Towards Security and Privacy Issues from Single Cloud to MultiCloud

[1]M. Menaka, [2]C. Deepa, [3]K. Sankar
[1,2,3]Dept. of CSE, Sri Balaji Chockalingam Engineering College, ACS Nagar, Irumbedu, Arni, India

Abstract
Cloud computing provides an exclusively latest model for enterprise computing since it switches a fixed-cost infrastructure into a new prototype based on utility-oriented services on the subscription basis. Distributed resources and services that belong to different organizations or sites can be shared among the users who significantly reduce the need for investment in computing resources by the organizations. Success of cloud storage providers can present a considerable risk to customers, as it becomes exceptionally expensive to change storage providers. Dealing with "single cloud" providers is less popular due to risks of reliability, failure, service availability and security of data stored. Contrarily, multi-cloud, improves the availability, integrity and confidentiality of information stored in the cloud through encryption, encoding and replication of the data on diverse clouds. Multi-clouds improve the perceived data availability and, in most cases, reduce the access latency significantly, when compared with cloud providers individually. We explored that there has been very little attention devoted by the research community on security and privacy issues of multi cloud providers than with the use of single clouds. This paper is aimed at surveying privacy and security issues of single and multi-cloud and suggests promoting the use of multi-clouds due to minimized security risks that affects the cloud computing user.

Keywords
Cloud Computing, Security, Privacy, Trust, Confidentiality, Integrity, Availability

I. Introduction

Cloud computing supports elasticity and seamless scalability of IT resources that are recommended to end users as a service through Internet medium. Cloud computing can assist enterprises ameliorate the formation and dispatch of IT solutions by providing them to access services in a most cost-effective and flexible manner. Although Cloud computing has developed mainly from the appearance of public computing utilities, there exists differing deployment models, with diversities in physical location and distribution. Apart from the cost savings [23] and yield benefits of cloud computing is the major fascination of an accessible on-demand model for network access to a shared reserve of configurable computing resources that can be rapidly trafficked in and unleashed with inconsequential management endeavor or service provider fundamental interaction. The key consideration is that the cloud providers should address privacy and security problems as a matter of important and critical priority. "Single cloud" [10, 20] providers are eventually becoming less widespread due to service accessibility failure and the probability of vicious insiders.

Multi-cloud approach is the concomitant utilitization of two or more cloud services to reduce the risk of widespread data loss or downtime due to a localized hardware, software, or infrastructure failures in a cloud computing environment [7]. A multi-cloud strategy significantly enhances overall enterprise performance by carefully preventing "vendor lock-in" and generally exploiting varied infrastructures to meet the requirements of dissimilar partners and customers. Reasons for an adverse cloud event can vary from a simple cable connector failure or from a natural disaster to an act of cyber warfare. If a defect develops at a critical point in the system such as a host computer, can collapse the entire network. A multi-cloud approach can navigate traffic from various customer bases or partners through the fastest possible parts of the network. Some clouds are better suited for a particular task than its alternatives. As an example, a specialized cloud might deal with large numbers of requests per unit time demanding small data transfers on the average, but another cloud might behave better for smaller numbers of requests per unit time entailing large data transfers on the average. Some organizations may exploit a public cloud to arrange resources over the Internet, ready for use to consumers and provide hosted services with a private cloud to a restricted number of people behind a firewall. Contrarily, another classification of cloud, called a hybrid cloud, may also cast off managing miscellaneous internal and external services. Disastrous or ubiquitous failures of cloud-based systems are not simple hypothetical events. An electrical transformer breakdown ostensibly caused a breakdown On August 7, 2011, in Amazon's cloud computing hub located in Dublin, Ireland. Microsoft's azure cloud management system failed and disconnected users in the regions of the United States and Europe for a couple of hours On February 29, 2012. In both situations, a multi-cloud approach might have impeded the failures from inducing consequential service interruption.

This paper stems on the data security and privacy aspects of cloud computing. Protecting private and sensitive information from assailants or spiteful insiders is of significant importance. Rest of the paper is organized as follows. Section 2 deliberates the background works related to privacy and security of cloud computing. Section 3 elaborates the beginning of cloud computing and its components. Section 4 discusses security risks in cloud computing. Section 5 analyses the new generation of cloud computing, that is, multi-clouds and recent solutions to address the security of cloud computing.. Section 6 presents current solutions of security and investigation of their limitations. Section 7 concludes the paper.

II. Related Works

Cloud computing is internet based development that is dynamically scalable and often virtualized resources are provided as a service. High availability, data accessibility, data persistence, better efficiency, low cost and agility are some of many benefits cloud computing provides to the users. Leading organizations consider pruning their data in data centers into the cloud owing to the increased popularity of cloud storage. Users need not have knowledge of expertise in, or control over the technology infrastructure "in the cloud" that supports them. Outward facing side of cloud computing has a growing set of associated standards. However reliability, privacy and security of data stored in the cloud still remains a major issue.

The author of [11] enumerates their skilled expertise working with Amazon.com's Simple Queue Service, Simple Storage Service

and Elastic Compute Cloud and found that the congregation of Amazon Web Services has distinguished promise but are staggered by service compatibility complications, the scarcity of a Service Level Agreement, and a complex Web Services Licensing Agreement. In paper [29], the authors assert that moving the software applications and databases to the cloud may not be fully reliable and may give rise to many new security and privacy threats. To guarantee the correctness of users' data in the cloud, the authors proposed an efficient and amenable distributed scheme with two remarkable features, employing the homomorphic token with distributed authentication of erasure-coded data, and data error localization. The authors of paper [20] argue that clients of cloud computing services currently have no means of verifying the confidentiality and integrity of their data and computation. To address this problem the authors proposed the design of a Trusted Cloud Computing Platform (TCCP) which provides a closed box execution environment that guarantees confidential execution of guest virtual machines.

In paper [18], the authors state that the use of virtualization allows third-party cloud providers to maximize the utilization of their sunken capital costs by multiplexing many customer VMs across a shared physical infrastructure. The authors, however, strongly argue that this approach can also introduce new threats. The authors also have demonstrated with Amazon's EC2 service, that it is possible to map the internal cloud infrastructure, distinguish where a particular target VM is expected to remain and instantiate new VMs until one is placed to co-exist with the target. They also explored how such placement can then be used to mount cross-VM side-channel attacks to extract information from a target VM on the same machine. The authors [8] surveyed well-known cryptographic tools for providing integrity and consistency for data stored in clouds and examined recent research in cryptography and distributed computing addressing the above said problems. The authors [6] introduced a distributed cryptographic system named HAIL (High-Availability and Integrity Layer), that allows a set of servers to prove to a client that a stored file is intact and retrievable. The authors argue that their system improves on the security and efficiency of existing tools, like Proofs of Retrievability (PORs) deployed on individual servers. In paper [26], the authors explain Clients' lack of direct resource control in the cloud prompts concern about the potential for data privacy infringements especially abuse or leakage of extremely sensitive information by service providers. The authors argue that cryptography alone can't enforce the privacy demanded by common cloud computing services. They defined a hierarchy of natural classes of private cloud applications, and revealed that no cryptographic protocol can implement those classes where data is shared among clients. They also state that users of cloud services will also need to rely on other forms of privacy enrichment, such as tamper proofed hardware, distributed computing, and complex trust ecosystems. In paper [25], the authors explore Unique aspects exacerbate security and privacy challenges and also explain the roadblocks and solutions for providing a trustworthy cloud computing environment. Paper [23] details Security and complications with data privacy and data protection are the major issues which reduce the growth of cloud computing. A new model targeting at improving features of an existing model must not risk or threaten other important features of the current model. In this paper, the authors survey different security risks that have emanated due to the nature of the service-delivery models of a cloud computing system.

The paper [22], presents Venus, a service for securing user interaction with untrusted cloud storage. Particularly, Venus promises integrity and consistency for applications acquiring a key-based object store service, without needing fully trusted components or changes to the storage provider and whenever either integrity or consistency is violated, Venus alerts the application. The authors implemented Venus and evaluated it with Amazon S3 commodity storage service and claim that the evaluation shows no noticeable overhead added to storage operations. The paper [16], describes an implementation of a cloud storage system that minimizes trust assumptions and claims their assessment recommend cost of their design guarantees are modest. In paper [1], at the cloud storage level, the authors make a case for implementing RAID-like approaches used by disks and file systems. The authors also assert that striping user data transversely in multiple providers can enable customers to prevent vendor lock-in, minimize the cost of interchanging providers, and to a greater degree, tolerates provider failures with the launch of RACS, a proxy that transparently spans the storage load over numerous providers. In paper [4] the authors presented DEPSKY, a system that considerably enhances the privacy, security and confidentiality of information stored on diverse clouds that form a cloud-of-clouds. The authors claim that their implementation of protocols improved the perceived availability and the access latency when matched with cloud providers independently. The paper [2] proposes the architecture of a new model appropriate for NetDB2 architecture, known as NetDB2 Multi-Shares (NetDB2-MS). It is based on multi-service providers and a secret sharing algorithm.

III. Cloud Computing Components

Cloud computing model consists of 1. Five characteristics 2. Three delivery models and 3. Four deployment models. The five characteristics of the first layer in the cloud environment architecture are: 1. Location-independent resource pooling. 2. On-demand self-service 3. Rapid elasticity 4. Broad network access and 5. Measured service [25]. Three cloud delivery models are 1. Infrastructure as a service(IaaS) 2. Platform as a service(PaaS) and 3. Software as a service(SaaS).

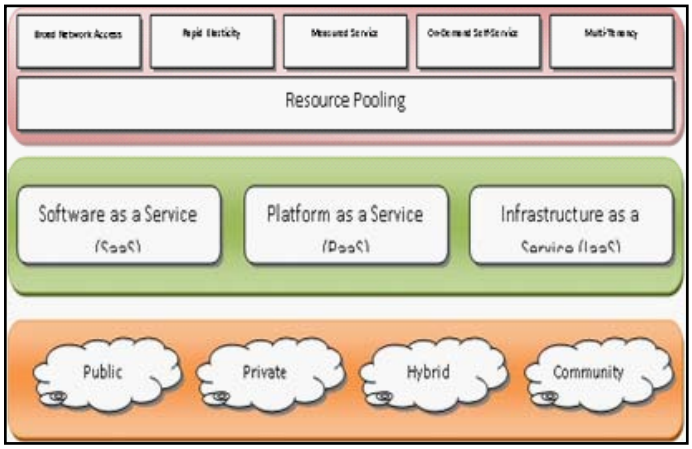

Fig. 1: Cloud Components

IaaS is enhanced from networking infrastructure services, which includes hardware, storage, networking components and servers [14]. PaaS, is a software distribution model in which the user executes custom applications utilizing the service provider's resources. SaaS is a software delivery model that runs licensed software and applications on the provider's infrastructure to users as services. Cloud deployment design comprises private, public, community, and hybrid clouds. A cloud environment that is publicly accessible for multi-tenants and is ready for use to the

consumers is called a public cloud. A private cloud is for use with a distinct group, whereas a community cloud is reorganized for a specific class of customers. Hybrid cloud infrastructure is a structure of two or more clouds.

In private cloud, data is accessed and controlled by trusted users in a safe and secured manner, where as the cloud service provider administers and controls the infrastructure in a public cloud [14]. Hence in public clouds the data is out of user's control, which is managed and shared with unreliable and untrusted servers. Customers can experience vendor lock-in: It can be extremely costly for clients to shift from one provider to other service providers. A client switching from one provider to another spends for bandwidth twice, in addition to the actual price of online storage. This doubled cost of shifting data initiates a kind of "data inertia"; the more data laid down with one provider, the more laborious it gets to move. Clients are susceptible to price hikes by vendors, and will not be able to move freely to latest and better alternatives when they become available.

A customer's optimal judgement now may warrant him cornered with an old-fashioned provider later, restrained as a hostage by vendor lock-in. Vendor lock-in exposes customers to the potential chance of data loss if their provider breaks out of business or sustains a catastrophe. Defects at cloud providers can culminate widespread data loss for customers, and that outages, though seldom, can last up to a couple of hours. One suggested solution to defend against vendor lock-in is to duplicate their data to several cloud providers. Extremely high storage and bandwidth cost will incur to accomplish the objectives of redundancy and market agility. The data is transparently striped across multiple cloud storage providers through Redundant Array of cloud Storage) which is a cloud storage proxy. RACS minimizes the one-time cost of switching storage providers in interchange for added operating cost. It is realizable to endure outages and soothe vendor lock-in with acceptable cost over-head.

IV. Security and Privacy Challanges

Policy changes, effectuation of highly dynamic applications, and securing the rapidly changing environment are some of the risks related to the fulfillment of a new technology service delivery model. The extenuation design for these risks depends on authenticating robust security program to device industry best practices and government policies in the management of programs[27]. The cloud community will also require placing latest privacy, security, safety measures, which will allow secured access to dynamic applications and information-sharing[8]. Specific challenges of privacy and Security in cloud computing include:

A. Privacy

Growing number of countries restricts and regulates handling and storing of personal information outside of the country. Providing a single level of service acceptable in every jurisdiction is highly impossible. Hence, many cloud service providers are interested in contractual commitments to accommodate privacy challenges for storing data within specific countries, though it is extremely difficult to verify. The providers must implement some sort of assessment strategy when customers use cloud services across the globe, and the term security takes the role of more compliance and risk management than the security operations. In the lifetime of a cloud provider that handles top secret and private customer data, when the outcomes and potential costs of mistakes are increasing swiftly, IT security specialists must learn to generate superior ways of assessing the security and privacy policies of the cloud services. An efficient assessment strategy must conceal data protection, privacy, identity management, security, compliance and other related legal issues.

B. Share Risk

In many occasions, the cloud operator will not be a cloud service provider. However, the operator may be offering a value-added service in coordination with other cloud provider's service[2]. As an illustration, if a SaaS provider requires infrastructure, rather than assembling that structure, it makes more sense to procure that infrastructure from an IaaS provider. The cloud service providers stacks those infrastructures, get it built by layering SaaS on top of IaaS, can affect the security of data stored on cloud by customers. In this type of multi-tier service provider adaptation, each party significantly shares the risk of security since the risk potentially influences all parties at all layers. The detection of all parties involved in providing a cloud solution is a crucial aspect in a total risk management plan.

C. Physical Security

Choosing a cloud security provider requires a careful examination of physical external threats. Whether all the cloud provider's resources have the same degree of security? Are the customers being sold with the most secure facility without any guarantee that the customer's data will literally stay there? Do the services have, at a minimum, card or biometric access, close surveillance, onsite safeguards, a necessity that all residents be shepherded and all non-guarded exit points be armed with fully automated alarms? Do the facilities fit the standards and security prerequisites of the customer's department, business agency, or organization?

D. Data Leakage

From a security point of view, data leakage is one of the greatest organizational risks. Almost all governments worldwide have rules and regulations that warrant protections for specific data types. The cloud provider must have the potential to overlay its policy to the security mandate the customer must agree with and deliberate on the issues. To a minimum, the data should be encrypted while in transit and at rests, which is under legislative mandates, or contractual obligation. Moreover, risk assessment once in a year should be done just on the data in question to make certain the alleviations converge to the requirements. The cloud provider must take into account the data leakages in its security incident response and notification policy.

V. Introduction to Multi-Clouds

The organizations are probing inquiry into cloud management solutions to furnish a level of abstraction from individual cloud potentials and empower "liberation from the workload" — the capability to select and settle on the cloud's infrastructure that is optimal for all applications at any point of time [7]. Merging a cloud management result with a multi-cloud wide portfolio permits organizations to safeguard choice while equalizing technical, business and financial precedences. In most cases, the organizations should understand that they need to formulate and leverage a portfolio of private and public clouds. Whatsoever the inspiration for establishing a multi-cloud architecture, the companies should ponder various causes:

- Cloud functionality gap
- Secure connection of clouds
- Overcoming latency and most important is
- Controlling cost.

A. Six Reasons to use Multicloud

Here are six reasons from the experiences of multicloud users in favor of use of multiple cloud services:

1. Data do not flow across international boundaries all the times. If a customer's IaaS supplier is in another part of the globe, the customer may demand a second service in the country where the customer wants to operate.
2. A Cloud provider must have a projection for a large data center and staff, before their business gets too big, otherwise the provider will develop a successful service that's set to implementation but misses serving demand as it materializes. Contrarily, the customer can depend on the cloud until they realise what data center they need practically.
3. If the customer owns a small company and doesn't ever desire to maintain a bulky data center, but wants to meet persistent spikes in demand, then the customer needs a way to alter traffic to reserve capacity elsewhere, and the inter cloud is one of the logical vendors.
4. If a cloud provider wants the pliability of offering their cloud service in either a public cloud context or a private infrastructure operation for a highly valued consumer, the provider will require a direction to establish a private cloud quickly without diverting all their engineering labor to do so.
5. A hybrid cloud operation will let a client to focus on the effects that capitulate on unparalleled business value, if a customer desires to run his own data center, but recognize a few universal workloads can operate more productively in an automated scaling and load-balanced circumstances.
6. Each cloud provider has distinctive capabilities, and a customer must think between the benefit of showing autonomy and circumventing vendor lock-in by maintaining an association with more vendors, in case, if none of the above appear suitable to their requirements. The consumer must always look for possibilities to extract potential benefit of the fit that matches their requirement.

B. Byzantine Fault Tolerant Protocol: An Introduction.

The objective of BFT is to guard against arbitrary failures of components within a system. Byzantine fault tolerant system components functioning as expected will be capable of providing the system's service properly, pretending there are not too many Byzantine faulty components [17]. Byzantine Failure / Resilience Failures in a protocol can be grouped under three types:

1. "Fail stop" fault - A failure which derives additional execution pace in the protocol.
2. "Random fault" or "random Byzantine fault." - A random failure to run the protocol properly.
3. "Byzantine fault" is an arbitrary failure where the protocol incorrectly executes the steps which include the preceding two forms of imperfections.

C. DEPSKEY – Introduction

The DEPSKY system is a cloud-of-clouds storage that overcomes the deficiencies of single clouds by employing a standardized collection of Byzantine quorum system protocols, erasure codes, secret sharing, cryptography and the dissimilarity[8]. The DEPSKY protocols necessitate a maximum of two communication round-trips for every task and save only half of the data in each cloud approximately.

1. The DEPSKY System

The following sections demonstrate the DEPSKY system. It introduces the system architecture, and then describes the data and system models.

2. DEPSKY Architecture

The following fig. 1, explains the DEPSKY system architecture [4]. Referring to our previous discussions, the clouds are storage clouds lacking the capability of running users' code, and hence they are accessed using their standard interface without changes. The DEPSKY algorithms are executed from a software library in the clients. Similar to parallel file systems, these libraries provide an object store interface, which enables reading and writing of data in the back-end.

3. Data Model

The DEPSKY library has to administer the heterogeneity of the interfaces of individual

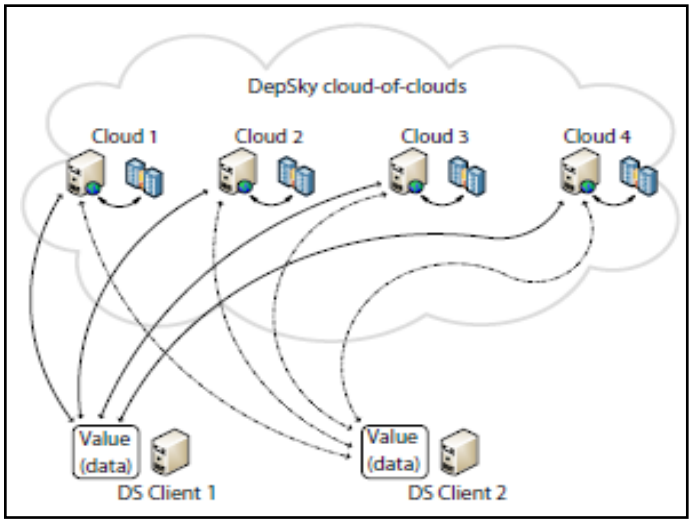

Fig. 2: DEPSKY Multicloud Computing Architecure

cloud providers for use with diverse clouds. The data format accepted by each cloud is an important factor, and the data model allows to disregard these particulars when presenting the algorithms. The DEPSKY data model has three abstraction levels. 1. The conceptual data unit, with which the algorithms work and, which corresponds to the basic storage object. 2. Generic data unit. Each generic data unit, or container, contains two types of files: a signed metadata file and the files that store the data and the data unit either conceptual or generic, can store different versions of the data. 3. The data unit implementation, in which the container is translated into the specific structures advocated by each cloud provider. The data unit can be stored data of arbitrary size, and for different versions of data, this size will be different. Every data unit object reinforces the usual object store processes: creation, destruction, write and read.

4. System Model

The DepSky system prototype comprises an asynchronous distributed system that is composed of readers, writers, and four cloud storage providers, in which readers and writers are the client's processes [4]. Readers can collapse arbitrarily (crash failures, fail in a duration of time, display any kind of behavior) but writers fail by crashing alone.

VI. Current Security Risks, Solutions and Limitations

Table 1: List of Current Security Risks

Risk	Risk Description	Solution	Limitations
1	Short-term and long-term ROI may not fit economic objectives.	Built into the majority of ROI models, and influences the estimates for investment, yield, price, and time of repayment.	ROI risk probability should include utilization, speed, scale, and quality.
2	Solution may not succeed in the scene of the user enterprise's organization and culture.	A clear organizational perception and focus for business transformation, an obvious roadmap for procurement or enforcement of cloud services and applications that exploit them, coordination of stakeholders and competing policies to obtain consensus for storage, computing, and network to prevent islands of demand usage.	Always begin with pilots to Institute reliance and fabricate buy-in and usage for cloud services in the user community.
3	It may not be promising to assimilate [multiple] cloud services with the currently existing system.	Think over interface remodeling expense, skill to transform the existing system, and present skills.	Considerable abilities are essential to accumulate and personalize multiple cloud services from various providers in a resilient, adaptable way, while caring for security, governance and backup procedures.
4	External cloud supplier dependence can proliferate the chances of noncompliance.	Stipulate the required assertions on location and confidentiality necessitate majeure, which may impede the supplier from esteeming them.	What would be the outcome of lawful action for the subpoena of data, not even be held under the tenancy in a cloud environment, but have been laid on the same system by other occupants? What would be the impact on the customer's corporate enviable reputation?
5	Business "disaster" on the part of cloud suppliers may be present from which the solution cannot improve	A Customer should distinguish the unintentional events that could harm them, and assess their likelihoods and major influences, as part of their risk evaluation.	An efficient backup and restore procedure, with the backup copy stored in a different place from the data, than the cloud supplier's system, can influence a catastrophe from malignant to simply crucial.
6	System quality may be unsatisfactory may not fit users' needs.	Assess external service's quality by same factors as that of system quality of customer's own solution.	Customer should examine the track records of suppliers very cautiously, just as it would be for any outsourcing provider.
7	Security may be inadequate	modern security models must be developed and applied	Must accommodate traditional security paradigms to suit cloud computing requirements and meditate on end-to-end security, comprising own internal practices for access control and user provisioning.
8	Lack of service orientation	Ability to move processes from current interfaces and underlying applications to more agile cloud services will ease the risk	Makes cloud more expensive than leaving things as it is

VII. Conclusion

There is no comprehensive explanation to assure customers that a cloud is completely reliable. The significance of privacy and security differs from organization to organization, pivoting on the data's value. Nevertheless, it's critical that consumers and providers switch their dispositions. Unlike other systems, trusting cloud computing is different, but the goals are the same— develop the business and be competitive applying the enhancements of a modern technology. Rapidly emerging technologies must progressively augment its distinction for good performance, privacy and security, reaping users' confidence over time. The annoyances of security by some cloud providers have instigated consumers to be more security conscious than they were before. Cloud providers must advance to a greater degree of transparency and more client entrustment of data and processes, for repossessing consumers' trust.

References

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

[2] M.A. AlZain, 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. Amazon, Amazon Web Services. Web services licensing agreement, October3,2006.

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

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

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

[6] K.D. Bowers, A. Juels, 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.

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

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

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

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

[11] 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.

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

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

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

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

[16] 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.

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

[18] T. Ristenpart, E. Tromer, H. Shacham, 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.

[19] F. Rocha, 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.

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

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

[22] A. Shraer, C. Cachin, A. Cidon, I. Keidar, Y.Michalevsky, D. Shaket,"Venus: Verification for untrusted cloud storage", CCSW'10: Proc. ACM workshop on Cloud computing security workshop, 2010, pp. 19-30.

[23] S. Subashini, 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.

[24] Sun, [Online] Available: http://www.blogs.sun.com /gbrunett/ entry/ amazon_s3_silent_data_corruption.

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

[26] M. Van Dijk, 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.

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

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

[29] C. Wang, Q. Wang, K. Ren, 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.

M.Menaka is a B.E Final Year Student of Computer Science and Engineering Specialization, SBC Engineering College,Arni, and her research interests includes Cloud Computing, Grid Computing, Distributed Data Processing

C.Deepa is a B.E Final Year Student of Computer Science and Engineering, SBC Engineering College, Arni. Her research interests include Cloud Computing, Software Engineering, and Cryptography & Network Security

K.Sankar is working as Assistant professor in the Dept. of Computer Science and Engineering SBC Engineering College, Arni. His research interests include Wireless Ad-Hoc networks, Mobile computing, Pervasive computing, etc.,