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. 3, Issue 11, November 2015

Improved Trusted Third Party Auditing in Shared Cloud Environment

B Nagarjuna, G Lakshmi Vara Prasad

M.Tech Student, Dept. of CSE, QIS College of Engineering and Technology, Ongole, Prakasam (Dt), Andhra Pradesh, India

Assistant Professor, Dept. of IT, QIS College of Engineering and Technology, Ongole, Prakasam (Dt), Andhra Pradesh, India

ABSTRACT: The security risks associated with each cloud delivery model vary and are dependent on a wide range of factors including the sensitivity of information assets, cloud architectures and security controls involved in a particular cloud environment. With public audit ability, a trusted entity with expertise and capabilities data owners do not possess can be delegated as an external audit party to assess the risk of outsourced data when needed. Such an auditing service not only helps save data owners' computation resources but also provides a transparent yet cost-effective method for data owners to gain trust in the cloud. All types of users who require the secure transmission or storage of data in any kind of media or network. Since the data transmission on the internet or over any networks are vulnerable to the hackers attack. We present information risk management framework for better understanding critical to support scalable and efficient trusted third party auditing in Cloud Computing. We propose a new model–driven methodology for the security testing of cloud environments, to support batch auditing for TPA upon delegations from multi-user. We also propose new scheme that enables the data owner to delegate tasks of Cloud storage data file encryption and trusted user secret key update to cloud servers without disclosing security data contents or user access privilege information. The trusted third party auditing process will bring in no new vulnerabilities towards user cloud storage data privacy. Our new method combined the secret key based homomorphism authenticator with random masking to achieve the privacy-preserving public cloud data auditing system.

KEYWORDS: Public auditing, shared data, user revocation, cloud computing.

I.INTRODUCTION

With data storage and sharing services (such as Drop box and Google Drive) provided by the cloud, people can easily work together as a group by sharing data with each other. More specifically, once a user creates shared data in the cloud, every user in the group is able to not only access and modify shared data, but also share the latest version of the shared data with the rest of the group. Although cloud providers promise a more secure and reliable environment to the users, the integrity of data in the cloud may still be compromised, due to the existence of hardware/software failures and human errors. To protect the integrity of data in the cloud, a number of mechanisms have been proposed. In these mechanisms, a signature is attached to each block in data, and the integrity of data relies on the correctness of all the signatures. One of the most significant and common features of these mechanisms is to allow a public verifier to efficiently check data integrity in the cloud without downloading the entire data, referred to as public auditing (or denoted as Provable Data Possession. This public verifier could be a client who would like to utilize cloud data for particular purposes(e.g., search, computation, data mining, etc.) or a third party auditor (TPA) who is able to provide verification services on data integrity to users. Most of the previous works focus on auditing the integrity of personal data. Different from these works, several recent works focus on how to preserve identity privacy from public verifiers when auditing the integrity of shared data. Unfortunately, none of the above mechanisms, considers the efficiency of user revocation when auditing the correctness of shared data in the cloud. With shared data, once a user modifies a block, she also needs to compute a new signature for the modified block.

DOI: 10.15680/IJIRCCE.2015. 0311243

Due to the modifications from different users, different blocks are signed by different users. For security reasons, when a user leaves the group or misbehaves, this user must be revoked from the group. As a result, this revoked user should no longer be able to access and modify shared data, and the signatures generated by this revoked user are no longer valid to the group. Therefore, although the content of shared data is not changed during user revocation, the blocks, which were previously signed by the revoked user, still need to be re-signed by an existing user in the group. As a result, the integrity of the entire data can still be verified with the public keys of existing users only.

II.RELATED WORK

Considering the large size of the outsourced data and the user‛s constrained resource capability, the tasks of auditing the data correctness in a cloud environment can be formidable and expensive for the cloud users. Moreover, the overhead of using cloud storage should be minimized as much as possible, such that a user does not need to perform too many operations to use the data (in additional to retrieving the data). In particular, users may not want to go through the complexity in verifying the data integrity [1] [2].

The first problem is establishing trust in remote execution. Essentially, a cloud is a distributed computing architecture in which the client‛s computation runs on a remote host in a data centre. In a cloud system, a customer must gain assurance that the base system executes his or her cloud instance while protecting its integrity and secrecy, tantamount to running on the customer‛s own machine. Compared to other distributed computing architectures, such as grid computing or Web applications, the cloud presents a tangibly higher bar to acceptance. This is especially true for businesses which often have regulatory or commercial incentives for protecting their data and need sufficient assurances that the cloud vendor will manage this data effectively. By comparison, scientific community- run grids might process sensitive data, but are often isolated and not a valuable target.

Data needs to be encrypted and packaged with a usage policy. When accessed, data should consult its policy and attempt to re-create a secure environment using
Virtualization and reveal itself only if the environment is verified as trustworthy (using Trusted Computing). The trusted monitor can provide ―proofs of compliance‖ to the data owner, stating that certain access policies have not been violated. To produce a ―proof of compliance‖, the code of the monitor is signed, as well as a ―statement of compliance‖ produced by the monitor.

Cryptographic primitives such as homomorphism encryption and Private Information Retrieval (PIR) perform computations on encrypted data without decrypting. As these cryptographic techniques mature, they may open up new possibilities for cloud computing security. The provider‛s computing resources are pooled to serve multiple consumers using a multi-tenant model with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

The third party auditor (TPA), who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service security on behalf of the user upon request. Users rely on the CS for cloud data storage and maintenance. They may also dynamically interact with the CS to access and update their stored data for various application purposes [2]. The users may resort to TPA for ensuring the storage security of their outsourced data, while hoping to keep their data private from TPA. We consider the existence of a semi-trusted CS as does. Namely, in most of time it behaves properly and does not deviate from the prescribed protocol execution [8] [9]. However, during providing the cloud data storage based services, for their own benefits the CS might neglect to keep or deliberately delete rarely accessed data files which belong to ordinary cloud users.

III.PROPOSED SYSTEM

The Trusted Computing Group (TCG) provided the trusted computing technology. This distinguishing technology is arguably the incorporation of ―roots of trust‖ into computer platforms. Because one of the biggest issues facing computer technology today is data security, and the problem has gotten worse because users are working with sensitive information more often, while the number of threats is growing and hackers are developing new types of attacks, many technology researchers advocate development of trusted computing systems that integrate data security mechanism into their core operations, rather than implementing it by using add-on applications [10] [22]. In this concept, TC systems would cryptographically seal off the parts of the computer that deal with data and applications and give decryption keys only to programs and information that the technology judges to be trusted.

The TCG made this mechanism as their core criteria to define the technology specification. The word trust is defined as ―A trusted component, operation, or process is one whose behaviour is predictable under almost any operating condition and which is highly resistant to subversion by application software, viruses, and a given level of physical interference.‖ TCP operates through a combination of software and hardware: manufacturers add some new hardware to each computer to support TC functions, and then a special TC operating system mediates.

Within the cloud computing world, the virtual environment lets user's access computing power that exceeds that contained within their physical worlds. To enter this virtual environment requires them to transfer data throughout the cloud. Consequently, several data storage concerns can arise [6]. Typically, users will know neither the exact location of their data nor the other sources of the data collectively stored with theirs. To ensure data confidentiality, integrity, and availability (CIA), the storage provider must offer capabilities that, at a minimum, include a tested Looking at the list of benefits, they actually highlight what we think are the top three concerns organizations have with Cloud computing. It revolves around understanding how:

Software as a Service (SaaS) provides a large amount of integrated features built directly into the offering with the least amount of extensibility and a relatively high level of security. Since the user can only access or modify the data on the pre-defined application the underlying security issues are not of much concern.

Platform As A Service (PaaS) generally offers less integrated features since it is designed to enable developers to build their own applications on top of the platform and is therefore more extensible than SaaS by nature, but due to this balance trades off on security features since user is responsible for program security and security issues. Infrastructure As A Service (IaaS) provides few, if any, application-like features, provides for enormous extensibility but generally less security capabilities and functionality beyond protecting the infrastructure itself since it expects operating systems, applications and content to be managed and secured by the consumer[3]

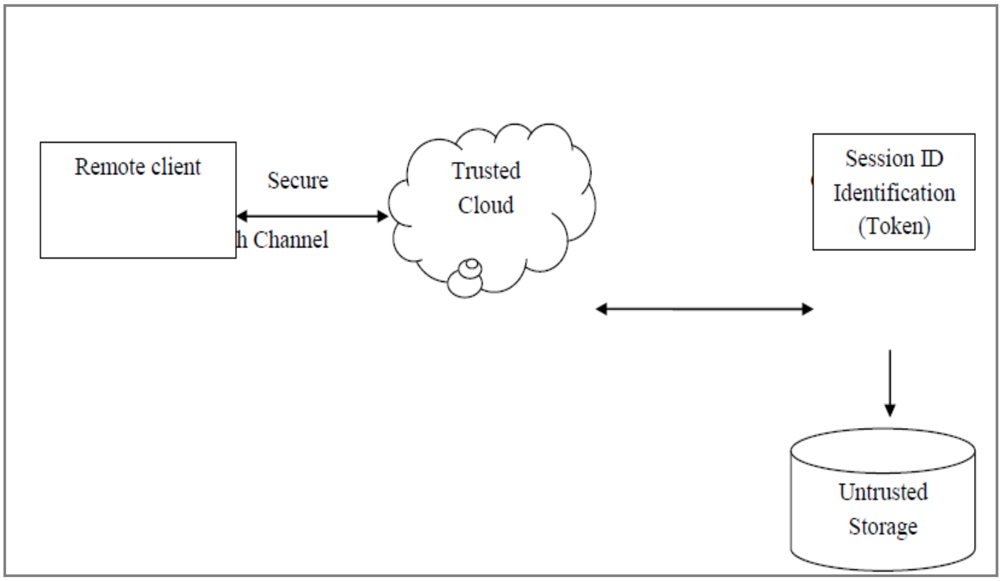

Figure 1-Session based Trusted Cloud Architecture

The function to be computed is first encrypted by an entity, called the constructor, with symmetric cryptography. Then, another party, called the evaluator, decrypts the function using the keys that correspond to the input data. The use of symmetric encryption algorithms endows efficiency in terms of implementation to the garbled circuits. However, this procedure is one-time-pad like [41]. That means that the garbled circuits can be used only once and their size is proportional to the size of the function to be computed. Several hardware implementations have been proposed to accelerate the procedure.

IV.IMPLEMENTATION

As an Operations management organizes a set of related authorizations together, it can simplify the authorization management [13]. Whenever a user needs a certain type of authority to perform an activity, s/he only has to be granted the authority of a proper role, rather than directly assigned the specific authorizations. Furthermore, when she changes her function inside the organization, she needs to revoke the permission function of the role.

Trust Under the cloud computing paradigm, an organization relinquishes direct control over many aspects of security and, in doing so, confers an unprecedented level of trust onto the service provider.

Insider Access Data processed or stored outside the confines of an organization, its firewall, and other security controls bring with it an inherent level of risk. The insider security threat is a well-known issue for most organizations and, despite the name, applies as well to outsourced cloud services. Insider threats go beyond those posed by current or former employees to include organizational affiliates, contractors, and other parties that have received access to an organization‘s networks, systems, and data to carry out or facilitate operations [36]. Incidents may involve various types of fraud, sabotage of information resources, and theft of information. Incidents may also be caused unintentionally. Moving data and applications to an external cloud computing environment expands the insider security risk not only to the service provider‘s staff, but also potentially among other customers using the service.

DOI: 10.15680/IJIRCCE.2015. 0311243

Server-Side Protection Virtual servers and applications, much like their non-virtualized counterparts, need to be secured in IaaS clouds. Following organizational policies and procedures, hardening of the operating system and applications should occur to produce VM images for deployment. Care must also be taken to make adjustments for the virtualized environments in which the images run. For example, virtual firewalls can be used to isolate groups of VMs from other groups hosted, such as production systems from development systems or development systems from other cloud-resident systems. Carefully managing VM images is also important to avoid accidently deploying images containing vulnerabilities.
Client-Side Protection A successful defense against attacks requires both a secure client and a secure Website infrastructure. With emphasis typically placed on the latter, the former can be easily overlooked. Web browsers, a key element for many cloud computing services, and the various available plug-ins and extensions for them are notorious for their security problems. Moreover, many browser add-ons do not provide automatic updates, increasing the persistence of existing vulnerabilities.

Identity Management Data sensitivity and privacy of information have increasingly become a concern for organizations, and unauthorized access to information resources in the cloud is a major issue. One reason is that an organization‘s identification and authentication framework may not naturally extend into the cloud and may require effort to modify the existing framework to support cloud services. The alternative of having two different systems for use authentication, one for internal organizational systems and another for external cloud-based systems is a complication that can become unworkable over time. Identity federation, popularized with the introduction of service oriented architectures, is one solution that can be accomplished in a number of ways, such as with the Security Assertion Markup Language (SAML) standard.

Access Control Besides authentication, the capability to adapt user privileges and maintain control over access to resources is also required, as part of identity management. Standards like the extensible Access Control Markup Language (XACML) can be employed to control access to cloud resources, instead of using a service provider‘s proprietary interface. XACML focuses on the mechanism for arriving at authorization decisions, which complements SAML‘s focus on the means for transferring authentication and authorization decisions between cooperating entities.

Development and maintenance support. Because they face a long list of challenges—bugs to find and fix, frequent software upgrades, continuous usage pattern changes, and user demand for high performance developers will receive both development and maintenance support. As shown in figure

In some cases, applications need to call outside services or APIs provided by third-party websites for example, the Google Maps API. An application might need to export user’s data to outside services in this process. Access controls, authorization, and auditing capability are common challenges for application developers. Incorporating these features within the platform is a significant improvement in terms of ease of use, and it doesn‘t constrain the types of computation that can be performed within the secure cloud.

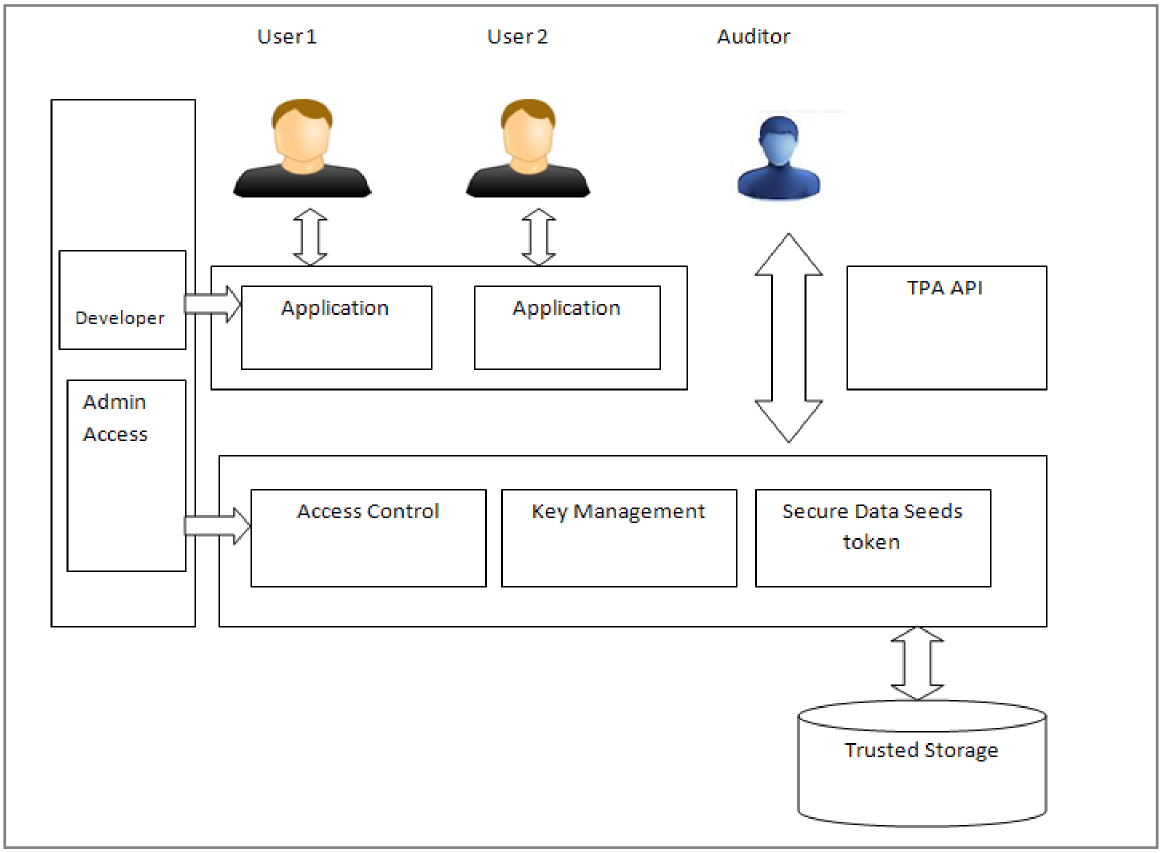

Figure 2-Proposed Architecture of Cloud Data Protection

Data can take many forms. For example, for cloud-based application development, it includes the application programs, scripts, and configuration settings, along with the development tools. For deployed applications, it includes records and other content created or used by the applications, as well as account information about the users of the applications. Access controls are one means to keep data away from unauthorised users; encryption is another.

V.PSEUDO CODE

```
1. Choose a and b: two distinct prime numbers.
2. Compute $m = a b$, Where m is used as the modulus for public and private keys.
3. Compute $\Phi (m) = (a-1) (b-1)$, Where $\Phi$ is function.
4. Choose an integer E such that, $1 < E < \Phi (m)$ and common divisor of $(E, \Phi (m)) = 1$.
5. Determine $D = 1/E \bmod \Phi (m)$.
6. All the above values of public key and private key must be kept secret.
```

Encryption Algorithm:

1. Sender A transmits her public key (m, E) to recipient B for the process of encryption data.
2. Represent the plaintext msg as a positive integer n.
3. Computes the cipher c = nE (mod m).
4. Sends the cipher text c to recipient B.

VI.SIMULATION RESULTS

As we store the data in encrypted form on cloud, and keep the keys and the algorithm itself, unknown from Cloud server, it is next to impossible for the server to either learn the data or to misuse them. **Security options** As all the data to be stored on Cloud may not be highly sensitive; we take inputs from the data owner himself, and accordingly select cryptographic algorithms for him. **Lightweight Verification** For integrity verification, cloud user/requestor can send request (in form of challenge) to cloud server for computing and submitting hash code of his encrypted file. Upon checking some validations, cloud server computes a hash code of the file and returns the same to the requestor (in form of response). The size of this code is very small (in terms of few bytes) which reduces communication overhead. Also note that, computing the hash code is an offline function at cloud server side. In this way, we save computation plus communication time, hence improve performance. **Key Management** We have used the hybrid approach of using a combination of symmetric and asymmetric key encryption. Data encryption is done in a symmetric way and the key used for it is transferred to the data requester in an asymmetric way. Hence, utilizing secure approach for data encryption and fast operation for key transfer is adopted. **Access Rights** Access rights can be granted from data owner to data requester with the help of small SQL grant operations. In case of revoking a grant, again the same kind of SQL revoke statement can be used. Important, thing here to mention is, in case of granting operation, data owner may be talking to data requester, but in case of revoking the rights, it will issue instructions directly to Cloud server, of course through SQL statement. Hence, it is quite a simple operation.

Error localization is a key prerequisite for eliminating errors in storage systems. However, many previous schemes do not explicitly consider the problem of data error localization, thus only provide binary results for the storage verification. Our scheme outperforms those by integrating the correctness verification and error localization in our challenge-response protocol: the response values from servers for each challenge not only determine the correctness of the distributed storage, but also contain information to locate potential data error(s).

In the first stage, the data owner determines the minimal set of attributes, redefines MK and PK for involved attributes, and generates the corresponding PRE keys. The user‘s ID, the minimal attribute set, the PRE keys, the updated public key components, along with his signatures on these components to Cloud Servers, and can go off-line again. In this research can adopt a system-driven policy framework to facilitate the management of security policies in heterogeneous environments and policy enforcement architecture.

Users can use remote attestation to get a report on the software stack that was executed on the platform. This report is a list of Platform Configuration Registers (PCRs) configuration values signed and certified by TPM. **Fig-3**

DOI: 10.15680/IJIRCCE.2015. 0311243

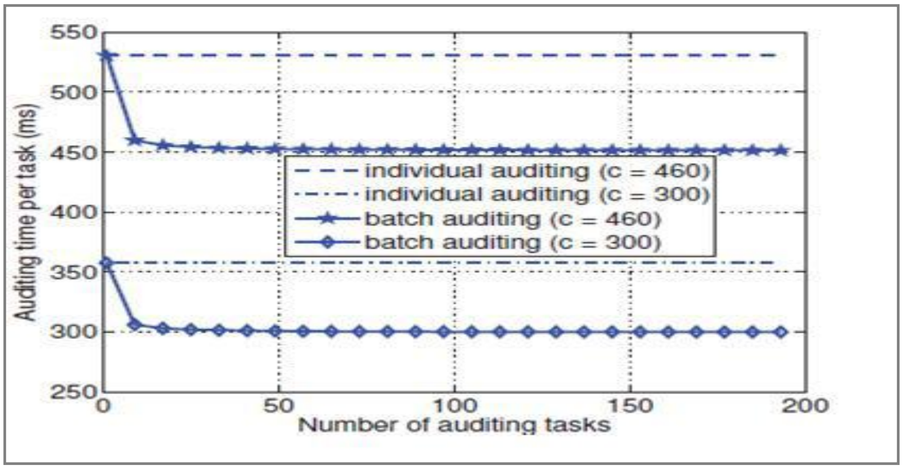

Figure 3-Performance Comparison of Batch Auditing

The SLA based information security metrics identified in this research are generic. The metrics are intended for all cloud computing services and deployment models. Because of time constraint, it is not possible for us to study the metrics to be applicable specifically for each cloud computing type of service and deployment model. We construct a secure and robust virtualization platform. Based on this platform, we divide the whole system into three parts: trusted part, un-trusted part, protected part.

VII.CONCLUSION AND FUTURE WORK

Finally, we addressed an important issue of secure data sharing on cloud storage. We investigated the challenges pertained to this problem and proposed to exploit a novel PKC Cloud Storage Attribute-Based Encryption to provide cryptographically enforced data access control. We addressed the threat by establishing universality criteria in which we intended to verify whether the frameworks found in the literature could be applicable in all industries in every part of the world. Toward providing a full-fledged cryptographic basis for secure data sharing on cloud storage, we proposed three security enhancing solutions for Attribute-Based Encryption: The first enhancement we made is to provide efficient user revocation in Attribute-Based Encryption. In this research finally developed and allows the users to establish information risk management framework. In this research also designed and implemented algorithms for bottleneck detection in multi tier Web applications hosted on a cloud. We have presented a comprehensive security framework for cloud computing environments. We have described its components, discussed existing solutions and identified possible approaches to deal with different security issues related to the cloud. The energy consumed in transporting data between users and the cloud is therefore an important consideration when designing an energy efficient cloud storage security service. To developed the dynamic Trusted Third Party auditing key role of public audit ability in the cloud storage security API. We evaluate our system confidentiality in the following aspects: hardware platform, memory isolation, storage, network, guest VM boot process, virtual devices. The evaluation shows that our architecture provides a good solution to protect the confidentiality of the cloud clients.

REFERENCES

1. C. Wang et al., ―Privacy-Preserving Public Auditing for Storage Security in Cloud Computing,‖ Proc. IEEE INFOCOM ‗10, Mar. 2010
2. P. Mell and T. Grance, ―Draft NIST Working Definition of Cloud Computing,‖ 2009; http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

3. M. Armbrust et al., ―Above the Clouds: A Berkeley View of Cloud Computing,‖ Univ. California, Berkeley, Tech. Rep. UCBEECS-2009-28, Feb. 2009.
4. Amazon.com, ―Amazon s3 Availability Event: July 20, 2008,‖ July 2008; http://status.aws.amazon.com/s3-20080720.html
5. M. Arrington, ―Gmail Disaster: Reports of Mass Email Deletions,‖ Dec. 2006;
6. T. Ristenpart et al., ―Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds,‖ Proc. 16th ACM Conf. Computer and Communications Security, ACM Press, 2009, pp. 199–212.
7. G. Klein et al., ―seL4: Formal Verification of an OS Kernel,‖ Proc. ACM SIGOPS 22nd Symp. Operating Systems Principles (SOSP 09), ACM Press, 2009, pp. 207–220.
8. Joseph, Randy Katz, Above the Clouds: A Berkeley View of Cloud Computing, University of California Electrical Engineering & Computer Science, February 10th, 2009.
9. Patel, Chandrakant D., Shah, Amip J., ―Cost Model for Planning, Development, and Operation of a Data Center,‖ Internet Systems and Storage Laboratory, HP Laboratories, Palo Alto, June 9, 2005

BIOGRAPHY

Mr. B. Nagarjuna Pursuing His M. Tech (CSE) from QIS College of Engineering and Technology, Prakasam(Dt), Andhra Pradesh. His areas of interest are Cloud Computing, Security and Data Mining.

Mr. G.Lakshmi Vara Prasad , working as an Assistant Professor, Department of IT, QIS College of Engineering and Technology, Prakasam(Dt), Andhra Pradesh. His areas of interest are Cloud Computing, Network Security and Data Mining.