Multi Cloud Architecture for Improved User Experience

S. B. Shivakumar, Ramesh B. E., Kavitha G. M., Mala M.

Abstract— Use of cloud computing has increased rapidly in many organizations. There are many commercial cloud providers. Each one provides different storage plans & different QOS like time delay, availability. The QOS parameters & plans vary over a period of time. Every time the user cannot move his data from one cloud provider to another for the cost & QOS optimization. Cloud users also have security & auditing requirement for his data in terms who are accessing it & what frequency in which his data is accessed.

To address these requirements of the users, we propose a solution using multi cloud architecture. Our solution will reduce the burden on the users in migration & meeting his security challenges. Our platform will provide the best cost optimization for the security & storage requirements of user.

***Keywords— Cloud computing, single cloud, multi-clouds, cloud storage, data integrity, data intrusion, service availability*.**

I. INTRODUCTION

The use of cloud computing has increased rapidly in many organizations. Cloud computing provides many benefits in terms of low cost and accessibility of data. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers but these providers may be untrusted. “Single Cloud” providers have risks of service availability failure and the possibility of malicious insiders, so we promote usage of "multi-clouds" which has emerged recently.

There are many cloud providers. But No cloud is perfect. And after some very public cloud outages, business customers are looking harder at divvying up their workloads among multiple clouds to mitigate risk. The latest glitch was a 19-minute Elastic Compute Cloud connectivity issue at Amazon’s U.S east region early March 2013. Earlier April 2012, a 12-hour Leap Day Azure outage afflicted Microsoft’s Windows Azure cloud. With these snafus, business customers are starting to realize that, while cloud computing can cut costs, it is no panacea: Clouds run on data centers and data centers go down.

To hedge their bets, businesses are looking into multi-cloud solutions Cloud users are increasingly worried about data security aspect of cloud computing. As data and information will be shared with a third party, cloud computing users want to avoid an untrusted cloud provider. Protecting private and important information, such as credit card details or a patient’s medical records from attackers or malicious insiders is of critical importance.

Information, such as credit card details or a patient’s medical records from attackers or malicious insiders is of critical importance.

Cloud user wants a simplified & powerful view of cloud. They set their SLA and expect the cloud platform to meet the SLA & deliver SLA within their budget. Also if the cloud platform can also automatically find the best configuration to meet SLA & also do cost saving on the budget, then it gives better user experience.

Moreover, users may not know the machines which actually process and host their data. While enjoying the convenience brought by this new technology, users also start worrying about losing control of their own data. The data processed on clouds are often outsourced, leading to a number of issues related to accountability, including the handling of personally identifiable information. Such fears are becoming a significant barrier to the wide adoption of cloud services

To allay users’ concerns, it is essential to provide an effective mechanism for users to monitor the usage of their data in the cloud. For example, users need to be able to ensure that their data are handled according to the service level agreements made at the time they sign on for services in the cloud. Conventional access control approaches developed for closed domains such as databases and operating systems, or approaches using a centralized server in distributed environments, are not suitable, due to the following features characterizing cloud environments. First, data handling can be outsourced by the direct cloud service provider (CSP) to other entities in the cloud and theses entities can also delegate the tasks to others, and so on. Second, entities are allowed to join and leave the cloud in a flexible manner. As a result, data handling in the cloud goes through a complex and dynamic hierarchical service chain which does not exist in conventional environments.

In this paper, we explore more about these challenges and provide a solution based on multi cloud architecture for improved user experience to the users of cloud.

II. LITERATURE SURVEY

Cloud computing has raised a range of important privacy and security issues [19], [25], [30]. Such issues are due to the fact that, in the cloud, users’ data and applications reside—at least for a certain amount of time—on the cloud cluster which is owned and maintained by a third party.

Although cloud service providers can offer benefits to users, security risks play a major role in the cloud computing environment [53]. Users of online data sharing or network facilities are aware of the potential loss of privacy [12]. According to a recent IDC survey [16], the top challenge for 74% of CIOs in relation to cloud computing is security. Protecting private and important information such as credit card details or patients’ medical records from attackers or malicious insiders is of critical importance [34]. Moving databases to a large data centre involves many security challenges [55] such as virtualization vulnerability,

Manuscript received on June, 2013.

Dr. S. B. Shivakumar, HOD (CS&E), SJMIT, Chitradurga, VTU University, Belgaum (Karnataka), India.

Ramesh B. E., Asst. Professor (CS&E), SJMIT, Chitradurga, VTU University, Belgaum (Karnataka), India.

Kavitha G. M., M.Tech., (CS&E), SJMIT, Chitradurga, VTU University, Belgaum (Karnataka), India.

Mala M., M.Tech., (CS&E), SJMIT, Chitradurga, VTU University, Belgaum (Karnataka), India.

accessibility vulnerability, privacy and control issues related to data accessed from a third party, integrity, confidentiality, and data loss or theft. Subashini and Kavitha [49] present some fundamental security challenges, which are data storage security, application security, data transmission security, and security related to third-party resources.

In different cloud service models, the security responsibility between users and providers is different.

According to Amazon [46], their EC2 addresses security control in relation to physical, environmental, and virtualization security, whereas, the users remain responsible for addressing security control of the IT system including the operating systems, applications and data.

According to Tabakiet al. [51], the way the responsibility for privacy and security in a cloud computing environment is shared between consumers and cloud service providers differs between delivery models. In SaaS, cloud providers are more responsible for the security and privacy of application services than the users. This responsibility is more relevant to the public than the private cloud environment because the clients need more strict security requirements in the public cloud. In PaaS, users are responsible for taking care of the applications that they build and run on the platform, while cloud providers are responsible for protecting one user's applications from others. In IaaS, users are responsible for protecting operating systems and applications, whereas cloud providers must provide protection for the users' data [51].

Ristenpartet al. [41] claim that the levels of security issues in IaaS are different. The impact of security issues in the public cloud is greater than the impact in the private cloud. For instance, any damage which occurs to the security of the physical infrastructure or any failure in relation to the management of the security of the infrastructure will cause many problems. In the cloud environment, the physical infrastructure that is responsible for data processing and data storage can be affected by a security risk. In addition, the path for the transmitted data can be also affected, especially when the data is transmitted to many third-party infrastructure devices[41].

As the cloud services have been built over the Internet, any issue that is related to internet security will also affect cloud services. Resources in the cloud are accessed through the Internet; consequently even if the cloud provider focuses on security in the cloud infrastructure, the data is still transmitted to the users through networks which may be insecure. As a result, internet security problems will affect the cloud, with greater risks due to valuable resources stored within the cloud and cloud vulnerability. The technology used in the cloud is similar to the technology used in the Internet. Encryption techniques and secure protocols are not sufficient to protect data transmission in the cloud. Data intrusion of the cloud through the Internet by hackers and cybercriminals needs to be addressed and the cloud environment needs to be secure and private for clients [49].

We will address three security factors that particularly affect single clouds, namely data integrity, data intrusion, and service availability.

One of the most important issues related to cloud security risks is data integrity. The data stored in the cloud may suffer from damage during transition operations from or to the cloud storage provider. Cachinet al.[12] give examples of the risk of attacks from both inside and outside the cloud provider, such as the recently attacked Red Hat Linux's distribution servers [40]. Another example of breached data occurred in 2009 in Google Docs, which triggered the Electronic Privacy Information Centre for the Federal Trade Commission to open an investigation into Google's Cloud Computing Services [12]. Another example of a risk to data integrity recently occurred in Amazon S3 where users suffered from data corruption [50]. Further examples giving details of attacks can be read in [12],[40],[50]. Cachinet al.[12]argue that when multiple clients use cloud storage or when multiple devices are synchronized by one user, it is difficult to address the data corruption issue. One of the solutions that they [12] propose is to use a Byzantine fault-tolerant replication protocol within the cloud. Hendricks et al.[23] state that this solution can avoid data corruption caused by some components in the cloud. However, Cachinet al. [12] claim that using the Byzantine fault tolerant replication protocol within the cloud is unsuitable due to the fact that the servers belonging to cloud providers use the same system installations and are physically located in the same place.

Although this protocol solves the problem from a cloud storage perspective, Cachinet al. [12] argue that they remain concerned about the users' view, due to the fact that users trust the cloud as a single reliable domain or as a private cloud without being aware of the protection protocols used in the cloud provider's servers. As a solution, Cachinet al. [12] suggest that using Byzantine fault-tolerant protocols across multiple clouds from different providers is a beneficial solution.

According to Garfinkel[19], another security risk that may occur with a cloud provider, such as the Amazon cloud service, is a hacked password or data intrusion. If someone gains access to an Amazon account password, they will be able to access all of the account's instances and resources. Thus the stolen password allows the hacker to erase all the information inside any virtual machine instance for the stolen user account, modify it, or even disable its services. Furthermore, there is a possibility for the user's email(Amazon user name) to be hacked (see [18] for a discussion of the potential risks of email), and since Amazon allows a lost password to be reset by email, the hacker may still be able to log in to the account after receiving the new reset password.

Another major concern in cloud services is service availability. Amazon [6] mentions in its licensing agreement that it is possible that the service might be unavailable from time to time. The user's web service may terminate for any reason at any time if any user's files break the cloud storage policy. In addition, if any damage occurs to any Amazon web service and the service fails, in this case there will be no charge to the Amazon Company for this failure. Companies seeking to protect services from such failure need measures such as backups or use of multiple providers [19]. Both Google Mail and Hotmail experienced service downtime recently [12]. If a delay affects payments from users for cloud storage, the users may not be able to access their data. Due to a system administrator error, 45% of stored client data was lost in LinkUp (MediaMax) as a cloud storage provider [12].

Garfinkel[19] argues that information privacy is not guaranteed in Amazon S3. Data authentication which assures that the returned data is the same as the stored data is extremely important. Garfinkel claims that instead of following Amazon's advice that organizations encrypt data before storing them in Amazon S3, organizations should use HMAC [26] technology or a digital signature to ensure data is not modified by Amazon S3. These technologies protect users from Amazon data modification and from hackers who may have obtained access to their email or stolen their password [19].

Concerns arise since in the cloud it is not always clear to individuals why their personal information is requested or how it will be used or passed on to other parties. To date, little work has been done in this space, in particular with respect to accountability. Pearson et al. have proposed accountability mechanisms to address privacy concerns of end users [30] and then develop a privacy manager [31]. Their basic idea is that the user's private data are sent to the cloud in an encrypted form, and the processing is done on the encrypted data. The output of the processing is de obfuscated by the privacy manager to reveal the correct result. However, the privacy manager provides only limited features in that it does not guarantee protection once the data are being disclosed. In [7], the authors present a layered architecture for addressing the end-to-end trust management and accountability problem in federated systems. The authors' focus is very different from ours, in that they mainly leverage trust relationships for accountability, along with authentication and anomaly detection. Further, their solution requires third-party services to complete the monitoring and focuses on lower level monitoring of system resources.

In the commercial world, various computing needs are provided as a service. The service providers take care of the customer's needs by, for example, maintaining software or purchasing expensive hardware. For instance, the service EC2, created by Amazon, provides customers with scalable servers. As another example, under the CLuE program, NSF joined with Google and IBM to offer academic institutions access to a large-scale distributed infrastructure [4]. There are many features of cloud computing. First, cloud storages, such as Amazon S3, Microsoft SkyDrive, or NirvanixCLoudNAS, permit consumers to access online data. Second, it provides computation resources for users such as Amazon EC2. Third, Google Apps or versioning repositories for source code are examples of online collaboration tools [12]. Cloud service providers should ensure the security of their customers' data and should be responsible if any security risk affects their customers' service infrastructure. A cloud provider offers many services that can benefit its customers, such as fast access to their data from any location, scalability, pay-for-use, data storage, data recovery, protection against hackers, on-demand security controls, and use of the network and infrastructure facilities [49].

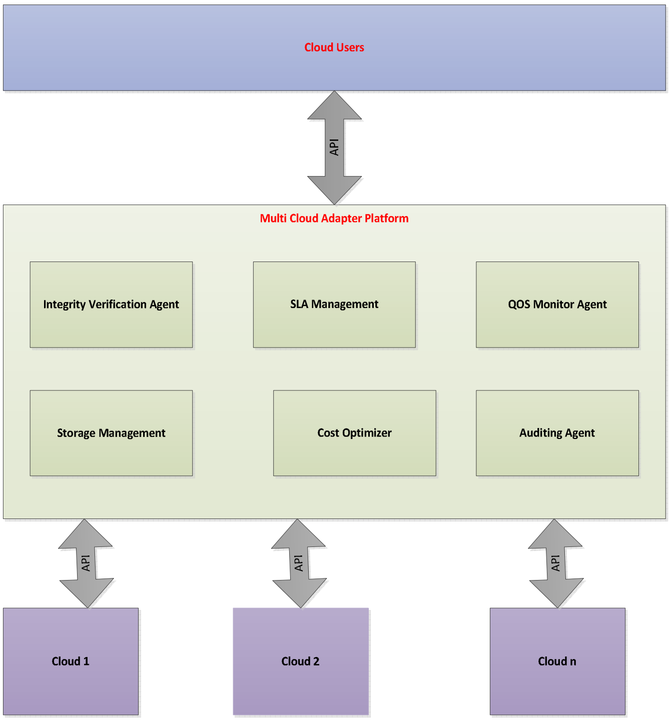
Reliability and availability are other benefits of the public cloud, in addition to low cost [25]. However, there are also concerning issues for public cloud computing, most notably, issues surrounding data integrity and data confidentiality. Any customer will be worried about the security of sensitive information such as medical records or financial information[25].

Researchers have investigated accountability mostly as a provable property through cryptographic mechanisms, particularly in the context of electronic commerce [10], [21]. A representative work in this area is given by [9]. The authors propose the usage of policies attached to the data and present logic for accountability data in distributed settings. Similarly, Jagadeesan et al. recently proposed logic for designing accountability-based distributed systems [20]. In [10], Crispo and Ruffo proposed an interesting approach related to accountability in case of delegation. Delegation is complementary to our work, in that we do not aim at controlling the information workflow in the clouds. In a summary, all these works stay at a theoretical level and do not include any algorithm for tasks like mandatory logging. To the best of our knowledge, the only work proposing a distributed approach to accountability is from Lee and colleagues [22]. The authors have proposed an agent-based system specific to grid computing. Distributed jobs, along with the resource consumption at local machines are tracked by static software agents. The notion of accountability policies in [22] is related to ours, but it is mainly focused on resource consumption and on tracking of sub jobs processed at multiple computing nodes, rather than access control.

III. DETAILS OF OUR ARCHITECTURE

A. *Our architecture*

Our proposed solution architecture is given below.



We develop a middle layer called as Multi cloud adapter platform to address the following requirements.

1. Storage Security on cloud.

2. SLA Management

3. Cost Optimization

4. Auditing for the users data.

Multi cloud adapter implements following functionalities to meet the requirements.

For providing storage security, the data is encrypted while stored in cloud. The storage management module will implement this functionality.

The integrity of data must be ensured in the cloud from attackers affecting the data. Integrity verification agent will implement this functionality.

One of the salient features in our proposed solution is Cost optimization. This module will continuously watch for discounts, offers, current plans and migrate the stored data from one vendor to another to provide the cost optimization without violating the SLA.

Users need the audit information of their data on when the data is accessed and the users who accessed it. Auditing agent module implements this functionality.

SLA in terms of delay, faults must be managed to meet the user expectation.SLA management module along with QOS monitor agent implement this functionality.
In the following sections we will explain in detail the working of each module to meet the functionalities.

B. *Integrity management*

Data must not be corrupted and when it is corrupted, it must be identified & corrupted copy must be replaced. For each file from the user, we calculate the integrity token for the encrypted file. The file is stored in two copies one name is publicly known, another name is formed by hashing the file with a key. The integrity token for the encrypted file is also stored locally. Periodically for each file stored on cloud, we calculate the hash key & verify if it is matching with hash key stored locally. If any mismatch is found, then it becomes sure that the file is corrupted. The corrupted file is replaced with the backup copy of file.

C. *Storage management*

Storage management module takes the file to store in cloud as input. It encrypts the file, with key which is generated based on filename. The encrypted file is stored in two copies on cloud. Storage management module stores on the cloud which matches the owners QOS requirements. The interaction between the storage management module & the cloud is using the API provided by the cloud vendor.

D. *QOS Monitor*

QOS monitor module collects performance metrics on the cloud in terms average time between failures, store & access delay. The parameters are collected frequently & averaged for a day period. The values are then given to the SLA Management module.

E. *SLA Management*

SLA Management module verifies the conformance of the cloud to the SLA conditions set by the user. When the SLA conditions are violated, then the user storage is shifted to another cloud which best suits the users SLA requirement. SLA management module migrate the user storage to meet the SLA. To migrate in easy way the user data are organized as container so it helps in easy migration.

F. *Cost Optimization*

Cloud provider’s offers different plans based on storage size, monthly base plan change etc. It is very difficult for the user to continuously check the packages & select package to optimize its cost. This is automated with the help of the Cost optimization module. This module use web services to interact with the cloud to get the current plan information in different cloud providers. With the current usage trend of the user, the Cost optimization module finds the optimum cost at each cloud matching to the users SLA requirement. The user storage space is then migrated to the optimum cost cloud at off peak hours without affecting the QOS.

G. *Auditing Agent*

User need auditing information in terms no of users accessed the user’s files, most accessed files, most accessing users etc. for his business needs. Also he wants to put restriction on user access. Current cloud storage does not implement such requirements. We implement this capability in the Multi cloud Adapter platform. The solution is for each user file, a jar file is created to collect parameters & mail it back to the users email id. Access of any data is made possible only through this jar. Through this jar we implement the accounting service & also impose restrictions on the access of the file.

IV. CONCLUSION AND ENHANCEMENTS

It is clear that although the use of cloud computing has rapidly increased; cloud computing security is still considered the major issue in the cloud computing environment. Customers do not want to lose their private information as a result of malicious insiders in the cloud. In addition, the loss of service availability has caused many problems for a large number of customers recently. Furthermore, data intrusion leads to many problems for the users of cloud computing.
In this paper, we have proposed solutions for three most common security threats in cloud storage. Also we have provided solution for auditing requirements of the user.

REFERENCES

[1] (NIST), http://www.nist.gov/itl/cloud/.

[2] I. Abraham, G. Chockler, I. Keidar and D. Malkhi,"Byzantine disk paxos: optimal resilience with Byzantine shared memory", Distributed Computing, 18(5), 2006, pp. 387-408.

[3] H. Abu-Libdeh, L. Princehouse and H.Weatherspoon, "RACS: a case for cloud storage diversity", SoCC'10:Proc. 1st ACM symposium on Cloud computing, 2010, pp. 229-240.

[4] D. Agrawal, A. El Abbadi, F. Emekci and A. Metwally, "Database Management as a Service: Challenges and Opportunities",ICDE'09:Proc.25thIntl. Conf. on Data Engineering,2009, pp. 1709-1716.

[5] M.A. AlZain and E. Pardede, "Using Multi Shares for Ensuring Privacy in Database-as-a-Service",44th Hawaii Intl. Conf. on System Sciences (HICSS), 2011, pp. 1-9.

[6] Amazon, Amazon Web Services. Web services licensing agreement, October3,2006.

[7] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L.Kissner, Z. Peterson and D. Song, "Provable data possession at untrusted stores", Proc. 14th ACM Conf. on Computer and communications security, 2007, pp. 598-609.

[8] A. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds", EuroSys'11:Proc. 6thConf. On Computer systems, 2011, pp. 31-46.

[9] K. Birman, G. Chockler and R. van Renesse,"Toward a cloud computing research agenda", SIGACT News, 40, 2009, pp. 68-80.

[10] K.D. Bowers, A. Juels and A. Oprea, "HAIL: A high-availability and integrity layer for cloudstorage", CCS'09: Proc. 16th ACM Conf. on Computer and communications security, 2009, pp.187-198.

[11] C. Cachin, R. Haas and M. Vukolic, "Dependable storage in the Intercloud", Research Report RZ,3783, 2010.

[12] C. Cachin, I. Keidar and A. Shraer, "Trusting the cloud", ACM SIGACT News, 40, 2009, pp. 81-86.

[13] C. Cachin and S. Tessaro, "Optimal resilience for erasure-coded Byzantine distributed storage", DISC:Proc. 19thIntl.Conf. on Distributed Computing, 2005, pp. 497-498.

[14] M. Castro and B. Liskov, "Practical Byzantine fault tolerance",Operating Systems Review,33, 1998, pp. 173-186.

[15] G. Chockler, R. Guerraoui, I. Keidar and M. Vukolic, "Reliable distributed storage", Computer,42, 2009, pp. 60-67.

[16] Clavister, "Security in the cloud", Clavister White Paper, 2008.

[17] A.J. Feldman, W.P. Zeller, M.J. Freedman and E.W. Felten, "SPORC: Group collaboration using untrusted cloud resources", OSDI, October2010, pp. 1-14.

[18] S.L. Garfinkel, "Email-based identification and authentication: An alternative to PKI?", IEEE Security and Privacy, 1(6), 2003, pp. 20-26.

[19] S.L. Garfinkel, "An evaluation of amazon’s grid computing services: EC2, S3, and SQS", Technical Report TR-08-07, Computer Science Group, Harvard University, Citeseer, 2007, pp. 1-15.

[20] E. . Goh, H. Shacham, N. Modadugu and D. Boneh, "SiRiUS: Securing remote untrusted storage",NDSS: Proc. Network and Distributed System Security Symposium, 2003, pp. 131–145.

[21] G.R. Goodson, J.J. Wylie, G.R. Ganger and M.K.Reiter, "Efficient Byzantine-tolerant erasure-coded storage", DSN'04: Proc.Intl. Conf. on Dependable Systems and Networks,2004, pp.1-22.

[22] E. Grosse, J. Howie, J. Ransome, J. Reavis and S. Schmidt, "Cloud computing roundtable", IEEE Security & Privacy, 8(6), 2010, pp. 17-23.

[23] J. Hendricks, G.R. Ganger and M.K. Reiter, "Lowoverhead byzantine fault-tolerant storage", SOSP'07: Proc. 21st ACM SIGOPS symposium on Operating systems principles, 2007, pp. 73-86.

[24] A. Juels and B.S. Kaliski Jr, "PORs: Proofs of retrievability for large files", CCS '07: Proc. 14th ACM Conf. on Computer and communications security, 2007, pp. 584-597.

[25] S. Kamara and K. Lauter, "Cryptographic cloud storage", FC'10: Proc. 14thIntl.Conf. on Financial cryptograpy and data security,2010, pp. 136-149.

[26] H. Krawczyk, M. Bellare and R. Canetti, "HMAC: Keyed-hashing for message authentication", Citeseer, 1997, pp. 1-11.

[27] P. Kuznetsov and R. Rodrigues, "BFTW 3: why? when? where? workshop on the theory and practice of byzantine fault tolerance", ACM SIGACT News, 40(4),2009, pp. 82-86.

[28] L. Lamport, R. Shostak and M. Pease, "The Byzantine generals problem", ACM Transactions on Programming Languages and Systems, 4(3), 1982, pp. 382-401.

[29] P.A. Loscocco, S.D. Smalley, P.A. Muckelbauer, R.C. Taylor, S.J. Turner and J.F. Farrell, "The inevitability of failure: The flawed assumption of security in modern computing environments", Citeseer, 1998, pp. 303-314.

[30] P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin and M. Walfish, "Depot: Cloud storagewith minimal trust", OSDI'10: Proc. of the 9th USENIX Conf. on Operating systems design and implementation, 2010, pp. 1-16.

[31] U. Maheshwari, R. Vingralek and W. Shapiro, "How to build a trusted database system on untrusted storage", OSDI'00: Proc. 4thConf. On Symposium on Operating System Design & Implementation, 2000, p. 10.

[32] D. Malkhi and M. Reiter, "Byzantine quorum systems", Distributed Computing, 11(4),1998, pp. 203-213.

[33] J.-P. Martin, L. Alvisi and M. Dahlin, "Minimal byzantine storage", DISC '02: Proc. of the 16thIntl. Conf. on Distributed Computing, 2002, pp. 311-325.

[34] H.Mei, J. Dawei, L. Guoliang and Z. Yuan,"Supporting Database Applications as a Service", ICDE'09:Proc. 25thIntl.Conf. on Data Engineering, 2009, pp. 832-843.

[35] R.C. Merkle, "Protocols for public key cryptosystems", IEEE Symposium on Security and Privacy, 1980, pp. 122-134.

[36] E. Mykletun, M. Narasimha and G. Tsudik, "Authentication and integrity in outsourced databases", ACM Transactions on Storage (TOS), 2,2006, pp. 107-138.

[37] C. Papamanthou, R. Tamassia and N. Triandopoulos, "Authenticated hash tables", CCS '08: Proc. 15th ACM Conf. on Computer and communications security, 2008, pp. 437-448.

[38] M. Pease, R. Shostak and L. Lamport, "Reaching agreement in the presence of faults", Journal of the ACM, 27(2), 1980, pp. 228-234.

[39] R. Perez, R. Sailer and L. van Doorn, "vTPM: virtualizing the trusted platform module", Proc. 15th Conf. on USENIX Security Symposium,2006, pp. 305-320.

[40] RedHat, https://rhn.redhat.com/errata/RHSA-2008-0855.html.

[41] T. Ristenpart, E. Tromer, H. Shacham and S.Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds", CCS'09: Proc. 16thACM Conf. on Computer and communications security, 2009, pp. 199-212.

[42] F. Rocha and M. Correia, "Lucy in the Sky without Diamonds: Stealing Confidential Data in the Cloud", Proc. 1stIntl. Workshop of Dependability of Clouds, Data Centers and Virtual Computing Environments, 2011, pp. 1-6.

[43] N. Santos, K.P. Gummadi and R. Rodrigues, "Towards trusted cloud computing",USENIX Association,2009,pp.3-3.

[44] D. Sarno, "Microsoft says lost sidekick data will be restored to users", Los Angeles Times, October 2009.

[45] F. Schneider and L. Zhou, "Implementing trustworthy services using replicated state machines", IEEE Security and Privacy, 3(5),2010, pp. 151-167.

[46] G. Brunette and R. Mogull (eds), "Security guidance for critical areas of focus in cloud computing", CloudSecurityAlliance, 2009.

[47] A. Shamir, "How to share a secret", Communications of the ACM, 22(11), 1979, pp. 612-613.[48] A. Shraer, C. Cachin, A. Cidon, I. Keidar, Y. Michalevsky and D. Shaket, "Venus: Verification for untrusted cloud storage", CCSW'10: Proc.

[48] ACM workshop on Cloud computing security workshop, 2010, pp. 19-30.

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

[50] Sun, http://blogs.sun.com /gbrunett/entry/ amazon_s3_silent_data_corruption.

[51] H. Takabi, J.B.D. Joshi and G.-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments", IEEE Security & Privacy, 8(6),2010, pp. 24-31.

[52] M. Van Dijk and A. Juels, "On the impossibility of cryptography alone for privacy-preserving cloud computing", HotSec'10: Proc. 5thUSENIX Conf. on Hot topics in security, 2010, pp.1-8.

[53] J. Viega, "Cloud computing and the common man", Computer, 42, 2009, pp. 106-108.

[54] M. Vukolic,"The Byzantine empire in the intercloud", ACM SIGACT News, 41,2010, pp.105-111.

[55] C. Wang, Q. Wang, K. Ren and W. Lou, "Ensuring data storage security in cloud computing", ARTCOM'10: Proc. Intl. Conf. on Advances in Recent Technologies in Communication and Computing, 2010, pp. 1-9.