International Journal on Emerging Technologies 10(1): 68-73(2019)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

Analysis of Cloud Computing for Security Issues and Approaches

Sheeba Khan[1] and Shailja Sharma[2]
[1]*Assistant Professor, IPER College, Bhopal (Madhya Pradesh), India*
[2]*Associate Professor, Department of Computer Science & Engineering, RNTU University, Bhopal (Madhya Pradesh), India*

(Corresponding author: Sheeba Khan)
(Received 24 February 2019, Revised 22 April 2019 Accepted 02 May 2019)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Cloud computing is the practice of using a network of remote servers hosted on internet to store, manage and process data on demand and pay as per use. It provides access to a pool of shared resources instead of local servers or personal computers. As it do not acquire the things physically, it saves managing cost and time for organizations. Cloud computing is a completely internet dependent technology where client data is stored and maintain in the data center of a cloud provider like Google, Amazon, Microsoft etc. Cloud computing is an emerging domain and is acclaimed throughout the world. There are some security issues creeping in while using services over the cloud. This research paper presents a review on the cloud computing concepts as well as security issues inherent within the context of cloud computing and cloud infrastructure. This paper also analyzes cryptography algorithms with the process and also describes the threats inside the security of cloud. These cryptography algorithms are premeditated and analyzed well in order to help in increasing the performance of the existing cryptography methods. The outcome shows the techniques that are useful for real-time encryption. All encryption methods have proven to have their advantages and setbacks and have proven to be appropriate for different applications.

Keywords: Cloud Storage, Cloud Performance, Cloud Scalability, Cloud Availability, Cloud Security, Cloud Access Control, Document Sharing.

I. INTRODUCTION

The Computing of cloud paradigm has bulged as an dexterous technique which enables omnipresent, access on demand to a common pool of flexibly reconfigurable computing resources by the elevation of the same time as networks, servers, storage space, applications, and services with the intend. of quickly deployed with least management efforts and service provider interactions. A very popular and simplest definition of cloud is, "a solution of network for provided that economical, trustworthy, uncomplicated and straightforward permission to IT resources" [1]. The service oriented approach of Computing in cloud is not merely reduces the operating cost of infrastructure and ownership cost furthermore provides improved performance and flexibility to the customer [13]. NIST has defined the apparatus that are used in computing of cloud with essential features and two models these models are [13] a) Deployment Model.
b) Service Model
Deployment Model are classified as [23]:
a) Public
b) Private
c) Hybrid
d) Community
Basically depends upon on demand of the organization.
Computing of cloud Service models being classified as [13,23]:
Software as a Service (SaaS): Providing Software's as a service for the patrons according to their necessities, enable patrons to utilize the services that are available on the servers of cloud.
Platform as a Service (PaaS): Clients are provided platforms access, which enables them to put their own customized software's and other applications on the clouds.

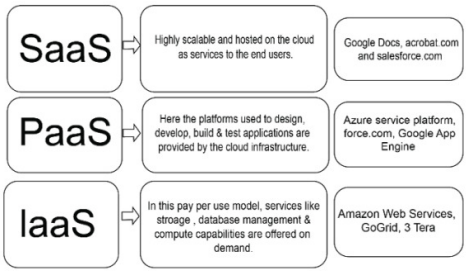

Fig. 1. A conceptual view of computing in cloud.

Infrastructure as a Service (IaaS): Rent processing, storage, network capacity, and other basic computing resources are granted, enables patrons to deal with the operating systems, applications, storage, and network connectivity.
Performance, availability, scalability, and Security of data are the biggest challenges in adaptation of cloud [1]. Data integrity, privacy and protection are some of the mandatory issue for the services of cloud. For thisreason, numerous service providers are using variant policies, techniques and methods that depend upon, the following parameters:
• Size of data.
• Nature of data.
• What Types of data.
• Size of data.

II. LITERATURE REVIEW

So as to comprehend the fundamental concepts of Computing in the cloud and storing secure data on the cloud, diverse wherewithal have been consulted. This segment is for literature review to locate an

underpinning of discussing different aspects of Computing in the cloud environment.
Previous study provides that how to improve performance in the computing of cloud and how many parameters effected performance of cloud. The endeavor of this research was depends in the lead of the following factors [1].
a. How can performance with in Cloud Computing be improved?
b. Workload analysis and innovative cloud resource management?
Previous study adopted the resource allocation technique to increasing the cloud performance and applies encryption process to the files. By using these existing methods decrease the downloading and uploading time of file on cloud to enhance the performance [1].
Previous study also provides the concept of Scalability means that when increase the load lying on the workstation then performance of the system ought to be constant in every environment without the harm the customer requirements. According to study various scaling techniques are available for improve scalability in the computing of cloud [1].
a. Vertical Scaling.
b. Horizontal scaling.
c. Diagonal scaling.

Another meaning of Scalability is that various user can share their data simultaneously without any collision.
Previous study also provides Cloud availability is the another issue in the computing of cloud .It means that when any user want anything in case he is using cloud It should be available. Availability is directly proportional to reliability. Everyone is familiar with this term if system is reliable then user will work more on such kind of system. There are choices of factors which will effect on availability of cloud these are [1]:
a. Human error
b. Software Failure
c. Hardware failure
d. Migration of machine from one server to another.

Previous study provides the concept in cloud computing according to these Security has a major role in computing of cloud. It means that users data safe form attackers and hackers. Every user worried about the security, privacy and confidentiality of their data. If any system which provides this feature strongly which will the success system for the future aspect? Any of the unauthorized users will not be admittance to the system this will be another security aspects for the system. Security parameters which are required for the successful system [3, 24].
a. Privacy
b. Confidentiality
c. Unauthorized Access
d. Safe for attacker
e. Safe for hackers etc.

Every aspects in the computing of cloud is mandatory for this researcher have various security algorithms over and above rules as they can implement for the security point of view.
Previous study endow with a commendable approaching into the basic concepts of cloud computing. In this paper, numerous key concepts are explored that examples of applications that can be developed using Computing of cloud and how they can help the developing world in getting benefit from this emerging technology.
Previous study Cloud computing provides highly scalable resources accessed via Internet. Since Computing in cloud is growing quickly day by day used by individuals and companies throughout the world, data protection problems in the Computing of cloud have not been tackled currently? In the cloud, cloud services users have serious threat of losing confidential data. To take in hand data privacy issues of users, they have proposed data protection framework. The proposed data protection framework addresses the challenges throughout the cloud services life cycle.
Their proposed framework comprises of three key components: policy ranking, policy integration and policy enforcement. For each component, they have presented various models and analyzed properties of each component. This paper includes a discussion on general guidelines for weighing up designed systems based on such kind of framework. This study also accessible numerous models of data protection and defined cost functions [7].
Previous method provided a standard to secure data-in-transit within the cloud. A yardstick for encryption technique has been discussed for guarding information for the duration of immigration. Other standard of encryption is required for stout security although it involves superfluous computation. The yardstick discussed in their study presents equilibrium for the security and encryption overhead [14, 25, 27].

III. SECURITY THREATS IN CLOUD

Cloud computing is facing a lot of security issues. Those issues are listed below [6, 10, 26]:
a. Data Loss.
b. Malicious.
c. Insecurity of interfaces and APIs.
d. Hijacking of account and service.
e. Leakage of data.
f. Denial of service.
g. Technology sharing risk.
h. Integration of data and protection.

A. Data Loss

Companies outsource their data on the cloud because of low cost and safety point of view but there is the chance of data loss. There are many possibilities of data loss during out sourcing of data some are given below [4].
1. Malicious attack
2. Server crash
3. Deletion of data by the providers
4. No data backup
5. Loss of encryption key.

There are many solutions to avoid loss of data in cloud computing some are:
1. Use of strong API for access control.
2. Analysis of data protection at runtime as well as compile time.
3. Use of strong key generation scheme.
4. Apply proper backup and retention schemes.

B. Malicious insiders

Malicious insiders Means the person who have authorization for accessing the information regarding cloud data that can be DBA (Data Base Administrator), employee, partners, etc of the cloud organization. Those people can theft and corrupt the information if any other company paid higher amount [27].

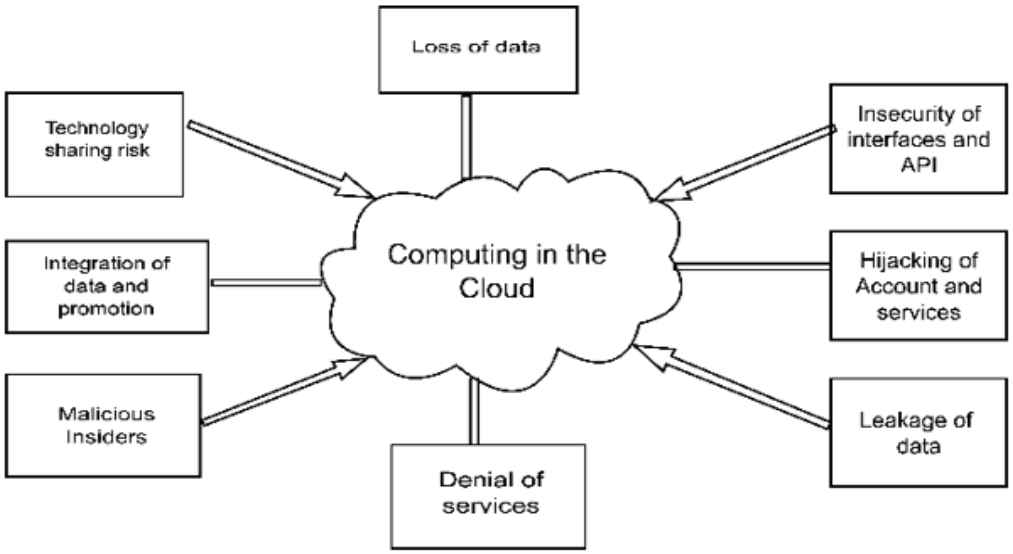

Fig. 2. Threats of Security in computing of cloud.

C. Insecurity of interfaces and APIs:
The interaction between cloud service providers and client should be through application programming interface (APIs). So these APIs should be secure for preventing unauthorized access.

D. Hijacking of account and service
Every cloud user having their account over internet (bank account, e-mail account or social media account). Account hacking can cause severe destruction to users data,.integrity and reputation.

E. Leakage of data
The cloud service provides the facility to the every user for transferring and accessing data of any location in the world so there is the chance of data leakage. This will shows the weakness in the security of cloud and physical transport system of cloud.

F. Denial of service
Availability is the important parameter in the computing of cloud for this many of the company need their system to be available all the time. One more thing in computing in cloud is resource sharing among the users. If any attacker use all the resources of computing in the cloud then no one can use his desired resources this is called denial of service. When this is occur user will access their resource very slow and this will also effect on the availability of cloud.

G. Technology sharing risk
Infrastructure as a service is based upon shared infrastructure. This service has not been designed with multi-tenant architecture so this architecture is important for removing this risk.

H. Integration of data and protection
Many of the organization must be sure its own data is sheltered moving between the end user and the cloud data center because unsecured data is more accountable to interrupt in the transmission [12].

IV. REQUIREMENTS FOR SECURITY IN CLOUD COMPUTING

ISO (International standard organization), Information Security should cover a number of recommended substance. Computing of cloud security should besides guided in this regard in order to become an impressive and secure technology solution.

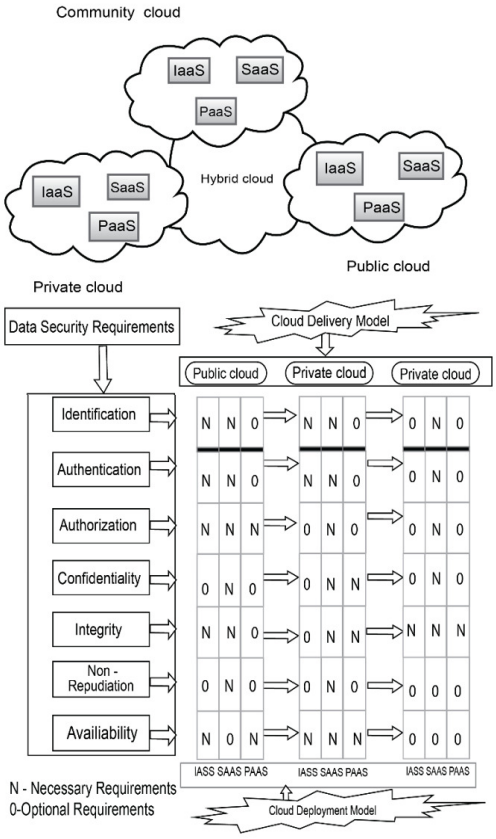

Fig. 3. Security requirements in computing of cloud.

Fig. 3 represents the security requirements in information tightly joined with the deployment model of cloud and delivery models. [13]. In Fig. 3, the different cloud delivery models and deployment models are matched up against the security requirement for information where "N" represents necessary requirements and "O" represents the optional requirements.

However future task is needed in investigating of the optimal balance required in securing Cloud computing. Figure 3, should be viewed in context as a guideline in assessing the security level. The cloud requirements of security will be highlighted below in context of Cloud computing.

a. Identification
b. Authentication
c. Anonymity
d. Authorization
e. Confidentiality
f. Integrity
g. Non-repudiation
h. Availability

V. SECURITY ALGORITHMS AND ITS PARAMETERS

In cloud computation, data security is not only concerned with encryption but also many other processes. Risk of data loss depends upon the Following parameters.

a. Reset of data
b. Transit of data

a. *Reset of data*

When cloud user accesses their data from the cloud with the help of internet this is referred as Reset of data. This process works with live data whereas backups of data.

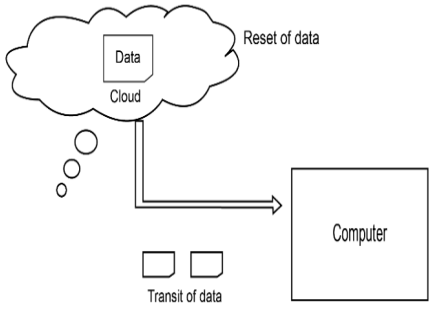

Fig. 4. Data at Reset and transit.

B. Transit of data

Moment of data in the process of in and out in the cloud is referred as transit of data. When user upload their information on the cloud at that time it refereed as transit of data. So this is the time for the hacker to hijacking user's data, to prevent this Encryption and Decryption process should be adopted [18].

Encryption [11] and decryption has an important role in cryptography techniques. Now day's two types of cryptography methods used for encryption and decryption of data those are:

1. Encryption with Symmetric key
2. Encryption with Asymmetric key

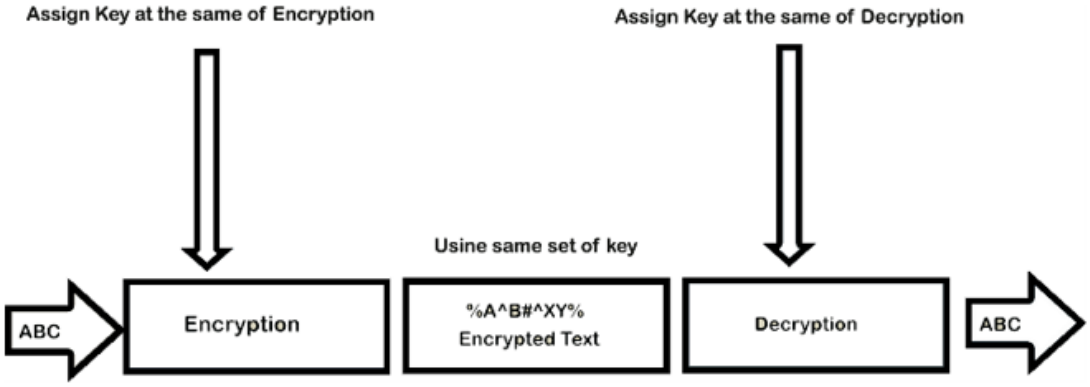

Fig. 5. A Basic Cryptography Approach.

Researcher concludes that Encryption with Asymmetric key is the most excellent technique for the data security. In this technique two keys specifically private and public will be used between sender and receiver to encrypt and decrypt the data.

Now a day's Different cryptography techniques are used for data encryption. By means of the use of Cryptography level of security will be improved the same as some important parameters also is increased these are:

1. Level of data protection
2. Integrity of contents
3. User authentication
4. Availability.

Cryptography is the process for hiding original content at the time of sending plain text. The Process of *C*.

Hash function: Hash function is the mathematical function .Hash function replaces the input text value to string of alphanumeric. This technique also ensures that no two strings can have same string of alphanumeric as an output. Hash function is very simple mathematical function shown as below [9].

$F(x) = x \bmod 10$ .....(1)

All of these above mentioned methods and techniques are widely used for encrypting the data in the cloud to ensure security of data. These techniques may vary from one scenario to another. Whatever technique is used. These are highly recommended techniques to ensure the data security in both private and public clouds.

VI. COMPARISON OF CRYPTOGRAPHIC ALGORITHMS

The table 1 gives the comparison between all algorithms that are previously discussed from the reference section. On the basis of these comparison following parameters is comparedfor finding best suitable security algorithm these parameters are:

1. Name of algorithm
2. Size of Key and block that are used in Algorithm
3. Round, 4. Structure, 5. Flexibility
6. Features of security

Table 1: Security algorithms comparison.

Name of Algorithm	Size of Key	Size of Block	Round	Structure	Flexible	Feature of key
DES	64 Bits	64bits	16	Festiel function(F)	No	Not Strong Enough
E-DES	1024 bits	128 bits	16	Festiel function(F)		Good Security and fast speed
T-DES	112 or 168	64 bits	48	Festiel function(F)	Yes	Adequate Security and Fast
T-DES	112 or 168	64bits	48	Festiel function(F)	Yes	Adequate Security and Fast
RSA	1024 to 4096	128 bits	1	Public key algorithm	No	Excellent Security and low speed
BLOW FISH	32–448	64 bits	16	Festiel function	Yes	Fast Cipher in SSL
DSA	Variable			Public key Algorithm	Yes	Good Security and fast Speed
RC6	128bits to 256 bits	128 bits	20	Festiel function	Yes	Good Security
AES	128, 192, 256 Bits	128 bits	10,12,14	Substitution Permutation	Yes	Security is excellent It is best in security and Encryption performance

One more algorithm in the aspect of cloud is Attribute based encryption algorithm (ABE). It has access polices for the attribute set to identifying the owner who want to share their data and one more this that is good for security is encrypted data and key are stored on the servers of cloud. Hence to enhance the security of the data on the servers AES algorithm is used. First data is encrypted using AES algorithm [21] and later it is encrypted using ABE.

VII. RESULT AND DISCUSSION

From the above, the comparisons of the algorithms are based upon the following factor to find out which security algorithm is best in providing security in computing of cloud:

1. Key size
2. Size of block
3. Round
4. Structure
5. Flexibility

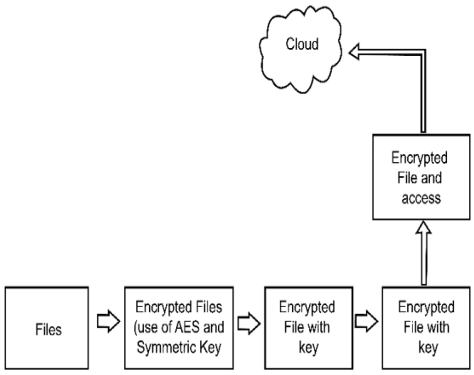

Fig. 6. Encryption process of files with use of AES and ABE algorithm.

So researcher conclude his survey on the basis of above parameters That has been applied on DES, E-DES, RSA, Blow fish, DSA, RC6, AES and ABE algorithm [18] has fastest in encryption time, speed, flexibility. The results also prove that the AES algorithm is the best in security, flexibility andencryption performance strongest. It is most efficient when compared to others. Cloud environment required more security so researcher decides that AES with ABE Algorithms is best suitable for the future work [13] because this concept provide double encryption to providing the best security in computing of cloud paradigms. The overall encryption process by using AES with ABE in Fig. 6 [18].

VII. CONCLUSION

This paper presents brief introduction and functionality of the mainly significant cryptography algorithms with the process and also describes the threats inside the security of cloud.

These cryptography algorithms are premeditated and analyzed well in order to help in increasing the performance of the existing cryptography methods. The outcome shows the techniques that are useful for real-time encryption. All encryption methods have proven to have their advantages and setbacks and have proven to be appropriate for different applications. The comparison between Symmetric and Asymmetric algorithms shows that Symmetric algorithms are faster than their Asymmetric counterparts. Through the previous studies and the comparison of possible outcomes, researcher find that the most reliable algorithm is AES in term of speed encryption, decoding, complexity, the length of the key, structure and flexibility. If researcher will use AES with ABE (Attribute based encryption). It will give best outcome in the aspect of security in the computing of cloud paradigms.

Conflict of interest: No

REFERENCES

[1].Shoaib Hassan, Asim Abbas kamboh, Farooque Azam, (2014). "Analysis of Cloud Computing Performance, Scalability, Availability & Security". *In the Proceedings of the 2014 International Conference on Information Science & Computing Basics", International Journal of Advanced Research in Computer and Communication Engineering*, Vol. **1**, Issue. 5, pp. 3-22.

[2]. M.A. Vouk, (2008). "Cloud computing - Issues, research and implementations", *In Proceeding of the 2008 30th International Conference. On Information Technology Interfaces (ITI),* Cavtat, Croatia, pp. 31-40.

[3]. P.S. Wooley, (2011). "Identifying Cloud Computing Security Risks," University of Oregon, pp.1-88 February, 2011.

[4]. F.B. Shaikh and S. Haider, (2011). "Security Threats in Cloud Computing", *In Proceeding of the 2011 International Conferenceon Internet Technology and Secured Transactions,* Abu Dhabi, pp. 11-14.

[5]. Abdulrahman, Alharthi, Fara Yahya, Robert J. Walters and Gary B. Wills, (2015). "An Overview of Cloud Services Adoption Challenges in Higher Education Institutions", *In Proceedings of the 2nd International Workshop on Emerging Software as a Service and Analytics (ESaaSA-2015),* pp.102-109.

[6]. Dan Lin and Anna Squicciarini, (2010). "Data Protection Models for Service Provisioning in the Cloud", *In Proceedings of ACM Symposium on Access Control Models and Technologies (SACMAT, 2010), Pittsburgh, Pennsylvania, USA.*

[7]. J. Hu and A. Klein, (2009). "A benchmark of transparent data encryption for migration of web applications in the cloud,". *In Proceeding of 2009 8th International conference on Dependable, Autonomic and Secure Computing, Chengdu, China,* pp. 735-740.

[8]. J. Srinivas, K. Reddy and A. Qyser, (2012). "Cloud Computing Basics",. *International Journal of Advanced Research in Computer and Communication Engineering,* Vol. **1**, Issue 5, pp. 3-22.

[9]. S.B. Bele, (2018). "An Empirical Study on 'Cloud Computing". *International Journal of Computer Science and Mobile Computing*, Vol. **7** Issue 2, pg. 33-41.

[10]. B. Sri Varsha *et al.* (2014). "Data Privacy and Protection Schemes in Cloud Computing". *International Journal of Computer Science and Information Technologies*, Vol. **5**(5): 6395-6399.

[11]. Cyber Investigation Challenges Faced by Future Technology Trends. Cloud Security and Forensics. https://raymondleo.wordpress.com/2018/10/17/cyber-risks-in-the-near-future/ (fig.2)

[12]. Issa M. Khalil, Abdallah Khreishah and Muhammad Azeem (2014). Cloud Computing Security: A Survey. *Computers,* **3**(1): 1-35.

[13]. Jitendra Kumar Seth and Satish Chandra, (2013). A Novel Design to Increase Trust in Cloud. *International Journal of Computer Science Issues*, Vol. **10**, Issue 4, No 1, 329-336.

[14]. H. Suo, J. Wan, C. Zou, and J. Liu, (2012). "Security in the internet of things: a review," *In Proceedings of the International Conference on Computer Science and Electronics Engineering (ICCSEE),* pp. 648–651.

[15]. Security for cloud computing ten steps to ensure success version. Available from: http://www.cloud-council.org.

[16]. M. Zhou (2010)."Security and Privacy in Cloud Computing: A Survey," *Proceedings of the 2010 Sixth International Conference on Semantics, Knowledge and Grids-2010*, Pages 105-112.

[17]. Firas A. Abdulatif, Maanzuhiar (2017). *"Cloud Security Issues and Challenges:"* Important Points to Move towards Cloud Storage. *International Journal of Science and Research*, **6**(8): 6-391.

[18] Monjur Ahmed, Mohammad Ashraf Hossain. (2014). "Cloud Computing and Security Issues in the Cloud". *International Journal of Network Security & Its Applications* (IJNSA), Vol. **6**, No.1, 25-36.

[19]. Rohini H. Joshi, Divya P. Rathi, Asma Khan, Medha Jain (2018). "A Survey on Various Security Issues and Challenges to Secure Cloud Computing". *International Journal of Innovative Research in Computer Science & Technology*, Vol. **6**, Issue 3, 31-35.

[20]. Pushpalatha V., Sudeepa K.B., Mahendra H.N., (2018). "A Survey on Security Issues in Cloud Computing", *International Journal of Engineering & Technology*, **7**(3.34): 758-761.

[21]. Nisha, Nasseb Dillon, (2016). "A Novel Approach to Enhance the Security in Cloud Computing using AES Algorithm", *International Journal on Emerging Technologies* (Special Issue on RTIESTM-2016) **7**(1): 76-79(2016).

[22]. Parmar, Sapna and Mangane, Gangambika (2016). "Security Issues in Cloud Computing: A Review". *International Journal on Emerging Technologies (Special Issue on ICRIET-2016)* **7**(2): 269-274.

[23]. Jain, Sweta and Richhariya, Vineet (2017). "Strong Authentication Policy for Cloud Computing Environment Using Modified Kerberos Authentication Protocol. *International Journal of Theoretical & Applied Sciences,* **9**(2): 227-231.

[24]. Thakur, Priyanka and Thakur, Pawan (2016). "Cloud Computing: A Comprehensive View". *International Journal of Electrical, Electronics and Computer Engineering,* **5**(2): 11-15.

[25]. Adeppa, Sudarshan (2015). Data Sharing in Cloud Storage using Identity Encryption Technique. *International Journal on Emerging Technologies,* **6**(1): 115-117.

[26]. Thakur, Pawan and Awasthi, Sachin (2017). Infrastructure as a Service (Iaas) Security Issues in Cloud Computing. *International Journal on Emerging Technologies,* **8**(2): 01-06.

[27]. Pandey, Akanksha and Sharma, Sanjeev (2017). Hybrid Encryption Technique for Security of Cloud Data. *International Journal of Theoretical & Applied Sciences,* **9**(2): 283-287.

How to cite this article: Khan, Sheeba and Sharma, Shailja (2019). Analysis of Cloud Computing for Security Issues and Approaches. *International Journal on Emerging Technologies,* **10**(1): 68-73.