Efficient Cloud Storage Using Data Partitioning With Secure Encryption Using Blow Fish Algorithm

S.Dhara,M.Kamarunisha,S.Aarthi

Department of computer Applications,Dhanalakshmi Srinivasan College of Arts and Science for Women,,Perambalur , 621 212, Tamilnadu, , India.

Email: dhara78956@yahoo.com*(Dhara Ss) Corresponding author: Dhara S*

Abstract— Cloud computing combines computational and storage resources managed by separate operating structures and makes them accessible to customers in the form of high-scale statistics storage and high-performance computing. Improved security concerns are one of the most important problems preventing widespread adoption of cloud computing, despite the benefits of cheap cost, less maintenance (from the perspective of the user), and increased flexibility. There must be a strong desire to protect the data entrusted to a public cloud. For the most dependable performance and safety, this work provides DROPs inside the Cloud, which judicially splits individual documents and copies them at key sites within the cloud. To ensure that the character fragments no longer include any relevant data, the departmenting of files into fragments is done entirely depending on the needs of a certain patron. The Grid Topology collection of principles ensures the node separation. Reflect fragments over the nodes that create the best study/write requests to further improve retrieval speed. The Blowfish algorithm was used to encrypt the data.

Keywords: File splitting, Replication, T-Coloring, Blowfish Encryption.

1. INTRODUCTION

When referring to distributed computing architectures, the term "cloud" has been used to describe the term. An internet-based service that provides dynamic resources, virtualization, elasticity and scalability is known as cloud computing. [1] In order to reduce costs and enable customers to benefit from all of the services given by cloud computing, cloud computing was created. Grid computing is closely related to cloud computing, although it is distinct from it. With the help of a variety of operating systems, cloud computing enables users to access services such as large-scaled data storage and high-performance computing. Compared to grid computing, cloud computing allows for a far more efficient transfer of data. Groups and businesses are transferring and dispersing their workforce by embracing cloud computing in order to reduce their costs [2]-[6]. As a result of cloud computing, consumers of cloud services don't need to know in great depth about the implementation of any particular technology, and they can simply access their data and do computer tasks through the Internet. Customers don't even know where the data are stored or where the records are located when they first obtain access to the facts and computing. Thus, a safety concern is immediately raised at this location. Security of data in the cloud computing is more difficult to manage than the security of conventional records systems.

The cloud storage benefits include flexible, cost-effective, and limit the risk of data loss, among other things. When it comes to third-party auditing and document integrity testing, numerous cloud techniques have recently gained attention. Keeping the data in pristine condition is the responsibility of the archiving service provider. Using the remote data integrity checking protocol, a cloud storage server that is corrupted or misbehaving may be identified.

Enhancing cloud security with the assistance of Fragmenting and duplicating information that divides the user's files into amounts, and mirrors them at an algorithmically determined location inside the cloud is outlined in the suggested method A series of regulations will be implemented in order to improve the overall performance of the blowfish. Also be aware that a single node assault will not expose the locations of pieces in cloud-based files. Make sure that the nodes are not close to each other so that the attacker doesn't know where the record fragments are, as well as make sure that there is a positive distance between them. For node separation, utilise the Graph Topology Grid set of rules.

In order to prevent criminals from entering, the article sets out to provide a tool that provides stronger authentication.

Secondly, the use of blowfish encryption may help to alleviate some of the security concerns.

Managed replication is needed to increase performance [7]-[12].

To make it easy for consumers to share their records with one other in a timely manner.

2. History Paintings

The problem with the existing method is that it takes a lot of time and money to perform the dynamic processing of data encryption and decryption techniques to store data in the cloud with security. Such limitations may be avoided by the suggested approach of records partition and replication, which provides high performance, low cost, and limited cloud storage space. Additional protection is provided against threaded assaults and server misbehaviour.

An whole new field of study in cloud computing security has been developed using the DROPs methodology. This might provide a more secure method of storing data than the current encryption method. For data protection and data retrieval, the DROPs method includes replication and a department dedicated to protecting the process. The fragmented papers were encrypted using a green encryption method. The data owner, cloud provider, and data consumer are all taken into account in this method.

3. IMPLEMENTATION

BLOWFISH ENCRYPTION

An encryption algorithm called Blowfish was supposed to be quick and symmetric: On big 32-bit microprocessors, it took 26 clock cycles each byte to encrypt data.

It's small enough to fit in a RAM of less than 5 kilobytes.

XOR, research table with 32-bit operands, and the addition feature are all that is needed.

blowfish has a flexible key period, which may range from 32 to 448 bits: the default is 128 bits. It is best suited for applications where the key does not change often, such as a communication connection or an automated document encryptor. Blowfish Encryption

Blowfish algorithm Steps:

Encryption

The first step is to split a 64-bit plaintext message into 32 bits.

Next, the "left" 32 bits are XORed with the first detail of a P-array to make a cost I'll name P, then passed though a change function I'll call F to produce a new value I'll call F'.

Step 3: The "left" half of the message is replaced by F', and the "proper" half is replaced by P', and the method is repeated 15 more times with consecutive members of the P-array.

To generate the sixty-four-bit ciphertext, the P' and F' values are recombined with the remaining items in the P-array (numbers 17 and 18). .

Decryption:

A 32-bit input is divided into four bytes and used as indices into an S-array.

Research findings are combined and XORed together to get the final result.

A symmetric algorithm, Blowfish uses the same method to encrypt and decode the same data. For encryption, plaintext is entered, whereas for decryption, ciphertext is entered.

Blowfish precomputes the P-array and S-array values depending on the consumer's key. The person's key is turned into the P-array and S-array upon impact, and the key itself may be deleted when the transformation is complete. Insofar as the core component no longer trades, the P- and S-array do not need recompilation, but they must be kept secret.

GRAPH TOPOLOGY GRID

In the first step, you'll need to post jobs to the grid.

In the second step, each request is submitted to the local server's duplication manager.

Using the replica Catalog, the reproduction manager asks which grid page contains the desired replication (Candidate websites).

If the report is no longer found on the lower level, its manager should send a Request to the higher level.

The fifth step is to figure out the charge for online communication between the requester's website and the candidate's site.

The spherical journey time is computed in step six (RTT).

If (d>RTT) then acquire access to the document from a distant location or, alternatively, make a copy.

This is the last step in testing the web page's storage part. Request the replacement set of rules if there is no storage space available, otherwise.

After determining whether the site is under a minimum amount of access load, the edge controller interacts with the Reservation Supervisor.

Once reservations are made, the Allocation manager is known as the source allocation manager.

In Step 11, the Replication Placement is carried out once the Allocation Manager has assigned the assets.

Reservation manager can't always succeed, thus LCA rules are called in Step 12.

Steps 8 and 9 are repeated once the LCA delivers a website with an identified web page.

Step 14: Select one of the sister nodes and proceed with step 10aeleven if the threshold Controller results in the highest access to load.

PROCEDURE

Report Fragmentation in the Cloud Framework

Replication of Blowfish Encryption

Access to control is granted on a time-based basis

Searching for and retrieving documents

Framework for the Cloud

Data owner, data consumer and service provider are all part of the cloud structure. Data may be stored in a cloud service provider's secure environment. Record encryption, fragmentation, and replication are all handled by CSP. When the owner of the data wishes to transmit a file to a cloud server, the user must first log in. A cloud file can only be sent if all the user's credentials are correct. Stats are used to show the cloud's surroundings to the user. To access cloud-based data, a user must first sign up and get authorization from the cloud service provider.

Fragmentation of a report

Fractionation plays an important role in ensuring the best possible balance between the amount of data that can be stored and its safety. In the process of fragmentation, every sensitive document is divided into several pieces in such a way that it is hard to accomplish the whole file in a single attempt. Encryption begins immediately after the report is uploaded to a cloud storage service. The cloud management will then begin fragmentation using the fragmentation engine. The record is broken up into a certain number of parts dependent on the value of the fragmentation threshold. Then, the data will be stored on cloud nodes utilising allocation algorithms. " Prior to saving any other nodes, the principal node is identified and prioritised for preservation. Afterwards, all of the last kth pieces will be arranged in the final nodes that are left. To reduce the total cost of data transfer, record splitting is performed. Finding every single split record is likewise quite unlikely. Horizontal, vertical, and mixed fragmentation are all types of fragmentation.

Blowfish Encryption

With the use of this plaintext or another kind of data, encryption may change this information into an encryption version that can only be deciphered by other entities if they have access to a certain decryption key. End-to-end encryption is one of the most important methods for securing data, particularly when it is being transported via networks. Blowfish encryption rules are used to encrypt encrypted report fragments in our system. Asymmetric key encryption implies that the same secret key is used for both encrypting and decrypting communications using Blowfish. Block cypher set of rules is also known as Blowfish, which indicates that it splits a message into fixed-period blocks during encryption and decryption. Blowfish has a block length of 64 bits.

It is possible to maintain part of the replicas on the same server or on other servers using the Replicationfacts replication mechanism. Replication is the process of copying and distributing data from one database to several others. Because of this, the stress on the original server is reduced, and the data on the server where it's duplicated is always there, which isn't always the case with mirroring. Increased performance, availability, and reliability may be achieved by data replication. Replication will lead to a rise in the number of cloud-based report copies. Consequently, the chance of the node defending the record being targeted by an attack is increased. In order to prevent any one carrier from lowering the alternative, replication and safety must be balanced.

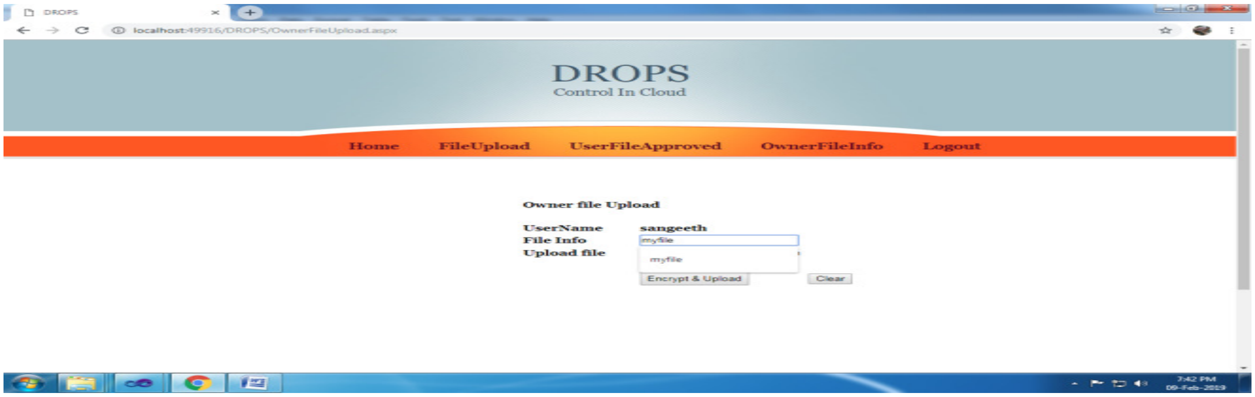
Time based get admission to control

A communication is encrypted by the business owner with the intention of allowing consumers to decode it at a later time. The information owner receives the record request from the user. The statistics owner selected a time period for accessing the data. Using the user's secret key and time token, the encrypted ciphertext may be decrypted. It is the combination of the individual's attribute constraint set and his or her permitted access time that decides whether or not the individual fulfils the policy[13-22].

Report Retrieval

By entering a secret record key, a user may receive a full splits file that has been merged and can be saved. Decryption is possible only if an individual's attribute set is inside the coverage of the ciphertext, and if the individual's get entrance time is later than the predetermined freeing time.

4. EXPERIMENTAL RESULT



Owner file Upload

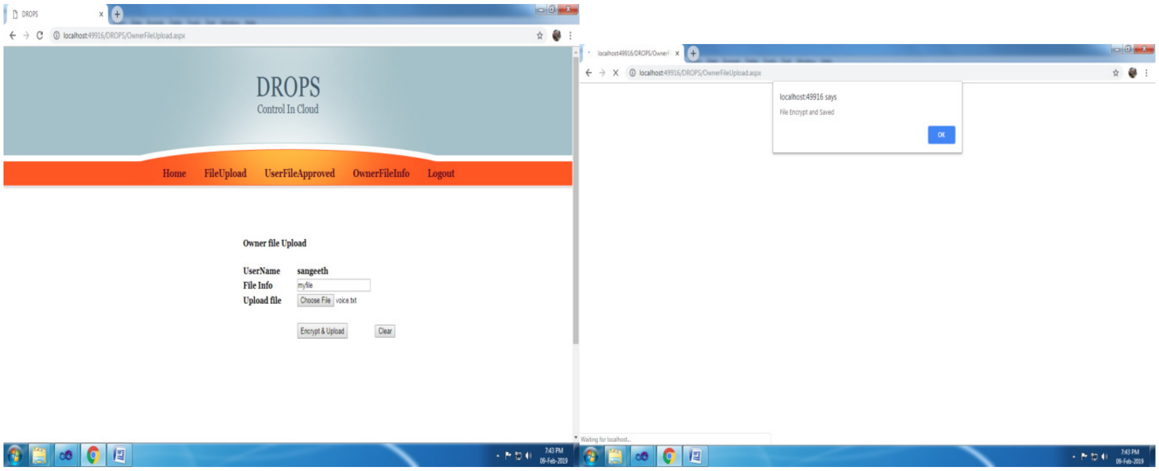
UserName sangeeth
File Info myfile
Upload file myfile

Figure.1. DROPS

The suggested system's overall performance is shown by the experimental results. Right here, a modification was made to increase file security by using fragmented record storage.

Fig. 1. This figure shows the details of the file storage. The person who owns the information may see the papers that they have submitted.

File Encryption



Owner file Upload

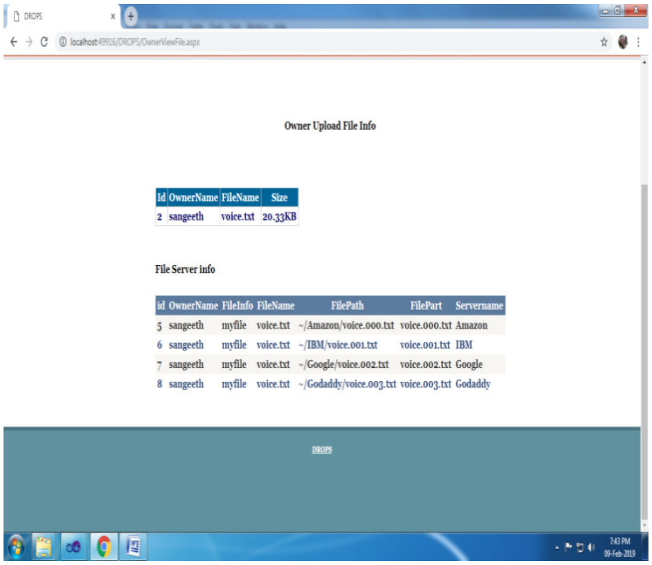
UserName sangeeth
File Info myfile
Upload file voice.txt

localhost:49916 says

File Encrypt and Saved

Figure.2. Blowfish encryption

Fig 2.: This determine shows the method of record encryption. Uploaded files are encrypted using Blowfish encryption algorithm then stored on database with securely.



Owner Upload File Info

Id	OwnerName	FileName	Size
2	sangeeth	voice.txt	20.33KB

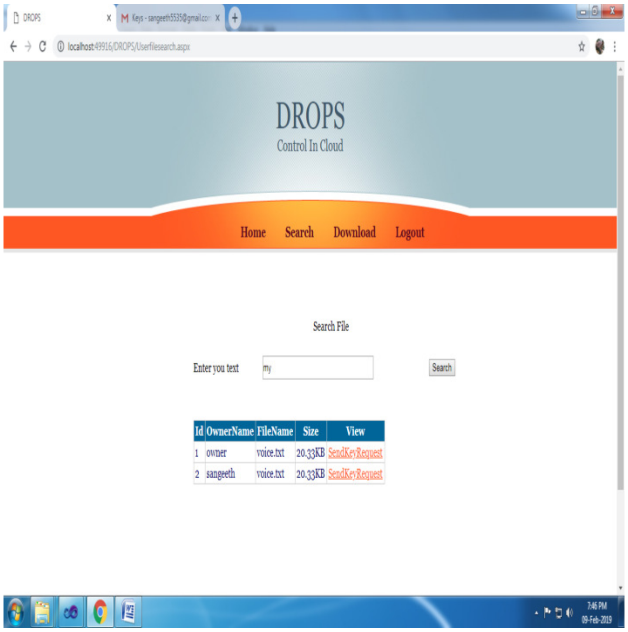
File Server info

id	OwnerName	FileInfo	FileName	FilePath	FilePart	Servername
5	sangeeth	myfile	voice.txt	~/Amazon/voice.000.txt	voice.000.txt	Amazon
6	sangeeth	myfile	voice.txt	~/IBM/voice.001.txt	voice.001.txt	IBM
7	sangeeth	myfile	voice.txt	~/Google/voice.002.txt	voice.002.txt	Google
8	sangeeth	myfile	voice.txt	~/Godaddy/voice.003.txt	voice.003.txt	Godaddy

Figure.3. File Division

Figure.3: Above determine indicates the file division and storage method. Uploaded files are fragmented and saved on one of a kind area.

file Request



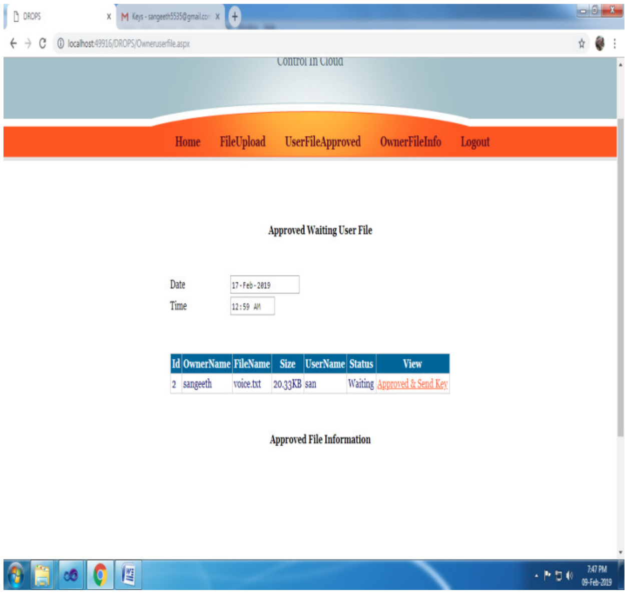
Search File

Enter you text: my

Id	OwnerName	FileName	Size	View
1	owner	voice.txt	20.33KB	SendKeyRequest
2	sangeeth	voice.txt	20.33KB	SendKeyRequest

Figure.4. File Request

Fig 4. This diagram indicates the technique of file request. right here person can search file and send request to the precise record proprietor for mystery key.



Approved Waiting User File

Date: 17-Feb-2019

Time: 12:59 AM

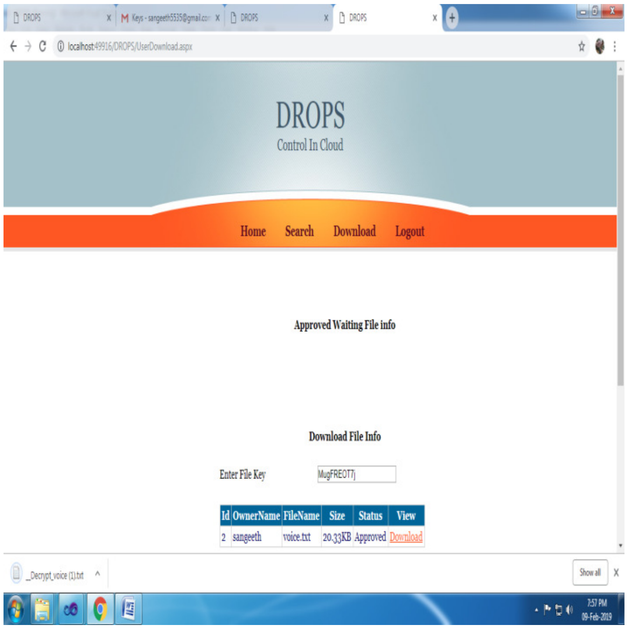
Id	OwnerName	FileName	Size	UserName	Status	View
2	sangeeth	voice.txt	20.33KB	san	Waiting	Approved & Send Key

Approved File Information

Figure.5. Key Sharing

Fig 5: Key sharing is the process of share mystery key to the asked consumer to get entry to record. whilst proprietor accepts the user request secret key will be send to the owner thru e mail or SMS.

Report Download



DROPS

Control In Cloud

Approved Waiting File info

Download File Info

Enter File Key MugFREOT7j

Id	OwnerName	FileName	Size	Status	View
2	sangeeth	voice.txt	20.33KB	Approved	Download

Figure.6. Report Access

Fig 6. : This diagram indicates the system of record down load. After were given permission from report access person can down load the file decrypt using mystery key shared via facts proprietor.

5. Conclusion

Using a division and replication system, the data was stored in a secure manner. The user must log in to the cloud, for each registered user, and get access to the provider's permissions from both patron and community levels. A secret document key is also produced for each new file added by the user. When a user wishes to download and access a file, they must enter a mysterious file key into their document, after which the separated chunks are united and the content may be downloaded. Security for the future is provided by this. Drops approach is used to ensure safe file access. An access control system that is time-based will be put in place to provide data users more control over their data. It will save time and resources in the future by not having to download, update, and reupload the material again.

REFERENCES

[1] k. Bilal, S. U. Khan, L. Zhang, H. Li, k. Hayat, S. A. Madani, N. Min-Allah, L. Wang, D. Chen, M. Iqbal, C. Z. Xu, and A. Y. Zomaya, “Quantitative comparisons of the country of the artwork facts center architectures,” Concurrency and Computation: exercise and experience, Vol. 25, No. 12, 2013, pp. 1771-1783.

[2] ok. Bilal, M. Manzano, S. U. Khan, E. Calle, ok. Li, and A. Zomaya, “at the characterization of the structural robustness of facts center networks,” IEEE Transactions on Cloud Computing, Vol. 1, No. 1, 2013, pp. 64-77.

[3] D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya, “electricity-green records replication in cloud computing datacenters,” In IEEE Globecom Workshops, 2013, pp. 446-451.

[4] Y. Deswarte, L. Blain, and J-C. Fabre, “Intrusion tolerance in disbursed computing structures,” In lawsuits of IEEE computer Society Symposium on research in protection and privacy, Oakland CA, pp. one hundred ten-121, 1991.

[5] B. Grobauer, T.Walloschek, and E. Stocker, “expertise cloud computing vulnerabilities,” IEEE safety and privacy, Vol. nine, No. 2, 2011, pp. 50-57.

[6] W. ok. Hale, “Frequency challenge: principle and programs,” court cases of the IEEE, Vol. sixty eight, No. 12, 1980, pp. 1497-1514.

[7] k. Hashizume, D. G. Rosado, E. Fernndez-Medina, and E. B. Fernandez, “An analysis of protection problems for cloud computing,” journal of internet services and packages, Vol. 4, No. 1, 2013, pp. 1-thirteen.

[8] M. Hogan, F. Liu, A.Sokol, and J. Tong, “NIST cloud computing requirements roadmap,” NIST unique e-book, July 2011.

[9] W. A. Jansen, “Cloud hooks: security and privateness problems in cloud computing,” In forty fourth Hawaii IEEE worldwide conference on device Sciences (HICSS), 2011, pp. 1-10.

[10] S.Kannadhasan, G.Karthikeyan and V.Sethupathi, A Graph Theory Based Energy Efficient Clustering Techniques in Wireless Sensor Networks. Information and Communication Technologies Organized by Noorul Islam University (ICT 2013) Nagercoil on 11-12 April 2013, Published for Conference Proceedings by IEEE Explore Digital Library 978-1-4673-5758-6/13 @2013 IEEE.

[11] A. Juels and A. Opera, “New techniques to protection and availability for cloud statistics,” Communications of the ACM, Vol. fifty six, No. 2, 2013, pp. 64-seventy three.

[12] S.Kannadhasan, M.Shanmuganantham and R.Nagarajan, System Model of VANET Using Optimization- Based Efficient Routing Algorithm, International Conference on Advances in Material Science, Communication and Microelectronics (ICAMCM-2021), Jaipur Engineering College and Research Centre, Jaipur, 19-20 February 2021. Published for IOP Conference Series: Materials Science and Engineering, Vol No: 1119, 2021, doi:10.1088/1757-899X/1119/1/012021

[13] Singh, D., Buddhi, D., & Karthick, A. (2022). Productivity enhancement of solar still through heat transfer enhancement techniques in latent heat storage system: a review. Environmental Science and Pollution Research, 1-34.

[14] Haseena, S., Saroja, S., Madavan, R., Karthick, A., Pant, B., & Kifetew, M. (2022). Prediction of the Age and Gender Based on Human Face Images Based on Deep Learning Algorithm. Computational and Mathematical Methods in Medicine, 2022.

[15] Jasti, V., Kumar, G. K., Kumar, M. S., Maheshwari, V., Jayagopal, P., Pant, B., ... & Muhibbullah, M. (2022). Relevant-based feature ranking (RBFR) method for text classification based on machine learning algorithm. Journal of Nanomaterials, 2022.

[16] Babu, J. C., Kumar, M. S., Jayagopal, P., Sathishkumar, V. E., Rajendran, S., Kumar, S., ... & Mahseena, A. M. (2022). IoT-based intelligent system for internal crack detection in building blocks. Journal of Nanomaterials, 2022.

[17] Chidambaram, S., Ganesh, S. S., Karthick, A., Jayagopal, P., Balachander, B., & Manoharan, S. (2022). Diagnosing Breast Cancer Based on the Adaptive Neuro-Fuzzy Inference System. Computational and Mathematical Methods in Medicine, 2022.

[18] Saroja, S., Madavan, R., Haseena, S., Pepsi, M., Karthick, A., Mohanavel, V., & Muhibbullah, M. (2022). Human centered decision-making for COVID-19 testing center location selection: Tamil Nadu—a case study. Computational and Mathematical Methods in Medicine, 2022.

[19] Kumar, R. R., Thanigaivel, S., Priya, A. K., Karthick, A., Malla, C., Jayaraman, P., ... & Karami, A. M. (2022). Fabrication of MnO2 Nanocomposite on GO Functionalized with Advanced Electrode Material for Supercapacitors. Journal of Nanomaterials, 2022.

[20] Karthick, A., Mohanavel, V., Chinnaiyan, V. K., Karpagam, J., Baranilingesan, I., & Rajkumar, S. (2022). State of charge prediction of battery management system for electric vehicles. In Active Electrical Distribution Network (pp. 163-180). Academic Press.

[21] Bharathwaaj, R., Mohanavel, V., Karthick, A., Vasanthaseelan, S., Ravichandran, M., Sakthi, T., & Rajkumar, S. (2022). Modeling of permanent magnet synchronous motor for zero-emission vehicles. In Active Electrical Distribution Network (pp. 121-144). Academic Press.

[22] Jayalakshmi, Y., Subramaniam, U., Baranilingesan, I., Karthick, A., Rahim, R., & Ghosh, A. (2021). Novel Multi-Time Scale Deep Learning Algorithm for Solar Irradiance Forecasting. Energies 2021, 14, 2404.