IPHV7I10006X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

An Efficient Scheme To Cover The Testimony Over The Area Of Multitude

[1]N.Indiravathi,
Dept of CST
GITAM University, Hyderabad

[2]G.Rathnamma
Asst. Prof, Dept of CSE
Madanapalli Institute of Technology & Sciences, Anantapur

Abstract:-Cloud computing represents a huge change in the way a business functions, and that's especially true for an organization's IT infrastructure. Nobody is affected more by this transition than the network administrators tasked with keeping an organization's data and network users safe. Every individual has the right to control his or her own data, whether private, public or professional.

Data that a user chooses to store in the cloud may not require protection if it is not sensitive or if it can easily be recovered. But generally, protecting data is a universal requirement regardless of its value, if for no other reason than failing to do so leads to all manner of complexity, consequence, and mischief. In identifying and categorizing data, what we face is a multifaceted problem. Besides identifying classes of information that are sensitive or otherwise have value and labeling such information according to its characteristics, we need to protect such data, usually by means such as file permissions, encryption, or more sophisticated container approaches. We also need identity-based access controls to support organizational access policies. We explore a new cloud platform architecture called Data Protection as a Service, which dramatically reduces the per-application development effort required to offer data protection, while still allowing rapid development and maintenance. In addition to this, we suggest a network audit to see how your network defenses match up to your own data security, integrity and availability policies, regulatory requirements and industry best practices. The benefits of such an audit are many. Once these have been remedied with better security controls and revised procedures, establish an acceptable baseline for the network, the devices, users and applications it hosts and the traffic it handles. This baseline can be referenced during future audits and security configuration checks to determine how the security of the network is affected with the move to cloud computing. Finally, in the event of a security breach, it is also important to be informed about the contractual remedies available to your organization. Assessing the limitation of liability clause in the provider agreement is important to understanding your organization's rights in the event of a breach. Furthermore, organizations should consider the ability to terminate the agreement with a Cloud Provider in the event of security breach.

General Terms- Data protection, network traffic

Keywords- *Data security, integrity, availability policy*

I.INTRODUCTION

The concept of cloud computing is globalised, and within the cloud there are no borders. Computers that are used for processing and storage of user data and ICT information and communication technology)network infrastructure can be located anywhere on the globe, just depending on where the requisite capacities are available for execution of the ICT tasks in accordance with optimization-oriented resource management in the global

computer networks used for cloud computing. Some cloud service providers such as, for example, Amazon, offer their customers the option of choosing between certain availability zones. The customer's data then remains within the selected zone. Regarding data protection, cloud computing raises a number of interesting issues. Data protection law is based on the premise that it is always clear where personal data is located, by whom it is processed and who is responsible for data processing. Cloud computing appears to fundamentally conflict with this evidence. For example, if a customer uses an e-mail service based on cloud computing, the customer's data can be stored anywhere in the world, depending on where the servers on which the necessary storage capacity is available are located. Different services supplied by a wide range of providers are regularly bundled to produce an end-user proposal, for example, if the mail service provider obtains the storage capacity required to store its customers' data from other providers. Therefore, with cloud computing it is no longer possible to say where the data is at a certain moment and by whom and how it is being processed. This means that it is doubtful whether those responsible for data processing, in accordance with data-protection regulations, are in a position to effectively assume their responsibility at all.
If the data circulates freely around the globe via the internet, it is also no longer clear which data-protection authorities at which location are responsible for ensuring the observance of the principles of data protection. If a provider in country "A" stores large volumes of personal data that relate to customers of companies that use the CRM solution of a provider with its headquarters in country "B", it is therefore not immediately certain which authorities in which country (country "A", country "B" or the countries where the companies using the CRM solution or their customers are domiciled, or both) are responsible or should appropriately be responsible for observance of data protection involving the storage of data.

Network Auditing:

By now, everyone has heard that cloud computing is changing the world, and there is no question that it will. However, as with any new technology model or innovation, there are many bumps and detours along the way. The channel customers have spoken and, far and away, the number one reason they consistently hold back on cloud service deployment is their perception that the cloud is insecure. Fortunately, as a channel partner, you have direct insight and knowledge of both cloud technologies and the specific needs of your customers, so you are in a unique position to offer valuable cloud consulting services. This powerful combination puts the channel partner in the perfect spot to guide clients through the seemingly impenetrable thicket of cloud services, while avoiding potential security potholes along the way.

In this tip, we'll pinpoint common challenges and best practices that will help you simplify cloud computing security audit procedures. Ultimately, as a trusted advisor, your goal is to identify and articulate to your customers their cloud security challenges and provide solutions that both save your customers' money, and build stronger client relations.

The top cloud security challenges for businesses can be categorized into five broad areas:

Business: A lack of integration between cloud vendors, limited data portability and vendor lock-in (isn't that what the cloud is supposed to avoid?!) is giving business executives and IT departments heartburn. Deciding what data must stay in-house and what data can migrate to the cloud can be complex and fraught with hidden gotchas. As a trusted advisor, you can guide your customer through the audit process, pointing out potential problems and solutions. Look for systems that are already touching outside customers and networks -- a customer service system or Web portal is a good example of a natural cloud migration.

Financial: Companies need to determine if it makes more financial sense to purchase cloud services or build customized systems in house. Often companies underestimate the risks and cost of data loss, or the cost of mitigating and preventing the occurrence in the first place. With your knowledge of the real business cost of data loss, you can educate your clients about their level of exposure.

Legal: Companies need to determine the level of archiving and protection they need to provide for potential legal actions and e-discovery requests. In this day and age, it is not enough to say that the files are no longer accessible; companies can and will be held liable for the data recovery. As a channel partner, you can provide services, like information lifecycle management (ILM) or data privacy audits to ensure your clients are fully protected in the cloud.

Regulatory: HIPAA, state data protection laws, SOX and a myriad of other regulations affect your clients differently depending on their business and industry sector. Regulations are rapidly catching up with cloud technology, so understanding the often complex and sometimes contradictory regulatory environments are valuable skills to help your clients navigate the traitorous waters of using cloud services in a regulated industry. This is particularly true for PCI DSS and banking regulatory compliance.

Technical: Cloud vendors are not always forthcoming about the details of their services, particularly related to how customer data is authenticated, secured and protected. Understanding the technology behind cloud services is often a mystery to even the most sophisticated customer. As a channel partner who really does know cloud architectures, your guidance is invaluable for clients who need to protect their data no matter where it is located. Each of these areas represents unique issues that must be addressed properly to ensure a cloud deployment project is successful. As with anything, half the battle is knowing what to look for when reviewing a potential channel opportunity with your client. To help with the audit process, here is a quick checklist to get you started. Not only will the answers to these questions help determine the appropriate cloud security offerings, but they will also deepen the client's understanding of their own business and how IT and the cloud might enable (or not enable) efficient process flows to meet their business objectives.

Cloud security audit best practices checklist:

***Perform a data flow and privacy assessment*:** Look at where the client's data is and how it flows through the organization. Is it vulnerable at any point? Is it all internal, or is some data already out on the cloud?

***Probe customer data for its suitability for the cloud*:** Rank the data into three pools: belongs on the cloud, does not belong on the cloud, and might belong on the cloud. For example, your corporate financial statements probably do not belong on the cloud, while your customer service systems and archives (as long as they are proper encrypted) do.

Evaluate the client's application portfolio: Evaluate the portfolio from both the business and data security perspectives. Which applications are available on the cloud and which ones are likely to be available in the future? Can some of the specialized applications currently in use be migrated to the cloud relatively easily or will they require extensive configuration and modification to business processes?

Audit the existing IT infrastructure, servers and networks: Look for potential cloud migration opportunities. Help your client understand what systems will benefit from moving to the cloud and which ones will not. Some good targets for cloud migration would be a client's email system or CRM system. Both of these systems are not only essential, but there are quite a few relatively mature cloud options available to choose from.

Review cloud vendor contracts: Watch for potential service-level discrepancies and make sure your customer understands the relative responsibilities of each party.

Help your customer develop a contingency plan: If a cloud vendor relationship does not work out, do not forget to include data extraction and portability as a key design goal to minimize vendor lock-in.

Four steps in a cloud computing audit
Rapid advances in cloud services have generated many on-demand and scalable benefits. At the same time, however, cloud computing has significant and unprecedented risks related to the security of information as well as a loss of control over the IT infrastructure.Security solution providers, in their role as auditors, can provide an independent audit of a CSP's policies, procedures, security measures and practices for safeguarding electronic information against unauthorized disclosure, alteration or denial of availability. They can evaluate the cloud service provider's security and offer recommendations for reducing security risks to an acceptable level.

Auditing a CSP involves the following steps:

Plan and prepare – become familiar with the CSP and its products and services.

- Establish audit objectives – determine the audit scope (will it be a general security audit, or will it include auditing for compliance with certain industry regulations?), review audit areas and desired deliverables.
- Perform the audit – evaluate the CSP's security controls against standards, guidelines and frameworks, and collect evidence to support findings and audit objectives.
- Create the audit report – summarize findings, prioritize risks and deliver the report.

II. CLOUD COMPUTING AUDIT: STANDARDS, FRAMEWORKS AND GUIDELINES

The solution provider's proposal to audit a CSP should include references to appropriate standards, audit frameworks and guidelines that will provide a systematic approach to securing and assessing systems and services during the audit.

Some of the standards, frameworks and guidelines that auditors use in security audits include:

- ISO 27001/27002 standards
- Control Objectives for Information and Technology (COBIT) framework
- ISACA's IT Assurance Framework (ITAF)
- IT Audit and Assurance Guidelines
- SysTrust and WebTrust frameworks

Depending upon the services provided by the CSP, the security solution provider should also look to the Cloud Security Alliance (CSA) for guidelines on cloud computing security and security assurance. Examples of CSA's resources include:

- For compliance audits, the security solutions provider may need to evaluate the CSP against regulatory requirements such as the Payment Card Industry Data Security Standard (PCI DSS), Health Information Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX) and others.

- Deciding which standards, frameworks and guidelines to use in the audit is an important decision in the auditor's job. Most of the time, the auditor can look at the customer's industry, check with special interest groups to see what others are doing, and work with the customer to establish the benchmark that will be used for the audit. Or the auditor may use their past experience and knowledge, as well as their own judgment to choose whatever standards, frameworks or guidelines are relevant to the audit's scope.

- **The cloud computing audit process** During the audit, the CSP's systems, people and processes are compared with the appropriate standards, frameworks, guidelines and compliance requirements. Deviations are "gaps" or risk areas that require additional analysis.

- Once the evaluation and analysis are complete, an audit report is compiled, identifying the services performed, audit findings and recommendations for the customer. Findings are prioritized according to the likelihood of the event and the impact on the CSP and its customers, stakeholders, etc.

- Each audit engagement is unique, and it is important that the security solutions provider's services are aligned to meet the engagement's audit objectives. Security solution providers that allocate resources to closely monitor security standards, frameworks and guidelines will have a more complete service offering and a competitive advantage over other firms.

III. AUDIT CONSIDERATIONS

Auditors need to be involved with their organization's cloud computing plans right from the idea conception stage to help ensure identification and mitigation of risks. A number of aspects should be considered by auditors when reviewing a cloud computing project: Criticality of the application being sent to the cloud. While it is less risky to start with, sending noncritical applications to the cloud (for example, budgeting and expense tracking tools), significant applications such as a business-to-business (B2B) or business-to-consumer (B2C) web site should be moved to the cloud only after careful consideration. Country/regional regulations that affect the organization's business and require specific safeguards. Industry regulations such as the Gramm-Leach-Bliley Act (GLBA) in the US require safeguards to protect a client's nonpublic personal information, depending on how the organization collects, stores and uses the information. Under the US model of privacy, consumers have the choice to opt out of the information being shared with affiliated parties; in the European Union, Canada and some other countries, privacy laws are stringent and require specific opt-in by consumers. Auditors examining the cloud vendor's policy on vulnerability management and reporting (beyond basic "contact us" web site links), commitment to following up on potential security incidents, and ability to respond promptly to reports

Cloud users' experience with service level agreements (SLAs) and vendor management

Auditors gaining independent assurance about controls at the cloud service provider—whether through an independent auditor's report or through audit rights in the agreement. The independent auditor's report could be a Statement on Auditing Standards (SAS) No. 70 or Trust Services report, depending on the type of application and processes outsourced. See **figure 2**for details of the key differences.

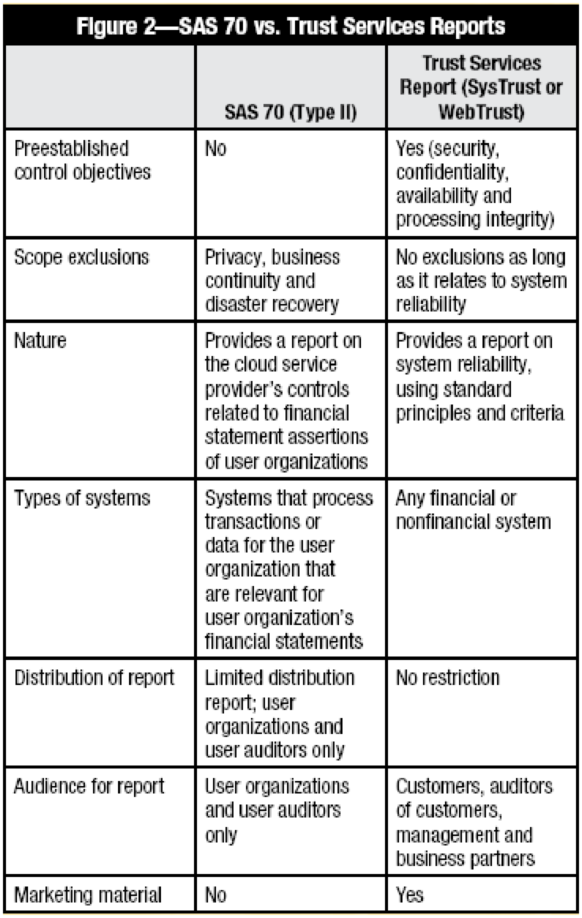

Figure 2—SAS 70 vs. Trust Services Reports

	SAS 70 (Type II)	Trust Services Report (SysTrust or WebTrust)
Preestablished control objectives	No	Yes (security, confidentiality, availability and processing integrity)
Scope exclusions	Privacy, business continuity and disaster recovery	No exclusions as long as it relates to system reliability
Nature	Provides a report on the cloud service provider's controls related to financial statement assertions of user organizations	Provides a report on system reliability, using standard principles and criteria
Types of systems	Systems that process transactions or data for the user organization that are relevant for user organization's financial statements	Any financial or nonfinancial system
Distribution of report	Limited distribution report; user organizations and user auditors only	No restriction
Audience for report	User organizations and user auditors only	Customers, auditors of customers, management and business partners
Marketing material	No	Yes

Components of Cloud Computing

Much has been written about cloud computing, SaaS and data centers, but often those technologies are melded as a composite service referred to as cloud computing. Actually, there is a simple framework for thinking about cloud computing that should help IT auditors in performing a risk assessment. The components are Infrastructure as a Service (IaaS) and Software as a Service (SaaS)—almost identical to the way we think of the body of technologies internal to an entity.

Cloud Computing: IaaS

Services of IaaS components replace or supplement the internal infrastructure. The key decision factors for management in deciding to move to IaaS (outsourcing part of its infrastructure) and choosing the appropriate vendor are usually efficiency-related. For instance, it takes one full-time employee (FTE) “blank amount of time” per year to manage about 70 servers. If the entity has a server farm, it can outsource those costs to an effective data center and reduce costs significantly. In addition, when the entity needs to upgrade its software, or acquire a new software application, the consideration of infrastructure is probably an insignificant consideration regarding cost, assuming the choice in IaaS provider was sufficiently sophisticated, and requires little to no changes to its own infrastructure. There is also the accounting consideration. Usually, infrastructure costs are substantial and, according to the Generally Accepted Accounting Principles (GAAP), are treated as a capital expense (CAPEX). However, if the infrastructure is outsourced, the expense associated with the IaaS infrastructure usually becomes an operating expense (OPEX). In the US, this leads to a tax advantage regarding income taxes. Thus, some of the key factors for management when choosing the IaaS provider are flexible performance (including scalability) and availability while achieving physical and virtual security needs.

There are various ways to break down IaaS, but here is one way:

- Connectivity
- Network services and management
- Compute services and management
- Data storage
- Security

Connectivity obviously refers to reliable access to the Internet and connectivity to associated systems and technologies, for instance, data storage to application servers. Examples of risks would be availability/downtime and speed of access.[4] The average entity experiences one day per annum of downtime. Network services and management includes not only providing network capabilities, but managing the network, monitoring the network and providing for efficient access through aspects such as load balancing. Examples of these risks are scalability for new technologies or expanding the level of transactions, availability, secured transmissions, and the level of access (e.g., load balancing). Compute services and management include appropriate resources such as core, processors, memory and managing the operating system (OS). Examples of the risks are availability (including system failure) and scalability. There has been significant growth in data centers over the last few years, and data centers are becoming more sophisticated in the scope of services. Examples of the risks for data storage include the obvious: security of data, recovery, availability and scalability. The security and recovery issues are particularly important. Management should ensure that the data storage aspect of IaaS can provide an appropriate level of physical and logical security and an appropriate recovery methodology to ensure a timely recovery if the data center is involved in a disaster.

Security issues are more or less ubiquitous for IaaS and include physical security, especially data storage, and logical security. They include security from unauthorized access by malicious intruders and rogue employees of the IaaS provider. In fact, the latter is an increased risk to the user entity that needs to be addressed via adequate controls by the service entity. Risks are always determined within contextual circumstances to the entity—for example, the industry, its own business processes, the current economy and other circumstances peculiar to the entity at that time. Some of the other issues that may be risks are ownership, insurance, project management and performance reporting.

Mitigating controls could be discoverable from a SAS 70 Type II audit report. If one exists for the IaaS provider, the IT auditor should certainly read it to see what level of assurance can be gained for the specific, identified risks. Controls the provider should be employing include best practices in security, support (e.g., IT Infrastructure Library [ITIL] v3) and business recovery.

Cloud Computing: SaaS

Some of the key points in deciding to use SaaS, or a particular vendor, are the complexity of the environment, the need to buy smaller pieces/modules, compatibility with existing systems and IT (including programming platform), ease of purchase, ease of integration, project management, scalable infrastructure, and billing/costs (metering).

There are various ways to break down SaaS, but here is one framework:

- Business process modeling
- Evaluation and analysis
- Process execution

Business process modeling involves the need to fit together workflow/business process structure, applications and data, organizational structure, and the integration of existing systems. Evaluation and analysis includes process cost accounting, balanced scorecards, service level agreements (SLA), process warehouse and optimization. Process execution includes workflow control, applications integration (enterprise application integration [EAI]), service orchestration (service-oriented architecture [SOA]), populating databases/conversion and business activity monitoring. Other issues include document and content management, collaboration, systems management and administration, and various aspects of management of SaaS.

Examples of risks would be related to these areas. Some examples include an improper fit of the business process to the application, inadequate connectivity between applications and data, improper integration with existing systems, and inadequate monitoring of SaaS business processes and events. Obviously, the SLA is a key audit objective. There is also a risk of cost control and estimates; that is, it is possible that the move could end up costing the entity more rather than less. One example of cost control is the metering/billing aspect of SaaS, which presents an area of potential risk.

IV. IT ASSURANCE FRAMEWORK

ISACA's IT Assurance Framework™ (ITAF™) includes a section (3630.6) on outsourcing and third-party activities (see **figure 1**). Cross-references are included—COBIT® PO4, PO7, PO8, PO9, AI2 and AI5, and ISACA IT Audit and Assurance Guidelines (formerly IS Audit Guidelines) G4, G18, G32 and G37. These referenced documents provide useful technical assistance in conducting an IT audit for cloud computing.

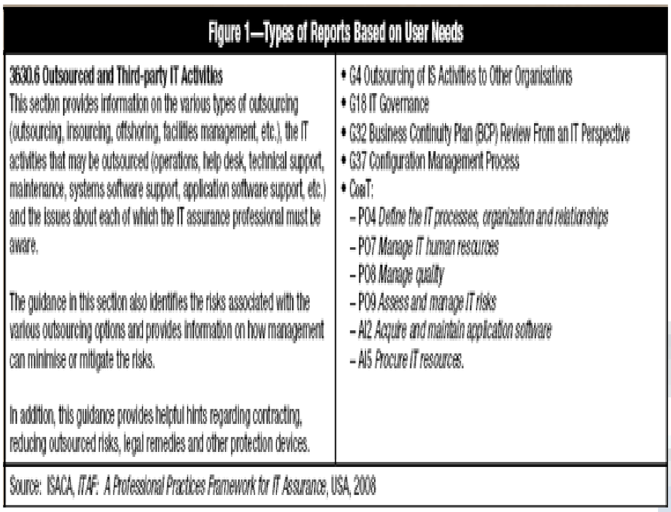

Figure 1—Types of Reports Based on User Needs

3630.6 Outsourced and Third-party IT Activities This section provides information on the various types of outsourcing (outsourcing, insourcing, offshoring, facilities management, etc.), the IT activities that may be outsourced (operations, help desk, technical support, maintenance, systems software support, application software support, etc.) and the issues about each of which the IT assurance professional must be aware. The guidance in this section also identifies the risks associated with the various outsourcing options and provides information on how management can minimise or mitigate the risks. In addition, this guidance provides helpful hints regarding contracting, reducing outsourced risks, legal remedies and other protection devices.	• G4 Outsourcing of IS Activities to Other Organisations • G18 IT Governance • G32 Business Continuity Plan (BCP) Review From an IT Perspective • G37 Configuration Management Process • CobiT: – PO4 *Define the IT processes, organization and relationships* – PO7 *Manage IT human resources* – PO8 *Manage quality* – PO9 *Assess and manage IT risks* – AI2 *Acquire and maintain application software* – AI5 *Procure IT resources.*

Source: ISACA, *ITAF: A Professional Practices Framework for IT Assurance*, USA, 2008

Obviously, the fact that a third party is involved means direct auditing of the service entity may not be practical or even possible. ITAF also supplies a list of potential documents that could provide service audit information that should be relevant (see **figure 2**)

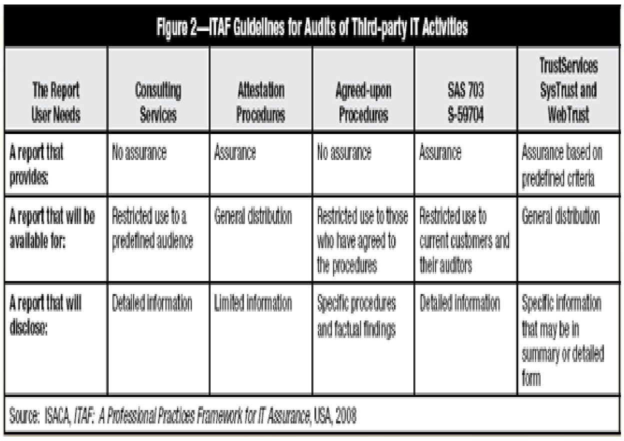

Figure 2—ITAF Guidelines for Audits of Third-party IT Activities

The Report User Needs	Consulting Services	Attestation Procedures	Agreed-upon Procedures	SAS 703 S-59704	TrustServices SysTrust and WebTrust
A report that provides:	No assurance	Assurance	No assurance	Assurance	Assurance based on predefined criteria
A report that will be available for:	Restricted use to a predefined audience	General distribution	Restricted use to those who have agreed to the procedures	Restricted use to current customers and their auditors	General distribution
A report that will disclose:	Detailed information	Limited information	Specific procedures and factual findings	Detailed information	Specific information that may be in summary or detailed form

Source: ISACA, *ITAF: A Professional Practices Framework for IT Assurance*, USA, 2008

V.CONCLUSION

In order to store personal data in to clouds we should provide protection, generally we can provide security though daas layer, but it doesn't control data flow in networks, so that we need to use network audit, Besides identifying classes of information that are sensitive or otherwise have value and labeling such information according to its characteristics, we need to protect such data, usually by means such as file permissions, encryption, or more sophisticated container approaches. We also need identity-based access controls to support organizational access policies. We explore a new cloud platform architecture called Data Protection as a Service, which dramatically reduces the per-application development effort required to offer data protection, while still allowing rapid development and maintenance. In addition to this, we suggest a network audit to see how your network defenses match up to your own data security, integrity and availability policies, regulatory requirements and industry best practices. it is used to see how network defenses match up to your own data security and control flow of data respective of multiple keys for identify cloud users in network.

REFERENCES

1. http://www.mydatacontrol.com.
2.The need for speed. http://www.technologyreview.com/files/54902/GoogleSpeedcharts.pdf.
3. C. Dwork. The differential privacy frontier. In TCC, 2009.
4.A. Greenberg, "IBM's Blindfolded Calculator," Forbes, 13 July 2009; www.forbes.com/forbes/2009/0713/breakthroughs-privacy-super-secret-encryption.html.

5. P. Maniatis et al., "Do You Know Where Your Data Are? Secure Data Capsules for Deployable Data Protection," Proc. 13th Usenix Conf. Hot Topics in Operating Systems (HotOS 11), Usenix, 2011; www.usenix.org/events/hotos11/tech/final_files/ManiatisAkhawe.pdf.

6. S. McCamant and M.D. Ernst, "Quantitative Information Flow as Network Flow Capacity," Proc. 2008 ACM SIGPLAN Conf. Programming Language Design and Implementation (PLDI 08), ACM, 2008, pp. 193-205.

7.M.S. Miller, "Robust Composition: Towards a Unified Approach to Access Control and Concurrency Control," PhD
dissertation, Dept. of Philosophy, Johns Hopkins Univ., 2006.

8. A. Sabelfeld and A.C. Myers, "Language-Based Information- Flow Security," IEEE J. Selected Areas Comm. , Jan. 2003, pp. 5 -19.

9. A. Sabelfeld and A. C. Myers. Language-Based Information-Flow Security. IEEE Journal on Selected Areas in Communications, 21(1):5–19, 2003.

10. L. Whitney. Microsoft Urges Laws to Boost Trust in the Cloud. http://news.cnet.com/8301-1009 3-10437844-83.html.

AUTHOR’S PROFILE:

1.N.Indiravathi working as an software Enginner in Sutherland global solutions pursuing her Master of Technology(compter science and Technology) from GITAM UNIVERSITY, Rudraram. Her Research area includes Cloud
Computing.

2. G.Rathnamma had received her Master of technology(computer science and engineering) from MADANAPALLI INSTITUTE OF TECHNOLOGY AND SCIENCES, Anantapur, affiliated to JNTU. Currently working at Gandhi institute of technology and management, hyderabad, A.P, as an Assistant Professor in department of CSE. Her research area includes cloud computing and distributed operating systems