Secure Cloud Storage with Multi Cloud Architecture

Kavitha G. M., Vinay Kumar A. N., Balasubrhamanya

***Abstract*— 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. Dealing with "single cloud" providers is predicted to become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud. A movement towards "multi-clouds", or in other words interclouds or cloud-of-clouds has emerged recently.**

In this paper, we provide solutions for secure cloud storage in multi cloud based system. This work aims to promote the use of multi-clouds due to its ability to reduce security risks that affect the cloud computing 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. Subashini and Kavitha [49] argue that small and medium companies use cloud computing services for various reasons, including because these services provide fast access to their applications and reduce their infrastructure costs.

Cloud providers should address privacy and security issues as a matter of high and urgent priority. Dealing with "single cloud" providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud. In recent years, there has been a move towards "multiclouds","intercloud" or "cloud-of-clouds".

This paper focuses on the issues related to the 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 Cloud providers should address privacy and security issues as a matter of high and urgent priority. Dealing with "single cloud" providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud. In recent years, there has been a move towards "multiclouds", "intercloud" or "cloud-of-clouds".

This paper focuses on the issues related to the 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. In addition, the potential for migration from a single cloud to a multi-cloud environment is examined and research related to security issues in single and multi-clouds in cloud computing are surveyed. Information, such as credit card details or a patient's medical records from attackers or malicious insiders is of critical importance. In addition, the potential for migration from a single cloud to a multi-cloud environment is examined and research related to security issues in single and multi-clouds in cloud computing are surveyed.

Revised Manuscript Received on June 06, 2013.

Kavitha G M, MTECH, CS&E SJMIT, Chitradurga VTU University, Belgaum, India.

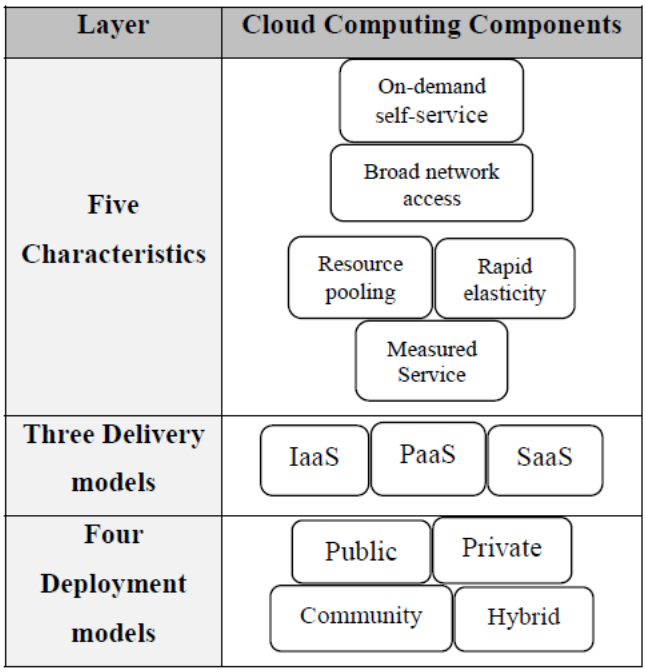
Vinay Kumar A N, MTECH, CS&E EPCET, Bangalore VTU University, Belgaum, India.

Balasubrhamanya, Thought Mac,Banglore, India

II. LITERATURE SURVEY

NIST [1] describes cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

The cloud computing model consists of five characteristics, three delivery models, and four deployment models [1]. The five key characteristics of cloud computing are: location-independent resource pooling, on-demand self-service, rapid elasticity, broad network access, and measured service [51]. These five characteristics represent the first layer in the cloud environment architecture (see Figure1).



The three key cloud delivery models are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). In IaaS, the

user can benefit from networking infrastructure facilities, data storage and computing services. In other words, it is the delivery of computer infrastructure as a service. An example of IaaS is the Amazon web service [25]. In PaaS, the user runs custom applications using the service provider's resources. It is the delivery of a computing platform and solution as a service. An example of PaaS is GoogleApps. Running software on the provider's infrastructure and providing licensed applications to users to use services is known as SaaS.

An example of SaaS is the Salesforce.com CRM application [25],[49],[51]. This model represents the second layer in the cloud environment architecture. Cloud deployment models include public, private, community, and hybrid clouds. A cloud environment that is accessible for multi-tenants and is available to the public is called a public cloud. A private cloud is available for a particular group, while a community cloud is modified for a specific group of customers. Hybrid cloud infrastructure is a composition of two or more clouds (private, community, or public cloud) [51]. This model represents the third layer in the cloud environment architecture.

Kamara and Lauter [25] present two types of cloud infrastructure only, namely private and public clouds. The infrastructure that is owned and managed by users is in the private cloud. Data that is accessed and controlled by trusted users is in a safe and secure private cloud, whereas the infrastructure that is managed and controlled by the cloud service provider is in a public cloud. In particular, this data is out of the user's control, and is managed and shared with unsafe and untrusted servers [25].

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].

III.SECURITY RISK IN CLOUD COMPUTING

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, 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 ccurs 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 faulttolerant 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].

IV. DETAILS OF PROPOSED SECURITY MECHANISM

A. Data integrity in Multi Cloud

We provide a fast and effective mechanism for providing data integrity for user data in multi cloud.

Our mechanism is a hash based approach. The users file is split to many blocks. At any instant of time the files are stored in two different clouds. For each block hash is calculated and the hash is also maintained in the cloud.

When any user requests for the cloud, the file blocks are retrieved from two cloud locations. The blocks are ideally kept in different storage servers in the cloud. The blocks are assembled to form wherever it is not corrupted. The corrupted blocks are replaced with valid block from other locations. Through the hash value of block matching with stored hash value the integrity is verified. We also keep track of number of times the files for corrupted for the user and the number of times the files are corrupted in the cloud server.

If the count of the number of times file corrupted for user are higher, then it concludes that the authentication of the user has a leakage and his files are purposely corrupted by compromise of authentication parameters. In our proposed system we will keep various levels of security and different security profiles will be enabled based on the file corruption threshold parameter.

Also from the count of number of times files getting corrupted in cloud server, reputation of storage server is found. This will help the administrators to use mechanism like firewalls to improve the security of lower reputation storage servers. Based on the reputation of all servers in the cloud storage the reputation of the cloud calculated. If the reputation of cloud is lower the cloud data is backed up to other cloud and cloud is removed all the contents and that storage cloud is drooped from use for storage.

While penalizing the cloud for its lower reputation , we should also consider that compromise in user security may be due to user fault and penalizing should not be done due to this fault. The file corruption condition must be

accounted in bas reputation only when highest security profile is allocated to user and still data corruption occurs.

B. Data Intrusion in Multi Cloud

To avoid data intrusion, ie user authentication is hacked and fake users login and corrupt the data we provided a multi level security profile for the user. The levels of security for the user are very adaptive. If the user data is corrupted , he is move to highest security profile level starting from the lower security profile level.

In our proposed solution we provide but many levels can be provided.

1. User name , password based authentication
2. Secure session id sent to user on his mobile phone for authentication
3. Biometric authentication.

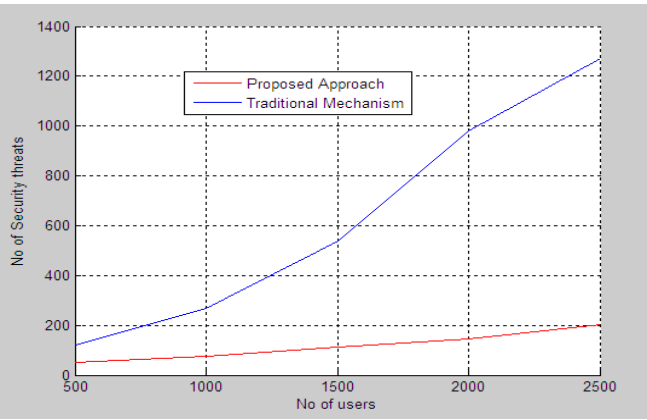
The default security profile is Level 1 user name/Password based authentication. If the user files are frequently corrupted with Level 1, than for the particular user Level 2 authentication is used. In Level 2 user has to enter his user id and get the password for access on his registered mobile number and he has to login using that password. This mechanism is more secure than Level 1. If the user file is still getting corrupted in Level 2 , the authentication is migrated to Level 2. In Level 2 biometric authentication is provided which is much more secure than Level 1.

C. Service Availability in Multi cloud

Service availability is multi cloud is guaranteed with replicated file storage in two clouds. The file is replicated in the minimum of two clouds so that any point of time one cloud is always available. At each cloud , the file blocks are kept in the cloud storage , to guarantee high availability for the block. 1+1 replication for blocks are kept in servers , so that even if one of server is down the blocks can be retrieved from other server.

V. PERFORMANCE ANALYSIS

We simulated the proposed solution for providing service availability, attack against data intrusion and data integrity. We measured the performance in terms of number of security threats with and without our mechanism. We varied the number of users in the cloud for 4 cloud accounts and 10 storage server in each cloud. From the performance chart that our proposed mechanism is able to reduce the number of security attacks gradually thanks to the adaptive user security profile setting and the reputation based server filtering.



VI. 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 threat in cloud storage. We have proved that our mechanism performs better in reducing the security threat on cloud.

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 cloud storage", 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 evalua tion 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 storage with 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. 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.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication