Review on Data Security in Cloud Computing

Ashwini D. Pradhan
P. R. Pote (Patil) Welfare & Education Trust's college of Engineering & Management, Amravati
Department of Computer Science & Engineering
Amravati, India
ashwini.pradhan123@gmail.com

Prof. K. K.Chhajed
P. R. Pote (Patil) Welfare & Education Trust's college of Engineering & Management, Amravati
Department of Computer Science & Engineering
Amravati, India
Krutika.chhajed@gmail.com

***Abstract* —** Cloud Computing is a set of Information Technology Services, like network, software system, storage, hardware, software, and resources and these services are provided to a customer over a internet. These services of Cloud Computing are delivered by third party provider who owns the infrastructure. This technology has a major potential to bring the numerous benefits, however, it faces the risks in terms of unintended economic and security impacts. Cloud computing technology offers a great potential to improve the civil military, interoperability, information sharing and infrastructure resilience. The great benefits offered by the cloud computing technology, data security concerns about their availability, confidentiality, integrity and loss of governance have a great influence on risk management decision process. The paper assesses how security and privacy issues transpire in the context of cloud computing and examines ways in which they might be addressed. This paper aims to solve privacy and security in cloud computing. The methodology used involves encrypting and decrypting data to ensure privacy and security in the cloud.

Keywords- *Cloud Computing, Data Security, Security Issue, Encryption, Decryption.*

*****

I. INTRODUCTION

Cloud Computing is the Internet-based computing. Where resources, software and information are provided to the computers on-demand, like a public utility; is emerging as a platform for sharing resources like infrastructure, software and various applications [1]. The majority of the cloud computing infrastructure consists of reliable services delivered through data centers and built on servers. Clouds are often appeared as single points of access for all consumers' computing needs [2].The cloud computing refers to manipulating, configuring, and accessing the applications online [3]. It also offers online data storage, infrastructure and application. Cloud Computing is a fundamental change in the way the IT Services are invented, deployed, scaled, updated, maintained and paid for.

Security is a key consideration in contemporary network environments. Early in the development of the Internet, protocols implicitly assumed a trusted and altruistic user base who would never attempt to snoop on routed traffic and pick up plaintext passwords, forge a sender address on an incoming email message, or attempt to subvert name services or end hosts [4]. Lot of the companies are shifting toward one of new trend which is cloud computing. According to Gartner researches, the cloud computing is one of four trends that will transform information technology and the way business is conducted. One of the reasons that limit the expansion of the cloud computing to all business functions is the data security concerns. Cloud computing faces a lot of different types of challenges.

Data Security is a key challenge. The data security problems can cause a great loss, even devastating blow [5]. Therefore to make the enterprise and the organization accept cloud computing services, it is necessary to solve security problems. With the benefit of wireless ad-hoc networking in terms of flexibility and ease of deployment come many challenges in network security. Wireless ad-hoc networks are exposed to a variety of security threats in that adversaries may disrupt or halt network operation, compromise the continuous flow of valid information, and violate the privacy of network users and their data. In particular, due to the extensive use of the wireless medium in ad-hoc networks, message communications are vulnerable to passive attacks such as eavesdropping and active attacks such as message insertion or jamming.

A. Data Security in Cloud Computing

Data security is the practice of keeping data protected from corruption and unauthorized access [7]. It protecting personal data and also helps with insuring privacy. In cloud computing the concerns of the data security are increasing due to the ongoing development of the internet and communication and also ease of data sharing. Data security is critical in all the aspects of our lives; banking information, personal files and businesses. Almost all of those are processed using the technologies and through network communication. One major reason security concerns are rising because the companies are conducting core and non-core business functions through other companies.

Figure 1 shows the data lifecycle. In this figure shows how to data is transfer from first phase up to tenth phase. Now there is first step is the collection. In this step data first goes through the collection phase, where the risk of losing data or data being manipulated is moderate. If data is loss in this phase there is possibility to lick your information. next it goes to the relevance phase, in this phase data is relevance. Next to the classification phase; the risk is low in this phase.

 ISSN: 2321-8169
233 – 238

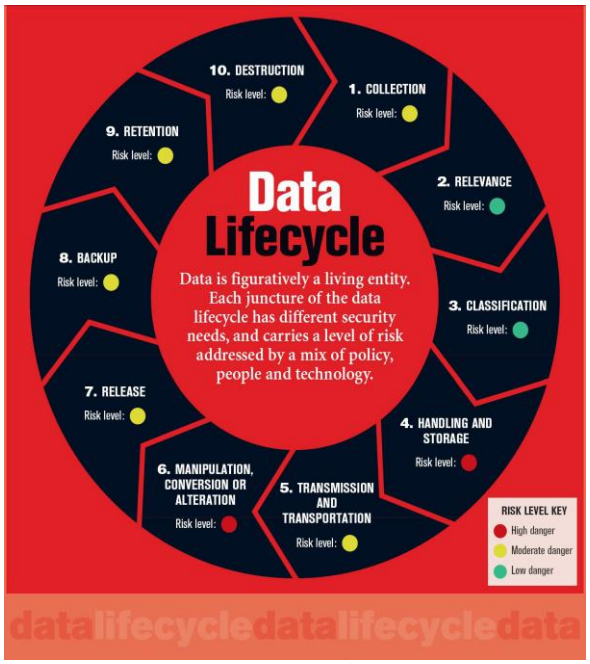

Figure 1: data lifecycle

Wherever Times is specified, Times Roman or Times New Roman may be used. If neither is available on your word processor, please use the font closest in appearance to Times. Avoid using bit-mapped fonts if possible. True-Type 1 or Open Type fonts are preferred. Please embed symbol fonts The next phase is handling and storing the data, where there is a high risk of the data loss or unprivileged access. Then the data is transmitted and transported, the risk here is moderate. The next phase is the manipulation, conversion or altering of the data, this phase has a high risk of losing data. The data then goes through the release, backup, and retention and then destruction phases, where the risk is moderate. The data is threatened the most are the handling and storage and the manipulation, conversion or altering of the data. Cloud computing provides the same ease of sharing the data and information but through the Internet.
Nowadays, the major companies such as Google and Microsoft provide this capability as a service. Gartner defined the cloud computing as "a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service to the external customers using Internet technologies" [8].*Data Security in Cloud*

A. Authentication

Authentication is verifying that the person who requested an access to the information is who he claims to be. It is a process of proving identity. Authentication is a major security measure for cloud computing service providers and users. It is important for service providers to insure that the technologies of authentication are accurate. The main techniques used in the authentication are: username and password, tokens, biometrics, certificates, and Kerberos. Username and password is the most common user technique which is most often used. A token is a security device which has a permission to access embedded in the token itself. This is about the authentication process [13].

B. Access Control

After the authentication and making sure that the user is who that claims to be, the next step is access control; which is restricting the user from access all information, and limiting his access to only material which the user has permission to access. Assigning rights to the groups is more efficient than assigning them to the specific users. Thus, the users should be assigned to groups and then getting the same privileges for all the group members. The models to determine the access control types are: Mandatory Access Control (MAC), Role-Based Access Control (RBAC), and Discretionary Access Control (DAC)[13].

C. Audit

Third and last part of the data security is Auditing. Information security configurations should be audited to ensure the access controls that are in place. Some of the auditing techniques are; logging and system scanning. Logging is keeping record of the activities performed by the users and the time at which it is occurred. The information recorded in the logging is useful when it is compared with the access control list (ACL) [13].

II. LITERATURE SURVEY

Cloud computing has been defined by US National Institute of Standards and Technology (NIST) [12] as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction ".The NIST definition is one of the clearest and most comprehensive definitions of cloud computing and is widely referenced in US government documents and projects.

NIST defines three main service models for cloud computing:
A. Software as a Service (SaaS) – The cloud provider provides the cloud user with the capability to deploy an application on a cloud infrastructure [9].

B. Platform as a Service (PaaS) – The cloud provider provides the cloud user with the capability to develop and deploy applications on a cloud infrastructure using tools, runtimes, and services supported by the CSP [9].

C. Infrastructure as a Service (IaaS) – The cloud provider provides the cloud user with essentially a virtual machine All title and author details must be in single-column format and must be centred. The cloud user has the ability to provision run by the virtual machine.

Brian Hay et.al [10] have focused on data authentication, data integrity, querying and outsourcing the encrypted data.

 ISSN: 2321-8169
233 – 238

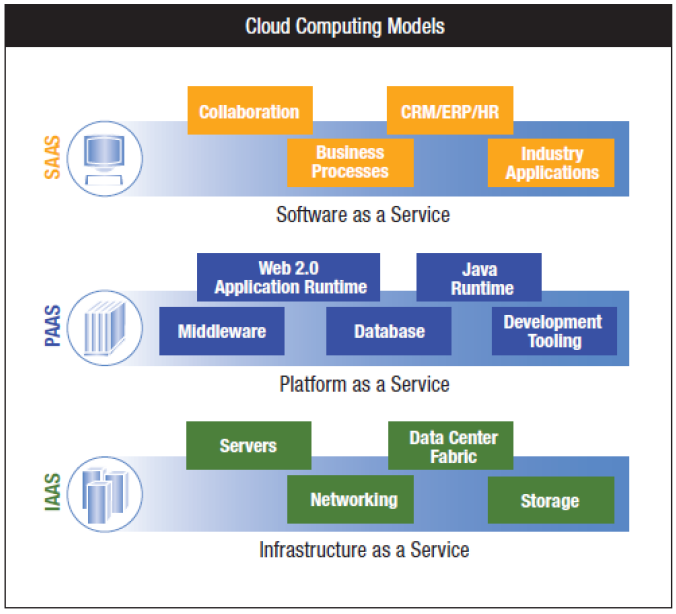

Figure2: Cloud Computing Delivery Models [18].

Brian Hay et. al [10] have focused on data authentication, data integrity, querying and outsourcing the encrypted data. Their research says that, the risks can arise at operational trust modes, resource sharing, new attack strategies. In operational trust modes, the encrypted communication channels are used for cloud storage and do the computation on encrypted data which is called as homomorphism encryption [14]. New attack strategies like Virtual Machine Introspection (VMI) can be used at virtualization layer to process and alter the data.

Kevin Curran et.al [15] mentions that Cloud Computing is a distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services. Cloud computing has become a variable platform for companies to build their infrastructures upon. If companies are to consider taking advantage of cloud based systems by storing their data in Cloud Storage they will be faced with the task of seriously reassessing their current security strategy.

Randeep Kaur et.al [16] mentions some of the notable challenges associated with cloud Storage. The challenges are Security, Privacy and Lack of Standards which slow down services in the cloud. Rashmi Nigoti et.al [11] defines some privacy and security-related issues that are believed to have long-term significance for cloud storage.

John C. Mace et.al have proposed an automated dynamic and policy-driven approach to choose where to run workflow instances and store data while providing audit data to verify policy compliance and avoid prosecution. They also suggest an automated tool to quantify information security policy implications to help policy-makers form more justifiable and financially beneficial security policy decisions.

The literature review contains the definitions of cloud computing defined by US National Institute of Standards and Technology (NIST)[19]. The NIST definition is one of the clearest and most comprehensive definitions of cloud computing and is widely referenced in US government documents and projects. A number of researchers have discussed the security challenges that are raised by cloud computing. It is clear that the security issue has played the most important role in hindering the acceptance of Cloud Computing. For security purpose of cloud storage various encryption techniques are being analyzed by researchers. As discussed in survey there are many security techniques which are currently applied to cloud storage. Apart from this there are still too many areas which require further enhancements like more efficient algorithms can be developed which can increase the security level in the cloud storage.

III. TECHNIQUES USE IN DATA SECURITY

A. RSA Algorithm:

The RSA algorithm named after Ron Rivest, Adi Shamir, and Leonard Adleman. It is based on a property of positive integers. RSA uses modular exponential for encryption and decryption. RSA is an algorithm for public-key cryptography, involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The process is shown in figure 3. RSA uses two exponents, e and d, where e is public and d is private. Let the plaintext is M and C is cipher text, then at encryption. And at decryption side C = Me mod n M = Cd mod n.

Where n is a very large number, created during key generation process.

Rashmi Nigoti et.al [11], uses DES algorithm and RSA algorithm for providing security to cloud storage

Key Generation

Select p, q	p, q both prime, p≠q
Calculate n = p×q	
Calculate $\phi(n) = (p-1)\times(q-1)$	
Select integer e	$\gcd(\phi(n),e) = 1;\ 1<e<\phi(n)$
Calculate d	
Public key	KU = {e, n}
Private key	KR = {d, n}

Encryption

Plaintext:	M < n
Ciphertext:	$C = M^e \pmod n$

Decryption

Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

Figure3. RSA Algorithm

RSA-public-key algorithm in detail

This rides on the model that user data is encrypted before storing it to the cloud. User is required to place a request to the cloud provider, gets authenticated and data rendered. RSA as a block cipher maps every message to an integer. The cloud provider encrypts the data using the public key while the cloud user decrypts the data using the private key.

RSA algorithm involves three steps key generation, encryption and decryption. Following figure gives how to process of encryption of data.

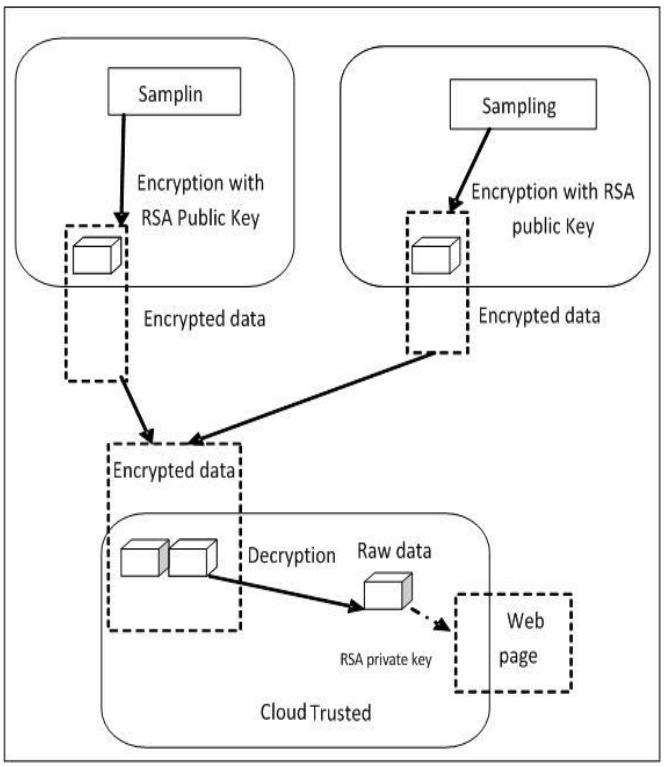

Figure 4. Advancing the User's Privacy and Security through Encryption of Data

A. Key Generation:

This process is carried out before data is encrypted between the cloud provider and cloud user.

Steps:

1: Two distinct prime numbers are chosen p and q, due to security, the integers p and q should be selected at random and should be of same bit length.

2: Calculate n = p * q.

3: Calculate Euler's totient function, Ø(n) = (p-1) * (q-1).

4: Pick an integer e, such that 1 < e < Ø(n) and greatest common divisor of e, Ø (n) is 1. At this stage e is the Public-Key exponent.

5: At this stage d is determined as follows: d = e-1(mod Ø(n)) such that d is multiplicate inverse of e mod Ø(n).

6: d is regarded as Private-Key component, therefore, d * e = 1 mod Ø(n)[20].

7: The Public-Key contain modulus n and the public exponent e for example, (e, n).

8: The Private-Key contains modulus n and the private exponent d, which are kept secret such as (d, n).

B. Encryption:

Encryption is a method of converting original plain data into cipher data.

Steps:

1: Cloud service provider should transmit the Public- Key (n, e) to the user who wants to store the data.

2: User information is now mapped to an integer through the use of agreed upon reversible protocol, referred to as padding scheme.

3: Data is encrypted and the resulting cipher data C is C = me (mod n).

4: This cipher data or encrypted data is presently stored with the Cloud service provider [20].

C. Decryption:

Decryption is the process of converting the encrypted data to the original data.

Steps:

1. In this process the cloud user requisite the Cloud service provider for the data.
2. Cloud service provider confirms the authenticity of the user and provides the encrypted data C.
3. The Cloud user decrypts the data by calculating, m = Cd (mod n).
4. Once m is achieved, the user can retrieve the original data by reversing the padding scheme [20].

D. Results of the experiment

Sample data is taken and implementing RSA algorithm over it. During the implementation, different bits are used and the time taken to generate a key depends on the amount of bits used for the value of n.

TABLE 1
RSA KEY GENERATION

Number of Bits	Computational time
512	0
600	0
800	0
1024	10
1700	15
2048	20
2300	65
3223	60
4200	75

How to generate key by using example

1. Two distinct prime numbers p=61 and q=53.
2. n = p*q, therefore n=61*53 = 3233.
3. Euler's totient function, Ø (n)=(p-1)*(q-1),therefore Ø(n)=(61-1)*(53-1) = 60*52 = 3120.
4. Integer e =17, such that 1 < e < 3120 that is co-prime to 3120.
5. To compute d, d = e-1(mod Ø(n)), therefore d=17-1(mod 3120) = 2753.
6. As a result the Public-Key is (e, n) = (17, 3233) and the Private- Key is (d, n) = (2753, 3233). This Private-Key is reserved secret and it is identified only to the user.

Encryption

1. The Public-Key (17, 3233) is given by the Cloud service provider to the user who wishes to store the data.
2. If the user mapped the data to an integer m=65.

3. Data is encrypted by the Cloud service provider through the use of corresponding Public-Key which is shared by both the Cloud service provider and the user. C = 6517(mod 3233) = 2790.
4. This encrypted data is stored by the Cloud service provider.

Decryption

1. Provided that the user is valid, Cloud service provider will authenticate the user and delivers the encrypted data when user requests for the data.
2. The cloud user then decrypts the data by computing, m = Cd (mod n) = 27902753(mod 3233) = 65.
3. Once the m value is obtained, user will get back the original data.
4. All above step solve the problems by using RSA by including generation key, encryption, decryption [12].

IV. CHALLENGES IN CLOUD COMPUTING

The term cloud computing is popularly used by the people in Information Technology industries because it provides various services as pay on demand. No consumer need to know working knowledge of cloud computing services and need not invest money for acquisition/maintenance to infrastructures/human resources/software &hardware. So this is becoming more worthy to any people for getting any service from cloud computing where some free services are also offered to the people.

So the cloud computing becoming an emerged technology and most popular research thrust area. But it faces many challenges in different aspects of data and information handling. Some of these are presented as follows[17].

A. Interoperability

It means the application on one platform should be able to incorporate services from the other platforms. It is made possible via web services, but developing such web services is very complex.

B. Security and privacy

Security and Privacy of information is the biggest challenge to cloud computing. Security and privacy issues can be overcome by employing encryption, security hardware and security applications. There is also challenge to solve the issue about overcome on all of that technique like encryption decryption ad also using RSA algorithm so this is the all information about the how to solve the issue about security.

C. Portability

This is another challenge to cloud computing that applications should easily be migrated from one cloud provider to another. There must not be vendor lock-in. However, it is not yet made possible because each of the cloud providers uses different standard languages for their platforms.

D. Computing Performance

Data intensive applications on cloud require high network bandwidth, which results in high cost. Low bandwidth does not meet the desired computing performance of cloud application. So this is challenge for cloud computing this is all about the computing performance in cloud computing.

E. Reliability and Availability

It is necessary for cloud systems to be reliable and robust because most of the businesses are now becoming dependent on services provided by third-part.

V. RELATED WORK

In the work [1] Identity-Based Cryptography (IBC) is in a very quick development [6, 7]. Identity-Based Encryption (IBE) provides a public key encryption mechanism where a public key is an arbitrary string such as an email address or a telephone number [17, 18]. The corresponding private key can only be generated by a Private Key Generator (PKG) who has knowledge of a master secret. Using this construct, anyone can encrypt messages or verify signatures without prior key distribution beyond the dissemination of public parameters and the public key “strings.” This is useful where the deployment of a traditional certificate authority-based PKI is inconvenient or infeasible, as IBE-based systems do not require certificate management. In the work [4] Cloud computing is a new computing model, and security is ranked first among its challenges. This paper reviews existing security monitoring mechanisms compared with new challenges which are caused by this new model. We highlight possible weaknesses in existing monitoring mechanisms, and propose approaches to mitigate them From time to time first-hand reputation information is exchanged with others. cloud computing defined by US National Institute of Standards and Technology (NIST)[19]. This is all related work to cloud computing and information about RSA algorithm.

CONCLUSION

Cloud computing is the set of resources or services provided through the internet to the users on their demand by cloud service providers. Since each and every organization is moving its data to the cloud, means it uses the storage service provided by the cloud provider. Therefore it is mandatory to protect that data against unauthorized access, modification or denial of services etc.Cloud environment is widely used in industry and research aspects; therefore security is an important aspect for organizations running on these cloud environments.

Using proposed approaches, cloud environments can be secured for complex business operations. So this research paper emphasizes on the how to data secure in cloud computing by using RSA algorithm and all information about data security in cloud computing.

ACKNOWLEGEMENT

The author would like to present their sincere gratitude towards the, Prof. K. K. Chhajed (Guide) and also special thanks to Prof. Vijay B. Gadicha (H.O.D - Department of Computer Science & Engineering) for their extreme support to complete this assignment.

REFERENCES

[1] Anthony T. Velte, Toby J. Velte, Robert Elsenpeter (2010), “Cloud Computing: A Practical Approach” pp. 3-7.
[2] Alkhatib, Ghazi I. (ed. 2010), “Web Engineering Advancements and Trends: Building New Dimensions of Information Technology”, Available at: https://books.google.co.in/books?isbn=160566720X
[3] Shefali Ojha (2014), “Relivence of Cloud Computing” pp. 28.
[4] J. Granjal, R. Silva, J. Silva (2008), "Security in Wireless Sensor Networks", CISUC UC,2008.
[5] K. W. Miller, J. Voas, and G. F. Hurlburt (2012), “BYOD: Security and Privacy Considerations,” IT Professional, vol. 14, no. 5, pp. 53– 55, Sep. 2012.
[6] Z. Lan, V. Varadharajan and M. Hitchens (2013), “Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage”,Information Forensics and Security, IEEE Transactions on, vol.8,no.12,pp. 1947-1960.
[7] "What Is Data Security?" Spam – Antivirus - Identity Theft – Scams and Fraud STOP IT.Web. 30 Nov. 2010. <http://www.spamlaws.com/data-security.html>
[8] STAMFORD, CONN. "Gartner Highlights Five Attributes of Cloud Computing."Technology Research & Business Leader InsightbGartner. 23 June 2009. Web. 11 Dec.2010. <http://www.gartner.com/it/page.jsp?id=1035013>.
[9] AL.Jeeva, Dr.V.Palanisamy And K.Kanagaram “Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms” International Journal Of Engineering Research And Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, pp.3033- 3037, May-Jun 2012.
[10] Brian Hay, Kara Nance, Matt Bishop, “Storm Clouds Rising: SecurityChallenges for IaaS Cloud Computing” Proceedings of the 44th Hawaii International Conference on System Sciences, pp.1-7, 2011.
[11] Rashmi Nigoti, Manoj Jhuria and Dr.Shailendra Singh, "A Survey of Cryptographic Algorithms for Cloud Computing" International Journal of Emerging Technologies in Computational and Applied Sciences,Vol. 4, pp.141-146, March-May 2013.
[12] Wayne Jansen ,Timothy Grance, "Guidelines on Security and Privacy in Public Cloud Computing", NIST Special Publication,NIST SP -800- 144 ,80 pp., 2011.
[13] Gens, Frank. "IT Cloud Services User Survey, Pt.2: Top Benefits & Challenges." IDC EXchange. 02 Oct. 2008. Web. 14 Dec. 2010.
[14] Maha TEBAA, Said EL HAJJI, Abdellatif EL GHAZI, “Homomorphic Encryption Applied to the Cloud Computing Security”, World Congress on Engineering, Volume I, ISBN: 978-988-19251-38;ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online) , 2012.
[15] Kevin Curran, Sean Carlin and Mervyn Adams, “Security issues in cloud computing”, Elixir Network Engg.38 (2011), pp.4069-4072, August 2011.
[16] Randeep Kaur, Supriya Kinger, "Analysis of Security Algorithms in Cloud Computing" International Journal of Application or Innovation in Engineering & Management (ISSN 2319 - 4847),Volume 3 Issue 3, pp.171-176, March 2014.
[17] Pearson, S., Benameur, A., Privacy, "Security and Trust Issues Arises from Cloud Computing", Cloud Computing Technology and Science (CloudCom), IEEE Second International Conference, pp.693-702,2010.
[18] Architectural Map of the Cloud Landscape.” IEEE Xplore, pp 23-31, Jun. 2009.
[19] Architectural National Institute of Standards and Technology, NISTDefinition of Cloud Computing, Sept 2011. M. Klems, A. Lenk, J.Nimis, T. Sandholm and S. Tai. “What‟s Inside the Cloud? An
[20] Map of the Cloud Landscape.” IEEE Xplore, pp 23-31, Jun. 2009.