A Framework of Enhanced Cloud Data Security and its analysis

Ashish A. Patokar Dr. V. M. Patil

Abstract- **Cloud Computing is the innovation over which users share data, services and resources using the networks. The thousands of users can use the same network for data transferring, due to this the data becomes further accessible various types of security attacks from the burglar (intruders). Cloud storage mainly provides the services for small and large scale organizations for storing data on the servers and maintain that data.**

The data stored on the cloud may be accessed by some unauthorized users so it creates the major problem of insecurity for data stored on cloud. To avoid such types of problem proposed a framework and different types of cryptographic schemes i.e. encryption of data and retrieval of that data in a adequate way. This paper produce approaches for data security attaining since storing it in cloud in proper way and decreasing the space required for storing the data on cloud. Compared the cryptographic algorithms by using various parameters such as security, key size, block size, attacks etc.

Keywords- **CLOUD COMPUTING, DATA SECURITY, AES, DES, RSA, TDES, BLOWFISH, AND IDEA,**

1. INTRODUCTION

Cloud Computing is flexible computing i.e. in cloud computing users can call the resources as per the need of users demand and resources can access from any side of the world using the network and only the authorized users can access these data. Some cloud storage are payable as per the users requirement for storage and some are free such as Amazon, drop box and Google drive etc[1,2]. Cloud computing provides three types of services such as IAAS (Infrastructures as a Service), PAAS (Platform as a Service), and SAAS (Software as a Service). IAAS provides business access to important web architecture like server connection and storage space and managed the internet infrastructure. PAAS can be expand and made accessible all over. Example of PAAS such as Google app engine [3,4]. The PAAS allow the lot of scalability. In SAAS record is completed based on the number of users and size of resources exhaust.

Cloud computing has deployment models such as public, private, hybrid and community. Due to the huge amount of usage of the cloud services pass on security to the user's data has more problematic in novel years. In the broad networks there are large chances of data loss. Providing data security to users has rise as main area of interest to the various cloud providers services. Two types of the cloud security such as Cloud storage security and cloud data security.

a) Cloud data security:- Providing data security is the key challenges in the cloud. The data security implemented using various encryption and decryption methods with providing security to data[2,4]. The users used the privacy and confidentiality of data techniques and the data is accessible by the authorized users and the data on the cloud should be confidential.

b) Cloud storage security:-
In cloud storage users can upload their data into the cloud [2,4]. Cloud storage is beneficial and gives user access to their data anywhere; at any time cloud storage security is excellent concern for organizations' IT and security departments.

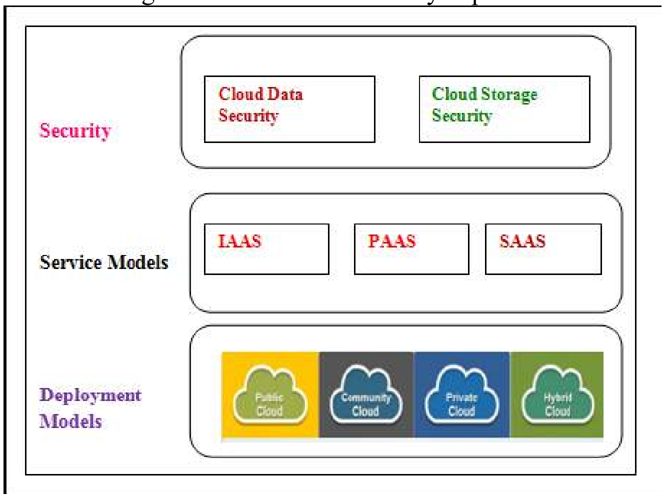

Figure:- Framework of cloud computing

II. LITERATURE SURVEY

Akhil M.. et.al discussed the encryption algorithm such as AES is designed in both hardware and software. AES encryption is used for the data transfer and it provides efficient AES based on encryption techniques to cloud user data[1]. Ankit Grover et. al focused on the securing data before storing on the cloud as well as reducing the amount of space required for storage and the cloud storage helps for small and medium scale industries to minimize their investment on storage server and maintains that server also discussed the serurity issues[2]. Mrinal kanti sarkar et. al. discussed the data security overview and propsed the framework based encryption. Also discussed the characterstics, benefits and security issues and cloud services. From the performance analysis proposed model is feasible, efficient and scalable[3]. S. Rajeswari et. al.focussed on the data and storage security in cloud computing and also compaired the existing work along with the strength and weakness of each access and also discussed the security classification in cloud[4].K. Priya et. al. discussed the data security and confidentiality in public cloud storage by extended QP Protocol. In the proposed work developed extended QP Protocol to achieve the security of expanded data and the data owner has more controls on data and there is no commitment to check the data later encryption and the proposed techniques achieve the target of security and high efficiency[5]. Ronald S. Cordova et. al. focused on the commarative analysis on the performance of selected security algorithm in cloud computing algorithms such as AES, Blowfish and RSA and the result shows that time efficiency ratio for Blowfish is higher to various data loads and memory size in comparison to RSA and AES[6]. Zhang Jing et. al. focused on cloud storage encryption security analysis. and the safety model with new encryption strategy for cloud storage and also resolve the models security[7]. D.I. George Amalarethinam et. al. discussed the enhanced RSA algorithm with varying key size for data security in cloud and the encryption is done by using the various types of symmetric or asymmetric key algorithm such as AAES, RSA, DES, 3DESa and Blowfish. The proposed algorithm reduces the encryption and decryption time by breaking the file into blocks and increasing the key size and also the security level of algorithm can approved using statical methods [8].Lalitha V.P. et. al.focussed on data security in cloud. From the data security and performance analysis the work is extremely efficient and by pass unauthorized users by accessing the data and it reduce the number of hackers to hack the resources[9]. Artan Luma et. al. discussed the strategy of cryptography for the proposed model of security in cloud computing and analysed the level of support to the proposed model for security in cloud and security in cloud controlled by the IT Specialist[10]. T. Subha et. al. proposed efficient privacy preserving integrity checking model for cloud data storage security and proposed the solution to protect the privacy of user data from the alive attackers and produce a techniques to sign the data by adopting digital signature algorithm in an organization with certificates[11]. Diao Zne et. al. discussed study on data security policy based on cloud storage and advantages and characterstics of cloud computing, development of cloud storage and security risk analysis of user data [12]. Kajal Rani et. al. discussed the cloud storage security issues and challenges and try to solve the problem associated to existing security algorithms and appliance superior version of existing security algorithm. The security can improve using steganography encryption and decryption techniques for improved security of cloud[13]. B.L. Adokshaja et. al. proposed efficient and securable privacy preserving public auditing scheme and use the AES algorithm for encryption. The proposed scheme consist of three essential entities i.e. data owner, cloud storage server and TPA. The data use is responsible for splitting the files into blocks and encrypting the blocks by using the AES algorithm and achieving hash value for each block and check the file is corrupted or not[14]. L.Arackiam et. al. proposed a new cryptographic techniques which is adopted to address to address this problem. The encrypted data are stored on storage servers and the secret keys are received by the data owner, approach to the user is permitted by issuing the analogous data decryption keys and the encryption obfuscation techniques used to increase the data confidentiality [15]. Shenling Liu et. al.focussed the improve security and availability for cloud storage . Designed efficient data fragment algorithms based on IDA(Information Dispersal Algorithm), IDA design a file encoding and decoding and propose a simple and efficient scheme for cloud storage[16].

Naveen Ghorpade et. al.proposed efficient and secure way to share the data and this system will supply superior security while sharing and transmitting the data in the cloud. Suppose the data is stored in any datacenter which is located in remote places user need not concern[17].Prakash G.L.et. al. propose efficient data encryption to encrypt conscious data before sending to cloud server from the security and performance analysis the proposed method is really efficient than the existing methods[18]. Saikumar Manku et.al. focuses on designed and analyzed a Blowfish encryption algorithm for information security and from the simulation results shows that the encryption and decryption done through blowfish algorithm [19]. S. Artheeswari focused on network security, computer security and information security and IDEA works in cloud security[20]. Karthik .S et. al. focused a technique for secret communication by using cryptography and performance comparison between the encryption algorithms AES, DES, 3DES and Blowfish[21].

3. EXISTING TECHNOLOGIES

The technologies are used in cloud data storage security is as fallows

a) AES Algorithm

AES is the efficient and widely supported on both hardware and software. AES is highly difficult for hackers to get the actual data when encrypting by AES algorithm. It is Block cipher encryption algorithm published by NIST (National Institute of Standards and technology. AES uses three types of key size for encryption and decryption data such as 128, 192 and 256 bits and the key size decides the number of rounds[1,6]. The operations perform on the AES in terms of bytes rather than bits.

b) DES Algorithm

DES is symmetric key block cipher. The block size of DES is 64-bit and key length is 64-bit. DES is developed by IBM in 1970s. The DES algorithm isinsecure due to its 56-bit key size being too short and implemented on hardware technology [21].

c) TDES Algorithm

TDES is a symmetric key block cipher which applies the DES cipher algorithm three times to individual data block. The key size of TDES is 168, 112 or 56- bit and block size of TDES is 64-bits. TDES published in 1998. TDES is more secured as compared to DES but the encryption process of TDES is slower than single DES [21].

d) RSA Algorithm

RSA used for encrypt and decrypt of messages and widely used for secured data transmission. RSA is asymmetric cryptographic algorithm means used two different keys for encryption and decryption [6]. The key size can be mixed to produce the encryption process strong due to this it is difficult for hackers to intrude the data.

e) Blowfish Algorithm

Blowfish is a symmetric key block cipher and invent in 1993 by Bruce Schneier. Key size of Blowfish is 32-448 bits and block size 64 bits. The algorithm is herewith placed in the public domain and freely used by anybody [6,19].

f) IDEA Algorithm

In cryptography, IDEA (International Data Encryption algorithm), known as improved proposed encryption standard (IPES). The key size of IDEA is 128 bits and Block size is 64-bits. IDEA is symmetric key block cipher and developed by James Maassey and Xuejia Lai in 1991[20].

4. Conclusion

This paper presented an overview of cloud data security and proposed framework. For the cloud data security an effective and efficient strategy used for the encryption. For the data security different types of cryptographic algorithm are used such as AES, DES,

TDES, RSA, IDEA and Blowfish and compared this algorithm by using various parameters such as security, key size, rounds, block size. From the above parameters conclude that the security of AES

algorithm is strongest as compared to other algorithm.

REFERENCES

1. Akhil K.M., Praveen Kumar M. and Pushpa B. R., "Enhanced Cloud Data Security Using AES Algorithm", International Conference on intelligent computing and control, 2017.

2. Ankit Grover and Banpreet Kaur, "A Framework for Cloud Data Security", 2016 IEEE, ISBN:978-1-5090-1666-2, 2016, pp 1199-1203.

3. Mrinal Kanti Sarkar and Sanjay Kumar, "A Framework to ensure data storage security in cloud computing", 2016 IEEE, ISBN: 978-1-5090-1496-5/16, 2016.

4. S. Rajeswari and R. Kalaiselvi, " Survey of data and storage security in cloud computing", 2017 IEEE, ISBN: 978-1-5090-6480-9/17, 2017,pp 76-81.

5. K. Priya and J. ArokiaRenjit, " Data security and confidentiality in public cloud storage by extended QP protocol", 2017 International conference on computation of power, energy, information and communication(ICCPEIC), 2017 IEEE, ISBN:978-1-5090-4324-8/17,pp 235-240.

6. Ronald S. Cordova, Rolou Lyn R. Maata, Alrence S. Halibas, Rula Al-Azawi, "Comparative analysis on the

performance of selected security algorithms in cloud computing", 2017 IEEE, ISBN:978-1-5386-0872-2/17,pp 1-4.

7. Zhang Jing, Wang Jinsu, Zheng Zhuangfeng, Zhao Chongan, "Cloud storage Encryption security analysis",2016 International conference on cloud computing and Big data analysis, 2016 IEEE, ISBN:978-1-5090-2594-7/16, pp 62-65.

8. D.I. George Amalarethinam, H.M.Leena, "Enhanced RSA Algorithm with varying key sizes for data

security in cloud", world congress on computingandcommunivcationTechnologies(WCCCT), IEEE 2017, pp 172-175.

9. Lalitha V.P. and Sagar M. Y., Sharanappa S, Shredar Hanji, Swarup R, "Data security in cloud", International conference on energy, communication

10. Dhurate Hyseni, Besnik Selimi, Artan Luma and Betim Cico, "The strategy of cryptography for the proposed model of security in cloud computing", 2017 IEEE, pp 24-28.

11. T. Subha and S.Jayashri, " Efficient privacy preserving integrity checking model for cloud data storage security", 2016 IEEE eighth international conference on advanced computing, pp 55-59.

12. Diao zhe, Wang Qinghong, SU Naizheng and Zhang Yuhan, " Study on data security policy based on cloud storage",2017 IEEE 3rd International Conference on Big data security on cloud, pp 145-149.

13. Kajal Rani, Raj Kumar Sagar, "Enhanced data storage security in cloud environment using encryption, compression and splitting techniques", 2017 2nd International conference on telecommunication and networks.

14. B.L.Adokshaja, S.J.Saritha, "Third party public auditing on cloud storage using the cryptographic algorithm", IEEE 2017,978-1-5386-1887-5/17,pp 3635-3638.

15. L.Arockiam, S. Monikandan, "Efficient cloud storage confidentiality to ensure data security", 2014 International conference on computer communication and informatics, jan 03-05 Coimbatore, India, 2014.

16. Shenling Liu, Chunyuan Zhang, Le Bo, "Improvesecurity and availabilityforcloud storage", 978-1-5090-1256-5/16, 2016 IEEE, pp 382-387.

17. Naveen Ghorpade, Vijaykarthik. P, Dhananjaya. V, Balasubramani. R, "Towards achieving efficient and

secure IEEE, ISBN:978-1-5386-0872-2/17,pp 11-14.

18. Prakash G L, Manish Prateek, Inder Singh, "Data encryption and decryption algorithms using key raotations for data security in cloud system",978-1-4799-3140-8/14, 2014 IEEE, pp 624-629.

19. Saikumar Manku & K. Vasanth, "Blowfish Encryption Algorithm For Information Security", ARPN Journal of Engineering and Applied Sciences, Vol. 10, No. 10, 2015, pp 4717- 4719

20. S. Artheeswari, RM. Chandrasekaran, "International Data Encryption Algorithm (Idea) For Data Security In Cloud", International Journal of Technology and Engineering System (IJTES), Vol 8. No.1 – Jan-March 2016 Pp.06-11.

21. Karthik .S, Muruganandam .A, " Data Encryption and Decryption by Using Triple DES and Performance Analysis of Crypto System", IJSER, Volume 2 Issue 11, November 2014, pp 24-31.