International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 06 | Jun 2023 www.irjet.net p-ISSN: 2395-0072

Analysis of Cloud Computing Security Concerns and Methodologies

Ms. Neetu[1], Mr. Varun Kumar Singh[2]

[1,2]Sunder Deep Engineering College, Dr. A. P. J. Abdul Kalam Technical University, Ghaziabad, India
Email: neetumaurya258@gmail.com, varunksingh07@gmail.com

Abstract - *Utilizing a network of remote computers maintained on the internet to store, manage, and analyse data on demand and on a compensation, basis is the technique of cloud computing. It allows access to a common pool of resources rather than local servers or individual PCs. As it does not acquire the objects physically, it saves businesses time and money on management. Cloud computing is a connectivity technology in which client data is kept and managed in the data centre of a cloud service provider such as Google, Amazon, Microsoft, etc. Cloud computing is an emerging field that is recognised globally. There are certain security concerns while utilising cloud-based services. This research paper examines the fundamentals of cloud computing as well as the security challenges inherent to cloud computing and cloud infrastructure. In addition to analysing cryptographic algorithms with the process, this study addresses the dangers to cloud security. These cryptography algorithms are well-planned and thoroughly examined to improve the performance of existing cryptography systems. The outcome reveals the strategies applicable to real-time encryption. All encryption techniques have proved to have benefits and disadvantages and to be suitable for various purposes.*

Key Words: Cloud Storage, Cloud Performance, Cloud Scalability, Cloud Availability, Cloud Security, Cloud Access Control, Document Sharing

1. INTRODUCTION

The cloud computing paradigm has expanded as a technique that enables ubiquitous, on-demand access to a shared pool of dynamically reconfigurable computing resources, including networks, servers, storage space, applications, and services, with the goal of being rapidly deployed with minimal management effort and service provider interaction. The most common and clear definition of cloud is "a network solution that provides affordable, trustworthy, uncomplicated, and straightforward access to IT resources" [1]. The service-oriented strategy of cloud computing not only decreases infrastructure operating costs and ownership costs, but also improves customer performance and flexibility [13]. NIST has specified the key characteristics and two kinds of cloud computing equipment [13].

a) Deployment Model.

b) Service Model

Deployment Model are classified as [23]:

a) Public

b) Private

c) Hybrid

d) Community

Fundamentally, it relies on the organization's requirement. The classification of cloud Service model computing is as follow [13,23].

Software as a Service (SaaS): Offering Software as a Service to customers according to their needs enables them to utilise the services that are hosted on cloud servers.

Platform as a Service (PaaS): Users are granted access to platforms, allowing them to deploy their own customised software and other applications in the cloud.

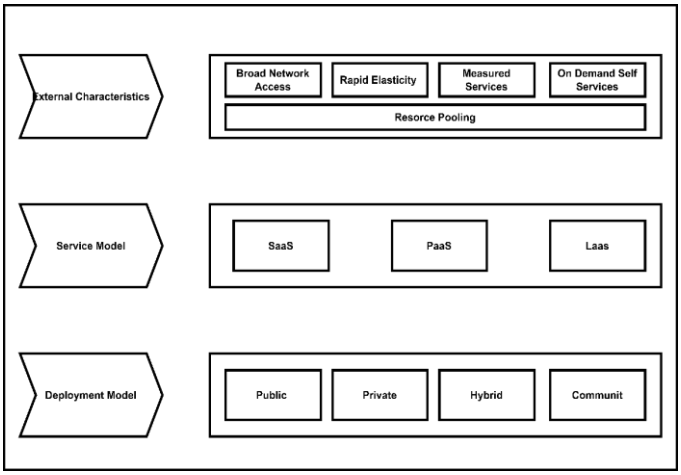

Fig 1. A conceptual view of computing in cloud

IaaS: Infrastructure as a Service The provision of processing, storage, network capacity, and other fundamental computing resources for rent enables customers to manage operating systems, applications, storage, and network connection. Performance, availability, scalability, and data security are the greatest obstacles to cloud adoption [1]. Integrity of data, privacy, and security are necessary concerns for cloud services. Numerous service providers employ diverse

policies, tactics, and procedures based on the following criteria:

• Size of data. • Characteristics of data. • Patterns of data.

2. LITERATURE REVIEW

Diverse resources were examined in order to appreciate the essential ideas of computing in the cloud and keeping safe data in the cloud. This section is devoted to a literature study to establish a foundation for examining various elements of cloud computing. Previous research reveals how to increase cloud computing performance and the number of criteria that affect cloud performance. The direction of this study was determined by the following variables [1]. Diverse resources were examined in order to appreciate the essential ideas of computing in the cloud and keeping safe data in the cloud. This section is devoted to a literature study to establish a foundation for examining various elements of cloud computing. Previous research reveals how to increase cloud computing performance and the number of criteria that affect cloud performance. The direction of this study was determined by the following variables [1].

a. How may Cloud Computing performance be enhanced?

b. Workload analysis and inventive management of cloud resources?

In a previous study, resource allocation was used to boost cloud performance, and data were encrypted using a cryptographic algorithm. Using these current techniques will lower the time required for downloading and uploading files to the cloud, hence improving performance [1]. Scalability, according to previous research, implies that, as the workstation's load increases, the system's performance must remain consistent in all environments without compromising client needs. According to a research, numerous scaling approaches exist to increase the scalability of cloud computing [1].

A. Vertical Scaling.

B. Horizontal scaling.

C. Diagonal scaling.

A second definition of scalability is that several users can exchange their data concurrently without causing a collision. The availability of the cloud is also a concern in cloud computing, according to prior research. It indicates that if a person is utilising the cloud, he should be able to obtain everything he desires. Availability and dependability are closely proportional. Everyone is familiar with this word; if a system is trustworthy, users will utilise it more. There are a variety of issues that can affect the availability of cloud computing.

a. Human errors

b. Software Failure

c. Hardware malfunction

d. Machine migration from one server to another

According to prior research, the following constitute the idea of cloud computing: In cloud computing, security plays a crucial role. It implies that attackers and hackers cannot access user information. Every user was concerned about their data's security, privacy, and secrecy. If there is a system that delivers this functionality robustly, which system will have the most success in the future? All unauthorised users will be denied access to the system. The security criteria need for a successful system is as follow [3, 24].

a. Privacy

b. Confidentiality

c. Unauthorized Access

d. Attacker-Safe

e. Hacker-Safe etc

Every part of cloud computing requires this researcher to have many security methods in addition to the guidelines they can implement from a security standpoint. Previous research provides a respectable introduction to the fundamental ideas of cloud computing. In this study, several essential topics pertaining to instances of applications that may be produced utilising cloud computing and how they might assist the developing world in benefiting from this growing technology are investigated.

Previous research Cloud computing enables Internet access to highly scalable resources. Since the usage of cloud computing by individuals and businesses throughout the globe is increasing rapidly, why haven't data protection issues in cloud computing yet been addressed? Users of cloud services face a significant risk of losing sensitive data. To address user data privacy concerns, they've established a data protection framework. The suggested paradigm for data protection covers difficulties across the life cycle of cloud services. Policy ranking, policy integration, and policy enforcement are the three major components of their suggested system. They have provided a variety of models and studied the attributes of each component. This study examines broad recommendations for evaluating created systems based on this type of paradigm. This study provides access to several models of data security and cost-function definitions [7]. Previous technique created a standard for securing cloud data in transit. For the length of immigration, a standard encryption mechanism has been suggested as a means of protecting sensitive information. Other encryption standard is essential for robust security, although requiring unnecessary processing. The metric presented in their

research provides a balance between the security and encryption overhead [14, 25, 27]. Every part of cloud computing requires this researcher to have many security methods in addition to the guidelines they can implement from a security standpoint. Previous research provides a respectable introduction to the fundamental ideas of cloud computing. In this study, several essential topics pertaining to instances of applications that may be produced utilising cloud computing and how they might assist the developing world in benefiting from this growing technology are investigated.

3. 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 to the cloud because it is inexpensive and secure, yet there is a risk of data loss. There are several opportunities for data loss during data outsourcing, some of which are listed below [4].

1. Malicious Attack

2. Server failure

3. Erasure of data by providers

4. No data backup

5. Loss of the encryption key.

There are several techniques to prevent data loss in cloud computing, including: Utilize a robust API for access control. Analysis of data protection at both runtime and compilation time. Utilize a robust key generation mechanism. Apply appropriate backup and retention strategies.

B. Malicious insiders

Contaminated insiders This might be a DBA (Data Base Administrator), an employee, a partner, etc. of the cloud business who is authorised to view cloud data. These individuals can steal and corrupt information if another firm pays a greater price [27]. Contaminated insiders This might be a DBA (Data Base Administrator), an employee, a partner, etc. of the cloud business who is authorised to view cloud data. These individuals can steal and corrupt information if another firm pays a greater price [27].

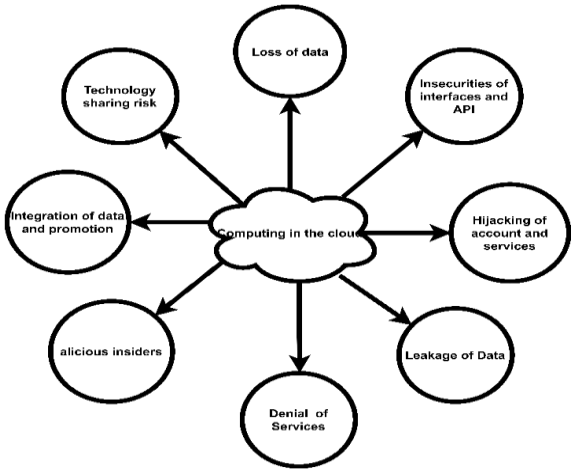

Fig 2: Threats of Security in computing of cloud.

C. Insecurity of interfaces and APIs:

The relationship between cloud service providers and customers must occur via application programming interface (APIs). Therefore, these APIs must be protected to prevent unwanted access.

D. Hijacking of account and service

Every cloud user has an internet-based account (bank account, e-mail account or social media account). Account hacking can result in catastrophic data loss for users Integrity and standing.

E. Leakage of data

The cloud service enables any user to move and access data from any location in the globe, therefore there is a possibility of data leakage. This demonstrates the vulnerabilities of cloud security and cloud's physical transport infrastructure.

F. Denial of service

In cloud computing, availability is a crucial factor; hence, many businesses want their systems to be always accessible. Another aspect of cloud computing is the sharing of resources among users. If an attacker uses up all the computational resources in the cloud, then no one else may utilise those resources; this is known as a denial of service. When this occurs, user access to their resources will be sluggish, and cloud availability will be affected.

G. Technology sharing risk.

The foundation of infrastructure as a service is shared infrastructure. This service was not built with a multi-tenant

architecture; hence this architecture is essential for mitigating this risk.

H. Integration of data and protection

Many organisations must ensure that their data is protected between the end user and the cloud data centre since unprotected data is more susceptible to transmission interruptions [12].

4. REQUIREMENTS FOR SECURITY IN CLOUD COMPUTING

The ISO (International standard organisation) Information Security standard should include several suggested elements. In addition, cloud computing security should be directed in this manner for it to be an outstanding and secure technological solution.

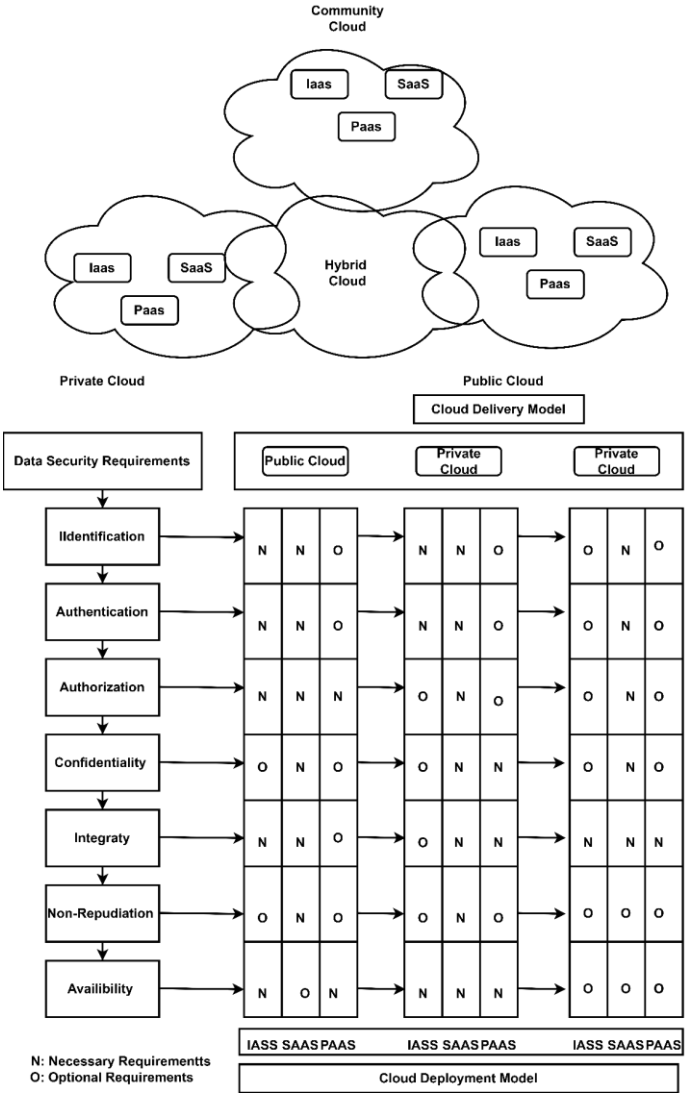

Fig 3: Security requirements in computing of cloud

Figure 3 depicts information security needs that are intimately coupled with cloud deployment and delivery methods. [13]. In Fig. 3, the various cloud delivery models and deployment models are compared to the security needs for information, where "N" denotes mandatory requirements and "O" denotes optional requirements.

However, further research is necessary to determine the best balance required to secure cloud computing. The context of Figure 3 should be considered when judging the security level. The security needs of the cloud will be discussed in the context of cloud computing.

a. Identification

b. Authentication

c. Anonymity

d. Authorization

e. Confidentiality

f. Integrity

g. non-repudiation

h. Availability

5. SECURITY ALGORITHMS AND ITS PARAMETERS

In cloud computing, data security encompasses not just encryption but also several additional procedures. Risk of data loss is contingent on the following elements.

A) Reset of data: Clearing of data When a cloud user accesses their data through the internet, this is referred to as the Reset of data. This procedure operates on live data, as opposed to data backups.

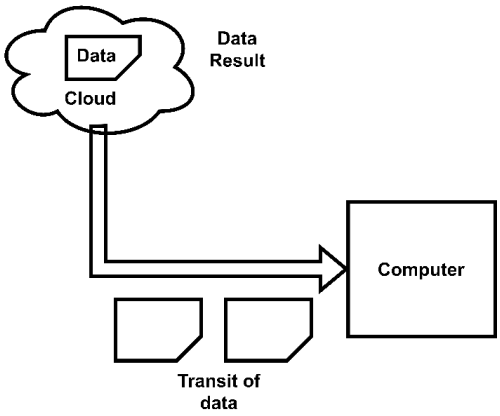

Fig 4 data at reset and transit

B) Transit of data

The passage of data in and out of the cloud is referred to as data transit. When users upload their data to the cloud, this is

referred to as data transit. To prevent this, it is now time for the hacker to steal user data. The procedure of encryption and decryption should be adopted [18]. Encryption and decryption play a crucial part in cryptography techniques. There are now two types of cryptography methods used for data encryption and decryption: 1. ciphering using a Symmetric key Encryption with an asymmetric key.

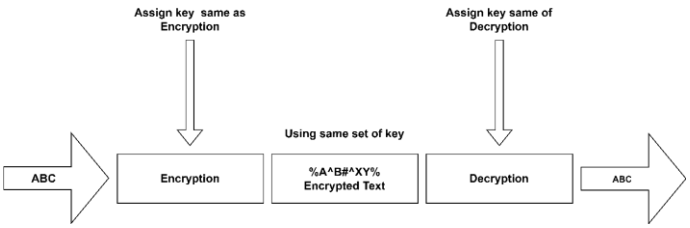

Fig 5. a basic cryptography approach

Encryption using an asymmetric key, finds the researcher, is the best solution for data protection. In this method, both private and public keys will be utilised to encrypt and decode data between sender and recipient. Various cryptography algorithms are now employed for data encryption. Using cryptography, the level of security will be strengthened, along with the following critical parameters: 1. Level of data protection 2. Contents' authenticity User identification 4. Availability. Encryption using an asymmetric key, finds the researcher, is the best solution for data protection. In this method, both private and public keys will be utilised to encrypt and decode data between sender and recipient. Various cryptography algorithms are now employed for data encryption. Using cryptography, the level of security will be strengthened, along with the following critical parameters: 1. Level of data protection 2. Contents' authenticity User identification 4. Availability.

Cryptography is the technique of concealing original information during the transmission of plaintext. The Method of C. Hash algorithm: The mathematical function is the hash function. The hash function converts the supplied text to an alphanumeric string. This method also assures that no two strings may provide identical alphanumeric output. The hash function is a straightforward mathematical operation, as given in [9] below. F(x) = x mod 10 ..... (1)

All the above-mentioned approaches and techniques are frequently employed for encrypting cloud data to maintain data security. These methods may differ depending on the circumstances. Whatever method is employed. These strategies are highly recommended for ensuring the security of data in both private and public clouds.

6. COMPARISON OF CRYPTOGRAPHIC ALGORITHMS

The table 1 provides a comparison of all previously described algorithms from the reference section. Based on this comparison, the following parameters are compared to determine the optimal security algorithm:

1. Name of the algorithm
2. Key and block sizes utilised in the algorithm
3. Round
4. Structure
5. Flexibility
6. Security features

Algorithm Name	Key Size(bits)	Block Size (bits)	Round	Structure	Flexible	Key Feature
DES	64	64	16	Festiel function (F)	No	Not enough robust
E-DES	1024	128	16	Festiel function(F)		Excellent Security and swiftness
T-DES	112,168	64	48	Festiel function(F)	Yes	Adequate Safety and Rapid
T-DES	112,168	64	48	Festiel function(F)	Yes	Adequate Safety and Rapid
RSA	1024 to 4096	128	1	Public key algorithm	No	Excellent Safety and low speed
BLOW FISH	32-448	64	16	Festiel function(F)	Yes	Fast Encryption in SSL
DSA	Variable			Public key algorithm	Yes	Excellent Security and swiftness
RC6	128 to 256	128	20	Festiel function(F)	Yes	Good Security
AES	128,192,256	128	10,12, 14	Substitution Permutation	Yes	Security is superior. It performs the best in terms of security and encryption.

A further cloud-related method is the Attribute-based Encryption Algorithm (ABE). It contains access policies for the attribute set to identify the owner who wants to share their data, and encrypted data and the encryption key are kept on cloud servers, which is beneficial for security. In order to increase the security of the data on the servers, the AES algorithm is employed. First, data is encrypted with the AES algorithm [21], then with the ABE algorithm.

7. RESULT AND DISCUSSION

The comparisons of the algorithms are based on the following criterion to determine which security algorithm provides the best cloud computing security: 1. Key size of the block 3. Round 4. Structure 5. Adaptability

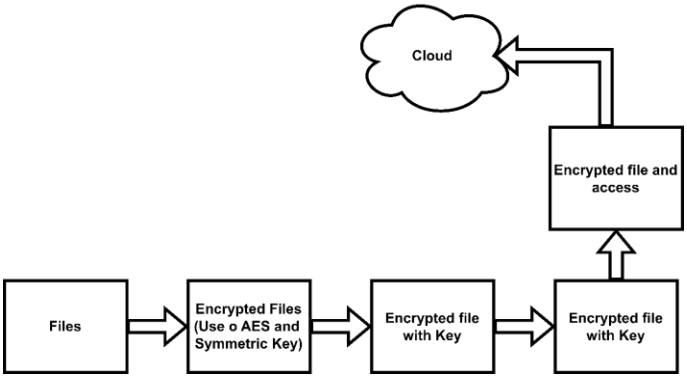

Fig: 6 Encryption process of files with use of AES and ABE algorithm

So, the researcher concludes his survey based on the aforementioned criteria. The algorithm [18] that has been applied to DES, EDES, RSA, Blow fish, DSA, RC6, AES, and ABE has the quickest encryption time, speed, and flexibility. The results also demonstrate that the AES algorithm provides the highest levels of security, flexibility, and encryption performance. It is the most effective in comparison to others. Researchers conclude that AES with ABE Algorithms is most appropriate for future work [13] since this approach provides double encryption to give the highest level of security in cloud computing paradigms. Figure 6 depicts the full encryption procedure using AES and ABE [18].

8. CONCLUSION

This paper provides a quick introduction to the most major cryptographic algorithms used in the process, as well as a description of the dangers to cloud security. These cryptography algorithms are well-planned and thoroughly examined in order to improve the performance of existing cryptography systems. The outcome demonstrates the relevant strategies for real-time encryption. All encryption techniques have proved to have benefits and disadvantages and to be suitable for various purposes. The comparison between Symmetric and Asymmetric algorithms demonstrates that Symmetric algorithms are more efficient. Based on prior research and a comparison of potential results, researchers conclude that AES is the most dependable algorithm in terms of encryption speed, decoding difficulty, key length, structure, and adaptability. If the researcher will combine AES and ABE (Attribute based encryption). It will yield the finest results in terms of security for cloud computing paradigms.

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. [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/cyberrisks-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.cloudcouncil.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.