challenges. It might be difficult to track the security issue in cloud

computing environments. So in cloud computing environments Security has become a major concern to provide protected communication between user and data storage.

Storing data in the cloud gives rise to the issue of data integrity verification at entrusted servers. If a client is able to log in from any particular location to access data and other applications, it is a matter of concern that client's privacy/confidentiality could be negotiated. Cloud computing companies will need to discover some strong techniques to preserve client privacy. To assure client's privacy, data file handling mechanism is auditing by token generation ensuring possession proof.

2. PROBLEM STATEMENT

Storing data in the cloud gives rise to the issue of data integrity verification at entrusted servers. If a client is able to log in from any particular location to access data and other applications, it is a matter of concern that client's privacy/confidentiality could be negotiated. Cloud computing companies will need to discover some strong techniques to preserve client's data integrity. Prevention of attack on data integrity and then detection of the same is considered as an issue in cloud environment. Many research papers who have solved this issue with introduction of a TPA does not seem practically profitable as it requires client to show its data to TPA and also reliability and neutratility of TPA still remains in question.

Understanding this concern solution is implemented with the help of a multilevel security application UEC which shares the hash code of data.

3. PROPOSED SOLUTION

For ensuring data integrity in cloud environment and secure retrieval of the data will be using a **multilevel security application UEC (Unified Exactness Checker)** which will prevent unauthorized access by the Tokenization technique to download the file in a secure way- and ensuring data integrity by matching hash code of file using md5 algorithm. The proposed solution in cloud data storage when user create an account the password will be stored in encrypted form and user can get that password from given mail id. And when user login into the system he will be ask to give the credentials (username, and password).when (password and username) all credentials match with data base only then user will be able to get access to the cloud storage, and here user can upload, download, delete files. When user download any file a token will be generated and that token will be sent to user by SMS if token matches only then user will be able to download the file. To proposed scheme it has used four classes of following algorithms to architect UEC.

- Hash code generation algorithms
- Password generation algorithm
- Token generation algorithm
- RSA algorithm.

The hash is a cryptographic checksum or message integrity code (MIC) that each party must compute to verify the message. For example, the sending computer uses a hash function and shared key to compute the checksum for the message, including it with the packet. The receiving computer must perform the same hash function on the received message and shared key and compare it to the original (included in the packet from the sender). Cloud Service Provider also keeps a database of hash codes with corresponding file Id's with timestamp of last modification.

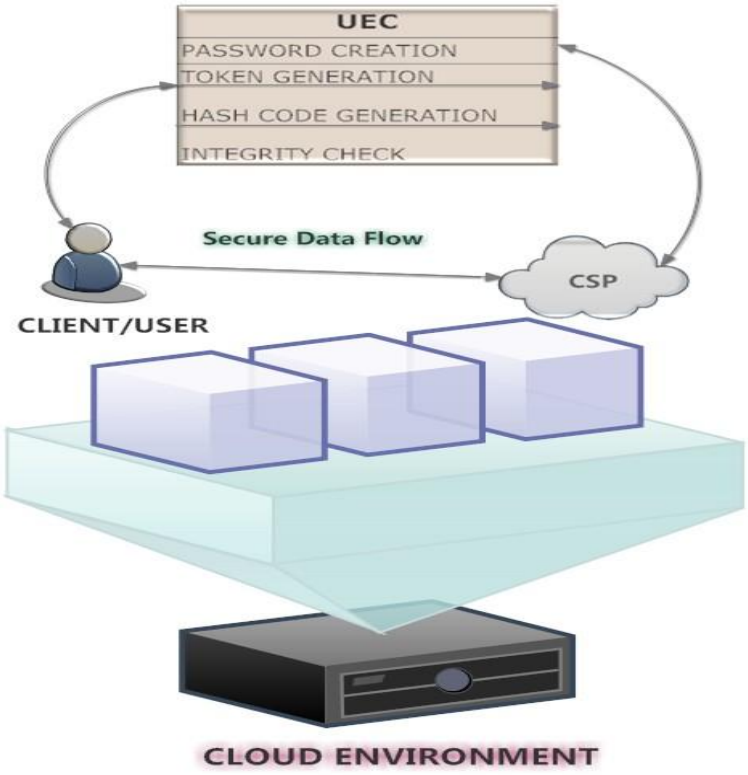

Figure 2: Working Model (UEC)

To run these applications on cloud have created a cloud environment with the following steps [27].

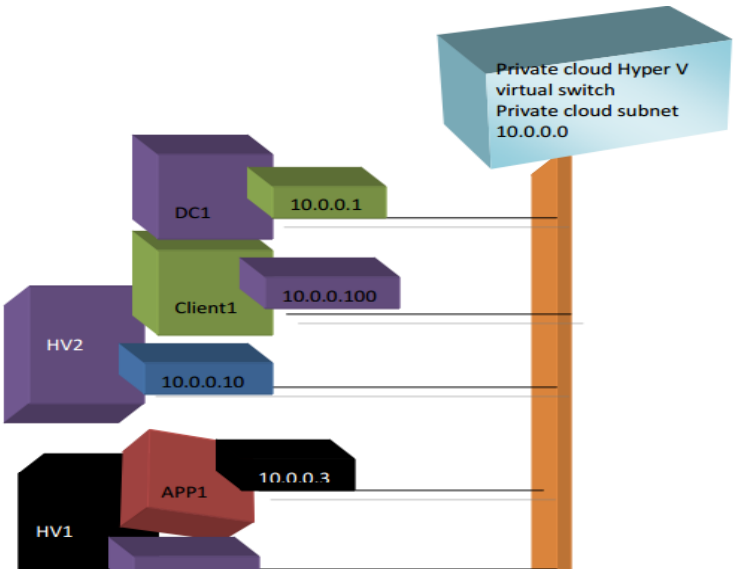

Figure 4: Private Cloud Setup

1. Configure Hypervisor1
2. ConfigureHypervisor2
3. ConfigureDomainController1
4. Configure Application Server1

5. Configure Client1
6. Join Hypervisor1 to the privatcloud.com
7. Join Hypervisor2 to the privatcloud.com

3.1 System Entities

- User- User is an entity whose responsibility is to create an account and store and download data in the cloud in a secure and easy way.
- Cloud Server- Cloud Server is managed by the Cloud service provider (CSP) to provide data storage service including storage space and computation resources in this implemented work , have user Oracle cloud database as our Cloud Storage Provider , have used Oracle cloud database to create database and store the data in the oracle cloud database.
- UEC- Unified Exactness Checker for data integrity check for both prevention and detection.

3.2 Implementation

Concept of Unified Exactness Checker is implemented keeping in view the importance of data integrity in a multi tenancy environment. Hashing of data before any upload process is the first function of UEC and it will store the hash code in local repository. The hash code of data will also be sent and kept at cloud service provider end in a repository against corresponding file ID and last modified timestamp. The data is encrypted using RSA encryption by UEC. Ensuring that the valid user only access the file, a unique token is generated and sent to user's email which is required by user to open/ download the file from cloud environment. User is able to match hash code from local repository to ensure integrity of data. Concept used for hash code.

$$h(s) = \sum_{I=0}^{n-1} s[i] - 31^{n-1-i}$$

Hash Code: 32-bit int addition, $s[i]$ denotes the ith character of the string, and n is the length of s.

A possession protocol ensure the secure retrieval of data, possession proof protocol introduce the new way of proving the secret data (TOKEN) .if the user does not know the secret data (TOKEN) cannot access the data and if not able to verify the what he possess cannot get access possession is stored in the session variable at server end and received by the user by mobile number. This method surely is the better way to retrieve the data in a secure and efficient manner.

Code is generated every time use uploads the file and is stored in database with corresponding file ID. Matching of hash codes after user downloads the file for use is done as a part of integrity check.

3.3 Scheme Details

PassGen (passkey) -Takes input string up to 8 times and initialize those eight charters to passkey.

Gen-Keys (Pub-Key, Private-Key,cipher) - Takes pass key as an input string and encrypt with Pub-Key cipher= (passkey.encript, Pub-Key) and store.

SendKey(MailId, passkey) –send the generated password to provided mail. MailId->passkey.

Retrieve (passkey)- Retrieve the encrypted passkey and decriptpasskey= (cipher.deript, Private-Key).

CheckUser((unm,pass),csp(unm,decriptpasskry))- match=(user(unm,pass)==csp(unm,decriptpasskry)) if match=1 within 3 times then access (cloud) otherwise blocked for next 24 hours.

Uploadfile – (file,hashcode, Pub-Key, Private-Key,cipher) –choose file (fl) compute the hashcode of file and stored. And Takes file as an input string and encrypt with Pub-Key cipher= (fl.encript, Pub-Key) and store.

GenToken – (token,tsk) : Takes securerandom numbers as input string and initializing secret key "tsk" for it and an evaluation key "token".

SendKey – (MobileNo,tsk) –send the token.MobileNo ->token.

Authtsk (b, τ)->σ: It creates a tag σ that authenticates the bit b {0, 1} of tsk under the label τ {0, 1}*.

Verifysk(e,P,Ψ){accept; reject}: The deterministic verification procedure uses the tag to check that e {0, 1} isthe output of the file (fl) on previously authenticated labeled data. If verified with the token accept the request and download the file otherwise rejected.

DownloadFile (fl) - Retrieve the encrypted file and decriptfile = (cipher.deript, Private-Key)

Integritycheck (chash,shash,t) – UEC get the hash-code of

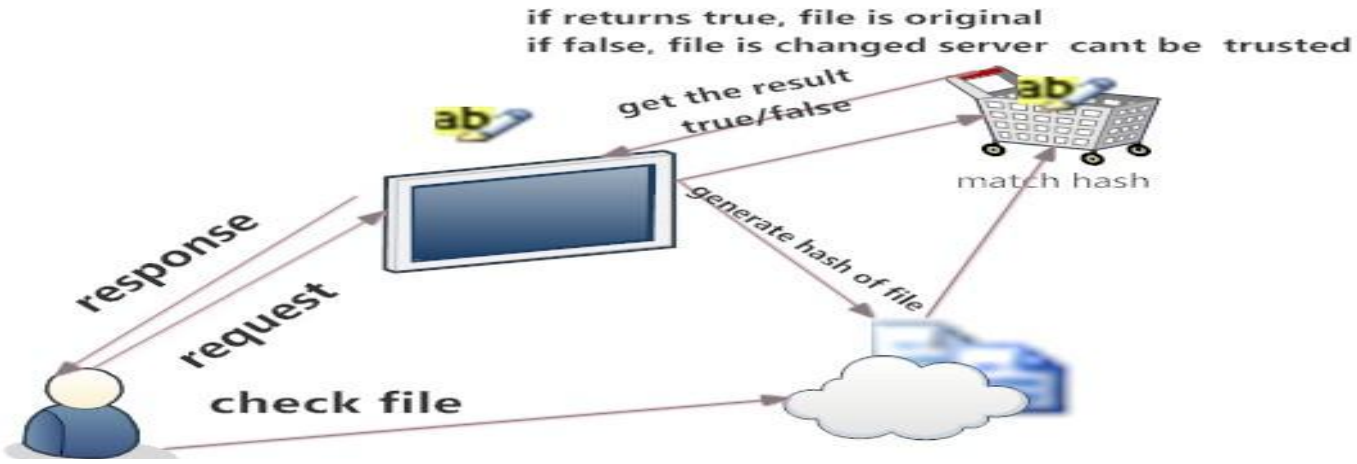

Figure 3: File Integrity Checking Process

file stores at server and check with the pre-computed hash-code.

Verify (fh1,fh2){true,false}- the procedure matches both the hash code.

Respond (t,f,user)- give response to the user with true or false if true file is original else server is misbehaving, fie is changed.

3.4 Algorithms

3.4.1 RSA

For this implementation , have used RSA algorithm for encryption and decryption, because it is considered that there are so many algorithms for encryption and decryption but they are not as secure as RSA .RSA is secure as well fast encryption/decryption technique.

RSA include a public key and a private key .the public is used for encrypting the message and known by everyone .the private key is used for decrypting the message. Message encrypted with the public key can only be decrypted in a reasonable amount of time using private key. The keys for RSA algorithms will be generated as follows.

- Choose two prime numbers p and q. for security reason the integers p and q should be chosen at random and also be of same bit length.
- Compute n=p*q. n is used as modules for public key and private key.
- Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1)$, where φ is Euler's totient function.
- Choose an integer e such that $1 < e < \varphi(n)$ and gcd $(e, \varphi(n)) = 1$; i.e., e and φ(n) are co-prime. e is released as the public key exponent.
- Determine d as $d \equiv e-1 \pmod{\varphi(n)}$;

The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and φ(n) must also be kept secret because they can be used to calculate d.

3.5 Results

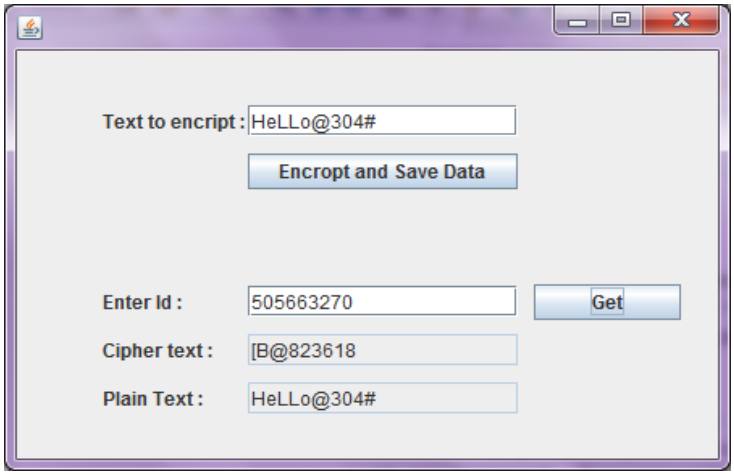

Figure 5: Encryption/ Decryption

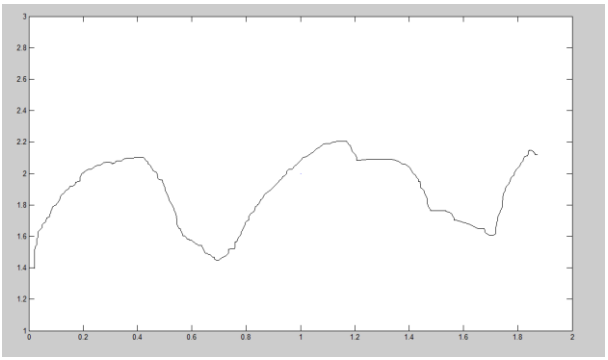

Figure 6 Performance Analysis

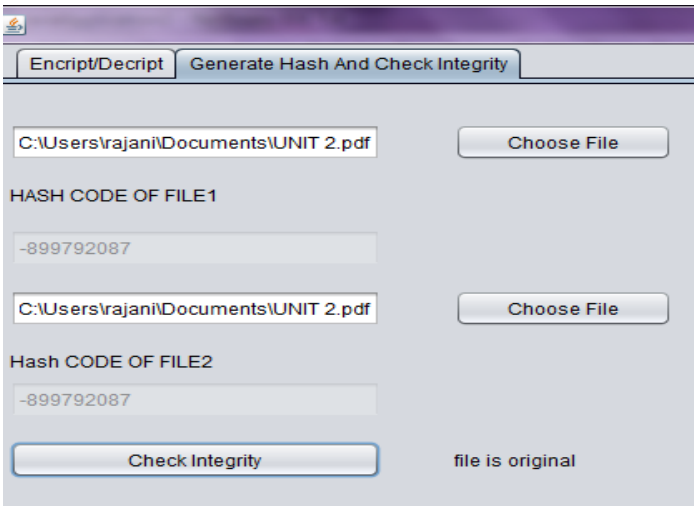

Figure 7 File Integrity Checking

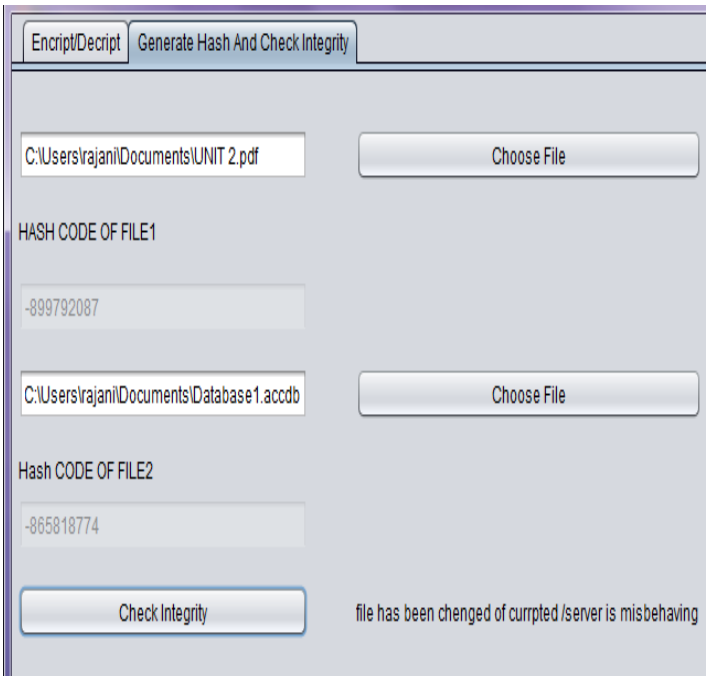

Figure 8 Server Misbehaving

4. CONCLUSION

In this paper we have presented that how can we retrieve files securely and also ensure that the integrity of file is maintained by using preventive methods and detecting integrity with local hash repository. With the help of password generation and sending it to user by email facility will proof that registered user is a valid user and after that when user download file at that a secure key/token will be generated and user has to give that key/token to download the selected file, he/she will receive the token by SMS. But this is not enough to secure data access from cloud storage and can make it more secure by providing to identify the error localization and misbehaving server. And used RSA algorithm for encrypting /decrypting messages as mention that RSA is secure but in some cases some attacks can form against RSA When encrypting with low encryption exponents (e.g., e = 3) and small values of the m, (i.e., $m < n1/e$) the result of me is strictly less than the modulus n. In this case, cipher texts can be easily decrypted by taking the eth root of the cipher text over the integers and If the same clear text message is sent to e or more recipients in an encrypted way, and the receivers share the same exponent e, but different p, q, and therefore n, then it is easy to decrypt the original clear text message via the Chinese remainder theorem. so these are some problem on which we have to concern more to make data transmission more secure and to make it more secure. Integrating various levels of security with single application UEC has ensured security of data in a multi tenancy environment to a great extent.

5. FUTURE WORK

We are planning to do future work in strengthening Security as a service model with minimum sharing of data among different parties including Cloud Service Provider or Security Service Provider.

6. REFERENCES

[1] Bowman, M., Debray, S. K., and Peterson, L. L. 1993. Reasoning about naming systems. .

[2] Ding, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Technical Report. University of Maryland at College Park.

[3] Fröhlich, B. and Plate, J. 2000. The cubic mouse: a new device for three-dimensional input. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems

[4] Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[5] Sannella, M. J. 1994 Constraint Satisfaction and Debugging for Interactive User Interfaces. Doctoral Thesis. UMI Order Number: UMI Order No. GAX95-09398., University of Washington.

[6] Forman, G. 2003. An extensive empirical study of feature selection metrics for text classification. J. Mach. Learn. Res. 3 (Mar. 2003), 1289-1305.

[7] Brown, L. D., Hua, H., and Gao, C. 2003. A widget framework for augmented interaction in SCAPE.

[8] Y.T. Yu, M.F. Lau, "A comparison of MC/DC, MUMCUT and several other coverage criteria for logical decisions", Journal of Systems and Software, 2005, in press.

[9] Spector, A. Z. 1989. Achieving application requirements. In Distributed Systems, S. Mullender

[10] Arkaitz Ruiz-Alvarez and Marty Humphrey. 2012. A Model and Decision Procedure for Data Storage in Cloud Computing. In Proceedings of the 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (ccgrid 2012) (CCGRID '12). IEEE Computer Society, Washington, DC, USA, 572-579. DOI=10.1109/CCGrid.2012.100 http://dx.doi.org/10.1109/CCGrid.2012.100Sangroya A, Kumar S, Dhok J, Varma V. Towards analyzing data security risks in cloud computing environments.Communications in Computer and Information Science; 2010;54:255–265.

[11] H. Takabi, J.B.D. Joshi, and G.-J. Ahn, "SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environments," Proc. 1st IEEE Int'l Workshop Emerging Applications for Cloud Computing (CloudApp 2010), IEEE CS Press, 2010, pp. 393–398.

[12] SRINIVAS, J., K. VENKATA SUBBA REDDY, and A. MOIZ QYSER. "CLOUD COMPUTING BASICS."International Journal of Advanced Research in Computer and Communication Engineering,Vol. 1, Issue 5, July 2012.

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

[14] http://dx.doi.org/10.1016/jRoopa,Manjunath." Secure Way of Storing Data in Cloud Using Third Party Auditor."CNE, CMRIT Bangalore, India.

[15] Martin, S. Schrittwieser, et al. Dark clouds on the horizon."using cloud storage as attack vector and online slack space". Proceedings of the 20th USENIX conference on Security. San Francisco, CA, USENIX Association.

[16] Giuseppe, R.Burns, et al. "Remote data checking using provable data possession." ACM Trans. Inf. Syst. Secure.14 (1): 1-34.

[17] L.chen."Using algebraic signatures to check data possession in cloud storage." Future Gener. Comput. Syst.29 (7): 1709-1715.

[18] Sowparnika,R.Dheenadayalu"Improving data integrity on cloud storage services," IEEE Transactions on Knowledge and Data Engineering, Volume 23, no. 9, pp. 1432-1437, September, 2011.

[19] Dawei, G.Chang,et al." Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments, ProcediaEngineering."Volume 15, 2011, Pages 2852-2856, ISSN 1877-7058.

[20] At Dropbox, Over 100 Billion Files Served–And counting, retrieved May 23rd, 2011. Online at http://gigaom.com/2011/05/23/at dropbox-over-100-billionfiles- served-and-counting/.

[21] Fatima Alkandari and Richard F. Paige. 2012. Modelling and comparing cloud computing service level agreements. In Proceedings of the 1st International Workshop on Model-Driven Engineering for High Performance and CLoud computing (MDHPCL '12). ACM, New York, NY, USA, , Article 3 , 6 pages.

DOI=10.1145/2446224.2446227
http://doi.acm.org/10.1145/2446224.2446227.

[22] TekinBicer, David Chiu, and Gagan Agrawal. 2012. Time and Cost Sensitive Data-Intensive Computing on Hybrid Clouds. In Proceedings of the 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (ccgrid 2012) (CCGRID '12). IEEE Computer Society, Washington, DC, USA, 636-643. DOI=10.1109/CCGrid.2012.95
http://dx.doi.org/10.1109/CCGrid.2012.95.

[23] Gang Sheng, Tao Wen, QuanGuo, and Ying Yin. 2013. Verifying correctness of inner product of vectors in cloud computing. In Proceedings of the 2013 international workshop on Security in cloud computing (Cloud Computing '13). ACM, New York, NY, USA, 61-68. DOI=10.1145/2484402.2484416
http://doi.acm.org/10.1145/2484402.2484416.

[24] Siani Pearson. 2009. Taking account of privacy when designing cloud computing services. InProceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing(CLOUD '09). IEEE Computer Society, Washington, DC, USA, 44-52. DOI=10.1109/CLOUD.2009.5071532
http://dx.doi.org/10.1109/CLOUD.2009.5071532.

[25] Jose Simão and Luis Veiga. 2012. VM Economics for Java Cloud Computing: An Adaptive and Resource-Aware Java Runtime with Quality-of-Execution. In Proceedings of the 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (ccgrid 2012)(CCGRID '12). IEEE Computer Society, Washington, DC, USA, 723-728. DOI=10.1109/CCGrid.2012.121
http://dx.doi.org/10.1109/CCGrid.2012.121.

[26] Kamal Dahbur, Bassil Mohammad, and Ahmad BisherTarakji. 2011. A survey of risks, threats and vulnerabilities in cloud computing. In Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications (ISWSA '11). ACM, New York, NY, USA, , Article 12 , 6 pages. DOI=10.1145/1980822.1980834http://doi.acm.org/10.1145/1980822.1980834.

[27] Rajender K Trivedi and Rajani Sharma. Article: Proposed Framework of Private Cloud Setup in Lab for Teaching and Research.International Journal of Computer Applications 92(1):26-31, April 2014. Published by Foundation of Computer Science, New York,USA.