ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 3, March 2014

Dynamic Massive Data Storage Security Challenges in Cloud Computing Environments

Chintada. SrinivasaRao[1] Chinta.ChandraSekhar[2]

Asst. Professor, Dept of IT, AITAM, Tekkali, Andhra Pradesh, India[1]

Asst. Professor, Dept of IT, AITAM, Tekkali, Andhra Pradesh, India[2]

ABSTRACT: Today, users effectively lose control of their data in the cloud, if either the cloud infrastructure or cloud applications are compromised, users' privacy will be at risk. The ubiquitous concern over cloud environment data privacy demands a paradigm shift, such that users can continue to have control of their data in the cloud environment, and verify that the cloud providers have correctly enforced their privacy policies .We offering strong data security to cloud users while enabling valuable applications is a challenging task. We explore a new cloud environment architecture called Data Security as a Service (DSaaS) and, which dramatically reduces the per-application development effort required to offer data security, while still allowing rapid improvement and maintenance.

KEYWORDS: Cloud computing, Data security as a Service, availability, privacy, Integrity, Confidentiality, PerspecSys.

I. INTRODUCTION

Cloud Computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing environment allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. Cloud computing technology allows for much more efficient computing by centralizing data storage, processing and bandwidth

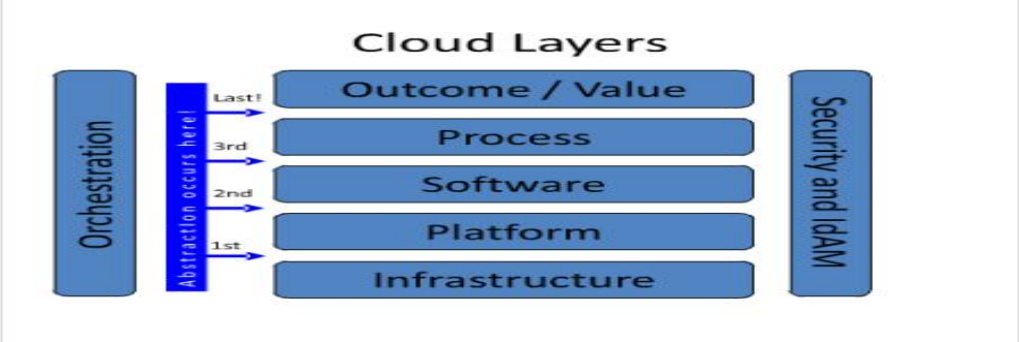

Fig 1: cloud layers

Cloud computing is mainly classified into 3 segments: application, storage, and connectivity. Each segment serves a different purpose and offers different products for businesses and individuals around the world. Cloud computing environment promises lower costs, easier maintenance, rapid scaling, and service availability anywhere, anytime, a key challenge is how to ensure and build confidence that the cloud can handle user data securely. A recent Microsoft survey found that "58% of the public and 86% of business leaders are excited about the possibilities of cloud computing. But more than 90% of them are worried about security, availability, and privacy of their data as it rests in the cloud." **[1]**

PerspecSys Inc. is a cloud security company that provides cloud data protection software. PerspecSys specializes in cloud data privacy, data residency/sovereignty, and data security software that helps organizations comply with industry regulations and directives, and security requirements when adopting cloud. Banking and financial

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 3, March 2014

services, healthcare, retail, and government organizations must adhere to strict guidelines when handling sensitive personal data in cloud applications. These organizations must comply with regulations that include: PCI DSS, ITAR, FERPA, HIPAA, and HITECH.

Cloud computing architecture refers to the components and subcomponents required for cloud computing environment. These components typically consist of a front end platform (fat client, thin client, mobile device), back end platforms (servers, storage), a cloud based delivery, and a network. Combined, these components make up cloud computing architecture.

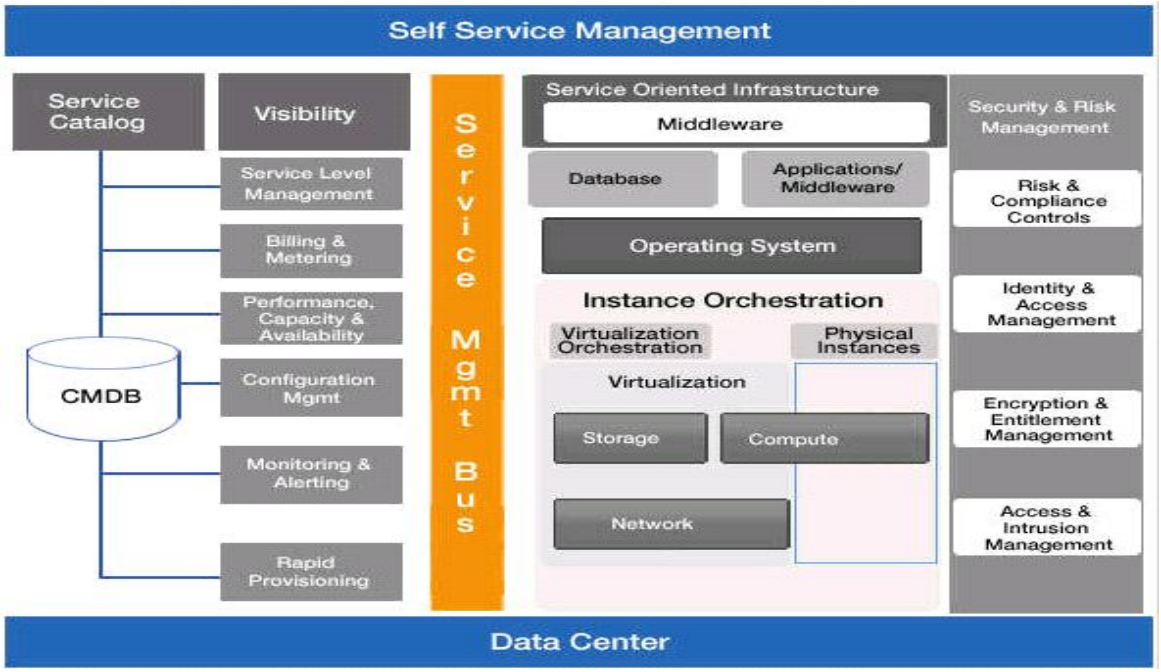

Fig 2: HCL cloud Reference Architecture

CLOUD STORAGE [2]

Online network storage where data is stored and accessible to multiple clients in cloud computing environment. Cloud storage is generally deployed into three configurations: public, private, community, or some combination of the three is also known as hybrid cloud. The cloud storage needs to be agile, flexible, consistent, scalable, multi-tenancy, and secure.

CLOUD BASED DELIVERY

Software as a service (SaaS) service-model involves the cloud provider installing and maintaining software in the cloud and users running the software from their cloud clients over the Internet. The users' client machines require no installation of any application-specific software - cloud applications run on the server. Software as a service is scalable, and system administration may load the applications on several servers. In the past, each customer would purchase and load their own copy of the application to each of their own servers, but with the Software as a service the customer can access the application without installing the software locally. Software as a service typically involves a monthly or annual fee. Software as a service provides the equivalent of installed applications in the traditional (non-cloud computing) delivery of applications. SaaS has four common approaches: single instance, multi instance, multi tenant, flex tenancy.

Development as a service (DaaS) is web based and community shared development tools. This is the equivalent to locally installed development tools in the traditional (non-cloud computing) delivery of development tools. Platform as a service is cloud computing service which provides the users with application platforms and

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 3, March 2014

databases as a service. This is equivalent to middleware in the traditional delivery of application platforms and databases. Infrastructure as a service (IaaS) is taking the physical hardware and going completely virtual system (e.g. all servers, networks, storage, and system management all existing in the cloud). This is the equivalent to infrastructure and hardware in the traditional method running in the cloud. In other words, businesses pay a fee to run proxy servers, networks, storage from the cloud. This will mitigate the need for a data center, heating, cooling, and maintaining hardware at the local level.

Fig 3: cloud computing service layers

Cloud computing security is an evolving sub-domain of computer security, network security, and information security. Cloud computing security refers to a broad set of policies, technologies, and controls deployed to secure data, applications, and the associated infrastructure of cloud computing. Cloud computing security is not to be confused with security software offerings that are cloud-based such as security as a service.

SECURITY ISSUES ASSOCIATED WITH THE CLOUD[9][10]

Organizations use the Cloud in a variety of different service models (SaaS, PaaS, IaaS) and deployment models (Private, Public, Hybrid). There are number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers and security issues faced by their customers. In most cases, the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information. The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service. Virtualization alters the relationship between the OS and related hardware - be it computing, storage or even networking. This introduces an additional layer - virtualization - that itself must be properly configured, managed and secured. Specific concerns include the potential to compromise the virtualization software, or "hypervisor". While these concerns are largely theoretical, they do exist. For example, a breach in the administrator workstation with the management software of the virtualization software can cause the whole datacenter to go down or be reconfigured to an attacker's liking.

CLOUD SECURITY CONTROLS [3]

Cloud computing security architecture is effective only if the correct defensive implementations are in place. Efficient cloud security architecture should recognize the issues that will arise with security management. The security management addresses these issues with security controls. Security controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. **Deterrent controls**: Deterrent controls are set in place to prevent any purposeful attack on a cloud system. Much like a warning sign on a fence or a property, deterrent controls do not reduce the actual vulnerability of a system. **Preventative controls**: Preventative controls upgrade the strength

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 3, March 2014

of the system by managing the vulnerabilities. This control will safeguard vulnerabilities of the system. If an attack were to occur, these controls are in place to cover the attack and reduce the damage and violation to the system's security. **Corrective controls:** These controls are used to reduce the effect of an attack. Unlike the preventative controls, these controls take action as an attack is occurring. **Detective controls**: These controls are used to detect any attacks that may be occurring to the system. In the event of an attack, this control will signal the preventative or corrective controls to address the issue.

SECURITY AND PRIVACY

Identity management: Every enterprise will have its own identity management system to control access to information and computing resources. Cloud computing providers either integrate the customer's identity management system into their own infrastructure, using federation or Single Sign-On technology, or provide an identity management solution of their own. **Physical and personnel security**: cloud computing Providers ensure that physical machines are adequately secure and that access to these machines as well as all relevant customer data is not only restricted but that access is documented. **Availability**: Cloud computing providers assure customers that they will have regular and predictable access to their data and applications. **Application security**: Cloud computing providers ensure that applications available as a service via the cloud are secure by implementing testing and acceptance procedures for outsourced or packaged application code. Application security requires application security measures be in place in the production environment. **Privacy**: Finally, cloud computing providers ensure that all critical data are masked or encrypted and that only authorized users have access to data in its entirety. Digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud. **Legal issues:** cloud computing providers and customers must consider legal issues, such as Contracts and E-Discovery, and the related laws, which may vary by country.

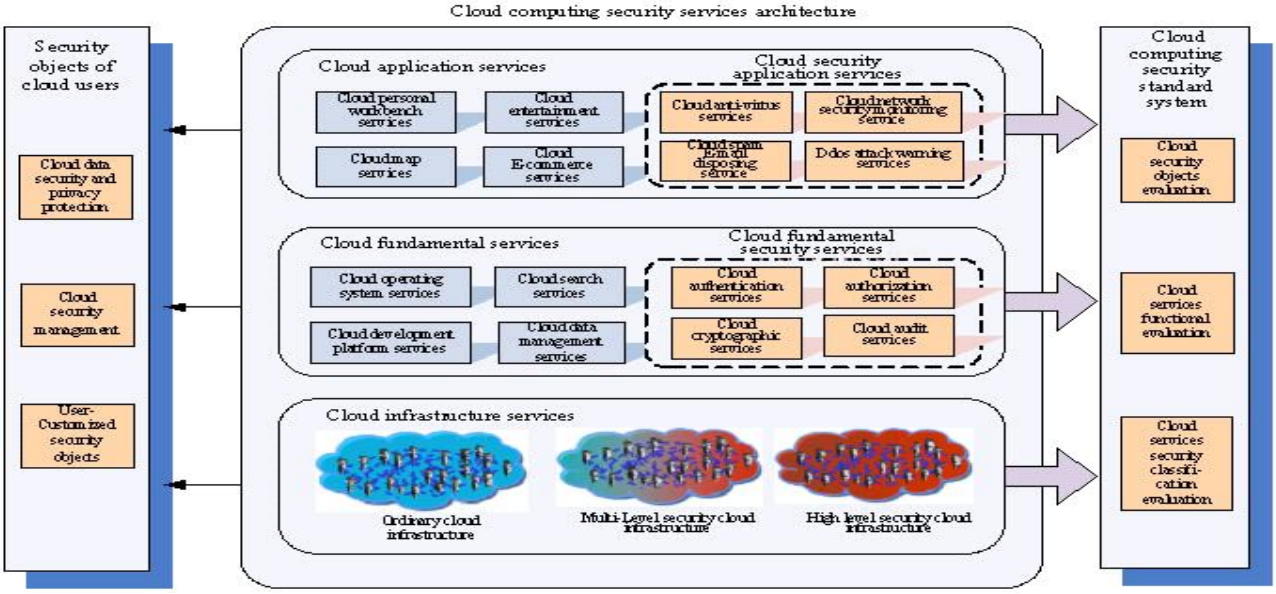

Fig 4: cloud computing security services architecture

II. LITERATURE SURVEY

Dr Elaine Shi **[4]** described several enabling technologies towards this vision. Specifically, she told about 1) how to safeguard users' data against potentially compromised applications; 2) how to safeguard users' data against a potentially compromised computation provider; and 3) how to safeguard users' data against a potentially compromised storage provider. She told about our ongoing effort at integrating these technologies to provide a cloud infrastructure which offers data security at the platform level. In this way, users can benefit from the rich cloud applications without

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 3, March 2014

worrying about the privacy of their data; and application developers can focus on developing functionality while offloading the burden of providing security and privacy to the cloud platform.

Performance According to a recent survey, 49% of users abandon a site or switch to a competitor after experiencing performance issues.**[5]** And the need for speed is only increasing: in 2000, a typical user was willing to wait 8 sec for a webpage to load before navigating away; by 2009, that number dropped to 3 sec.

Platform verifiability**:** The DSaaS approach provides logging and auditing at the platform level, sharing the benefits with all cloud computing applications running on top. Offline, the cloud auditor can verify that the platform implements each data protection feature as promised. At runtime, the cloud platform provider can use *trusted computing* (TC) technologies to attest to the particular software that's running. TC uses the tamper proof TPM as well as the virtualization and isolation features of modern processors, such as Intel VT-x or AMD-V.

TC also allows for a dynamic root of trust—while the system runs, the Central Processing Unit can enter a clean state, and the Trusted Platform Module (TPM) can verify, load, and execute a *trusted computing base* (TCB), TCB is responsible for security-critical functionalities such as access control, isolation enforcement, key management, and logging. Moreover, a third-party cloud auditor can verify the code of the *trusted computing base* that has been loaded on to the cloud computing platform. In this way, users and developers can gain confidence that the applications are indeed running on the correct *trusted computing base* and consequently trust the security guarantees and the audit logs the *trusted computing base* provides.

One challenge in code attestation is how to establish a set of acceptable binaries in the presence of rapid software updates such as bug fixes and latest features. One potential way is to log the history of software updates and perform verification a posteriori. For the application itself, getting from verifiable to verified isn't easy; in a system with a lot of cloud users, doing all cloud pairs verification is prohibitively expensive. This is where cloud auditors come in. Certifications such as Statement on ASN70 (Auditing Standards Number 70) and others serve the important function of reducing the verification burden on both clients and service providers compared to pair wise examinations. Since applications have the data-security piece in common from the platforms, the application verifications in turn can be simpler than they otherwise would have been.

III. MY WORK

Cloud computing Security primitives: Security, privacy, confidentiality, reliability liability, etc are the main concerns on the topic of cloud computing technique and the peak concern is security.. The security issues includes: (1) Data Integrity Problem (2) Privacy (3) Recovery (4) Data location (5) Long-term Viability (6) Freedom (7) Problem Related to Man in the Middle Attack (8). Related to passive Attacks.**[6]**

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 3, March 2014

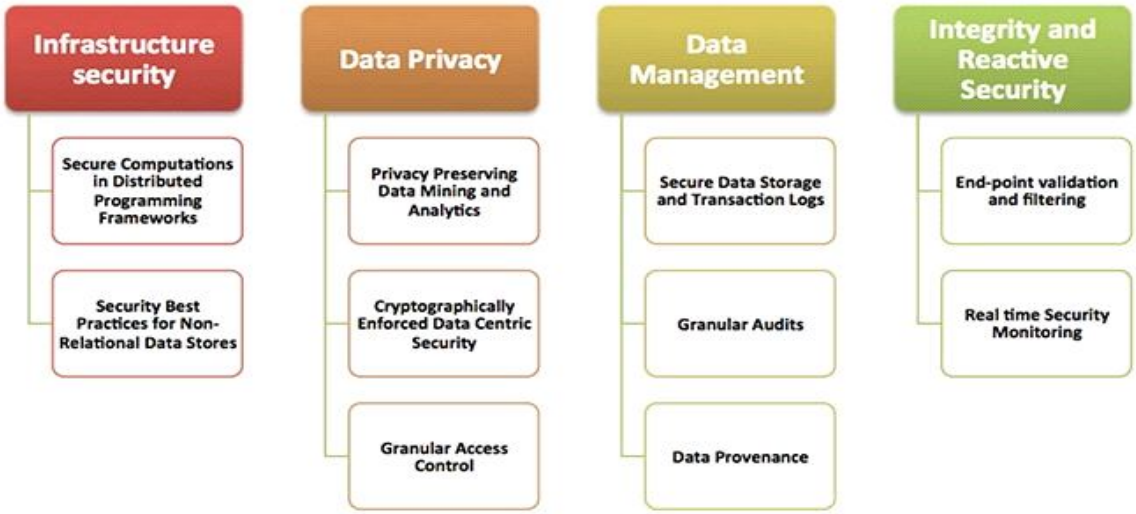

Fig 5: classification of the Top 10 challenges

In this paper propose a new cloud computing paradigm, ***Data Secuirty as a service*** **(DSaaS)** is a suite of security issues offered by a cloud computing platform, which enforces data security and privacy and offers evidence of privacy to cloud data owners, even in the presence of potentially compromised or malicious applications. Such as secure data by using access control, logging, data encryption and secure key management.

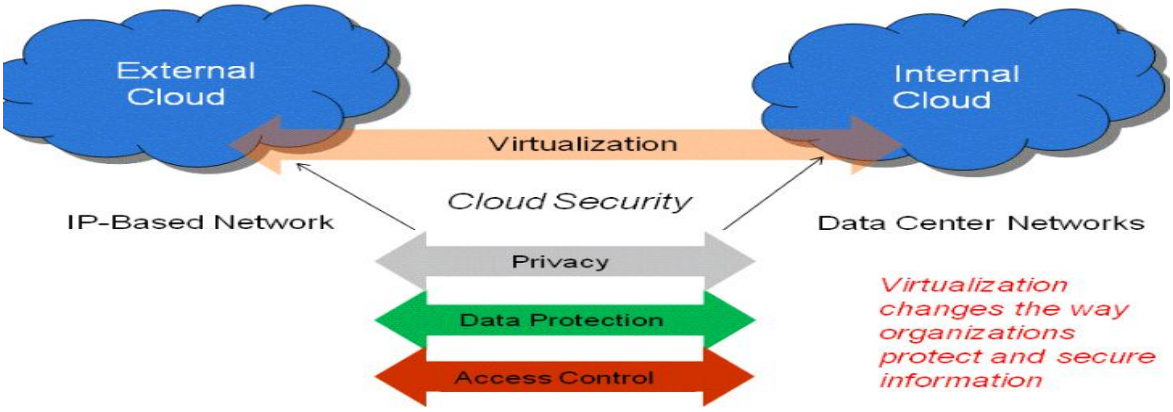

Fig 6: types of cloud environment

DSaaS paradigm focuses on dynamic massive data in cloud environment, by this access control mechanism we will restrict unauthorized users in cloud or outside of the cloud. Secure Data is key artifact in cloud, by using logging system we will restrict middle man attacks. *Data Security as a service* (DSaaS) a cloud platform could help achieve a robust technical solution by making it easy for developers to write maintainable applications that protect user data in the cloud platform, thereby providing the same economies of scale for security and privacy as for computation and storage; and enabling independent verification both of the platform's operation and the runtime state of applications on it, so users can gain confidence hat their data is being handled properly. **[7]**

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 3, March 2014

Fig 7: cloud security model

Secure Key management is the management of cryptographic keys in a cryptosystem. Secure Key management dealing with the generation, replacement, storage, use, and exchange of keys. Secure Key management includes cryptographic protocol design, user procedures, key servers, and other relevant protocols. Secure Key management concerns keys at the cloud user level, either between cloud users or systems. This is in contrast to secure key scheduling; key scheduling typically refers to the internal handling of key material within the operation of a cipher. Successful key management is critical to the security of a cryptosystem. It is arguably the most difficult aspect of cryptography because it involves cloud system policy, cloud user training, organizational and departmental interactions, and coordination between all security elements.

Challenges of Key Management: Several challenges IT organizations face when trying to control and manage their encryption keys are [**8**]: Complex Management: Managing a plethora of encryption keys in the millions. Security Issues: Vulnerability of keys from outside hackers or malicious insiders. Data Availability: Ensuring data accessibility for authorized users. Scalability: Supporting multiple cloud databases, applications and standards. Governance: Defining cloud policy driven, access, control and security for data.

IV CONCLUSION

In this paper we solve many problems that come in our cloud system like confidentiality and Integrity. By using this service we can make our cloud highly secure and efficient. Those users who have less resources and limited computing capability, they can use this service and it is most efficient service for them. Our service is also secured at the time of Dynamic Data operation like insertion deletion and updating.

FUTURE WORK

Based on this work anybody can implement key management system algorithms, and face challenges in key management and improve effectiveness in key management. This work may focus on how you can face new challenges in cloud computing environment.

ACKNOWLEDGEMENTS

1) The work of chintada srinivasarao and Chinta.Chandrasekhar is partially supported by AITAM college TEQIP grants. The work of chintada srinivasararo is partially supported by AITAM management and Department of IT grants.
2) The authors would like to thank Dr Elaine Shi is an Assistant Professor at the University of Maryland, College Park-College Park. She obtained her Ph.D. and Masters degrees in Computer Science from Carnegie Mellon University, and her B.E. from Tsinghua University

REFERENCES

[1] C. Dwork, "The Differential Privacy Frontier Extended Abstract," *Proc. 6th Theory of Cryptography Conf.* (TCC 09), LNCS 5444, Springer, pp. 496-502, 2009

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 3, March 2014

[2] Mell, P. and Grance, T. (September 2011). "The NIST Definition of Cloud Computing. NIST Special Publication 800-145 (September 2011). National Institute of Standards and Technology, U.S. Department of Commerce" Retrieved 2012-05-20.
[3] Krutz, Ronald L., and Russell Dean Vines. "Cloud Computing Security Architecture." Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Indianapolis, IN: Wiley, 179-80. Print., 2010.
[4] Richard Chow, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessica Staddon, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control" PARC Fujitsu Laboratories of America
[5] E. Naone, "The Slow-Motion Internet," *Technology Rev.*, www.technologyreview.com/files/54902/ GoogleSpeed_charts.pdf. Mar./Apr. 2011;
[6] Kartik Sharma, Renuka Sharma, Gitesh Dalal International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013 2348 ISSN 2229-5518 IJSER © http://www.ijser.org "A Secure Protocol for Data storage Security in cloud computing, 2013
[7] C. Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," *Proc. 41st Ann. ACM Symp. Theory Computing* (STOC 09), ACM, pp. 169-178. 2009.
[8] "Security Policy and Key Management: Centrally Manage Encryption Key". Slideshare.net. 2012-08-13. Retrieved 2013-08-06.
[9] E. Bertino, F. Paci, and R. Ferrini, "Privacy-Preserving Digital Identity Management for Cloud Computing," *IEEE Computer Society Data Engineering Bulletin*, Mar. 2009, pp. 1–4.
[10] M. Ko, G.-J. Ahn, and M. Shehab "Privacy-Enhanced User-Centric Identity Management," *Proc. IEEE Int'l Conf. Communications*, IEEE Press, 2009, pp. 998–1002.

BIOGRAPHY

Chintada. Srinivasa Rao is an Assistant professor in the department of Information Technology, Aditya Institute of Technology and Management, Tekkali, India. He received B. Tech degree computer science and Information technology degree from SISTAM (JNTU, Hyderabad, India), and received M. Tech degree in Computer Science & Engineering from NOVA college of engineering (JNTU, Kakinada). His area of interests includes Computer Networks, Network Security and cloud computing, etc.

Chinta. Chandra Sekhar is an Assistant professor in the department of Information Technology, Aditya Institute of Technology and Management, Tekkali, India. He received B.Tech degree in Computer Science and Information technology from SISTAM (JNTU, Hyderabad, India), and received M. Tech degree in Computer Science & Engineering from AITAM (JNTU, Kakinada). His research interests are Computer Networks (Network Security), Cloud Computing, Image Processing, Data Mining, etc.