International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 1 | Jan 2019 www.irjet.net p-ISSN: 2395-0072

A Novel Survey on Cloud Security using Digital Watermarking

Vaishali D. Kamble[1], Prof. Kanchan Doke [2]

[1,2]Bharati Vidyapeeth College of Engineering, University of Mumbai.

Abstract - *Cloud computing has been evolved as the next generation architecture of IT enterprise. With the use of traditional solutions, where IT services are under proper physical, logical and personnel controls so the cloud computing moves the application software and database to the large centre of data. But the management of data and services are not fully trustworthy. Telemedicine uses the information technology and telecommunication to provide the clinical heath care from various distance. The information privacy and security continues to plague due to wireless network in today's world. The information contains in the medical image are very sensitive therefore it is necessary to protect it from unauthorized users. By using encryption and digital watermarking we can provide the security and authenticity to the medical image.*

Key Words: **Cryptography, Medical Image, Digital Watermarking, Security and Privacy, Fog Computing.**

1. INTRODUCTION

Nowadays sharing of medical image using internet is become very popular to make clinical health care from various distance. We should provide the integrity, confidentiality and authenticity while sharing the patient data. Therefore we have combine the cryptography and digital watermarking technique for transmission of medical image. DWT and DCT techniques used for digital watermarking whereas ECDH(Elliptical Curve Diffie Helman) algorithm is used for cryptographic techniques. Watermarking is used to hide hiding the information in digital media like photographs, digital music and digital video. Medical image are very important in the field of medical image these images are then embeds into watermark s into medical image by physicians before storing. The authorized member of healthcare having the appropriate key can only extracts the embedded watermarks and gain the access of the information. The Encryption technique is used to provide security to the data. The information is nothing but the encoding to prevent from unauthorized access and the unauthorized person cannot read it. During the encryption process the information is encrypted using encryption algorithm with the help of private key. The encryption scheme used to encrypt medical image then only the authorized person can decrypt this medical image and can obtain the original image.

2. LITERATURE REVIEW

Pooja Prakash M, Sreeraj. R, Fepslin AthishMon, K. Suthendran [1] published in International Journal of Pure and Applied Mathematics (IJPAM 2018) **"**Combined Cryptography and Digital Watermarking for secure transmission of medical image in EHR system". In this paper, the medical image have been protected using encryption and digital watermarking techniques to protect the medical image from unauthorized users. Telemedicine is been rapidly in used therefore it is necessary to protect the medical image in healthcare.

Abdulaziz Hadeal [2] published in IEEE access (IEEE-November 2017) "Privacy of medical big data in a healthcare cloud using a fog computing". In this paper, the main focus is given to protect healthcare data in cloud using fog computing. Authenticated key agreement protocol is been proposed using bilinear pairing cryptography which will generate session key to securely communicate. The healthcare data are accessed and stored securely using decoy technique.

Osama Razi, Sumit Sanyal, Mohsin Raza, Shashi Sourav [3] published in International Journal of Advance Research in Computer Science (IJARCS 2018) "A survey paper on improving performance and enhancing security by using division and replication of data in cloud". In this paper, the given file is divided into fragments and then it is replicated. They are kept on every node and every node stores single fragment of data which provides security. The nodes which stores the replicas and fragments are not adjacent to each other by using T colouring method and hence it will prevent the attackers from gaining access.

Bhushan Rathod, Prashant Yelmar [4] published in International Journal of Advance Research in computer and Communication Engineering (IJARCCE 2017) "Efficient cloud security method for preventing insider attacks in cloud computing platforms". In this paper, the goal of proposed approach is to ensure that while using the cloud data it should not exposed to other cloud clients and administrator. The flicker method is been used to maintain the integrity of the cloud platform. For data security the new technique called hybrid cryptography method is been used for delivering the best efficiency performance.

Nour S. Darwazeh, Lo ai Tawalbeh, Raad S. Al-Qassa, Fahad AlDosari [5] published in Science Direct (MCSMS-2015) "A secure cloud computing model based on data classification". In this paper, a secure cloud computing model using data classification is been proposed. In this approach the cloud model minimizes the overhead and processing time require to secure the data using different security mechanism with variables key sized used to maintain the confidentiality at various levels. This model is been tested using different encryption techniques.

Sumit Chaudhary, N. K. Joshi [6] published in International Journal of Pure and Applied Mathematics (IJPAM-20180 " Secured blended approach for cryptographic algorithm in cloud computing". In this paper, the cloud security algorithm is been describe which is used to secure data at data centre. Blend technique is the advance technique is used to secure data. The combination of AES, RSA and Digital Signature is shown. The private jey generation is done using two different algorithm such as AES and RSA. Here the AES is symmetric while RSA is asymmetric algorithm.

Nandita Sengupta, Ramya Chinnasamy [7] published in Eleventh International Multi Conference on Information Processing (IMCIP-2015) "Contriving hybrid DESCAST algorithm for cloud security". In this paper, the encryption algorithm called hybrid DESCAST is been proposed. This technique is been proposed to secure the high volume of data which is sent through the media and same will be encrypted in cloud server. This cipher text will be decrypted only by authorized users. The main focus of this paper is provide security of data in cloud server as well as the for the data while transferring from client to cloud server and vice versa.

Vibhey Bhangotra, Amit Puri [8] published in International Journal of Advance Engineering Technology (IJAET-2015) "Enhancing cloud security by using hybrid encryption scheme". In this paper, the main focus on defining and accessing policies depend on data attributes and allowing the data owner to delegates the computer task involved in fine grained data access to untrusted cloud servers. The proposed scheme also has properties of user accessibility and customer private key accountability.

Prof. Hitesh Patel, Prof. Parin Patel, Prof. Kiran Patel [9] published in (IJEDR-2014) "Achieving data integrity in cloud storage using BLAKE hash function". In this paper, the integrity check is done without using TPA (Third Party Auditor) and use cryptographic hash function BLAKE to generate the signature of file. This proposed model achieves the storage correctness, confidentiality, authentication, integrity and efficient data access in cloud.

A. P. Jaware, N. R. Borkar [10] published in International Journal of Computer Science and Mobile Computing (IJCSMC) "A review paper on implementation of a secure and dynamic multi keyword ranked search scheme over encrypted cloud data". In this paper, the new scheme is proposed known as implementation of a secure and dynamic multi keyword ranked search scheme over encrypted cloud data. Here the vector space model and TF-IDF model are used as a record development and query generation. The greedy depth first search technique is used to calculate multi keyword ranked search with number of counts matching the multi keywords. The KNN classification is used to encrypt the file and query vector.

3. HEALTHCARE SYSTEM

Cryptography and digital watermarking two techniques have been proposed. The DWT and DCT are used for digital watermarking whereas the Elliptical curve diffie hellman algorithm are used for cryptography. The integrity of received image is also calculated. There will be three phases such as digital watermarking, cryptography and integrity checking.

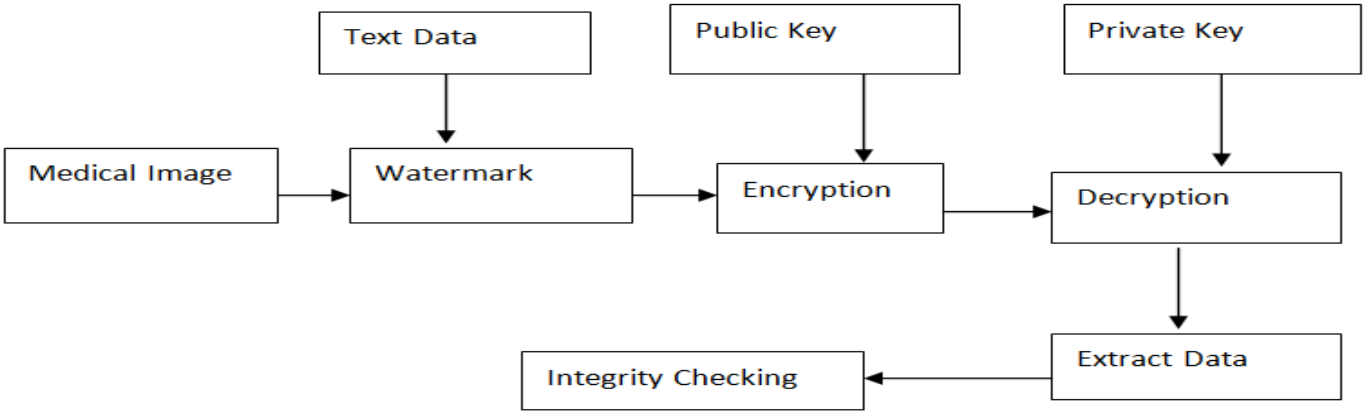


Fig. 3.1 Healthcare system

4. REQUIREMENTS

Hardware:

1. Processor: Pentium.
2. RAM: 4GB or more.
3. Hard Disk: 16GB or more.

Software:

1. Apache Tomcat Server.
2. Windows Operating System.
3. Eclipse
4. Java
5. MYSQL

5. RESULTS

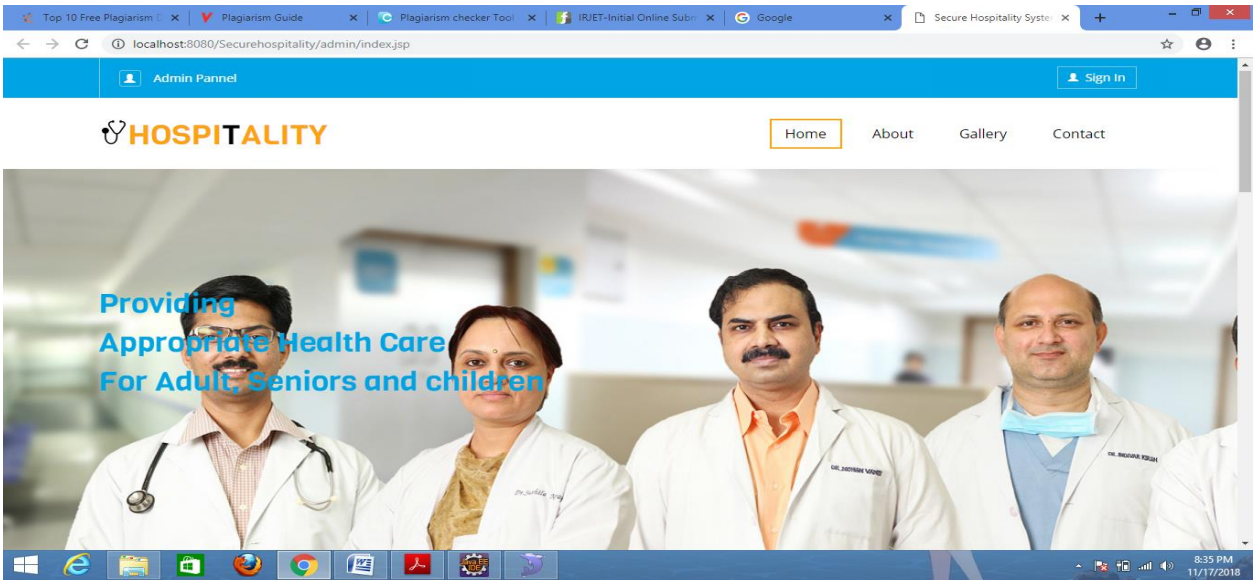


Fig 5.1 Admin Portal

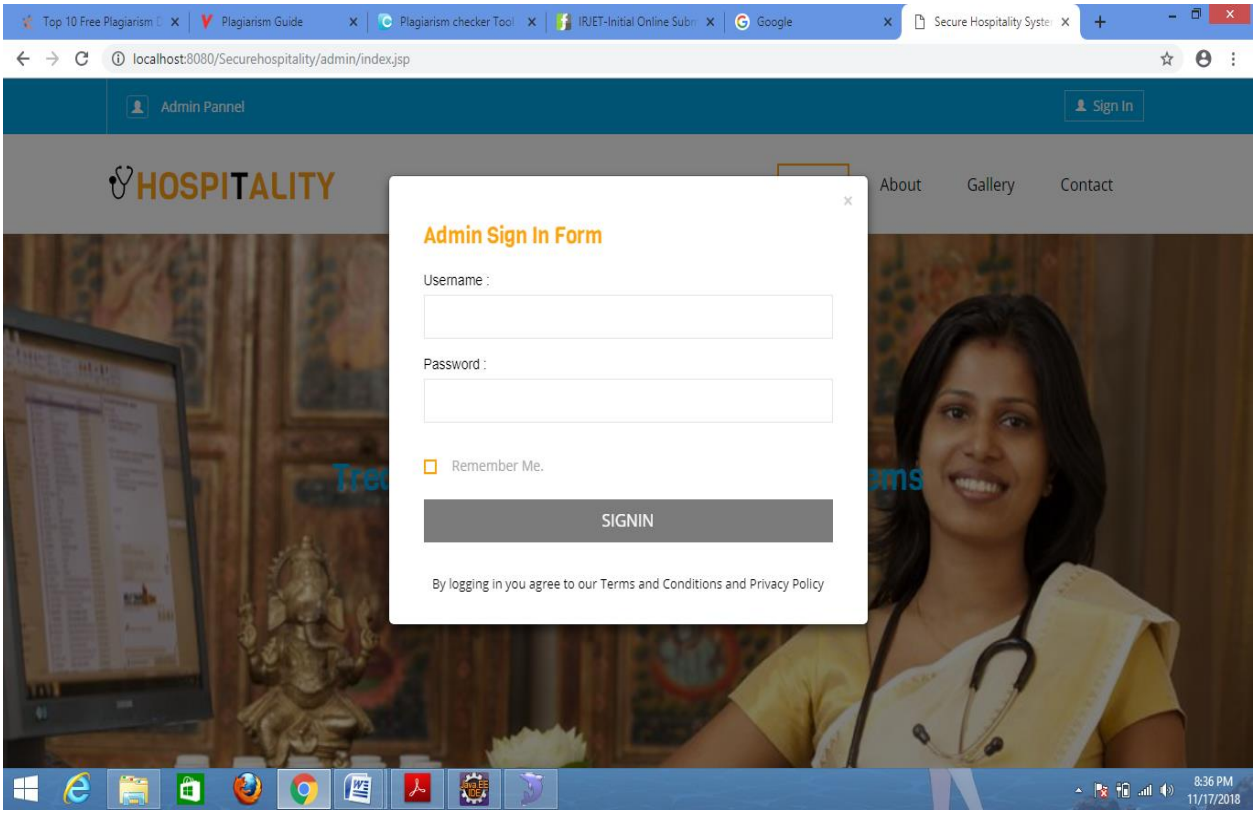


Fig 5.2 Admin login

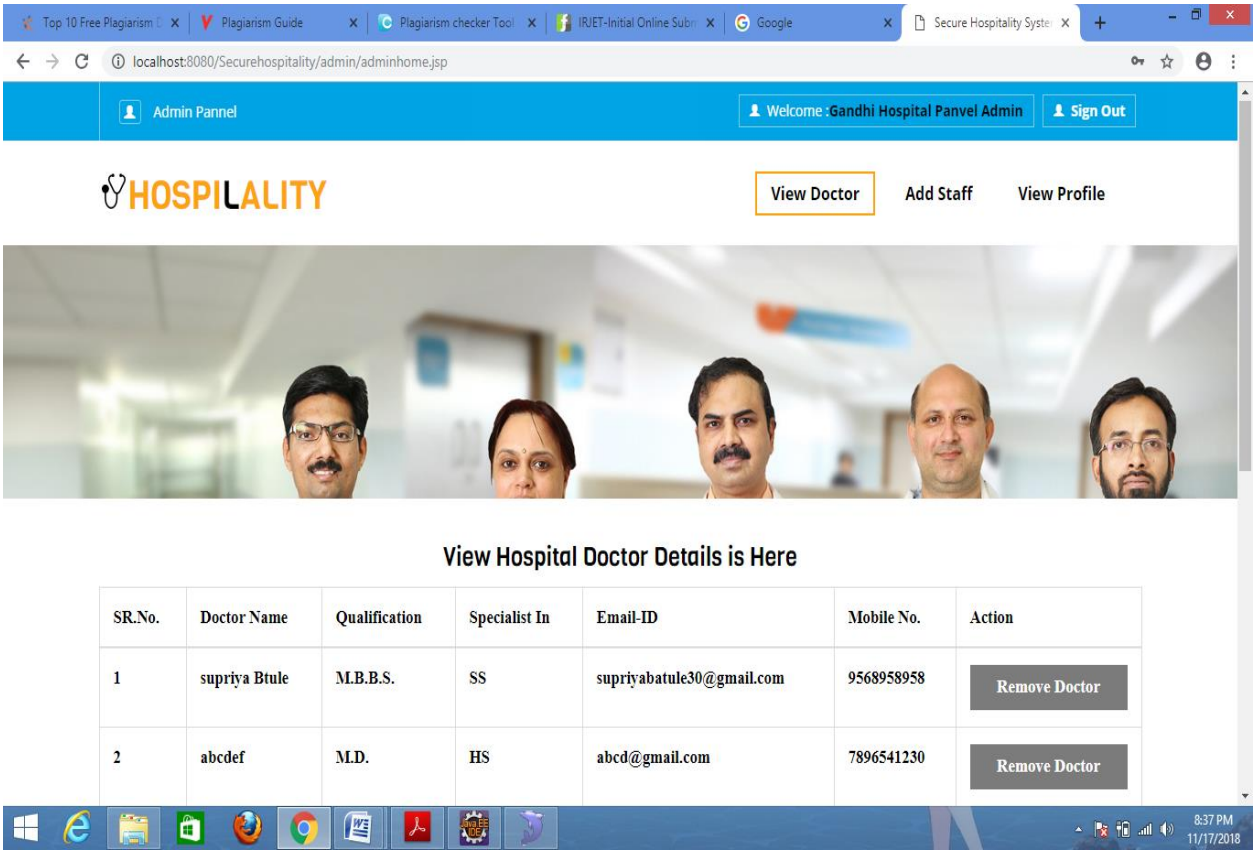


Fig 5.3 Admin panel

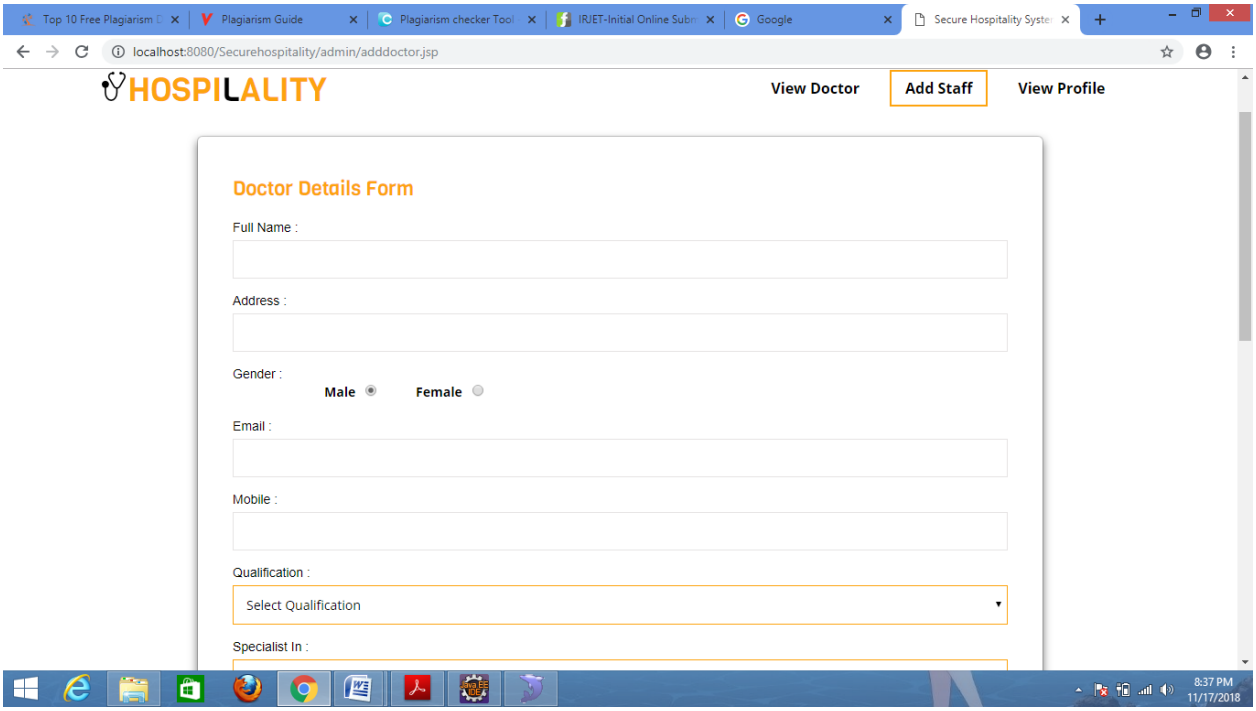
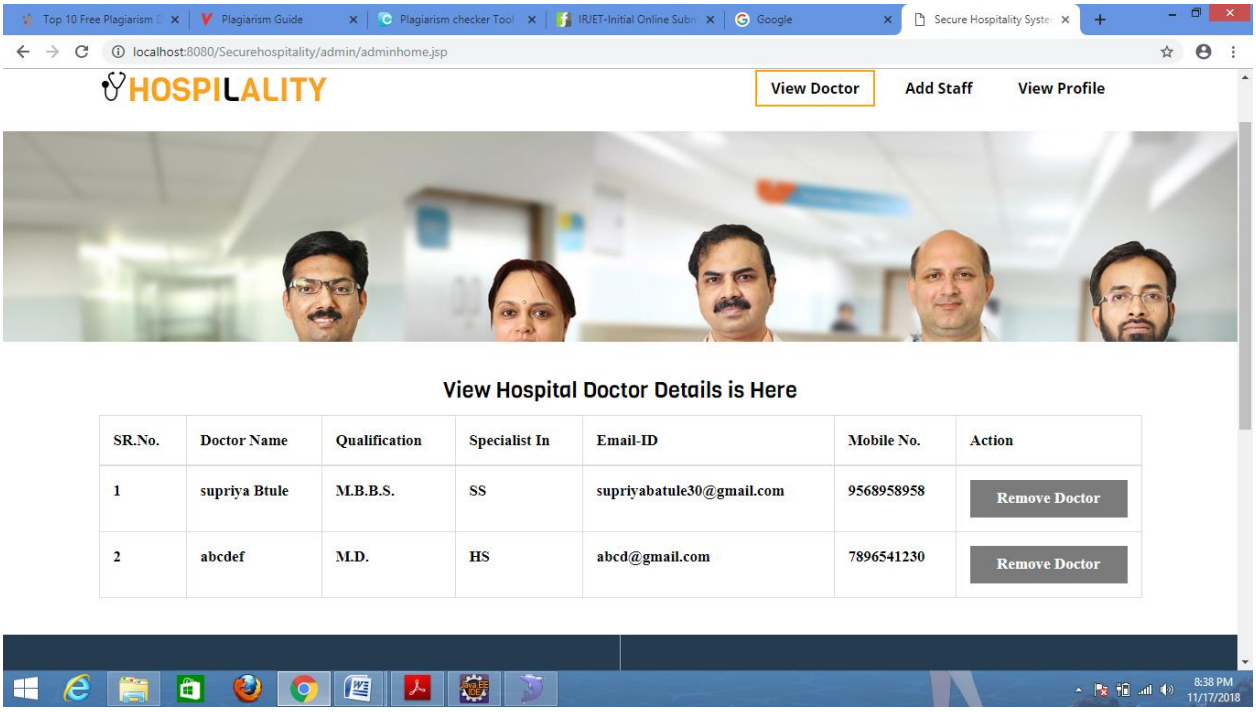


Fig 5.4 Add doctor form



SR.No.	Doctor Name	Qualification	Specialist In	Email-ID	Mobile No.	Action
1	supriya Btule	M.B.B.S.	SS	supriyabatule30@gmail.com	9568958958	Remove Doctor
2	abcdef	M.D.	HS	abcd@gmail.com	7896541230	Remove Doctor

Fig 5.5 View doctor details

6. CONCLUSION

Based on this paper it is studied cloud security is very important in every aspects of technology. Only the authorized can access the information. We studied the different cloud security techniques. Nowadays, the information are store in various cloud. The cloud consist of high volume of data. To secure such data it is necessary to provide security to the cloud. Therefore, the various new techniques is used so as to secure the cloud and make inaccessible to unauthorized users.

REFERENCES

[1] Pooja P, Suthendran K "To secure cloud computing using digital watermarking", 2018.

[2] Hadeal Abdulaziz Al Hamid, Sk Md Mizanur Rahman, M. Shamim Hossain, Ahmad Almogren, Atif Alamri "Privacy Of Medical Big Data In A Healthcare Cloud Using A Fog Computing", 7 November 2017.

[3] Osama Razi, Sumit Sanyal, Mohsin Raza, Shashi Sourav "A survey paper on improving performance and enhancing security by using division and replication of data in cloud", April 2018.

[4] Bhushan Rathod, Prashant Yelmar "Efficient cloud security method for preventing insider attacks in cloud computing platforms", June 2017.

[5] Nour S. Darwazeh, Lo ai Tawalbeh, Raad S. Al-Qassa, Fahad AlDosari "A secure cloud computing model based on data classification", 2015.

[6] Sumit Chaudhary, N. K. Joshi "Blended approach to secure cloud computing", 2018.

[7] Nandita Sengupta, Ramya Chinnasamy "Contriving hybrid DESCAST algorithm for cloud security", 2015.

[8] Vibhey Bhangotra, Amit Puri "Enhancing cloud security by using hybrid encryption scheme", 2015.

[9] Harish Patel"Blake hash function to secure cloud data", 2014.

[10] Borkar N."To secure cloud data using multi keyword ", May 2017.