A hybrid data encryption technique using RSA for cloud data storage

[1]Rohini,[2]Tejinder Sharma
[1]M.Tech Scholar,[2]Associate Professor
[1]Computer Science and technology,
[1]Amritsar College of Engineering and Technology, Amritsar,India

Abstract: Cloud computing is an data technology (IT) paradigm that enables repeated pierce to distributed pools of configurable process resources and higher-level companies which can be rapidly provisioned with small administration work, usually over the Internet. Cloud computing utilizes sharing of assets to accomplish coherence and economies of degree, just like a community utility[1]. Cloud computing protection could be the pair of control-based technologies and guidelines developed to adhere to regulatory conformity principles and protect data, information programs and infrastructure related to cloud computing use[2]. With an increase of companies using cloud computing and associated cloud providers for information procedures, proper security in these and different probably susceptible parts have grown to be a concern for companies acquiring with a cloud processing provider[3][4]. This paper is centered on safety dilemmas in cloud computing. In this we use cryptographic algorithm for obtaining security of information around our cloud[5]. We proposed a technique hybrid RSA to increase the confidentiality and security of data. We uses hash codes to keep the integrity of the information. We also raise the authentication of security of the cloud computing using multi-level authentication[6].

Index Terms **- Cloud computing, Algorithms, Security, Authentication, Confidentiality**

I. INTRODUCTION

Cloud computing is a technique for delivering information technology (IT) services where resources are retrieved from the Internet through web-based tools and applications, instead of an immediate link with a server[7]. Rather than keeping files on an exclusive hard disk or local storage device, cloud-based storage afford them the ability to save lots of them to a remote database[8]. Provided that a digital device has access to the internet, it's access to the information and programs to perform it **.**

It's called cloud computing because the data being accessed is within "the cloud" and doesn't require a person to stay in a particular destination to get access to it[9][10]. This sort of system allows employees to work remotely. Companies providing cloud services enable users to store files and applications on remote servers, and then access all the information via the internet[11].

II. LITRATURE REVIEW

Mbarek Marwan et al. [12] have focused on security of data on the cloud. In fact, this approach guarantees data confidentiality and enables users to perform arithmetic operation over encrypted data without decrypting them. In principle, the proposed techniques seek not only to secure client data, but also to perform mathematical operations on the ciphertext. In this paper, the author had proposed RSA and Paillier algorithms that ensure the two main homomorphic properties: addition and multiplication. The RSA algorithm is used to perform multiplication over encrypted data and to ensure data confidentiality. In parallel, Paillier is a homomorphic algorithm used mainly to carry out addition over encrypted data.

Ashutosh kumar debey et al. [33] have proposed a technique in whith they apply RSA and MD 5 algorithm. When the cloud user upload the data in the cloud environment, the data is uploaded in encrypted form using RSA algorithm and the cloud admin can decrypt using their own private key. For updating the data in the cloud environment admin request the user for a secure key. Cloud user sends a secure key with a message digest tag for updating data. If any outsiders perform a change in the key, the tag bit is also changed indicating the key is not secure and correct.

Manpreet kaur et al.[33] have mentioned about the security challenges and security issues while uploading the data on the cloud.

Varun Gandhi et al.[34] have discussed the main security issues existing in cloud computing environments. The security issues at various levels of cloud computing environment is identified in this paper and categorized based on cloud computing architecture. This paper also focuses on the usage of cloud services and security issues to build these cross-domain Internet-connected collaborations.

2.1 Summary on literature review:

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[12].

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[13]. 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[14][15].

III. SECURITY IN CLOUD COMPUTING

3.1 Importance of Authentication:

Authentication plays a significant role in cloud's security. Authentication is the procedure of to determine confidence in users identities. Authentication assurance levels must be appropriate and accurate for the sensitivity of the any application, information assets accessed and the danger involved[16]. In Authentication process the credentials provided are in comparison to those on file in a database of authorized users informative data on a local operating system or within an authentication server[17]. If the credentials match, the procedure is completed and an individual is granted authorization for access. Authorization is employed to regulate the access of data[18]. It's the mechanism through which a method determines what degree of access a specific authenticated user should need to secure resources controlled by the system.

3.2Importance of Confidentiality

It contemplates the abilities of the VMs as well as assigns superior amount of errands to the privileged facility VMs deployed on the supremacy specified to all of the VMs however it gets unsuccessful to consider the extent of the jobs to opt for the suitable VM.

Data confidentiality is essential for users to store their private or confidential data in the cloud. Authentication and access control strategies are accustomed to ensure data confidentiality[20][21]. The confidentiality, authentication, and access control of data issues in cloud computing could be addressed by increasing the cloud reliability and trustworthiness. Confidentiality, in the context of computer systems, allows authorized users to gain access to sensitive and protected data[22]. Specific mechanisms ensure confidentiality and safeguard data from harmful intruders[23]. Data confidentiality identifies the capability to share sensitive data among a community of users while respecting the privileges granted by the data owner to each person in the community. Any user external to the community is assumed to possess no privilege at all[24].

IV. EXISTING FRAMEWORK

The prevailing framework guarantees data confidentiality and enables users to do arithmetic operation over encrypted data. This framework was centered on conventional encryption methods, such AES, DES and RSA. However, clients had decrypted stored data before manipulating them. Consequently, these algorithms aren't suited to exploit the cloud database[25]. For that end, the writer proposed the homomorphic encryption scheme to secure clients'data. The key idea behind that method is to hold out computations on encrypted data. In reality, homomorphic algorithms allow anyone to compute arithmetic operations over encrypted data without decrypting them. In principle, the excisting techniques seek not merely to secure client data, but additionally to do mathematical operations on the cipher text. users count on homomorphic properties to do common mathematical operation, such as for example addition and multiplication[25]. For that end, the writer had presented two well-known algorithms: Paillier and RSA. In reality, Paillier can perform addition of two values without decrypting them while RSA is especially used to do multiplication. enerally, homomorphic encryption is just a technique where arithmetic operations are carried out over encrypted data. So, organizations encrypt their data using homomorphic algorithms before uploading them in to the cloud database[25].

V. PROPOSED FRAMEWORK

We proposes a platform to mitigate security issues at the particular level authentication and storage level in cloud computing. Efficient security mechanisms must be deployed in the form of encryption, authentication, and authorization or by various other method to guarantee the privacy of consumer's data on cloud storage.

5.1 We raise the authentication of security of the cloud computing using multi-level authentication.

Multilevel authentication:

It generates passwords at multilevel. In this password is entered in stages. On each correct password privilages for the entered stages are granted.

In this framework you can find three levels:-

- Owner level
- Administrator level
- User level
- **Owner-** top level security like giving the access after asking various security questions.

Administrator-second level security i.e. after asking various security questions then provide the access
User- third level security i.e. providing access after username and password matching.

5.2 We raise the confidentiality and security of the cloud computing through Hybrid RSA technique:

Uploading data on cloud securely by encrypting its data using RSA with HMAC i.e. hashed message authentication code. Data is encrypted using RSA and the HMAC code file of that data is generated and sending both the files Encrypted File + HMAC code file to the cloud. Also, saved HMAC code file to the LOCAL storage also in order to maintain the integrity of the data in cloud. The cloud sends the encrypted file to the user by using the decryption key for file. After decrypting the file, the integrity check

can be applied by the user using HMAC. The user receives the HMAC along with the file. The user can compute the HMAC on the file and check if both are equal. It can therefore detect if there is any tampering of data during transmission

5.3 HMAC

Message authentication codes are employed between two parties that share a secret key to be able to authenticate information transmitted between these parties[13]. The standard defines a MAC which used a cryptographic hash function in conjuction with a secret key in order to authenticate information transmitted between two parties[13].Load balancing in cloud is the course of distributing the job load amongst different nodes in a distributed system used for enhanced reserve consumption and job reply time. The load balancer calculates observed in the particular time-span along with uses this value to estimate the virtual machine availability for the next time span. Load balancing ensures that all the processor in the system or every node in the network does roughly the equal quantity of work at any instant of time. It is a procedure of passing on the entire load to each nodes of the combined structure to create resource utilization efficient as well to get better response time of the situation, concurrently removing a situation in which some of the nodes are over loaded while several others are under loaded. It can be observed CPU utilization, throughput etc. will be improvised while balancing the load to virtual machines on the basis of utilization of resources on an immediate time. The goal of this research work is to set aside resources with the intention that we can assign the assets to additional number of processes in order to boost productivity plus make it environmental friendly [15].

5.4 Performance parameters

- Encryption time:
- Decryption time

5.5 Simulation Agenda

NetBeans is an open-source project dedicated to providing rock solid software development products (the NetBeans IDE and the NetBeans Platform) that address the needs of developers, users and the businesses who rely on NetBeans as a basis for their products; particularly, to enable them to develop these products quickly, efficiently and easily by leveraging the strengths of the Java platform and other relevant industry standards.

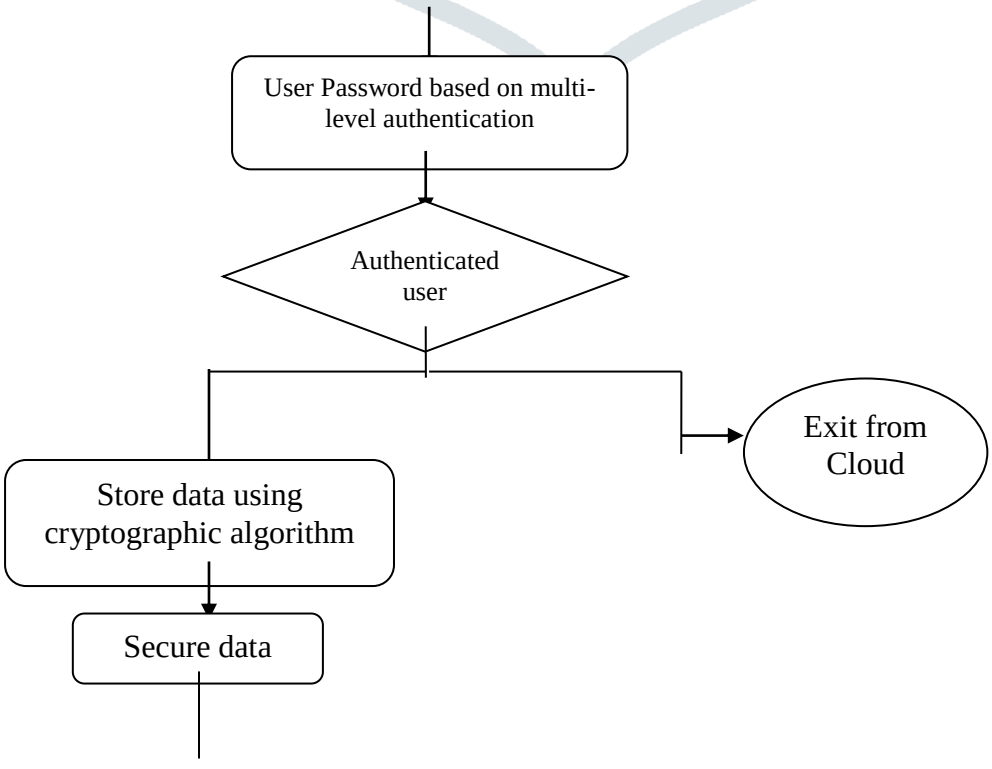
All the functions of the IDE are provided by modules. Each module provides a well-defined function, such as support for the Java language, editing, or support for the CVS versioning system, and SVN. NetBeans contains all the modules needed for Java development in a single download, allowing the user to start working immediately. Modules also allow NetBeans to be extended. New features, such as support for other programming languages, can be added by installing additional modules. For instance, Sun Studio, Sun Java Studio Enterprise, and Sun Java Studio Creator from Sun Microsystems are all based on the NetBeans IDE.

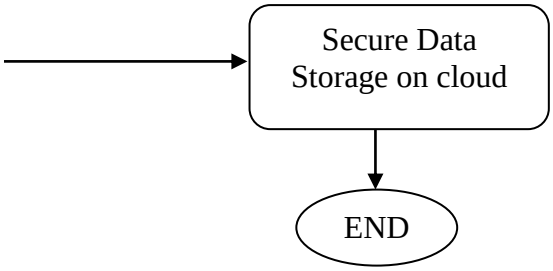
Best Support for Latest Java Technologies

NetBeans IDE is the official IDE for Java 8. With its editors, code analyzers, and converters, you can quickly and smoothly upgrade your applications to use new Java 8 language constructs, such as lambdas, functional operations, and method references

With its constantly improving Java Editor, many rich features and an extensive range of tools, templates and samples, NetBeans IDE sets the standard for developing with cutting edge technologies out of the box.

VI. FLOWCHART OF PROPOSED FRAMEWORK





VII. IMPLEMENTATION AND RESULTS

We develop an application to store medical information. To meet security requirement we encrypt the data using RSA with HMAC and upload the data to the cloud. The proposed application is developed using netbeans ide 8.2 and cloudsim 3.0. we use MYSQL as a database.

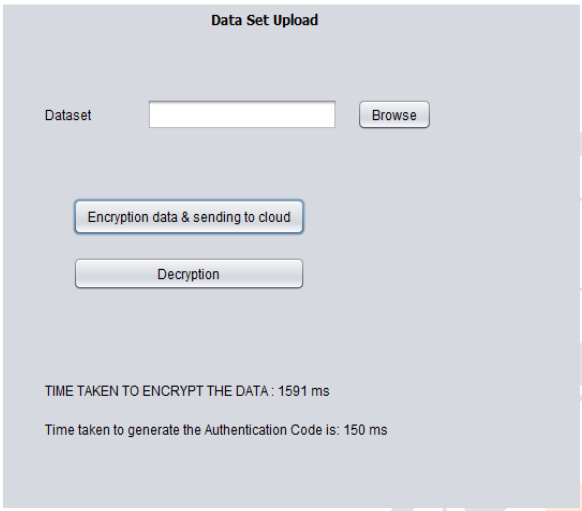


Fig 7.1. Dataset uploading to the cloud

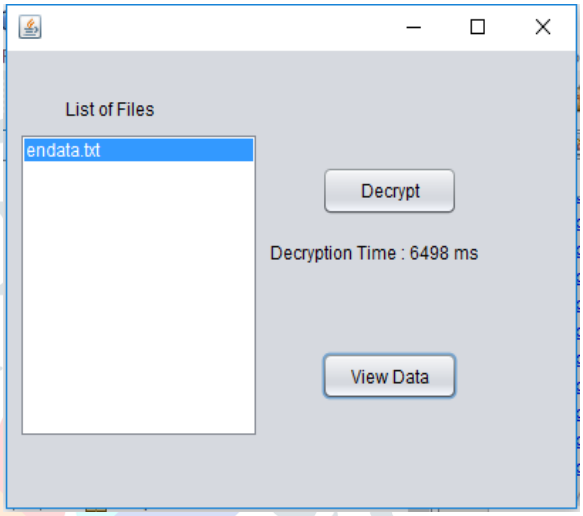
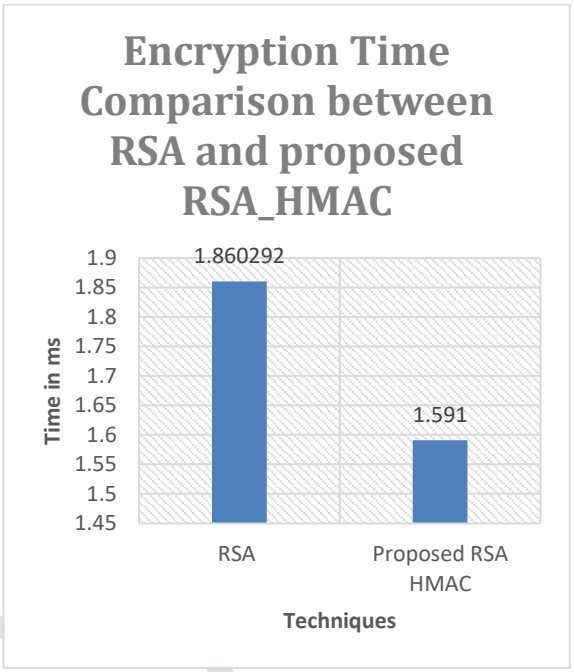


Fig 7.2. Dataset decrypting from the cloud

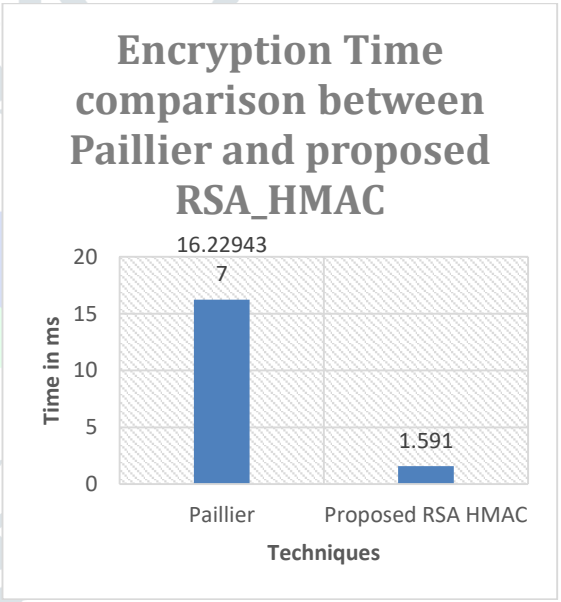
Case I- Comparison of encryption time of base paper technique with RSA and proposed encryption with RSA_HMAC

Encryption	Time
Homomorphic base paper technique with RSA Marwan mbarek et al.[23]	1.860292
Proposed Encryption with RSA_HMAC	1.591



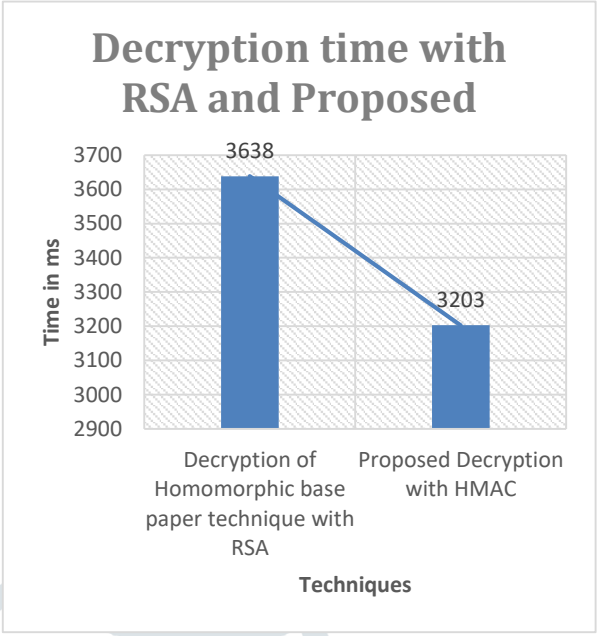
Case II- Comparison of encryption time of base paper technique with pailier and proposed RSA_HMAC

Encryption	Time
Homomorphic base paper technique with Pailier, Marwan mbarek et al.[23]	16.22944
Proposed Encryption with RSA_HMAC	1.591



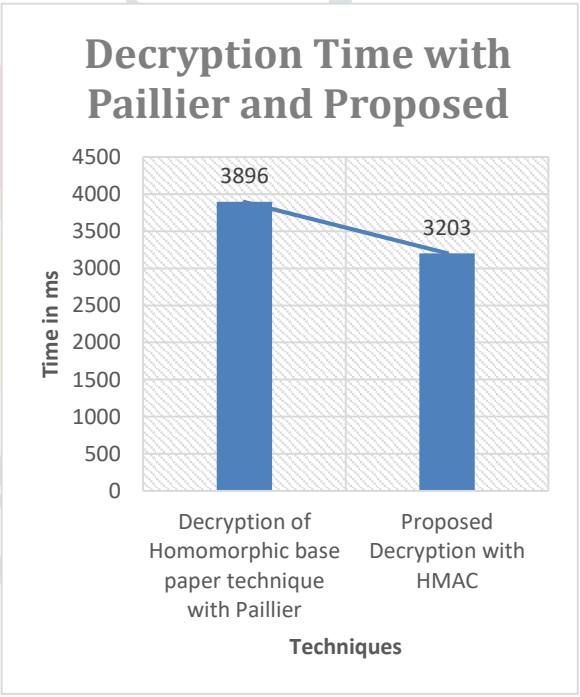
Case III- Comparison of decryption time of base paper technique with RSA and proposed decryption with RSA_HMAC

Decryption	Time
Homomorphic base paper technique with RSA, Marwan mbarek et al.[23]	3638
Proposed Decryption with RSA_HMAC	3203



CaseIV- Comparison of decryption time of base paper technique with Pailier and proposed decryption with RSA_HMAC

Decryption	Time
Decryption of Homomorphic base paper technique with Paillier	3896
Proposed Decryption with HMAC	3203



VIII. CONCLUSION

Cloud database is an approach that aims at reducing operating costs and improving availability and reliability. Indeed, it provides a scalable structured repository to store and manage data. In this concept, the cloud provider is responsible for maintaining and upgrading the delivered database. Also, users are charged only for the database utilization. Despite its multiple advantages, the migration to cloud database faces several challenges. In this context, the security and privacy of clients' data need to be addressed before implementing this new concept. In this regard, we suggest a hybrid RSA based on RSA and HMAC algorithms to overcome these challenges. Indeed, this solution ensures the confidentiality and integrity of the stored data in the cloud database. In this study, we use RSA with HMAC to secure the data. The proposed techniques guarantee the confidentiality and integrity of clients' data. Using proposed system we need less time to encrypt and decrypt the files we also increase the confidentiality and integrity of the data using HMAC. In this proposed technique we also increase the authentication of security using multilevel authentication.

TABLE 8.1: Comparison table of exiting technique with proposed technique

Particulars	Parametrs	Work	Time
Excisting technique	Encryption	Homomorphic base paper technique with RSA Marwan mbarek et al.[23]	1.860292
Proposed technique	Encryption	Proposed Encryption with RSA_HMAC	1.591
Excisting technique	Encryption	Homomorphic base paper technique with Pailier, Marwan mbarek et al.[23]	16.22944
Proposed technique	Encryption	Proposed Encryption with RSA_HMAC	1.591
Excisting technique	Decryption	Homomorphic technique with RSA, Marwan mbarek et al.[23]	3638
Proposd technique	Decryption	Proposed Decryption with RSA_HMAC	3203
Excisting technique	Decryption	Decryption of Homomorphic technique with Paillier	3896
Proposed technique	Decryption	Proposed Decryption with HMAC	3203

REFERENCES

[1] Komal ganndhi and Parul Gandhi. "Cloud computing security issues: An analysis", 3rd International Conference on Computing for Sustainable Global Development (INDIACom), pp. 3858-3861. IEEE, 2016.

[2] Priya Anand, Jungwoo Ryoo, Hyoungshick Kim,"Addressing Security Challenges in Cloud Computing—A Pattern-Based Approach", International Conference on In Software Security and Assurance (ICSSA), pp. 13-18. IEEE 2016.

[3] Y. Benslimane, Z. Yang, & B. Bahli, "Key Topics in Cloud Computing Security: A Systematic Literature Review " , 2nd International Conference on Information Science and Security (ICISS), (pp. 1-4) IEEE 2015.

[4] T. K. Damenu, & C. Balakrishna, "Cloud Security Risk Management: A Critical Review", 9th International Conference on Next Generation Mobile Applications, Services and Technologies, (pp. 370-375), IEEE 2015.

[5] B. K. Dewangan, A. Agarwal, & A. Pasricha, "Credential and security issues of cloud service models", 2nd International Conference on Next Generation Computing Technologies (NGCT), (pp. 888-892), IEEE 2016.

[6] T. Agrawal, & S. K. Singh," Analysis of security algorithms in cloud computing.", 3rd International Conference on Computing for Sustainable Global Development (INDIACom), (pp. 106-108). IEEE 2016.

[7] H. Hammami, H. Brahmi, I. Brahmi, & S. B. Yahia," Security Issues in Cloud Computing and Associated Alleviation Approaches", 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), (pp. 758-765). IEEE 2016.

[8] Abdallah Ali Z. A. IBRAHIM, Dzmitry KLIAZOVICH, Pascal BOUVRY and Ariel OLEKSIAK," Virtual Desktop Infrastructures: architecture, survey and green aspects proof of concept", Seventh International conference on Green and Sustainable Computing Conference (IGSC0), (pp. 1-8) IEEE 2016.

[9] Napoleon C. Paxton, "Cloud security: a review of current issues and proposed solutions", 2nd International Conference on Collaboration and Internet Computing (CIC), pp. 452-455 IEEE 2016.

[10] Engr: Farhan Bashir Shaikh and Sajjad Haider, "Security threats in cloud computing" international conference Internet technology and secured transactions (ICITST), (pp. 214-219) IEEE 2011.

[11] Faraz Fatemi Moghaddam, Iman Ghavam, Shirin Dabbaghi Varnosfaderani and Soroush Mobedi, "A client-based user authentication and encryption algorithm for secure accessing to cloud servers based on modified Diffie-Hellman and RSA small-e", IEEE Student Conference on Research and Development (SCOReD)", pp. 175-180, IEEE 2013.

[12] Varsha K and Rachel Mathias, "International journal of innovative research in computer and communication engineering" vol.5, issue 6, IEEE 2017

[13] Kumar, Santosh, and R. H. Goudar. "Cloud Computing-Research Issues, Challenges, Architecture, Platforms and Applications: A Survey", International Journal of Future Computer and Communication 1, vol. no. 4, IEEE 2012.

[14] Pooja Bindlish and Pawan Kumar. "Study of RSA, DES and Cloud Computing." International Journal of Advanced Research in Computer Science , vol. no. 3,IEEE (2016)

[15] Gajender Pal, Kuldeep Kumar Barala, and Manish Kumar,"A review paper on cloud computing", International journal for research in applied science and engineering technology, vol. 2, issue 9, sept 2014.

[16] Majda Omer Elbasheer and Dr.Taring Mohammed, "Signing and verifying certificates by NTRU and RSA algorithm" International Conference on Cloud Computing (ICCC), pp. 1-4. IEEE.2015.

[17] Vijay Kumar Pant, Jyoti Prakashand Amit Asthana, "Three step data security model for cloud computing based on RSA and Stegnography techniques" International Conference on Green Computing and Internet of Things (ICGCIoT), pp. 490-494. IEEE. 2015.

[18] Sakinah Ali Pitchay, Wail Abdo Ali Alhiangem, Farida Ridzuan and MadihahMohd Saudi, "A proposed systemconcept on enhancing the encryption and decryption method for cloud computing"17th UKSim-AMSS International Conference on Modelling and Simulation (UKSim), pp. 201-205. IEEE. 2015

[19] Mr.Rupesh R Bobde, Prof.AmitKhaparde and Prof.Dr.M.M.Raghuwanshi, "An approach for securing data on cloud using data slicing and cryptography" 9th International Conference on Intelligent Systems and Control (ISCO), (pp. 1-5). IEEE. 2015.

[20] PreetiGarg and Dr.Vineet Sharma, "An efficient and secure data storage in mobile cloud computing through RSA and hash function",International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), pp. 334-339. IEEE. 2014.

[21] Vishwanath S Mahalle and Aniket K Shahade, "Enhancing the data security in cloud by implementing hybrid(RSA & AES) encryption algorithm", International Conference on Power, Automation and Communication (INPAC), pp. 146-149. IEEE. 2014.

[22] Mr.Prashant Rewagad and Ms.Yogita Pawar, "Use of digital signature with diffie hellman key exchange and AES encryption algorithm to enhance security in cloud computing" International Conference on Communication Systems and Network Technologies (CSNT), pp. 437-439. IEEE.2013.

[23] Yi, Xun, Russell Paulet, and Elisa Bertino, "Homomorphic encryption and applications." Cham: Springer, vol 3.pp 27-49.2014

[24] Kota, C.M. and Aissi, "Implementation of the RSA algorithm and its cryptanalysis," In proceedings of the ASEE Gulf-Southwest Annual Conference, pp. 20 – 22.march 2002.

[25] Marwan, Mbarek, Ali Kartit, and Hassan Ouahmane, "Applying homomorphic encryption for securing cloud database."IEEE International Colloquium on Information Science and Technology (CiSt), pp. 658-664. IEEE. 2016.

[26] L. Qian, Z. Luo, Y. Du and L. Guo, "Cloud computing: an overview," 1st International Conference on Cloud Computing Beijing, China, pp. 626–631.2009.

[27] B.P. Rimal, A. Jukan, D. Katsaros and Y. Goeleven, "Architectural requirements for cloud computing systems: an enterprise cloud approach," Internatinal Journal of Grid Computing, Vol. 9. pp. 3-26.2011.

[28] G. Devi and M. Pramod Kumar, "Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish Algorithm", International Journal of Computer Trends and Technology, Vol. 3. Issue 4.ISSN: 2231-2803. pp.592-596. 2012

[29] Mohit Marwaha, Rajeev Bedi, Amritpal Singh and Tejinder Singh, "Comparative Analysis of Cryptographic Algorithms", International Journal of Advanced Engineering Technology, E-ISSN 0976-3945. 2013.

[30] Rashmi Nigoti, Manoj Jhuria and Dr. Shailendra Singh, "A survey of Cryptographic Algorithm for Cloud Computing", International Journal of Emerging Technologies in Computational and Applied Science. ISSN 2279-0047. 2013.

[31] Rachna Jain and Ankur Aggarwal, "Cloud Computing Security Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4. Issue 1. 2014.
[32] Thilakanathan, Danan, "Secure Data Sharing in the Cloud." Security, Privacy and Trust in Cloud Systems. Springer Berlin Heidelberg, 2014.
[33] Ashutosh Kumar Dubey, Animesh Kumar Dubey, Mayank Namdev, and Shiv Shakti Shrivastava. "Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment." Software Engineering (CONSEG), 2012 Sixth International Conference on Software Engineering (CONSEG), pp. 1-8. IEEE.2012.
[34] Varun Gandhi, Sanchit Bansal, Raveesh Kapoor, Aakarsh Dhawan, "Cloud computing security architecture- implementing DES algorithm in cloud for data security" International Journal of Innovative Research in Engineering & Science, ISSN 2319-5665 vol 9. issue 2. September 2013.

[1] Ragmani, A., El Omri, A., Abghour, N., Moussaid, K. and Rida, M,. "A performed load balancing algorithm for public Cloud computing using ant colony optimization". In Cloud Computing Technologies and Applications (CloudTech), 2nd International Conference (PP. 221-228),May 2016 IEEE.
[2] Devi, D. Chitra, and V. Rhymend Uthariaraj. "Load balancing in cloud computing environment using improved weighted round robin algorithm for nonpreemptive dependent tasks." The scientific world journal (2016).
[3] Wickremasinghe, B., Calheiros, R.N. and Buyya, R., "Cloudanalyst: A cloudsim-based visual modeller for analysing cloud computing environments and applications". In Advanced Information Networking and Applications (AINA), PP.446-452. April 2010, IEEE.
[4] Kaur, R. and Patra, P.K. "Resource Allocation with improved Min Min Algorithm". International Journal of Computer Applications, Vol.76-(15), PP.0975-8887, August,2013.
[5] Mishra, R. and Jaiswal, A., "Ant colony optimization: A solution of load balancing in cloud". International Journal of Web & Semantic Technology, Vol.3(2), PP.33,April 2012.
[6] Bhadani, A. and Chaudhary, S."Performance evaluation of web servers using central load balancing policy over virtual machines on cloud". In Proceedings of the Third Annual ACM Bangalore Conference, PP. 16. ACM, January 2010
[7] Liu, X., Pan, L., Wang, C.J. and Xie, J.Y. "A lock-free solution for load balancing in multi-core environment". In Intelligent Systems and Applications (ISA),3rd International Workshop PP. 1-4, may 2011, IEEE.
[8] Kaur, G. and Kamboj, S, "A REVIEW ON BALANCING THE LOAD ON CLOUD USING ACCLB HYBRID LOAD BALANCING TECHNIQUE". In International Journal of Technology and Computing (IJTC) ,Vol. 2, No. 7 (July, 2016).
[9] Wickremasinghe,B. and Buyya, R., "CloudAnalyst: A CloudSim-based tool for modelling and analysis of large scale cloud computing environ-ments". MEDC project report, Vol.22(6), pp.433-659.2009.
[10] Efficient Load Balancing using Improved Central Load Balancing Technique.
[11] Soni, G. and Kalra, M, "A novel approach for load balancing in cloud data center". In Advance Computing Conference (IACC), International (pp. 807-812), 2014, February IEEE.
[12] Patel, S., Patel, R., Patel, H. and Vahora, S. "CloudAnalyst: A Survey of Load Balancing Policies". International Journal of Computer Applications, Vol.117(21),2015.