Flame Text Algorithm for Storing Secure Information in Cloud

M.Parthiban, S.Akilarasu, S.Arunkumar, S.Gopi

Abstract: ***In the present age, we are putting away our information in the cloud; however, there is a great deal of security requests. So as to improve the security, our venture proposes another encryption calculation called Flame Text Algorithm and furthermore 3 stage check forms takes places for putting away the Electronic Health Records (EHR) data in the cloud. At first, the medicinal expert people can enter their username and the secret key. On the off chance that the client is legitimate and login acknowledged methods, at that point the subsequent stage unique mark verification process takes places. In the unique mark Authentication process the medicinal specialist individual unique finger impression is checked, on the off chance that it is confirmed effectively, at that point a verification code will be sent to the mail id of the specific individual. At that point the individual needs to sign in their very own mail id for the check code. After unique finger impression confirmation, an alarm input box will show up, in that the individual needs to put the verification code to transfer or view the reports of Electronic Health Records of patients. After validation code effective then the therapeutic individual can transfer the archives of their worry tolerant subtleties in the cloud. Before putting away the information in the cloud an encryption procedure happens. This is the new Algorithm system where the security can be more on the grounds that the encryption and decoding take puts similarly. At that point the client can view and impart their subtleties to someone else too. The main feature of this project is the use of own Encryption and Decryption Algorithm (FLAME TEXT) which will secure our data more compared to other techniques.***

Keywords: Electronic Health Records (EHR), Authentication, Flame Text Algorithm, Decryption Algorithm etc.

I. INTRODUCTION

At first, a dispersed stockpiling system condition is appropriate for mass document stockpiling. Be that as it may, there are a great deal of disadvantages is accessible, for example, Data issue tolerant, steering productivity, trust, security, framework extension, the hunt calculation, access, execution or numerous different issues. So distributed storage is broadly used to conquer these issues. In the present age, the information is created to an ever increasing extent and there is a great deal of requests to store, get to and oversee them. So distributed storage is made to help the business movement and every one of the information to be overseen. Distributed storage has two sections, for example, a great deal of capacity gadgets and numerous servers. By utilizing the distributed storage framework the client can pick up information visiting administrations. The fundamental Core of distributed storage is application programming and capacity gadgets. It's anything but a memory yet really the administration. The distributed storage administrations incorporate three modules, for example, customer, the executives server and capacity server. The customer programming is conveyed in various geographic areas which are needing a reinforcement have, which can be any web empowered gadget to get to the system. Customer and the board server impart between one another for the reinforcement activities. The Management Server is the administration framework checking and the executives focus, and capacity server for client the executives, task booking, status observing. The association between the capacity servers screen the usage of the status of the assignment and furthermore screen the status of every capacity server, all the time. Capacity Server is the legitimate administration server guarantees stockpiles server hub stockpiling. In the administration server the administration, continuous reaction from the customer's solicitation, to get the reinforcement information, information stockpiling the board and is in charge of sending information to the suitable customer recuperation. So as to help the effective running of reinforcement and recuperation tasks, we have to store server-side plan sensible techniques for capacity and information relocation. The framework bolsters numerous capacity servers, and various documents inside a solitary server to accomplish very versatile capacity side, the best approach to meet the administration prerequisites of mass information stockpiling.

In the distributed storage administrations, clients can remotely store their information to the cloud and understand the information offering to other people. Distributed computing is characterized as a parallel and dispersed registering framework comprising of an interconnected and virtualized PCs. It empowers clients to remotely run their applications just as store their information with the advantage of an on-request and exceptionally accessible administration without the bother of neighborhood equipment and programming the executives. With Cloud stockpiling, information is put away on numerous outsider servers, as opposed to on the specific single server utilized in customary arranged information stockpiling. Distributed computing is decidedly changing the IT scene utilizing the Internet as it empowers clients to pay on according to administrations dependent on the use premise. At that point the client concerns are in this manner moved from securing and support to the use of offices made accessible by Cloud

Revised Manuscript Received on April 12, 2019.

M.Parthiban,Department of Computer Science and Engineering, V.S.B. Engineering College, Karur, Tamil Nadu, India.

S.Akilarasu,Department of Computer Science and Engineering, V.S.B. Engineering College, Karur, Tamil Nadu, India.

S.Arunkumar,Department of Computer Science and Engineering, V.S.B. Engineering College, Karur, Tamil Nadu, India.

S.Gopi,Department of Computer Science and Engineering, V.S.B. Engineering College, Karur, Tamil Nadu, India.

specialist organizations. Distributed computing means moving administrations, calculation or information to the cloud for ease and business points of interest, for example, area straightforward, brought together offices and so on and it has the qualities that incorporate asset pooling and multi-occupancy.

There are three essentials administration types in Cloud figuring, for example, the Software-as-a-Service (SaaS), where applications are made accessible by Cloud Service Providers (CSPs) over the Internet to the Cloud clients; Platform-as-a-Service (PaaS), wherein the CSPs offers the Cloud clients stages for advancement and arrangement of their own applications and Infrastructure-as-a-Service (IaaS), where the CSPs offers to register, stockpiling, organize and, other processing assets to the Cloud clients. Distributed computing additionally has four arrangement models, the private Cloud, open Cloud, people group Cloud and, the cross breed Cloud. The private Cloud is claimed and constrained by a different individual association. Open Cloud is possessed and overseen by major CPSs. This cloud has possess enormous server farms, now and then spread crosswise over various land areas. The people group Clouds have a place with a few associations that meet up dependent on shared basic intrigue and it is overseen by the network or an outsider. Cross breed Cloud is a mix of the private or open cloud. The cross breed Cloud has a similar framework yet the associations are discrete. A noteworthy segment of Cloud registering is capacity.

The distributed storage design is made out of different stockpiling gadgets which are grouped by the system, dispersed records framework and, other stockpiling middleware to give Cloud stockpiling to clients. When all is said in done, the capacity can be in type of remain solitary clusters, joined foundation, hyper-merged framework, programming characterized capacity or open Cloud stockpiling. Capacity could likewise be a square, document or article stockpiling. The system foundation is for the most part utilized in a significant number of the capacity frameworks. The system foundation interconnects capacity frameworks which could be NVMe-based, mixture exhibits, HCI, open Cloud for essential and reinforcement, and capacity for holders. The primary structure of Cloud stockpiling incorporates a capacity asset pool, appropriated record frameworks, administration level understandings and administration interfaces among others. A five-layer Cloud stockpiling model including the system and capacity foundation layer, the capacity the board layer, metadata the board layer, a capacity overlay layer and administration interface layer. System and capacity framework comprises of circulated wired and remote systems interconnecting capacity gadgets. The capacity the executives will topographically circle the capacity assets are sorted out by areas and intelligent elements. The information can be put away by document or squares away media. The Metadata Management incorporates the groups and the worldwide space information stockpiling metadata data and works together various areas for burden adjusting purposes. The capacity overlay comprises of virtualization, administration recovering and diverting are handles at this layer. Middleware can be utilized to connections conveyed information stockpiling gadgets and afterward present them as a solitary and rearranged virtual capacity system to the clients. At long last, the Service Interface will furnish customers with a uniform interface to get to the Cloud stockpiling framework.

II. RELATED WORKS:

Jie Zhu, Qi Li et al Proposed a distributed storage framework. In this paper the creator proposes a distributed storage framework rather than conveyed stockpiling framework .Cloud stockpiling is a model that enables the client to utilize the storerooms accessible on the Internet. The distributed storage will turn into the general population's entrance to the store and recover the information proficiently. The information that are put away in the cloud will be progressively effective to get to. The distributed storage in the distributed computing base at the job and status is broadly perceived by the business working framework, administration methodology, client application, or immense measures of information are put away in the capacity framework. The client can store their information at the distributed storage framework and access the information anyplace whenever paying little respect to the spot they put away their information. The significant downside in this paper is there is no security to guarantee and check our information isn't utilized by others.

Maithilee Joshi et al Proposed a distributed storage security dependent on the property based encryption strategy. It is an open key (PKI) based encryption strategy that enables the clients to scramble and decode information dependent on client traits. In this, the mystery key (SK) of a client and the figure content (CT) both are reliant upon properties. The unscrambling of a figure content happens just if the arrangement of characteristics of the client key matches with the qualities of the figure content. The significant disadvantage with quality based encryption (ABE) plot is that the information proprietor needs to utilize each approved client's open key to encode information. The use of ABE technique plan is confined in the genuine condition since it utilizes the entrance of monotonic credits to control client's entrance in the framework.

Dr.N. Venakatesan et al Proposed a fortifying the cloud security dependent on unique mark validation technique. In this strategy, a client id and secret phrase are consolidated together and a client biometric unique finger impression is utilized to improve the security of the information stockpiling. The validation is finished by a machine just that might be a PC framework or some other electronic gadgets. The clients biometric are not alterable in the databases that are being put away. The significant disadvantage in unique mark validation is if a client may apply henna or different issues may jump out at his/her finger then the finger impression isn't verified despite the fact that the right individual is endeavoring to get to the information in the database. Furthermore, there are loads of issues with the clients biometric on the grounds that it isn't increasingly verify and effectively hackable.

ShwetaKaushik et al Proposed cloud security dependent on half breed symmetric encryption strategy. In this paper, the creator presented an idea of crossover encryption and decoding, by utilizing these procedures the information proprietor can store their information in the cloud. At the season of their stockpiling, the information is scrambled by the crossover encryption procedure. While putting away the information the information proprietor will get an unscrambling key to their enlisted mail id or message to the cell phone. By utilizing that key the information proprietor can get to the information put away in the cloud. The fundamental disadvantage happened in this framework is the decoding key isn't increasingly verify, in light of the fact that it is sent to the mail id or as a message to the cell phone. In the event that our secret key is seen by others, at that point it is anything but difficult to take or peruse the information from the cloud without the authorization of the information proprietor. What's more, another weakness is that the employments of symmetric key are progressively damageable in light of the fact that it is undermined. When we are utilizing symmetric encryption for two-way correspondence, the two sides of the discussion get traded off.

III. PROPOSED WORK:

In this method, the doctors can store their patient's details in a good security manner. Initially, the doctors can register using their own mail id and password for their login purpose to update or add the contents to the database of their own and also they can share their details to others if they get permission. Then after login, a fingerprint authentication process takes places to authenticate the doctors once again. The fingerprints of the doctors are stored in the databases and if it matches then an authentication code will be sent to the mail id of the person, then he/she must sign in their own mail id to see the authentication code. Then the authentication code must be put in the registration login page to do further process. Then after all the process completed the doctor can store their patient's details in the cloud storage in the word, pdf, ppt or any other file formats. Then the data stored will be encrypted and stored in the databases. The Encryption takes place based on the concept of Flame text Algorithm method.

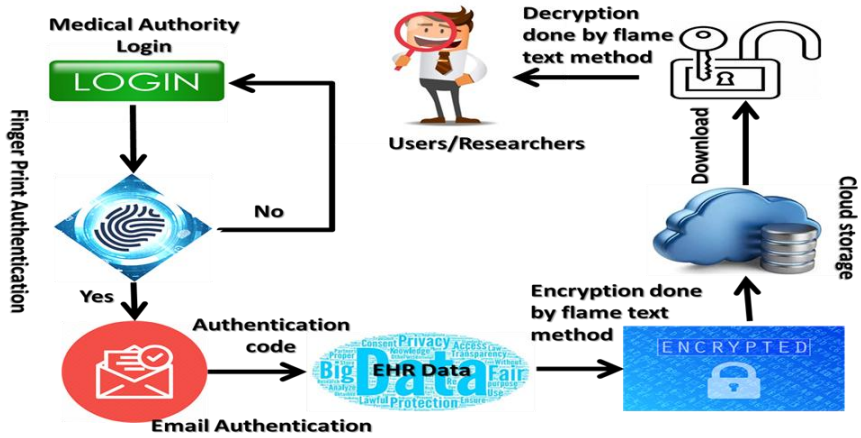


Fig:- Flame Text Cloud Storage

FLAME TEXT ALGORITHM:

Encryption:

Initially, the username and the password are taken from the login page of the user at the time of their registration or login. Then the key is generated based on the combination of user name and password and the duplicate elements are removed from that and then they are arranged in the sorted order to generate the key. All the characters of the username and passwords ASCII value is added and then the total ASCII Value is calculated by subtracting the username ASCII value from Passwords ASCII value. The text to be stored is rotated based on the total ASCII value. Then after rotating the first value of the rotated array and the first value of the key is added and stored in a hexadecimal format. This process continues for each and every letter of the document and stored in the database. This is the encryption process. This method is more secure because the key generated is based on the username and the password, so it is more secure compared to normal techniques.

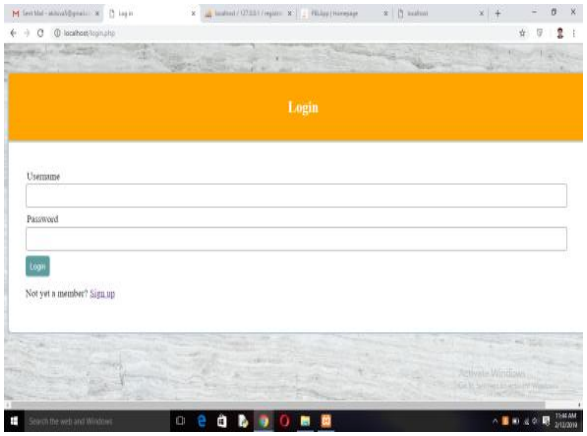
Decryption:

In this method, the decryption takes places by encrypting the encrypted data to get the decrypted document. So the decryption is also more secure because unlike other methods it is not a reverse process of the encryption technique.

IV. EXPERIMENTAL ANALYSIS:

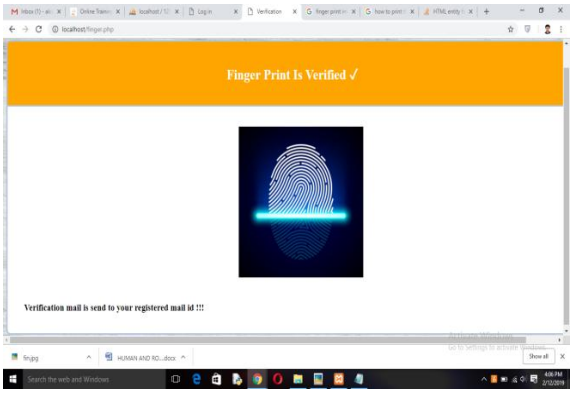
A.USER LOGIN:

In this module, each medical authority person has username and password. The user name is the mail id of the particular person. By using that they can log in and upload the details of their corresponding patients Electronic Health Records (EHR) to store it in the cloud securely and also can be shared with others. After login, they redirected for the fingerprint authentication process. If the login fails the medical authority person has to log in once again.



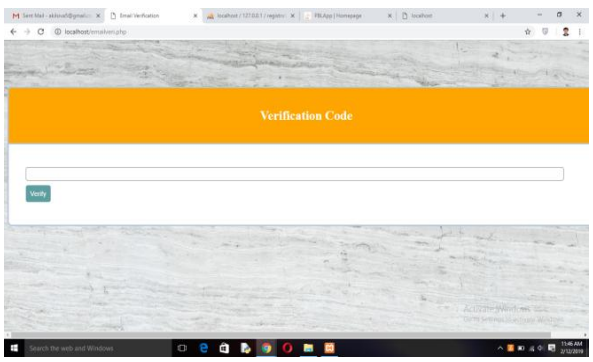
B. FINGERPRINT AUTHENTICATION METHOD:

In this process once again the verification involves in order to verify whether the correct person is uploading the data or not. Initially, the entire medical authority fingerprint is collected and stored in the database. When the doctor's fingerprint matches, then he/she is authenticated and a 6 digit code is sent to the particular mail id of the concerned person. After this process, a verification box will appear.



C. E-MAIL VALIDATION PROCESS:

In this module, the doctor must log in their own mail id to upload their patient's details. The 6 digit code will be available in the mail for a minute after the fingerprint authentication process. Then they can upload their contents to store it in the cloud by again putting the authentication code in the verification box. And if they want to share their patient's details with others they can be shared.



D. FLAMETEXT ENCRYPTION METHOD:

After doctor's uploading the data to store in the cloud, an encryption process takes places to securely store the data in the cloud. For encryption, the Flame text method is introduced.

ALGORITHM:

ENCRYPTION:

The encryption steps are

STEP 1: Initially the medical authority person has to register with their own details and get the user name and password from that for encryption and decryption processes.

STEP 2: Calculate the total ASCII value of user name and total ASCII value of password and subtract both the values to generate the first key.

STEP 3: Join both the user name and password as a single word and store in a separated array.

STEP 4: Then remove all duplicates element from the array.

STEP 5: Next sort the array A, now we get a second key to encrypt or decrypt.

STEP 6: Take an element one by one from the array which is to be encrypted or decrypted.

STEP 7: Rotate the array A for first key generated times.

STEP 8: Take each and every value of an entire document and add the first value of the rotated array and converted it to Hexadecimal format.

STEP 9: And store the encrypted or decrypted value in the separated array B.

STEP 10: Now the variable B contains the encrypted or decrypted data.

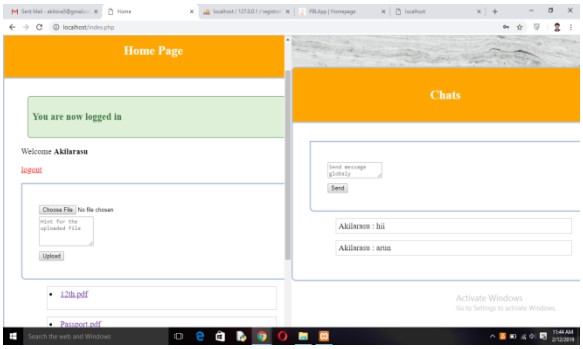
After the encryption process, the data is stored in the database in an encrypted format and then it is more security.

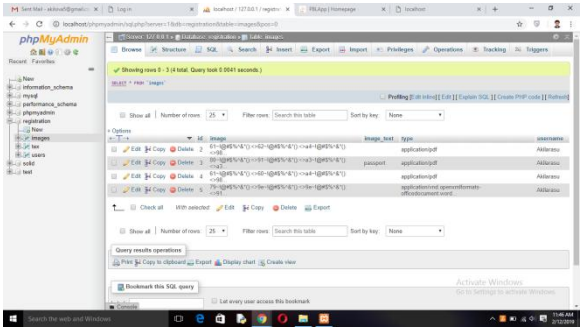
DECRYPTION:

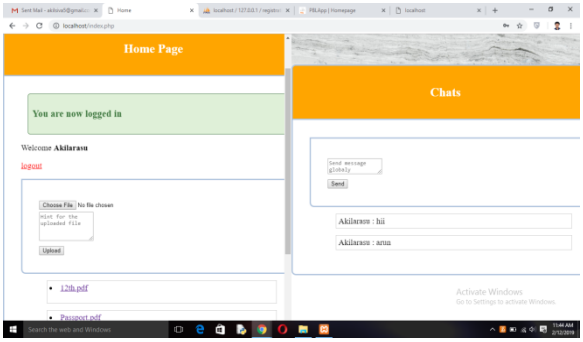
The decryption is done as like the encryption process the decryption is done by again encrypting the encrypted data in order to get the original data. After decrypting the doctors can share their details or view the uploaded contents.

V. RESULT ANALYSIS:

The result of the project is we can securely store the data in the cloud and can be shared if the medical authority person grants access. Initially, the admin can log in with the user name and password and a fingerprint authentication process takes places then again an e-mail verification code is authenticated means, the admin can upload their patient's details. A Flame text encryption Algorithm takes place to encrypt the data and it stores in the cloud and while we want to retrieve or need to download the documents a decryption process takes places and we can view our own original data.







VI. CONCLUSION:

The proposed framework utilizes the fire content strategy for encryption and decoding. The fundamental bit of leeway of the fire content encryption procedure is, the key produced depends on the client name and the secret key, so it is progressively secure contrasted with the ordinary encryption process. Furthermore, in the decoding not at all like different techniques it's anything but a turn around procedure of encryption; it is the way toward scrambling the encoded information by and by to get the unscrambled information. At long last we can store the electronic wellbeing records in a decent secure way.

REFERENCES:

1. Wentingshen, Jing Qin, Jia Yu, RongHao, and Jiankun Hu, "Enabling Identity-Based Integrity Auditing and Data Sharing with Sensitive Information Hiding for Secure Cloud Storage", IEEE Transaction on Information Forensics and Security,Vol.14,No.2,Feb 2019.
2. Qinlu He, Zhanhuai Li, Xiao Zhang, "Cloud Storage System Based on Distributed Storage Systems" , Published in: 2017 International Conference on Computational and Information Sciences,17-19 Dec. 2017.
3. Maithilee Joshi, Karuna Joshi, Tim Finin, "Attribute Based Encryption for Secure Access to Cloud Based EHR Systems", 2018 IEEE 11th International conference on Cloud Computing 2-7 July 2018.
4. Dr.N.Venakatesan, M. Rathan Kumar, "Finger print authentication for improved Cloud Security", Published in: 2016 International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS) 6-8 Oct. 2016.
5. Jie Zhu, Qi Li, Cong Wang , Xingliang Yuan , Qian Wang , KuiRen, "Enabling Generic, Verifiable, and Secure Data Search in Cloud Services" Published in: IEEE Transactions on Parallel and Distributed Systems , 20 February 2018.
6. K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, Jan 2012.
7. C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," IEEE Transactions on Computers, vol. 62, no. 2, pp. 362–375, 2013.
8. S. G. Worku, C. Xu, J. Zhao, and X. He, "Secure and efficient privacy-preserving public auditing scheme for cloud storage," Comput. Electr. Eng., vol. 40, no. 5, pp. 1703–1713, Jul. 2014.
9. C. Guan, K. Ren, F. Zhang, F. Kerschbaum, and J. Yu, "Symmetric-key based proofs of retrievability supporting public verification," in Computer Security – ESORICS 2015. Cham: Springer International Publishing, 2015, pp. 203–223.
10. J. Sun and Y. Fang, "Cross-domain data sharing in distributed electronic health record systems," IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 6, pp. 754–764, June 2010.
11. Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847–859, May 2011.
12. J. Yu, K. Ren, and C. Wang, "Enabling cloud storage auditing with verifiable outsourcing of key updates," IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1362–1375, June 2016.
13. J. Yu and H. Wang, "Strong key-exposure resilient auditing for secure cloud storage," IEEE Transactions on Information Forensics and Security, vol. 12, no. 8, pp. 1931–1940, Aug 2017.
14. Y. Luo, M. Xu, S. Fu, D. Wang, and J. Deng, "Efficient integrity auditing for shared data in the cloud with secure user revocation," in Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA - Volume 01, ser. TRUSTCOM'15, 2015, pp. 434–442.
15. H. Wang, "Identity-based distributed provable data possession in multicloud storage," IEEE Transactions on Services Computing, vol. 8, no. 2, pp. 328–340, 2015.
16. H. Wang, D. He, and S. Tang, "Identity-based proxyoriented data uploading and remote data integrity checking in public cloud," IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1165–1176, June 2016.
17. Y. Yu, M. H. Au, G. Ateniese, X. Huang, W. Susilo, Y. Dai, and G. Min, "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage," IEEE Transactions on Information Forensics and Security, vol. 12, no. 4, pp. 767–778, April 2017.
18. Y. Zhang, J. Yu, R. Hao, C. Wang, and K. Ren, "Enabling efficient user revocation in identity-based cloud storage auditing for shared big data," IEEE Transactions on Dependable and Secure Computing, 2018.
19. G. Ateniese, D. H. Chou, B. de Medeiros, and G. Tsudik, "Sanitizable signatures," in Proceedings of the 10th European Conference on Research in Computer Security, ser. ESORICS'05. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 159–177.
20. Y. Li, Y. Yu, G. Min, W. Susilo, J. Ni, and K. K. R. Choo, "Fuzzy identity-based data integrity auditing for

reliable cloud storage systems," IEEE Transactions on Dependable and Secure Computing, 2017.

21. H. Wang, "Proxy provable data possession in public clouds," IEEE Transactions on Services Computing, vol. 6, no. 4, pp. 551–559, 2013.
22. Manisha D Karad, Milind B Vaidya, "Anonymous user authentication with secured storage and sharing of data on cloud", **Published in:** 2016 International Conference on Information Processing (ICIP) 16-19 Dec. 2016.
23. ShwetaKaushik, Charu Gandhi, "Cloud data security with hybridsymmetric encryption", Published on: 2016 International Conference on ComputationalTechniques in Information and Communication Technologies (ICCTICT)11-13 March 2016.
24. Samydurai A, Revathi K, Prema P, Arulmozhiarasi D S, Jency J, Hemapriya S, "Secured Health Care Information exchange on cloud using attribute based encryption", published in 2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN) 26-28 March 2015.