Research Article

A Data Security Model for Improving the Privacy Cloud Computing

Pratibha Mundra[1], Devender Kumar Dhaked[2], Dr Subhash Chandra Jat[3]

[1]M Tech Scholar, Department of Computer Science, Rajasthan College of Engineering for Women Jaipur, India.
[2]AssistantProfessor, Departmentof Computer Science,Rajasthan College of Engineering for Women, Jaipur, India.
[3]Associate Professor, Department of Computer Science, Rajasthan College of Engineering for Women, Jaipur, India.

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 20 April 2021

Abstract: The category of services provided to clients, such as the storage of information systems, the network, and hardware, is cloud computing. Cloud storage can be accessed conveniently anywhere since the cloud operates remotely. The Cloud provider uses the computing service. Data in the cloud is not safe since private data can be accessed by an unauthorized user. Therefore, it uses a distinct encryption method to secure the data to provide data protection. This paper explores data protection in cloud computing. It is the analysis of data in the cloud & aspects of safety-relevant to it. In this research, we have used two data encryption and decryption techniques for a better result than the previous research work which had some limitations. This algorithm is faster and more robust than that of the RSA-BlowFish.

Keywords: Cloud computing (CC), Data security, RSA-AES, Twofish, encryption, decryption, Python.

I. INTRODUCTION

The future of the next-generation computing paradigm in Cloud Computing is considered to allow convenient network access to shared computing resources on request. Virtualization, service-based computing, utility computing, load balance, multi-lease setting, the capability to make payments by using computing resources, lower high capital costs and operating expense are the innovations behind the achievement of CC [1].

While cloud computing data protection has many advantages, anonymity, honesty, and confidentiality are some most important obstacles to the broad acceptance of CC [2].

Cloud users need protection from tampering or unauthorized access to their sensitive data. The cloud infrastructure stage is exposed from time to time to interior & exterior security threats, different failures, and safety threats for cloud services. The alliance mentioned the case of the wired magazine writers Mat Honan, whose Gmail, Twitter, and Apple accounts had been breaking down in the summer of 2012, and who had removed all the childhood photos of his 18-month-old daughter [3].

To preserve data privacy, private protection, and faith in the cloud world, there is a significant need to resolve data security concerns. [4]. In recent times, numerous algorithms & protocols (MD5, RSA, PDP, PoR) were developed and applied to protect privacy, credibility, and confidence issues. [5], [6].

The goal of this research is to protect data against various threats towards data protection, like data privacy, data integrity & cloud-based information confidence. The paper contains the encryption of sensitive data that frightens potential users and the business to use their sensitive data through cloud storage services.

The paper will support and inspire researchers to explore security strategies that help the trustworthy cloud environment. [7]. The data protection framework is designed to provide the cloud user with improved protection. Data authentication at different levels contributes to improved data protection. The implementation of forensic VMs & many encryption methods helps successful data protection control, data confidentiality, data integrity & trust.

II.LITERATURE REVIEW

The connected work on data protection is explained in this section. Various scholars have previously suggested a few methods and models for ensuring compliance with data security. In this Paper the author [8] suggested an adaptive privacy scheme, which encrypted some of the highly sensitive with a predefined privacy policy. The author in the paper[9] suggested anonymity-based cloud computing algorithms process microdata, which would also give the unidentified data to the cloud provider for extra info. In paper [10] Author also provides temperature proof encryption co-processor configured by a trusted third party. Tempe proof makes a stable, logically, and physically protected execution domain in cloud computing possible.

The author addressed the RACS technique in paper [11], which is redundancy of cloud storage techniques that

avoids supplier lock-in and decreases costs. The writer of the paper [12] obtainable data security manager for data taken or changed as well as supporting CC provider to comply with privacy rule through the definition of the private information protection architecture. The above methods are good for maintaining data protection, but efficiency is compromised elsewhere.

The author suggests a public audit method in paper [13] and retains cloud data. The author addressed the public accessibility for the safety of cloud-saved data. 3RD party auditors (TPA) speak about auditing cloud-based data storage without any extra online burden for the cloud customer.

This [14] model has implemented an efficient data integrity assurance system without allowing third parties to infringe on data confidentiality. model is evaluated & effects of integrity & data protection algorithms are explored, wherever findings show that the model performs effectively in terms of data protection and latency. Because of Amazon S3's limitation on uploading big files which can be solved through multi-part uploads, large files are split into smaller chunks and the file can be uploaded individually.

The model [15] proposed offers multi-level encryption that is not easy to break because an unauthorized user will need the encryption keys and decryption keys to access or acquire data that is automatically a hard job without a valid key to execute. It is expected to deliver more data protection for cloud storage by using multi-level encryption than using single-level encryption.

A. Data Security in Cloud

Various methods have been used to process and secure sensitive data in conventional data protection. The encryption technique was widely used for data protection to protect outsourced data. It is not very cost-effective to download all data and to decrypt it at local sites as a wide bandwidth is essential for the decryption at local processing sites. Another big security problem for outsourcing information is evidence of ownership that stops the customer from being exposed to his information. the remote service provider collects external data but the owner doesn't know how to analyze information. Disaster recovery is another challenging security problem. It depends on the data handling of a service provider in the event of a disaster that occurs due to cloud limitations in the event of remote drive failures [2]. The traditional security techniques are not as applicable as the security mechanism decreases the data stored every day. The provider processes important and confidential information for the user, so that data confidentiality, privacy, and trust are not always guaranteed [16].

III. RESEARCH METHODOLOGY

A. Problem Statement

AES algorithm is not good in security and performance.

Due to an accumulator that repeated thousands of bits, the encryption method provides a simple difference in time between the encryption and the decryption, thereby showing the difference.

AES 128-bit secure encryption may not be ideal for big data and other new, major applications such as secure cloud storage. These large-data applications may therefore require a bigger mathematical and structural basis algorithm with a greater range of trading speed.

B. Proposed Methodology

Cyber attackers can now quickly access the stored data. When private information is stored in personal cloud storage, a third party is automatically trusted to make data protection a cloud issue. Information can be retrieved by any distributed or linked cloud services when saved in any business or consumer cloud. Verification of such data storage becomes a necessary duty for safe communication here.

The most trusted model, the proposed model, reliable, safe block ciphers, namely AES and RSA, can help to give individuals more protection in the data stored and thus to enhance their security, through many levels of encryption and decryption processes.

C. RSA Algorithm

RSA's algorithm is named after the 1977 [RIVE78] inventor Ron Rivest, Adi Shamir & Len Adleman. RSA is applied to the public key cryptography algorithm worldwide. You may use it to separate encryption messages without a requirement for a private key.

RSA algorithm may be applied for both public & digital signatures. It is covered by the complexity of big integer factoring.

Party A sends an encryption message to Party B without previous secret key exchange. An only usages B's public key to encryption message & B usages personal key, that he knows only. To sign A with a private key,

RSA may also be used to sign the message & B with a Public key to validate it.

a) Algorithm for Key Pairs Generation by RSA

I/P: kbit length.

O/P: The main pair of RSA ((N,e),d)) with N being a module of 2 primes of the same form (N=pq) that is of no more than k bits in length.

And d is that ed um 1.mod(p−1)(q-1). and d is a private exponent.

1. Select a number of e from 3,5,17,257,65537
2. reiteration
3. p ← genprime(k/2)
4. until (pmode)≠1
5. repeat
6. q ← genprime(k - k/2)
7. until (qmode)≠1
8. N ← pq
9. L ← (p-1)(q-1)
10. d ← modinv(e, L)
11. return Value Of (N,e,d)

Encryption: Sender A does the following: -

1. Get public key for receiver B (n,e).
2. Plain text message is interpreted as a positive mm integer with 1<m<n.
3. Calculates ciphertext c=memodn.
4. Sends ciphertext c to B.

Decryption: Recipient B does the following: -

1. Usages his private key (n,d) to calculate m=cdmodn.
2. Extract plaintext from mm message.

D. Blowfish

The blowfish is a symmetrical block chip, which can be used to substitute DES for drop-in. It has a variable-long 32-bit to 448-bit key that is both suited for home and export. In 1993, Bruce Schneier created Blowfish for existing encryption algorithms as a simple and free option. It has since been extensively studied and steadily gained recognition as a good encryption algorithm. Blowfish is free for all purposes and is unpatented and license-free.

It offers a good software encryption rate and has not been found to date to be effective.

Schneier developed Blowfish as an algorithm for general purposes, designed as an alternative to aging DES & without any difficulties and limitations with other algorithms. It is a Feistel 16-round cipher with tall, S-boxes. It is identical to CAST-128 with fixed S-boxes on the structure.

The encryption routine of Blowfish is shown in Figure 1. Every line is 32 bits. Five main arrays are available: one 18 P-array (identified as P, to avoid confusion) and four 256 S-boxes. The diagram includes two subkey-arrays (S0, S1, S2 & S3).

TABLEI
EVERY ROUND R CONSISTS OF 4 ACTIONS

Action 1	XOR left half of the r^th P-array input data (L).
Action 2	Using XORed details for the F-function of Blowfish
Action 3	XOR output of F function by the right half of the data (R)
Action 4	Swap L & R

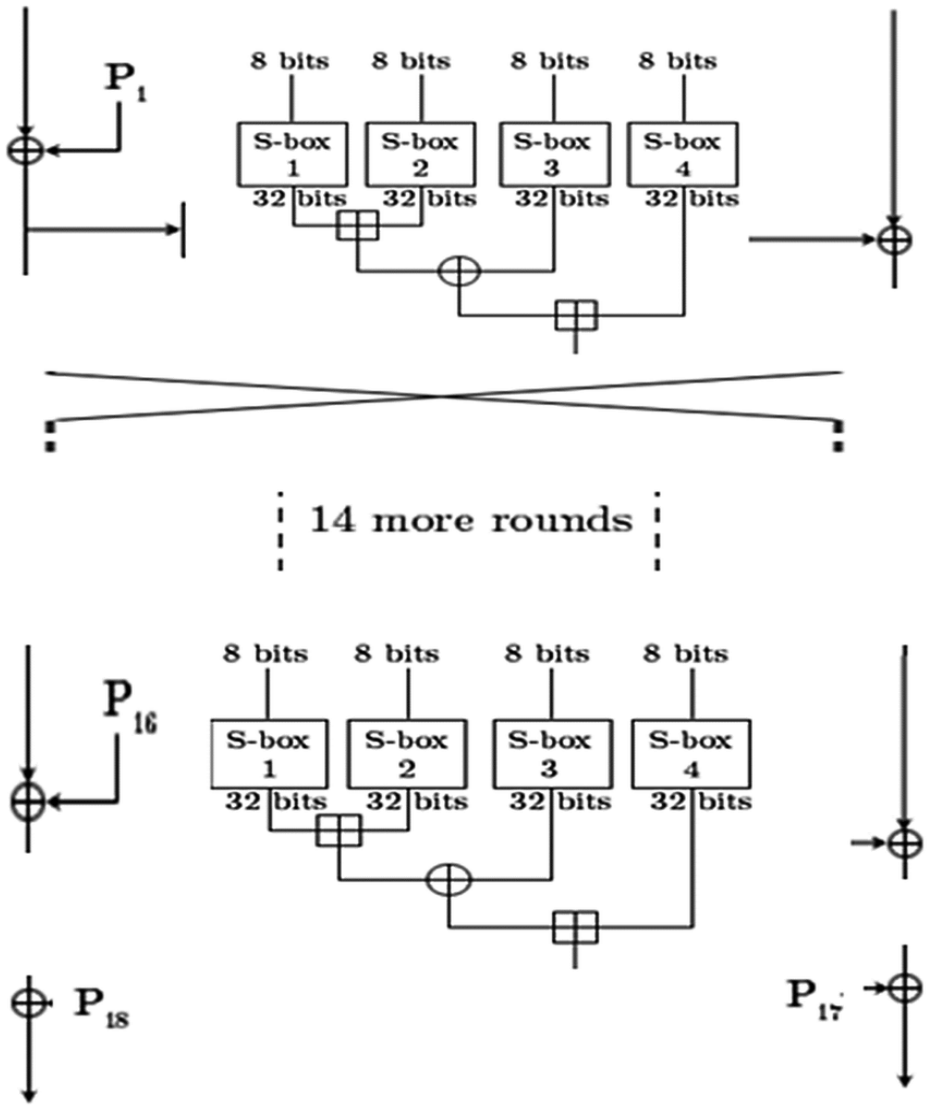

Fig.1. Data flow Diagram of the Feistel structure of Blowfish

32-bit i/p of this F-function is separated into four 8-bit quarters and used as input in the S-boxes. 8-bit i/p & 32-bit o/p are supplied in S-boxes. Outputs for the final 32-bit output are applied modulo 232 & XORed (see an image in the upper right corner).

Drop the final swap & XOR L with P18 & R with P17 after the sixteenth round (output whitening).

Decryption is like encrypting, except P1, P2,..., P18 is applied in reverse order. The fact that xor is switchable and associative is not that easy.The reverse encryption order as the decryption algorithm is a common mistake (i.e. first XORing P17 as well as P18 to the ciphertext block, then the reverse order is used for the P-entries).

IV. RESULTS AND DISCUSSION

This research work is done in Python 3.6. The figures below provide a brief overview of the new & most widely applied lightweight encryption algorithms for IoT systems, namely RSA and Blowfish. Since, in previous papers, the AES algorithm, i.e. current works, has been used. In the above model, the Blowfish algorithm has been used instead of AES, as it has proved to be safer, efficient, and faster than the AES algorithm used in previous studies.

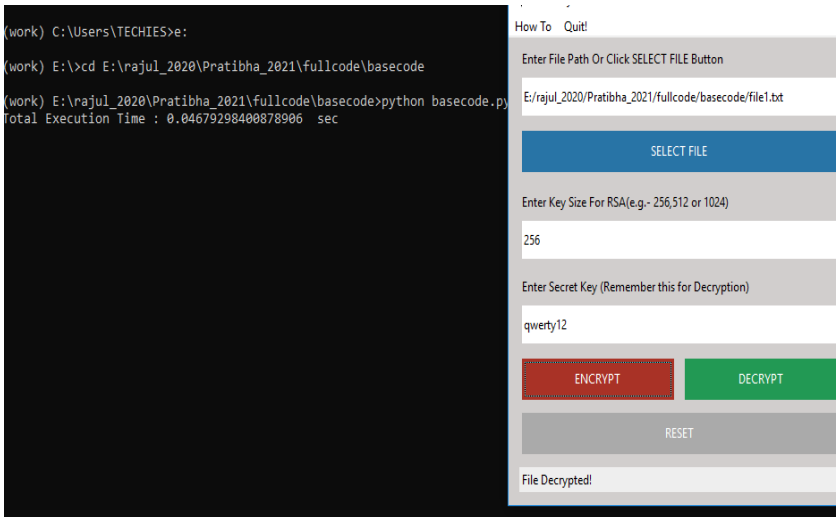

Fig.2.The 256-size key generation in RSA-AES

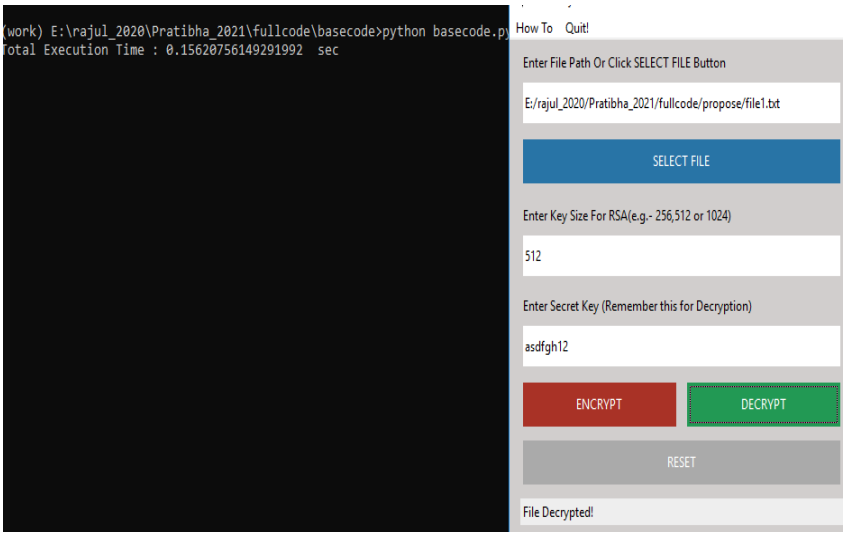

Fig.3.The 512-size key generation in RSA-AES

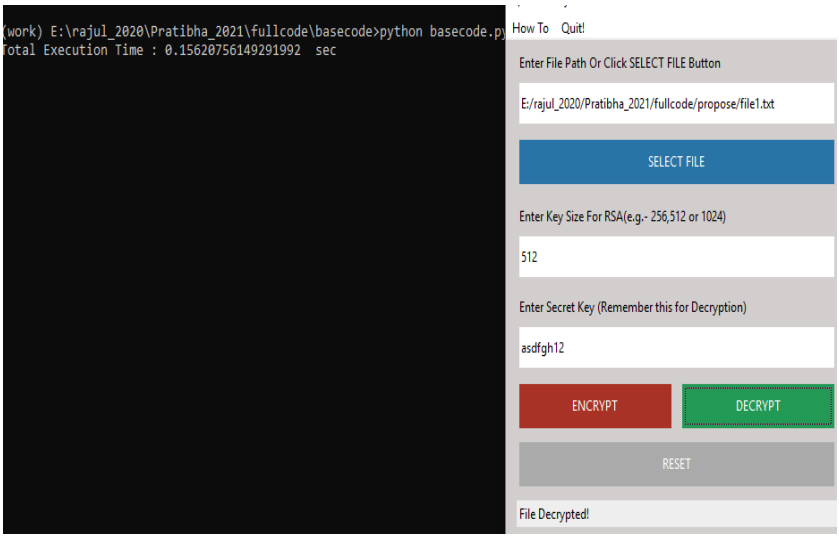

Fig.4.The 512-size key generation in RSA-AES

Also, it has been found that Blowfish is much faster than AES that has been used in research previously performed about data protection in the cloud, but my model is AES, in terms of reliability, increased storage space, faster data extraction & reduced time consumed. Also, the Blowfish algorithm is much faster than AES, which is also used in my proposed model.

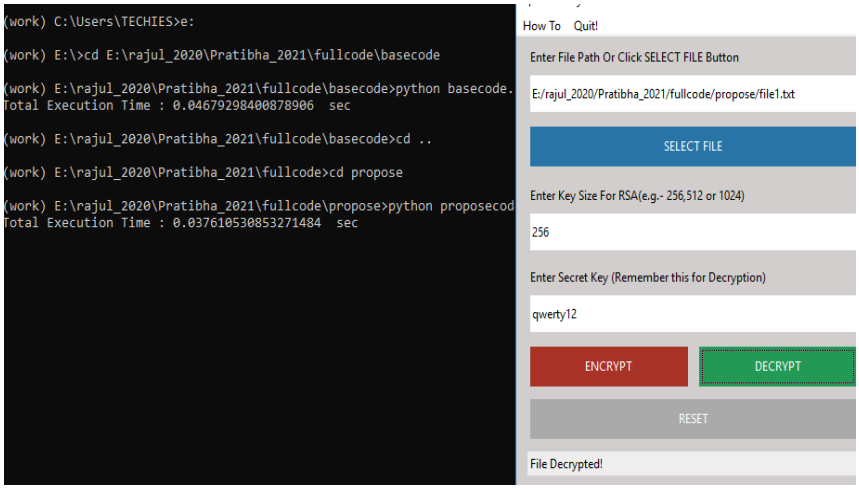

Fig. 5.The 256-size key generation in RSA-BlowFish

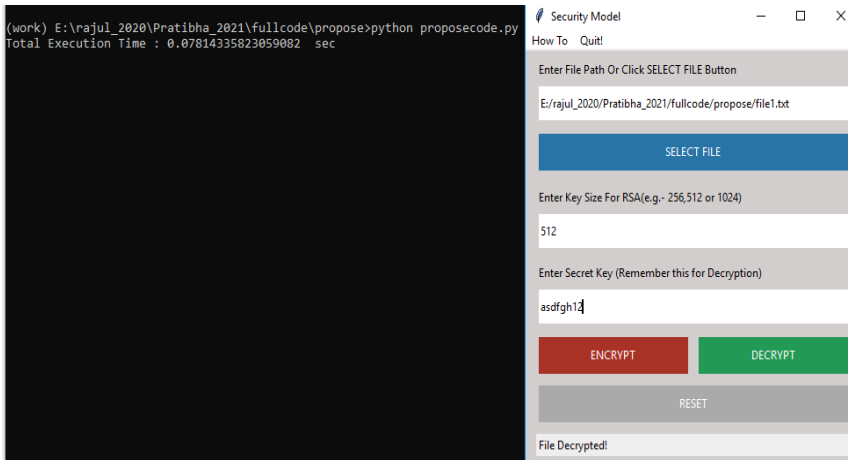

Fig.6.The 512-size key generation in RSA-BlowFish

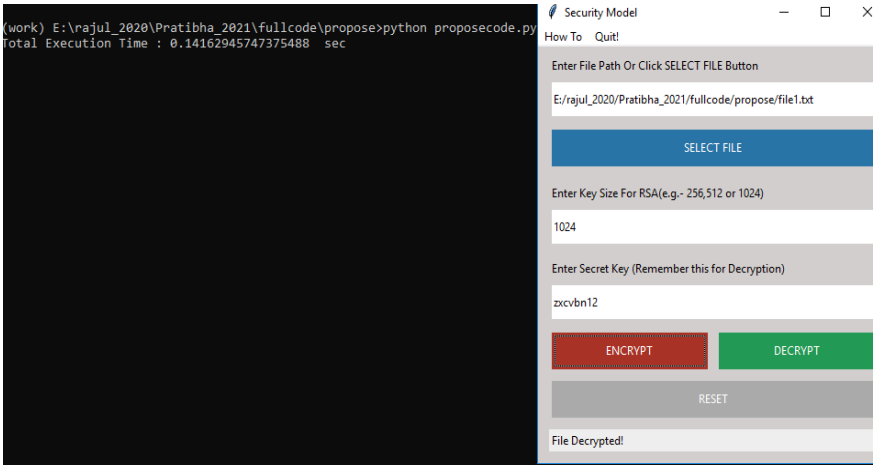

Fig.7.The 1024-size key generation in RSA-BlowFish

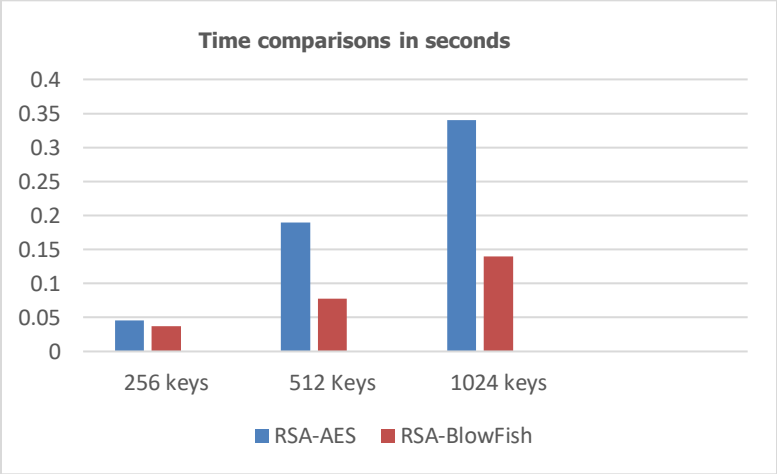

Fig.8. Comparison of time duration between existing and current research on various key sizes

V. CONCLUSION

The use of cryptographic algorithms will make cloud computing safer. Cryptography is the protected data technique by translating data into coded or unreadable types. But there are only current cryptographic methods, Algorithms for level encryption. An unauthorized individual can easily break the encryption on a single level. This is why the system uses Encryption and decryption at multi-level offers more Cloud Storage Protection.

As the algorithm proposed is cross-level encryption andAlgorithm to decrypt. So only the approved user can access the data in our proposed work. And if there is an intrusion (Unauthorized user) gets data accidentally or purposely, he must decrypt the data at any level, which without a valid key is an extremely difficult job.

REFERENCES

1. Meng, "Data security in Cloud Computing", *Computer Science and Education (ICCSE), 2013 8th International Conference*, pp 810- 813, 2013.
2. Shawish and M. Salama, "Cloud Computing: Paradigms and Technologies".
3. Xhafa and N. Bessis (eds.), "Interco-operative Collective Intelligence: Techniques and Applications", Studies in Computational Intelligence 495, Springer-Verlag Berlin Heidelberg, 2014.
4. Babcock and Charles,"9 Worst Cloud Security Threats Leading Cloud Security Group Lists the Notorious Nine",Top Threats to Cloud Computing in 2013; Most Are Already Known but Defy 100% Solution, Information Week, UBM Tech Sites, 2014-2015.
5. S.M. Khan, and K.W. Hamlen, "Anonymous Cloud: A Data Ownership Privacy Provider Framework in Cloud Computing",IEEE 11th International Conference on Trust, Security, and Privacy, Computing and Communications (TrustCom), 2012.
6. S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications,Vol. 34, No. 1, pp 1-11, 2011.
7. Ning., et al. "Privacy-preserving multi-keyword ranked search over encrypted cloud data", INFOCOM, 2011 Proceedings IEEE, 2011.
8. Y. Sun, J. Zhang, Y. Xiong, and G. Zhu, "Data Security and Privacy in Cloud Computing", International Journal of Distributed Sensor Networks, 2014
9. Mont, and Pearson, "An Adaptive Privacy Management System for Data Repositories, Trust, Privacy and Security in digital business", Vol. 3592, pp 236-245, 2005.
10. D W. Chadwick and K. Fatema, "A privacy-preserving authorization system for the cloud", Journal of Computer and System Sciences, pp. 1359-1373, 2012.
11. W. Itani, A. Kayssi and A. Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures", Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009.
12. A.Libdeh, L. Princehouse, and H. Weatherspoon, "RACS: A Case for Cloud Storage Diversity", SoCC10:

Proc. 1st First ACM Symposium on Cloud Computing,pp. 209-240, 2010.
13. S. Pearson, Y. Shen, and M. Mowbray, "A Privacy Manager for Cloud Computing", Cloudcom2009, LNCS 5931, Springer 2009, pp. 90-106.
14. Prasad, B. R. Singh, M. Akuthota and M. Sangeetha, "An Etiquette Approach for Public Audit and Preserve Data at Cloud", International Journal of Computer Trends and Technology (IJCTT), Vol. 16, No. 1, 2014.
15. M. F.Al-Jaberi, & A. Zainal, "Data integrity and privacy model in cloud computing",2014 International Symposium on Biometrics and Security Technologies (ISBAST), 2014.
16. Y. Sharma, H. Gupta, S.K. Khatri, "A Security Model for the Enhancement of Data Privacy in Cloud Computing", IEEE,2019.