ISSN No. 0976-5697

Volume 4, No. 11, Nov-Dec 2013

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Survey on Cloud Computing Security Policies and Privacy Concerns for Information Security

Paresh D.Sharma
Research scholar,
Patel College of Science and Technology, Bhopal, India
paresh7sharma@gmail.com

Prof. Hitesh Gupta
Head of Department (Software system)
Patel College of Science and Technology, Bhopal, India
hitesh034@gmail.com

Abstract- This paper describes a study on the existing methods and techniques for the cloud computing. Cloud computing is a style of computing in which dynamically scalable and often virtualized resources are provided 'As a service' over the Internet. Cloud computing provides on demand and at scale services for network infrastructure, platforms, and applications based on an off premise, pay-as-you-go operational model. Files and other data can be stored in the cloud and be accessed from any Internet connection. But some security or privacy issues should be taken into account while using this services such as private information disclosure problem while data being shared within the cloud, unauthorized access to personal data, Unauthorized secondary storage, Uncontrolled data propagation etc. various service providers use Identity Management to solve privacy problems but it's not sufficient. In this paper, a survey on the security policies, trust & privacy issues are studied & based on that the proposed system created. For providing the security to the network and data different encryption methods are used. So, the proposed approach can be used by the service providers in order to get a secured cloud computing environment.

Keywords- Cloud computing; Trust; Security; Privacy;

I. INTRODUCTION

Cloud computing refers to the processing and storage of data through the Internet. Computing and storage become 'services' rather than physical resources. The common characteristics most share are on-demand scalability of highly available and reliable pooled computing resources, secure access to metered services from nearly anywhere, and dislocation of data from inside to outside the organization. While aspects of these characteristics have been realized to a certain extent, cloud computing has become one of the most significant information security issues in recent years. To utilize the benefits of cloud safely sufficient assurance of information and network security such as confidentiality, authentication, non repudiation, and integrity is the most critical factor for adoption. Since cloud computing uses distributed resources in open environment, thus it is important to provide the security and trustworthiness for sharing the information over the cloud. Cloud computing raises a range of important issues, which include issues of privacy, security, anonymity, telecommunications capacity, overnment surveillance, reliability, and liability, among others [1].

The three cloud delivery models are as follows: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The Cloud Computing model has three service delivery models and main three deployment models as shown in Fig. 1 models are:

- ***a. Private cloud****:* a cloud platform is dedicated for specific organization,
- ***b. Public cloud*** available to public users to register and use the available infrastructure, and
- ***c. Hybrid cloud****:* a private cloud that can extend to use resources in public clouds.

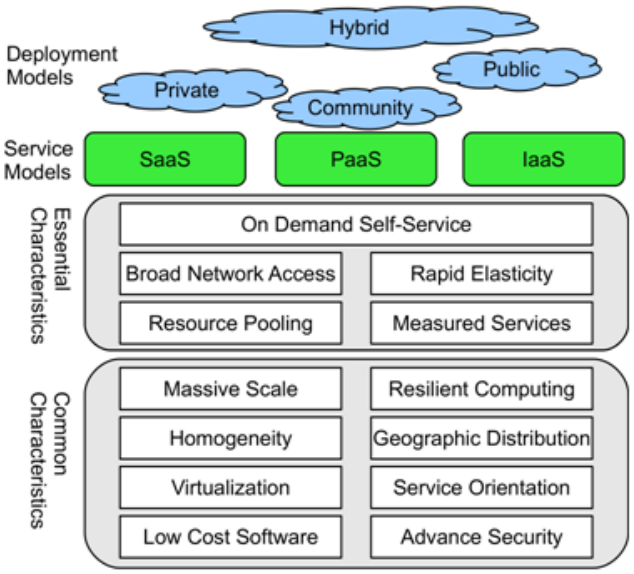


Figure: 1 Cloud Computing Definition

Issues such as trusting the virtual machine images, hardening hosts, and securing inter- host communication are critical areas in IaaS. PaaS enables the programming environment to access and utilize additional application building blocks. Such a programming environment has a visible impact on the application architecture. One such impact could be the constraints on the services that the application can request from an OS. In SaaS, the cloud providers provision application software as on-demand-services. As clients acquire software components from potentially different providers, securely composing them and ensuring that information handled by these composed services are well protected become crucial issues [2].

Table: 1 Actors Activities in Different Service Models

Service Model	Consumer Activity	Provider Activity
SaaS	Use provided service for business activities	Manage[2] the software application over underlying infrastructure
PaaS	Develops, integrates and administrates applications	Provide libraries and tools for consumers; control and maintain cloud resources and provided platforms
IaaS	Creates, configures and administrates virtual machines	Control physical resources and provide computing infrastructure for consumers

II. LITERATURE SURVEY & COMPARATIVE STUDY

Even though lots of cloud benefits its usage will have been immovable due to security problems which has to be addressed. There are various taxonomies related to security issues for cloud computing as it covers many technologies including transaction management, load balancing, concurrency control, memory management, networks, databases, operating systems, virtualization and resource scheduling. There are seven specific security issues which one should discuss with a cloud-computing vendor where equipment and software require substantial security attention [3].

A. Security Issues:

- ***a. Privileged user access*:** Inquire about who has specialized access to data, and about the hiring and management of such administrators.
- ***b. Regulatory compliance***: Make sure that the vendor is willing to undergo external audits and/or security certifications.
- ***c. Data location***: Does the provider allow for any control over the location of data?
- ***d. Data segregation***: Make sure that encryption is available at all stages, and that these encryption schemes were designed and tested by experienced professionals.
- ***e. Recovery***: Find out what will happen to data in the case of a disaster. Do they offer complete restoration? If so, how long would that take?
- ***f. Investigative support:*** Does the vendor have the ability to investigate any inappropriate or illegal activity?
- ***g. Long-term viability:*** what will happen to data if the company goes out of business? How will data be returned, and in what format?

Strong authentication is a mandatory requirement for any cloud deployment. User authentication is the primary basis for access control. In the cloud environment, authentication and access control are more important than ever since the cloud and all of its data are accessible to anyone over the Internet. A security policy should be seen as the foundation from which all security requirements derive. Security policy should not detail technical or architectural approaches (as these may change more frequently than the policy) rather the policy should set forth the underlying requirements from an organizational or business standpoint [4].

B. Security Framework Policies:

Following are some types of security frameworks policies that ensure the cross domain accesses which are properly specified, verified, and enforced.

SAML Security Assertion Markup Language. XML-based open standard for exchanging authentication and authorization data between security domains, basically SAML designed to solve Single Sign-on problem. The Organization for the Advancement of Structured Information Standards (OASIS) developed SAML [5].

XACML *eXtensible Access Control Markup Language*. The standard defines a declarative access control policy language implemented in XML and a processing model describing how to evaluate authorization requests according to the rules defined in policies [6].

OpenID It's a decentralized authentication protocol. No central authority must approve or register service providers or OpenID Providers. With OpenID a user uses single username and password to access many web applications. The user authenticate to an OpenID server to get his/her OpenID and use the token to authenticate to web applications. A user of OpenID does not need to provide a service provider with Private details or other sensitive information such as an email address, security questions.

WS *WS-Security, WS-Trust, WS-Secure Conversation, WS-Federation, WS-Security Policy.*

PRIME *(Privacy and Identity Management for Europe)*

Its single application console that manages end user personal information and provides protection against disclosure of personal data (e.g. providing permissions to the established user and privacy risk to be conveyed, through user interface) is the interface to the PRIME technology [7].

Many cloud vendors implement their own proprietary standards and security technologies, and implement differing security models, which need to be evaluated on their own merits. In traditional security models, a security limit is set up to create a trust boundary within which there is self control over computing resources and where sensitive information is stored and processed. In a third party managed module service providers (e.g., Google and Amazon) manage and control various aspects of the cloud.

C. Privacy Issues:

Privacy in cloud computing is defined as the ability of a consumer to control what information they disclose over the cloud and the ability to control who can access that information. Privacy most often concerns the digital collection, storage, and sharing of information and data, including the lucidity of such observation. There is lots of existing privacy protecting standards are available to protect the disclosure of personal identifiable information of consumer's, unauthorized access to data ,changing of services by the service providers to dynamic environment. Consumers will expect that the services provided by the cloud provider should prevent access to unauthorized both data, code and other sensitive data will remain private. To protect the privacy of cloud users, care must be taken to guard both users' data and applications for manipulating that data.

From a business point of view, privacy should represent an opportunity for cloud providers to promote brand image and differentiate services. It is necessary to find

technological and policy solutions for ensuring privacy and assuring data security. In these situations, ensuring anonymity will not be sufficient. Solutions have been developed to ensure user anonymity on peer-to-peer networks, and these technologies may transfer to the cloud concept. However, while anonymity of user's activities will clearly be a central aspect of protecting user privacy, much of the information sharing between the clouds will not only have to be protected in terms of who it belongs to, but also what it is [8]. That means the responsibility for protecting that information from attackers, hackers and internal data violation is job of hosting company to protect that information rather than the individual user.

Among the main privacy challenges for cloud computing is:

a. Complication of risk assessment in a cloud environment
b. Emergence of new business models and their implications for consumer privacy
c. Achieving regulatory compliance.
d. Identity Theft.
e. Multi-tenancy.
f. Lack of Trust.

To gain the trust of organizations, a cloud provider must deliver levels of security and privacy that assembles or exceeds what is achievable with on-premises solutions. In the context of computing, the terms security, privacy, and trust are related, but have different meanings. As shown in the Figure 2.When a cloud computing system is reliably secured and private, its consumers develop trust in the system.

Figure: 2 The Intersection of good Security and Privacy Builds in a Cloud Computing System

As a tenant with legal privacy commitment, you are managing the private information which is not going to the different place if you are using a cloud. Just as you would not store such information on a server that lacked adequate controls, you wouldn't select any cloud provider without verifying that they meet the same standard for how they protect data at rest, in transmission, or while it is processed. In spite of all of the privacy concerns, cloud computing ultimately has the likely to help bridge certain gaps in access to digital content. By moving computing and storage away from the users, cloud computing reduces the demands and requirements on local hardware that individuals have to purchase [9]. We can argue that it is not a matter of whether cloud computing will become ubiquitous because the economic forces are inescapable but rather what we can do to improve our ability to provide cloud computing users with trust in the cloud services and infrastructure[10].

D. Identity Supervision:

Identity is a key element in the security of an operating cloud. This information must be correct and available to cloud components that have a validated need for access. Identity supervision in cloud has to manage provisioning/deprovisioning, policies, assignment, and password maintenance task, so, as in traditional Identity Management, simply managing users and services is not sufficient in Cloud environment. An IDM in cloud services is to supervise the virtual machines, dynamic environment machines, managing their identities etc. When services of cloud of Virtual machines withdraw from deployment services, the Identity supervision informed so that potential access is cancel [11].

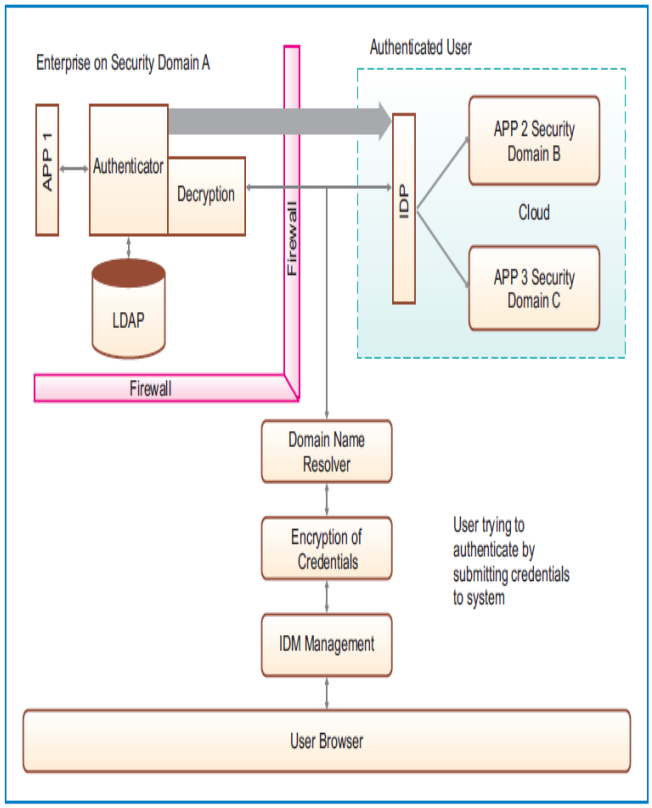


Figure 3: Trusted IDM Pattern *Source: Infosys Research*

The main feature of the pattern is that the authentication is always performed within the firewall. The credentials are submitted to the IDM component and it takes care of encrypting and tunneling the credentials through a secure channel to the authenticator. IDM is independent of the authentication mechanism [12]. Hence deployment and integration is fast and efficient. Once the user is authenticated in by any authentication mechanism, then rest of the participating servers trust the user. The attributes of the user can be shared using some mechanism like SAML. Authorization can be effectively handled by XACML [13].

Jian Wang develops an anonymity based algorithm to attain and preserve privacy in cloud computing. Where the information that are scattered over the servers or on internet is anonymise first before releasing it to the cloud. At this point it will use background data if needed & integrates these details with the anonymous data to mine the needed information. The attributes that has set to anonymous is varies and it depends on the cloud service provider. This

approach will be suitable only for limited number of services.

On the basis of study in the above survey is that there is lots of security & privacy issues is uncovered in the universe. Users or company started to shift their data or information towards cloud but the cloud users are using these services without hesitation that is they directly trust on the service provider without getting the needed information about service provider. We have to check if they are suffering from vulnerabilities, unauthorized user access to the data, low security towards IDM, disclosures of privacy information while sharing the data between the clouds. So the private information disclosures problem related to the user or organization is exposed when the data being shared or released over the cloud. After studying all these aspects we proposed following methodology.

III. PROPOSED METHODOLOGY

The information or data stored in cloud and personal identifiable information that are moving within an Institute or within organization boundaries, in these circumstances sufficient security actions must be taken to protect information despite the changes. So the following method is applied to protect the privacy in cloud computing that must meet the dynamical exchange of data. In the proposed system we use the AES cryptography algorithm for stored data as well as for the data that are moving within the cloud or for outsider service provider. Then this service provider can't use these data if it didn't get the key of cryptography. So the service provider in the cloud should use the key to get & use these data. Following diagram show the overall system flow.

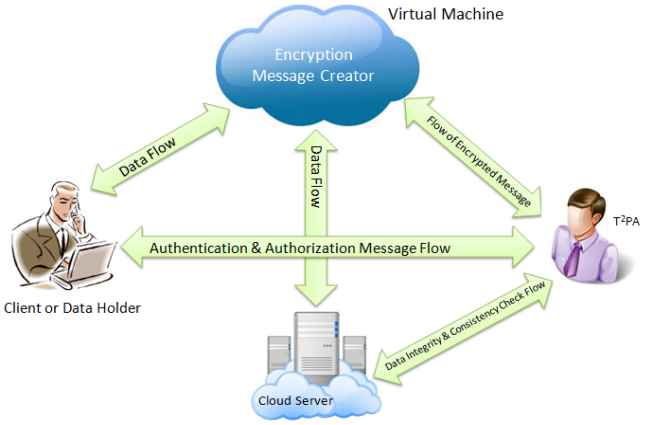
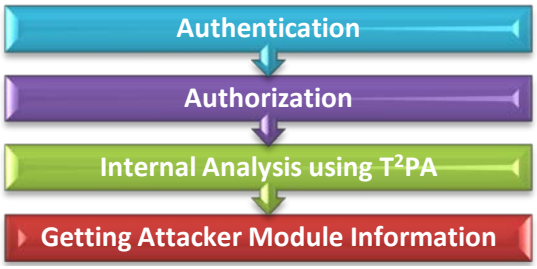


Figure 4: Data flow process between client & T^2.P.A.

Our work proposed here in this paper will focus on the conserving privacy by doing internal analysis to manage this data we use trusted third party analyst (T^2PA) for providing consistency to the data or information. Since T^2PA not only read the data but also he can modify the data, therefore a mechanism should be provided who solved this problem. We first examine the difficulty and new potential security scheme used to solve this problem. Our system encrypt the file at user level by providing three keys security key, private key & public key which ensure the data owner and client that there data are intact to do this we use AES algorithm & XML file signature. By providing XML file content & encryption at the file level the data inter-process between the systems will be highly secured.

Following are major phases that are followed in the proposed system.



A. Why to choose AES algorithm:

As AES is used widely now-a-days for providing security to the cloud. Implementation proposal states that First, User decides to use cloud services and will migrate his data on cloud [14]. Then User submits his services requirements with Cloud Service Provider (CSP) and chooses best specified services offered by provider. AES algorithm ensures that the hash code is encrypted in a highly secure manner. Advanced Encryption Standard is the new encryption standard recommended by NIST in 2001 to replace DES.AES is a symmetric block cipher with a block size of 128 bits. Key lengths can be 128 bits, 192 bits, or 256 bits; 8 called AES-128, AES-192, and AES-256, respectively. AES-128 uses 10 rounds, AES-192 uses 12 rounds, and AES-256 uses 14 rounds [15].

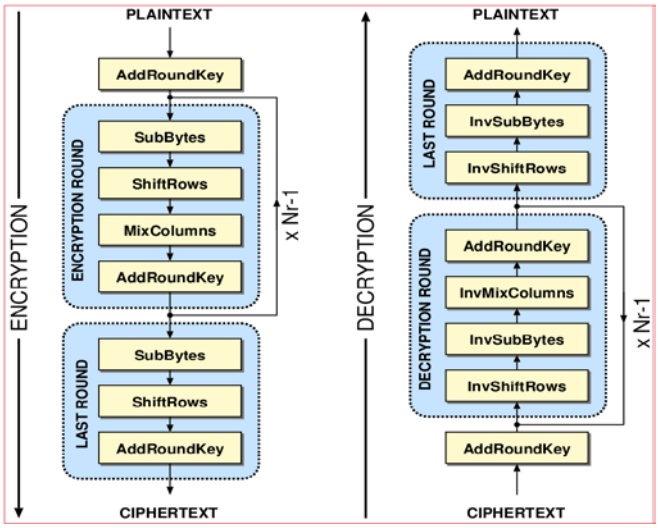


Figure 4: AES algorithm process

For encryption, each round consists of the following four steps:

i. Substitute bytes,
ii. Shift rows,
iii. Mix columns, and
iv. Add round key.

The last step consists of XORing the output of the previous three steps with four words from the key schedule.

For decryption, each round consists of the following four steps:

i. Inverse shift rows.
ii. Inverse substitute bytes.
iii. Add round key, and
iv. Inverse mix columns.

The third step consists of XORing the output of the previous two steps with four words from the key schedule [16].

Table 3.1: Keys and Key size

Key Name	Key Size
AES	256
DES	64
RSA	80
MD5	128

B. Features of AES algorithm:

a. AES also has the notion of a word. A word consists of four bytes that is 32 bits. Therefore, each column of the state array is a word, as is each row.
b. AES was designed from the ground up to be fast, unbreakable and able to support the tiniest computing devices imaginable.
c. Very good Code length and memory utilization while comparing with other algorithms
d. Efficient implementation both in hardware and software phases.
e. It requires less memory for implementation if we compare it with other encryption algorithms, making it beneficial when low space condition arises.
f. There are no severe weak keys in AES.
g. It works in parallel over the whole input block.
h. This algorithm has quick setup time & key alertness.
i. It supports any block sizes and key sizes that are multiples of 32 (greater than 128-bits).
j. No differential and linear cryptanalysis attacks have been yet proved on AES.

Table 3.2: Characteristics and comparison of algorithms [14] [17]

Characteristics		AES	RSA	BLOWFISH	DES
Platform		Cloud Computing	Cloud Computing	Cloud Computing	Cloud Computing
Key Size		128,192,256 bits	1024 bits	32-448 bits	56 bits
Key Used		Same key is used to encrypt and decrypt the blocks.	Public key is used for encryption and private key, for decryption	Same key is used for both encryption and decryption of data.	For encryption and decryption same key is used.
Scalability		Scalable	Not Scalable	Scalable	Scalable
Initial Vector Size		128 bits	1024 bits	64 bits	64 bits
Security		Secure for both provider and user.	Secure for user only	Secure for both providers and user/client side	Security applied to both providers and user
Data Encryption Capacity		Used for encryption of large amount of data	Used for encryption of small data	Less than AES	Less than AES
Authentication Type		Best authenticity provider	Robust authentic implementation	Comparable to AES	Less authentic than AES.
Memory Usage		Low RAM needed	Highest memory usage algorithm	Can execute in less than 5 kb	More than AES
Input* (Time in milli seconds)	10kb	1.5	274.25	4	7.5
	13kb	2	331.5	4.7	10
	39kb	3	351.7	8.25	31.5
	56kb	3.75	415.25	15.7	50.25
Execution Time		Faster than others	Requires maximum time	Lesser time to execute	More time than AES

***Mean processing time (Milliseconds) of the algorithms on local system as well as on cloud network**

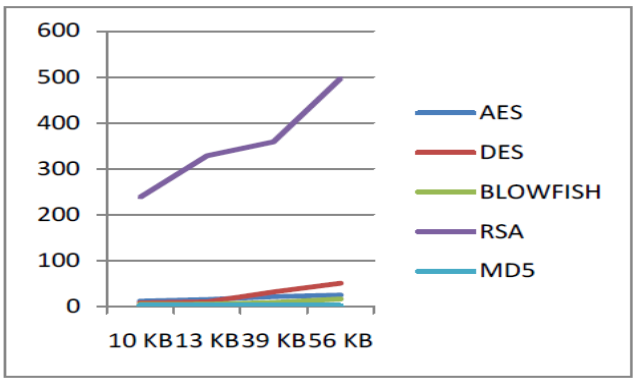


Figure 5: Comparison of Local mean time for algorithms with different input sizes [17].

IV. CONCLUSIONS

In cloud data or information security is an important factor for the client while using cloud services. In this paper we have seen that to protect the user's data from unauthorized access or when the data moving between two clouds traditional techniques for privacy conserving is not sufficient to achieve security. So to solve this problem trusted third party analyst can be used to check for security & integrity of data within the clouds without T^2PA we can't ensures for data consistency between the cloud users. To attain this encryption and decryption algorithms are used to provide the security at the client level by using T^2PA.Here we have proposed a framework where we provide XML file signature in each file & also generates encrypt & decrypt keys by using AES (Advanced Encryption Standard). This is one of the most secure encryption algorithms. According to research done and studying literature survey it can be found that AES algorithm is most efficient in terms of speed, time, and throughput for cloud services.

V. REFERENCES

[1]. Wayne Jansen, Timothy Grance" Guidelines on Security and Privacy in Public Cloud Computing, "Special Publication 800-144,Computer Security, NIST, Dec 2011.

[2]. Hewlett-Packard & Cloud security alliance"Securing Applications in the Cloud," June 2009.

[3]. Jaydip Sen "Security and privacy issues in cloud computing," Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA. [Online]. Available: http://arxiv.org/pdf/1303.4814.

[4]. Jon Brodkin, Network World ",Gartner: Seven cloud-computing security risks" [Online]. Available: http://www.infoworld.com/article/08/07/02/Gartner_Seven_cloudcomputing_security_risks_1.html. Retrieved 20 Feb 2009.

[5]. Cover Pages hosted by OASIS."Security Assertion Markup Language (SAML)" February 23, 2010. [Online]. Available: http://xml.coverpages.org/saml.html.

[6]. XACML from Wikipedia, the free encyclopedia. [Online]. Available: http://en.wikipedia.org/wiki/XACML.

[7]. Bharat Bhargava, Noopur Singh, Asher Sinclair," Privacy in Cloud Computing through Identity Management," Computer Science, Electrical and Computer Engineering [resp], Purdue University [Online]. Available:

http://www.dtic.mil/cgibin/GetTRDoc?AD=ADA552741.[PDF]

[8]. Paul T. Jaeger, Jimmy Lin, Justin M. Grimes," Cloud Computing and Information Policy: Computing in a Policy Cloud?" Journal of Information Technology and Politics, 5(3).University of Marylan. [Online]. Available: http://www.umiacs.umd.edu/~jimmylin/publications/Jaeger_etal_2008.pdf.

[9]. Rohit Ranchal, Leszek Lilien, Bharat Bhargava and others, "An Approach for Preserving Privacy and Protecting Personally Identifiable Information in Cloud Computing" [Online]. Available: http://www.researchgate.net/publication/228649245_An_Approach_for_Preserving_Privacy_and_Protecting_Personally_Identifiable_Information_in_Cloud_Computing/file/d912f50c64caf967c8.pdf.

[10]. Bret Michael, Associate Editor in Chief "In Clouds Shall We Trust?" IEEE Computer And Reliability Societies, September/October 2009 [Online]. Available: http://www.computer.org/csdl/mags/sp/2009/05/msp2009050003.pdf.

[11]. Anu Gopalakrishnan," Cloud Computing Identity Management" SETLabs Briefings,VOL 7 NO 7,2009. [Online]. Available: http://cis.cau.edu/cms/files/CIS509-OAUTH/cloud-computing-identity-management.pdf.

[12]. Shivani Saxena," Network and Information Security –Cloud Privacy and Security implications" Proceedings of the 5th National Conference; INDIACom-2011 Computing For Nation Development, March 10 – 11, 2011 Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi.

[13]. Karunanithi. D, Kiruthika. B, Sajeer. K,"Different Patterns of Identity Management Implemented in Cloud Computing", 2011 International Conference on Advancements in Information Technology With workshop of ICBMG 2011 IPCSIT vol.20 (2011).

[14]. Rachna Arora, Anshu Parashar ,"Secure User Data in Cloud Computing Using Encryption Algorithms" International Journal of Engineering Research and Applications (IJERA) Vol. 3, Issue 4, Jul-Aug 2013, pp.1922-1926.ISSN: 2248-9622.

[15]. Federal Information Processing Standards Publication 197,"Specification for the Advanced Encryption Standard (AES) "National Institute of Standards and Technology (NIST), November 26, 2001.

[16]. Avi Kak,"AES: The Advanced Encryption Standard", Computer and Network Security ",February 26, 2013.

[17]. Gurpreet Kaur, Manish Mahajan" Analyzing Data Security for Cloud Computing Using Cryptographic Algorithms" International Journal of Engineering Research and Application, ISSN: 2248-9622, Vol. 3, Issue 5, Sep-Oct 2013, pp.782-786.