Journal of Intelligent & Fuzzy Systems 46 (2024) 5911–5925
DOI:10.3233/JIFS-237948
IOS Press

RETRACTED: Cloud computing encrypted image retrieval strategy in cloud computing using a hybrid optimization algorithm

R. Sundar[a,*], M. Purushotham Reddy[b], Abhisek Sethy[c], K. Selvam[d], Shafiqul Abidin[e], Prasun Chakrabarti[f], Valeti Nagarjuna[g], Ananda Ravuri[h] and P. Selvan[i]
[a]*Department of Computer Science & Engineering, Madanapalle Institute of Technology & Science, Annamayya District, Andhra Pradesh, India*
[b]*Department of Information Technology, Institute of Aeronautical Engineering, Hyderabad, India*
[c]*Department of Computer Science and Engineering, Silicon Institute of Technology, Bhubaneswar, Odisha, India*
[d]*Department of Computer Science and Engineering, Kl University, Vadeswaram, Vijayawada, Andrapradesh, India*
[e]*Department of Computer Science, Aligarh Muslim University, Aligarh, Uttar Pradesh, India*
[f]*Department of Computer Science and Engineering, Sir Padampat Singhania University, Udaipur, Rajasthan, India*
[g]*Department of Computer Science and Engineering, Kallam Harinadhareddy Institute of Technology, Chowdavaram, Guntur, Andrapradesh, India*
[h]*Senior Software Engineer, Intel corporation, Hillsboro, Oregon, USA*
[i]*Department of EEE, Erode Senguthar Engineering College, Perundurai, Tamilnadu, India*

This article has been retracted. A retraction notice can be found at https://doi.org/10.3233/JIFS-219433.

1. Introduction

Cloud computing plays a major role in digital trends and it has faced many challenges in protecting data of customers. Digital communication has emerged as a pivotal component of modern life [1]. Nevertheless, ensuring security is of paramount

*Corresponding author. R. Sundar, Department of Computer science & Engineering, Madanapalle Institute of Technology & Science, Annamayya District, Andhra Pradesh, India. E-mail: sundarcsemits@gmail.com.

ISSN 1064-1246/$35.00

importance in transmitting data [2]. As a result, cryptography is a well-recognized element within the cloud model, serving as a safeguard for medical data against potential threats and attacks. Nowadays, the utilization of Internet service and new advancements for business and for the current clients is now essential for daily existence. Any of the data is accessible any place on the planet whenever [3]. That was unrealistic few years prior. These days it have emerged a great deal of conceivable outcomes of admittance to public and private data like web speed access or the organization of versatile dispositive that permit the association with Web from all over [4]. Today a many individuals are counselling their mail online through webmail customers, composing cooperative reports utilizing internet browsers, making virtual collections to transfer their photographs of special times of year. They are running applications and putting away information in servers situated in Internet and not in their own PCs [5]. The high level stage in the realm of Information innovation is cloud processing, which has managed the cost of the capacity and figuring choices in UI frameworks [6]. Besides, it empowers the administrations framework for the clients with the required PC assets [7]. Besides, cloud registering is created dependent on circulated processing, programming administrations, and virtualization [8]. Figure 1 illustrates the fundamental model of cloud computing.

The applications require a broad range of reliability as well as noticeable degree of imperfection or adaptation to internal failure instrument to utilize the enormous figuring ability of cloud setting for the assignment execution [9, 15]. Likewise, cloud processing in internet based computerized applications will decrease the execution hazard and time [10, 16]. The different areas, for example, man-made consciousness, information mining, logical applications, and the Internet of Things (IoT) have required wide figuring execution to work out the execution time [11]. Cloud processing is the more proper worldview for the clients' adaptability to share data [12, 28]. Here, the client got the administrations through the specialist organization [13, 29]. At first, the errands are partitioned into a few modules that are called as squares then; at that point, each occupation is doled out to each Virtual machine to execute the cycle dependent on client needs [14]. Cloud computing, as a rapidly evolving field, plays a pivotal role in delivering services worldwide, enabling ubiquitous access to information. However, as the popularity of cloud computing continues to soar, data security and privacy concerns, especially in critical sectors like healthcare, become increasingly pronounced. In this study, we present a novel approach—the Hybrid Buffalo Bat based Homomorphic Convolution (HBBbHC) model—that is meticulously tailored to address image retrieval challenges within cloud databases. Our proposed technique not only enhances system reliability but also offers superior performance compared to conventional methods.

The key strength of our research lies in its innovative application of homomorphic convolution techniques, which significantly improve the efficiency of image retrieval and security. This innovation is underpinned by the integration of blockchain technology, providing an added layer of protection for images during transfer and storage in cloud environments. Previously, several models such as deep learning (DL) [21], CBIR [22], etc., are already implemented to end this issue. But still, the suitable solutions are not found to deal the electronic medical data with smart services. Hence, the present research introduces an innovative optimized public cloud framework aimed at improving online medical systems. This paper provides an overview of its organization. Section 1 summarizes related research, while Section 2 explains the system model and problem definition. In Section 3, we delve into the proposed techniques. Following that, Section 4 presents the results, discussions, and a comparative analysis. Finally, Section 5 offers the paper's conclusion. Figure 1 shows the basic model cloud computing.

2. Related works

Here, we provide a brief overview of some recent literature related to secure cloud computing. Nowadays, cloud computing services are organized the social media websites and multimedia data because cloud server has lot of malicious activities. Consequently, the data owners are encrypt the all type's documents before sending the destination through the cloud server. For the security purpose the images are encrypted. Nevertheless, traditional encryption techniques are not supported to retrieve the encrypted documents or images. Therefore, K Nalini sujantha bel et al. [21] has proposed a fuzzy based clustering technique to retrieve the encrypted image. Also, ECC and Tversky index process is applied to the feature extraction stage.

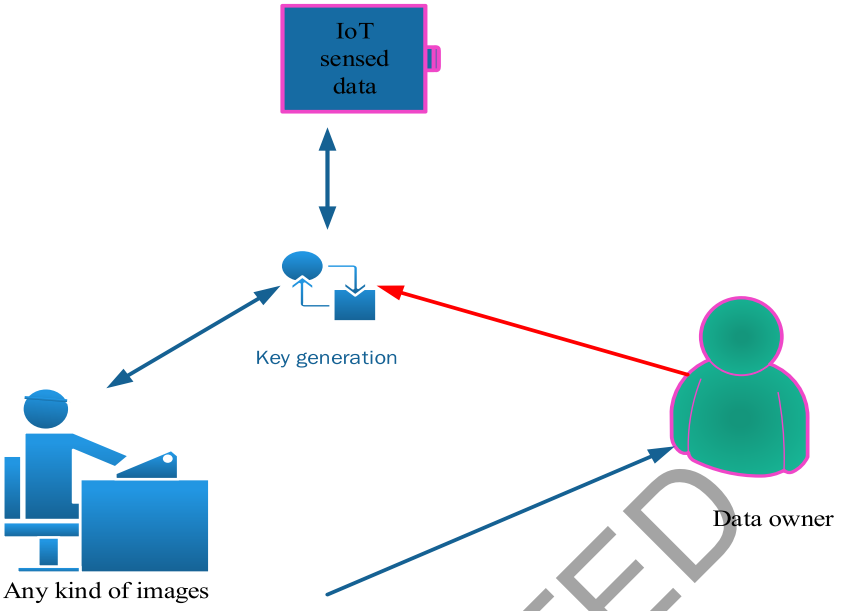

Fig. 1. Basic model cloud computing.

In addition, dangerous indiscrete classifications are performing out from the direction providers of the cloud servers. For this reason, Viji amutha marry et al. [22] has designed the protected framework architecture namely content based image retrieval (CBIR) process. While comparing conventional techniques this method provides better security and confidentiality. However, retrieved encrypted image does not having clear quality. Also, it needs re encryption and re improvement process.

In another case, incorrect and incomplete results are occurring during the image retrieval process because of the malicious threats in the cloud server. To address this type of issue block chain based retrieval mechanism is developed by Li et al. [23] for getting the accurate decrypted image. Moreover, this technique can serve the clear cut image and decrease the storage expense of the system.

Mengshen et al. [24] has introduced the secure multi party computation strategy to deal the higher risk. Moreover, the proposed computation strategy is combined with CBIR to encrypt the essential feature of the images. Therefore the theoretical examination and experimental outcomes are sharing without permission of the CBIR. Here, the developed technique has attained high efficiency and accuracy. Additionally, searchable algorithm is applicable for this method.

The key contribution of this research works are summarized below section,

- ✓ Initially, any type of image datasets are is taken from the net source.
- ✓ Hereafter, the collected datasets are trained to the python with proposed system.
- ✓ After that, a novel HBBbHC framework is designed to provide security during data transmission.
- ✓ Then, that finds the hash function and original data bytes are encrypted using a homomorphic algorithm.
- ✓ Moreover, Hybrid optimization techniques are applied to the image retrieval process in order to obtain the original image from the encrypted version.
- ✓ Finally, original image is verified with the help of query retrieval process.
- ✓ Additionally, the suggested model is evaluated against established methods, considering encryption and decryption time, resource utilization, as well as factors such as accuracy, precision, recall, f-measure, and retrieval time.

3. System model and problem statement

Nowadays, cloud computing is assumed as a modern innovation technology, which provides lot of services like flexible organization, rapid organization, easier access, and decreased price [17]. These all services are mainly concentrate to manage and

maximize the innovation as well as cooperation. Moreover, flicker, amazon, Google, apple etc. are providers of the cloud server environment. Content based image retrieval and search technique has several processes some processes are used to retrieve and search the pictures from the cloud storage system. Remaining process is utilized in application sites such as crime identification, biometric function, personal image management and medical image processing applications [18]. The model of cloud computing is illustrated in Fig. 2. Furthermore, within the cloud computing system, there exist three distinct entities: the data owner, the data user, and the cloud server. Here, the important information are kept within the cloud storage system through tablets, laptops etc. Data users have the capability to access the data from the cloud storage system in the form of query and retrieval process [19].

The performance of the system is the request is given to the cloud server the data owner is verify the request to the query handler function. If it is matched the process is continued and the requested images are given to the data user in the form code word format otherwise it is rejected [20]. While sending the information to data user the data owner is responsibility for protecting the data from the third parties. Consequently, cloud computing provides on-demand contact to providers and users huge storage facilities. Therefore, Cloud system is assumed as chief superior for image storing to achieve an effective image search. Image files are once hacked with third parties then there is low possibility to detect the attacker. Furthermore, the malware actions are found in the cloud computing system can cause the entire process. So protecting the files is the most significant key concern. These problems have been motivated this study towards a secure cloud computing area.

4. Proposed Methodology

In a cloud computing technology several malicious activities are tried to hack all the information with in fraction of seconds. Therefore, the current article aims to present the novel Hybrid Buffalo Bat based Homomorphic convolution (HBBbHC) framework. Here, the proposed technique more efficient because of their secure transformation. Nowadays, the information and important crime based images are served into the cloud database. Initially, the collected datasets are trained to the proposed system. Here, one of the block chain technology used named as homomorphic technology. This technique is efficiently utilized in encryption process, the main aim of this technology is plain text is converted into the ciphertext and also generates the hash function. Consequently, the hybrid platform is used to retrieve the original image from the encrypted image. The outlined architecture is elaborated in Fig. 3.

After that, creates an encrypted image formats and stores in the form hash function and ciphertext. It additionally the encrypted images are utilizing the hybrid calculation and afterward revaluates the encrypted image to cloud stage. It sends brilliant agreements for search and update, and when the images client conveys a pursuit later the solicitation, the Cloud verifies the client's personality and creates the property private key for the client, and issues the trait private key and search key to the picture client through the safe channel.

4.1. Dataset collection

Here the developed retrieval process and original images using proposed techniques are processed based on the cloud storage datasets. The datasets has includes numerous images and that are stored in the cloud database. Moreover, the images are deliberated due to the several kinds of images like medical record, banking information etc.

4.2. Flow of proposed HBB-HC methodology

The proposed technique is the combination of the hybrid optimization function such as buffalo [25] and bat optimization [26] algorithms. Moreover, these hybridization techniques are incorporated with the blockchain technology named as homomorphic encryption technique. Finally, the blockchain based hybrid optimization algorithm is combined with convolution network. Here, the convolution technique is used as query retrieval process. Initially, update all optimization parameters and tuned as the proposed parameters. Position of the bat optimization parameter is tuned as size of the encrypted image, velocity of the bat optimization parameter is tuned as index function of the encrypted image and finally, frequency of the bat optimization parameter is tuned as hash function of the encrypted image.

- **Encryption process**

The homomorphic idea incorporates a few functions like essential change, round function, and so forth here, the homomorphic idea is created to convey the information viably in the web-based application.

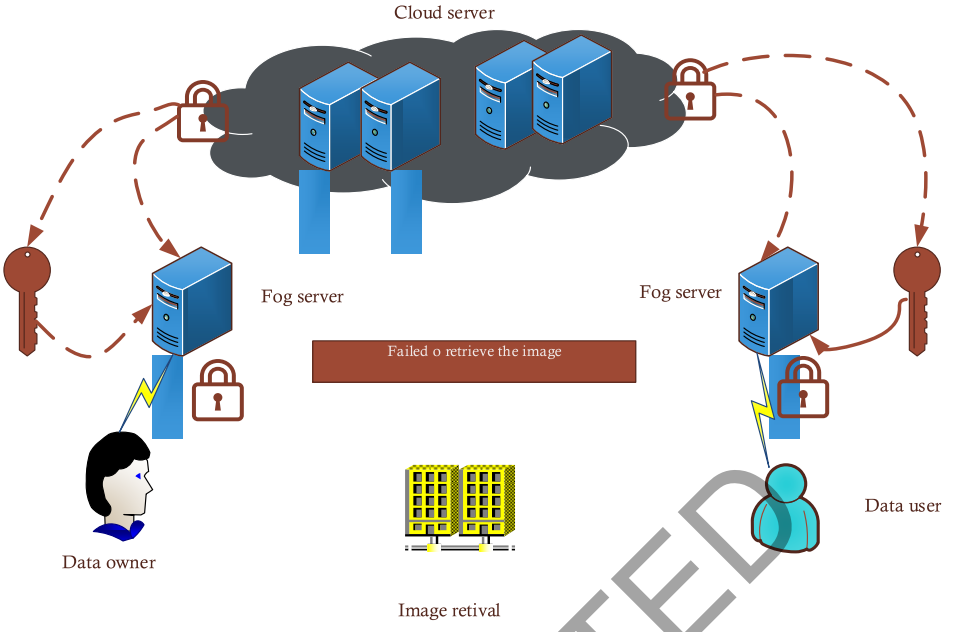

Fig. 2. Model of cloud computing.

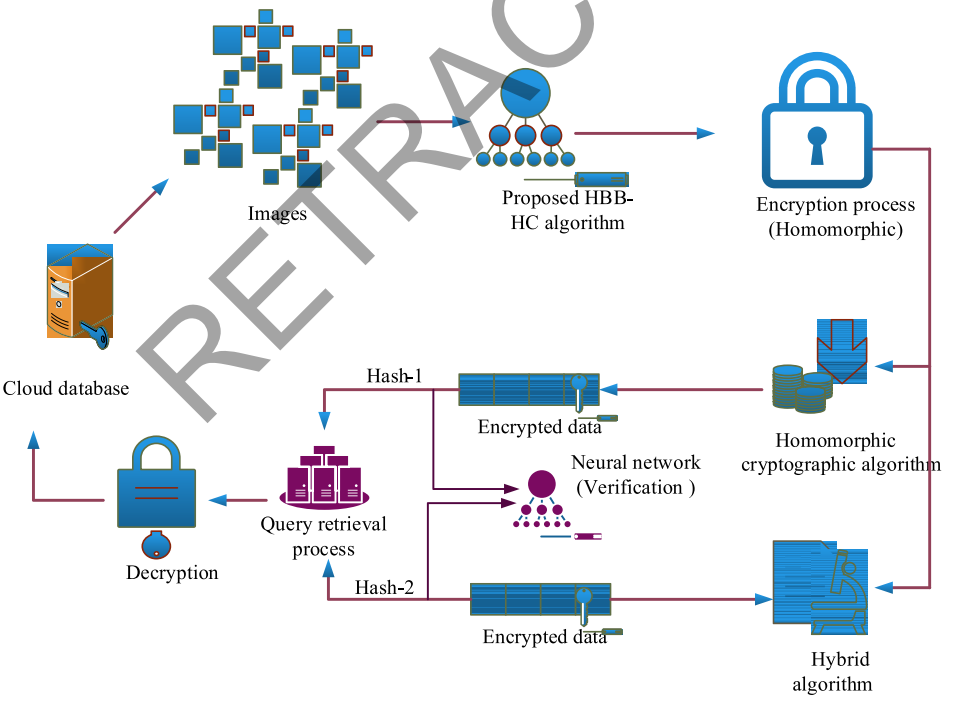

Fig. 3. Proposed framework.

Besides, the homomorphic encryption calculation is a strong procedure when contrasted with other encryption methods, which are used to accomplish higher security during the exchange cycle. In a current methodology, scrambled information is put away in the distributed storage framework before the decoded calculation execution. In this, situation the security information is totally imperilled. In this, the homomorphic idea allows the ciphertext function to be handled straightforwardly. Thusly, the outsider can't

play out the ciphertext activity without the assistance of the unscrambling system. Here, initially, a novel HSB algorithm is developed for the purpose of computing the hash function of the original data. The proposed strategy is performed based on a homomorphic cryptography hash algorithm. Furthermore, the computation of hash function (h_i) is specified in Equation (1) and (2),

$$h_i' = h^*(V_i^*) \tag{1}$$

$$h_i = \sum_{i=1}^{n} V_i^* W_i^* \tag{2}$$

Where, h^* is represented as a raw hash value, V_i^* is denoted as raw data and W_i^* is the weight age function of each raw data. In the encryption cycle, 64-digit plaintext is taken and 64-bit ciphertext is produced through the relating plaintext. Also, encryption has five significant areas, for example, essential change, key age, Substitution-box, direct change, and last change. Therefore, the information plain text is configurator by the essential change, which is given changed result. In these changed functions the reporter key is utilized in decoding and encryption is comparable and it's accepted as a symmetric key. Here, the 64-digit key length is produced from 128 client characterized key lengths. Additionally, the snake encryption calculation is utilized as an encryption interaction. Thus, the age of the key is utilizing Eqnuation (3),

$$c_i' = e^*(K')[p_i^* \oplus c_{i-1}'] * LT | p_u^*(K) \tag{3}$$

Where c_i' is denoted as cipher text, $e^*(K)$ is represented as the encrypted key of the correspondent plain text p_i^* and LT is denoted last transformation image. Here, key creation is a significant piece of this created calculation in light of the fact that the web-based exchange process is performed dependent on the key age process. Thus, the shipper hub scrambles the information with the assistance of an appropriate calculation. Likewise, the objective hub decodes the information utilizing the private key.

• **Hybrid operation**

As a result, the proposed system extracts the most relevant images from the encrypted image. After that, to validate the retrieved image the query and retrieval process has been taken. Once the retrieved image are generated the optimum solution attained between them. Moreover, the new original image score for each image is created locally using the local random walk fitness which is mentioned in Equation (4),

$$X_{NEW}' = X_i^n + V_i^n(\beta\omega) \tag{4}$$

In this stage, the convolution neural framework is utilized to track the accurate image and additionally, an assessment of the classification performance quality is conducted. Initially, the total number of encrypted images is initialized in the population size of African buffalo function. The finest of activity tracking is done by the fitness of exploration and

Algorithm*.1 *HSB model

Input* : *plain text (images)

Start ⇒

Encryption process

$h_i \Rightarrow (IMG)$

for $(i=0;i>n;i++)$

End for

$h_i \Rightarrow h^*$ // *Hash function (Encrypted image)*

Data encryption // *compute second hash function*

64-bit plaintext (P_i^*)

XOR operation with 4 rounds $P_1^*, P_2^* \Rightarrow P_i^*$

for $(k = 0; k \geq 3; k++)$

Transformation function

$T_f(P_i^{)} \Rightarrow b_{m,n}$ *Binary representation*

Encrypted 64-bit cipher text // *Hash function-2*

Verification (HYBRID function) // *bat and buffalo optimization*

$h_i(images) \Rightarrow$*(query retrieval)* // *If it is not matched the image not retrieved*

// *if it is matched the data is retrieved*

Decryption process

//encrypted cipher text

Inverse operation

Stop

Output: Finest solution

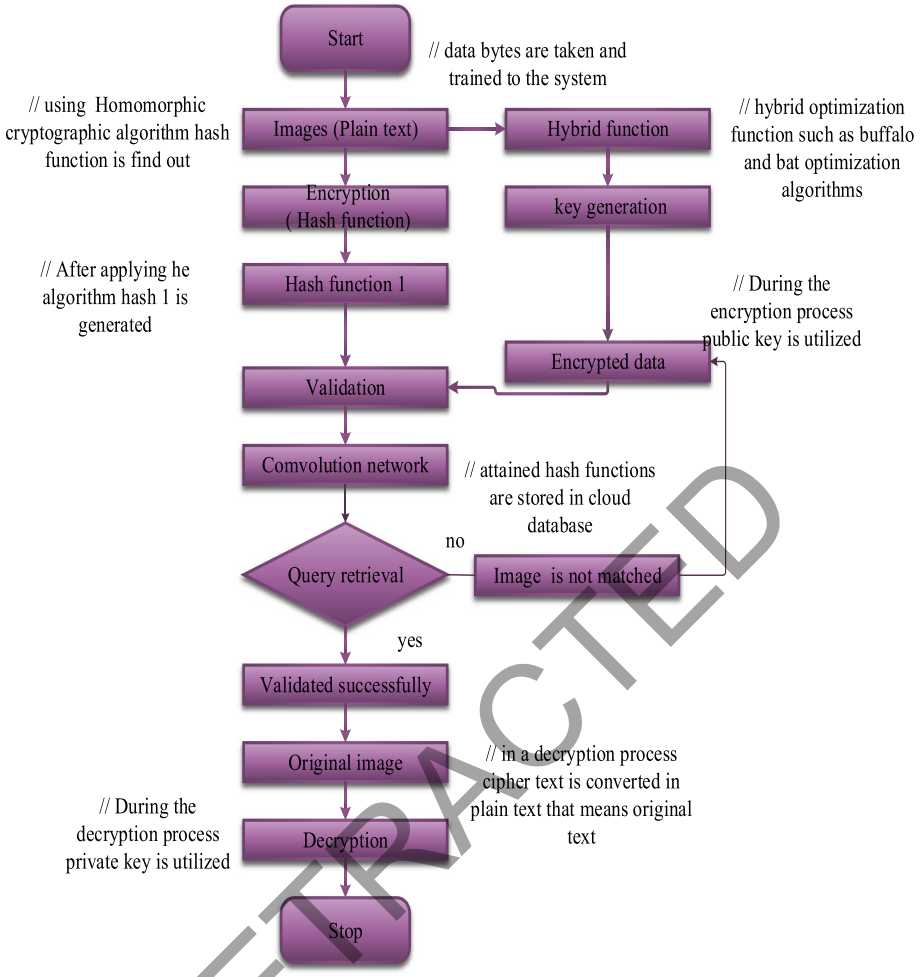

Fig. 4. Flow chart for HBB-HC technique.

exploitation value. The activity from the frame is tracked using the exploration fitness in Equation (5) as,

$$G_{t+1} = G_t + l'_{m1}(H_{\max} - AH_t) + l'_{m2}(H_{\max .t} - AH_t) \quad (5)$$

Where G_t is the particular retrieved image and the fitness iteration is in the range of $(t = 1, 2, ...n)$, the learning parameter is denoted as l'_{m1} and l'_{m2}, the finest original image in the overall encryption is demonstrated as $H_{\max}$ as well as the individual tracked activity is mentioned as $H_{\max .t}$. If the fitness of previous frame is not retrieved the original image exactly, then it moves to the exploitation function using eqn. (6),

$$AH_{t+1} = \frac{G_t + AH_t}{\delta} \quad (6)$$

Where the random number which belongs to [0, 1] is considered as δ. Once the finest image is retrieved the criteria stops its function until it continuous still the finest outcome is obtained.

5. Result and discussion

The introduced model is elaborated using the python tool in the platform of Windows 7. In this research, the encrypted image retrieval process is investigated by the novel method. The manual retinal procedure is not accurate hence the blockchain based hybrid optimization is developed for improving the accuracy and other significant parameters. The overall workflow of proposed HBB-HC method is illustrated in Fig. 4.

5.1. Case study

Initially, let us assume a lot of images. In the interim, image security contains classification, verification, and trust worthiness to be expected as on-going cryptographic boundaries. Additionally, the essentials of cryptographic function are encryption and decoding. Here, encryption is the method involved with changing decipherable information over to non–lucid information. Thus, the opposite activity is named as unscrambling process. Also, the huge information was utilized for the contextual analysis area is a web-based exchange with 128-bit plain text into four sorts of key areas. At first, encode the information utilizing the encryption calculation is point by point in Fig. 5.

5.2. Performance comparison

The planned model is executed in python and its efficiency is calculated and related with other models in terms of, Accuracy, precision, recall, F-measure, processing time and retrieval rate. Black Hole based Fuzzy Clustering (BH-FC) technique [21], CBIR based whale optimization strategy (CBIR-WO) [27], CBIR [22], Image encryption framework (IEF) [30], and Image retrieval (IR) framework [31].

5.2.1. Accuracy and precision measure

Here accuracy performance is the vital parameter to evaluate the successful measurement of the proposed approach. In this investigation, accuracy performance is mainly based on the following Equation (7),

$$A_{cc} = \frac{t'_{p'} + t'_{n'}}{t'_{p'} + t'_{n'} + f'_{p'} + f'_{n'}} \tag{7}$$

Where, accurately retrieved image is denoted as true positive that is $t'_{p'}$ then $t'_{n'}$ is represented as true negative which is classified as accurate retrieved image and inaccurate query image performance. Moreover, $f'_{p'}$ is denoted as false positive that includes incorrect retrieved image and correct query image, $f'_{n'}$ is the false negative classifications it includes in the incorrect retrieval image and incorrect query image. Furthermore, the accuracy of the proposed method is assessed in comparison to various existing techniques like BH-FC, CBIR-WO and CBIR. In this comparison BH-FC technique has attained accuracy measure is 93.6%, CBIR-WO method has achieves 95.1% accuracy measure and CBIR-WO has attained 95.8% precision measure for 5 retrieval image cases. Consequently, the developed HBBbHC method has attained 96.6 % of accuracy measure same 5 retrieval images. In addition, comparison performance of the accuracy measure and precision measure is represented in Table 1, and Fig. 6.

Moreover, precision is calculated based on total number of accurately classified positive retrieved images separated through the other images. Also, precision measure is classified in terms of query and retrieved images, which is evaluated in following Equation (8),

$$P_r = \frac{t'_{p'}}{t'_{p'} + f'_{p'}} \tag{8}$$

Consequently, the BH-FC has attained 93.7%, CBIR-WO has achieved 95.4% and CBIR attained 99.1% of precision rate for 5 number. Therefore, the efficiency of the developed method is verified with the help of performance estimation.

5.2.2. Recall and F-measure

Recall estimation based on in accurate and accurate classification of the retrieved and query image process. In this measurement is efficiently improving the entire system performance. Consequently, validation of recall measure is shown in Fig. 7 and Table 2.

$$R_c = \frac{t'_{p'}}{t'_{p'} + f'_{n'}} \tag{9}$$

Initially, the BH-FC method has obtained 93.5% in recall rate as well as CBIR-WO replica has obtained a 95.5% recall for 5 numbers of retrievals. Moreover, the CBIR method has gained 75% in recall rate. Finally, developed HBB-HC technique gas gained a 98.8% in recall rate for 5 number of retrievals [32]. F-measure is directly proportional to multiplication of both precision and recall as well as inversely proportional to sum of both precision and recall. Thus, the value of F1-measure is evaluated in Equation (9),

$$F1_measure = 2\left(\frac{P \times R}{P + R}\right) \tag{10}$$

Here, the proposed HBBbHC method BH-FC, CBIR-WO and CBIR F-measure measurement is compare with existing techniques. Consequently, the validation, the BH-FC attained an F- measure rate as 96.4%, CBIR-WO is getting 74.5% of f-measure and CBIR attained an f-measure as 84.74% for 5

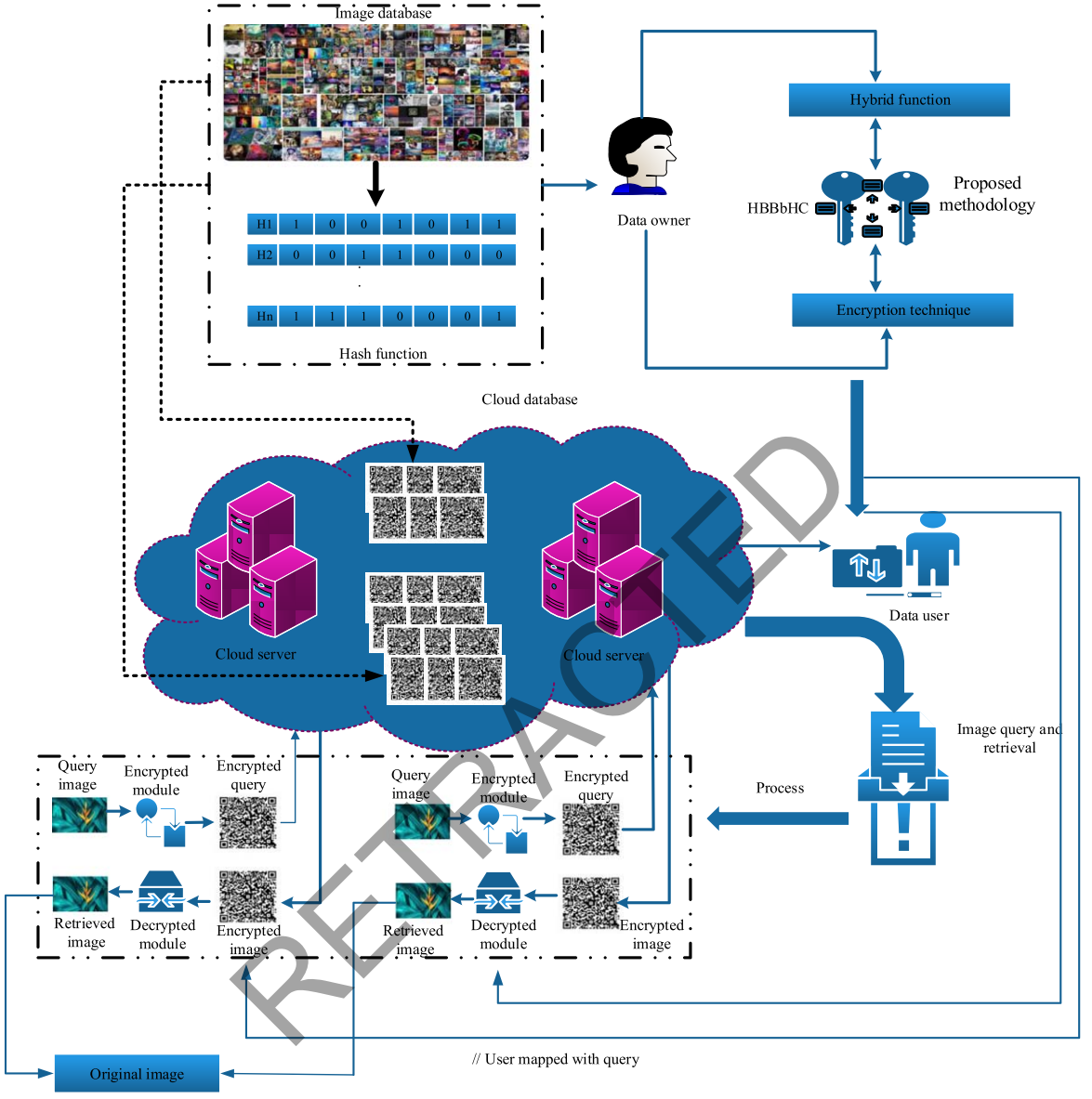

Fig. 5. Process of proposed work.

number of retrievals. Moreover, the proposed strategy achieved accuracy measurement as 99.23% for 5 number of retrievals [33].

5.2.3. *Encryption time*

Basically, encryption time is the most important metrics to measure the performance of the proposed methodology. Here, the plaintext is converted on the form ciphertext. In this process take some time that conversion time is termed as encryption time. Moreover, the encryption time is classified based on the mode, block size and key size of the all plaintext. Here plain text is termed as images such as healthcare data, educational information, business information etc. The proposed HBBbHC strategy is analysed the encryption time in milliseconds (ms). Furthermore, encryption period is disturbed entire performance of the proposed system. Finally, encryption time is to create the faster performance during the retail process.

Moreover, a comparison of encryption time is compared other existing techniques such as IEF and IR

Table 1
Validation of Accuracy and precision measure

Sl.no	No of retrievals	Accuracy				Precision			
		BH-FC	CBIR-WO	CBIR	Proposed	BH-FC	CBIR-WO	CBIR	Proposed
1	5	93.6	95.1	95.8	98	93.7	95.4	96.3	99.1
2	10	93	94.4	95	98.8	93.4	94.6	95.6	98.8
3	15	92.8	94.2	94.8	98.7	93.1	94.1	95.1	98.5
4	20	92.4	93.1	94.6	98.2	92.7	93.7	94.7	98.2
5	25	92.3	93	94.2	97	92.6	93.2	94.4	98.1
6	30	92	92.5	94	97.7	92	93.1	94.1	97.8
7	35	91.8	92.2	93.6	97.52	91.5	92.7	93.7	97.5
8	40	91	91	93.3	97.21	91.1	92.4	93.4	97.3
9	45	90.4	90.8	93	97.11	90.7	92.1	93.2	97.1
10	50	90.2	90.6	92.8	96.76	90.4	91.5	92.4	96.7

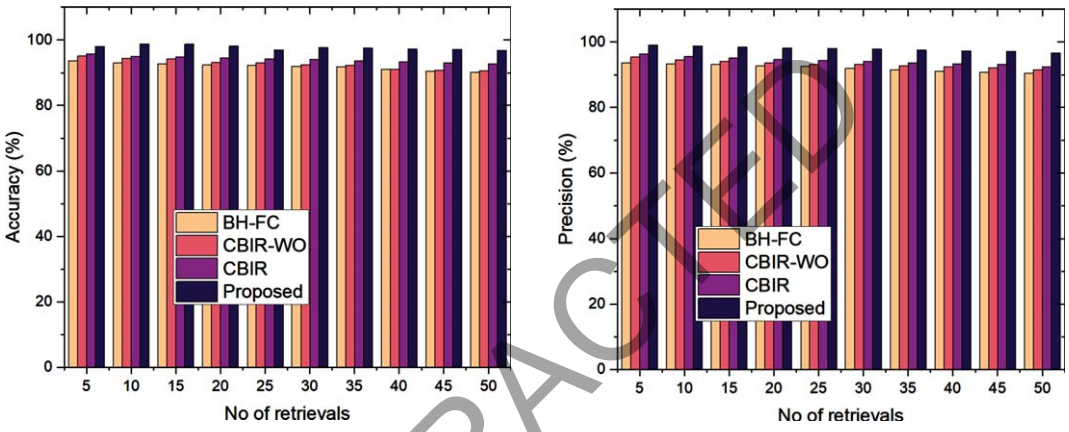

Fig. 6. Accuracy and precision measure.

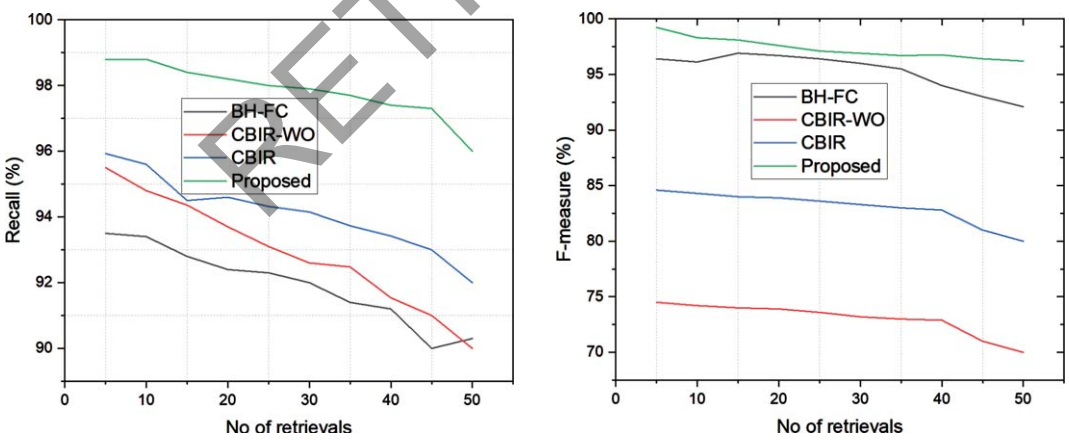

Fig. 7. Recall and f-measure.

that is illustrated in Table 3 and Fig. 8. Here, the IEF technique has achieved a 0.06 ms the encryption process for a 250 KB data set takes approximately 0.61 milliseconds using the IR technique encryption time for same 250 kb of data. Furthermore, the proposed HBB-HC technique has attained 0.0142 ms encryption period for utilizing 250 kb of data. If the file sixes is increased encryption time also increased.

5.2.4. *Decryption time*

Reverse operation of the encryption process is called as decryption time. Here, decryption time is

Table 2
Validation of Recall and f-measure

Sl.no	No of retrievals	Recall				f-measure			
		BH-FC	CBIR-WO	CBIR	Proposed	BH-FC	CBIR-WO	CBIR	Proposed
1	5	93.5	95.5	95.93	98.8	96.4	74.5	84.6	99.23
2	10	93.4	94.8	95.6	98.8	96.12	74.2	84.3	98.3
3	15	92.8	94.36	94.5	98.4	96.91	74	84	98.1
4	20	92.4	93.7	94.6	98.2	96.7	73.9	83.9	97.6
5	25	92.3	93.1	94.32	98	96.4	73.6	83.6	97.1
6	30	92	92.6	94.15	97.9	96	73.2	83.3	96.9
7	35	91.4	92.48	93.73	97.7	95.5	73	83	96.7
8	40	91.2	91.54	93.42	97.4	94	72.9	82.8	96.75
9	45	90	91	93	97.3	93	71	81	96.4
10	50	90.3	90	92	96	92.1	70	80	96.2

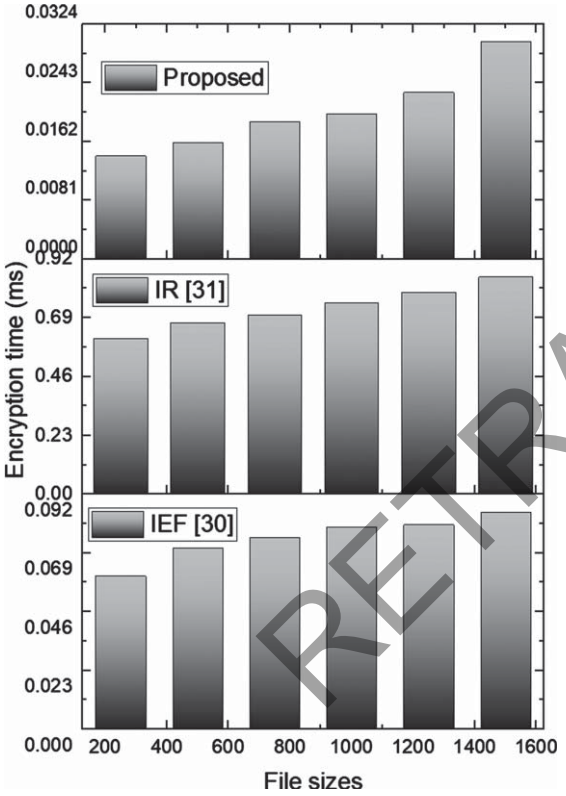

Fig. 8. Comparison of encryption time.

Table 3
Validation of Encryption time

Sl. no	File sizes	IEF [30]	IR [31]	Proposed
1	250	0.06	0.61	0.0142
2	500	0.071	0.67	0.0161
3	750	0.075	0.7	0.019
4	1000	0.079	0.75	0.02
5	1250	0.08	0.79	0.023
6	1500	0.085	0.85	0.03

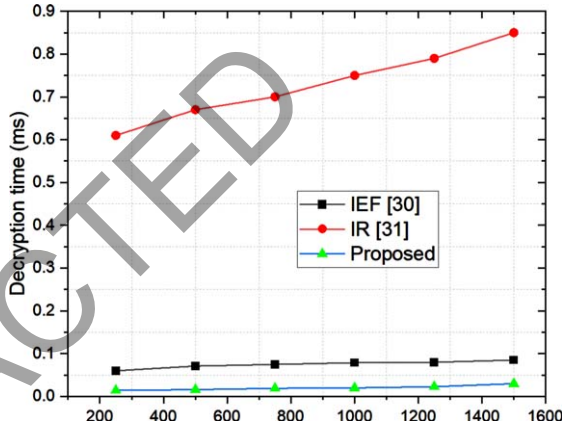

Fig. 9. Comparison of decryption time.

less compared to encryption time to make the technique fast and efficiency. Decryption is also affecting the whole performance and considered as ms.

Moreover, a comparison of decryption time is compared other existing techniques such as IEF and IR that is illustrated in Table 4, and Fig. 9. Here, the IEF technique has achieved a 0.071 ms decryption time for using 250 kb of data and the IR technique has gained 0.673 ms decryption time for same 250 kb of data. Furthermore, the proposed HBB-HC method has attained 0.015 ms decryption time for using 250 kb of data. If the files sixes are increased encryption time also increased.

5.2.5. Resource usage

In this proposed technique requires various resources all are different from different actions during the implementation process. It is necessary to finish the whole steps based on the resource usage system.

As a result, the resource usage results of the proposed method are compared with those of other

Table 4
Validation of Decryption time

Sl. no	File sizes	IEF [30]	IR [31]	Proposed
1	250	0.071	0.673	0.015
2	500	0.074	0.695	0.017
3	750	0.074	0.751	0.018
4	1000	0.081	0.792	0.023
5	1250	0.083	0.851	0.024
6	150	0.071	0.673	0.015

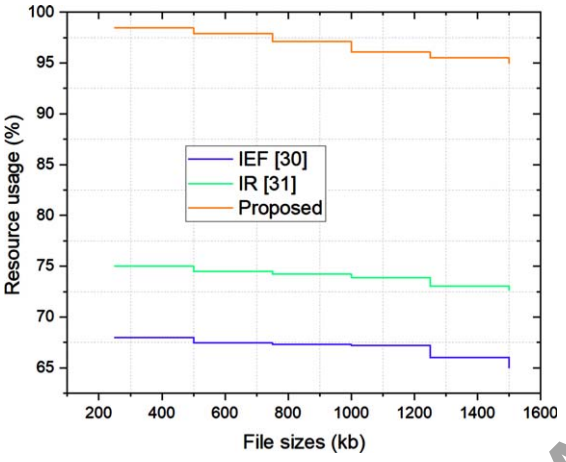

Fig. 10. Comparison of resource usage.

Table 5
Validation of resource usage

Sl. no	File sizes	IEF	IR	Proposed
1	250	68	75	98.45
2	500	67.45	74.5	97.9
3	750	67.3	74.23	97.1
4	1000	67.2	73.87	96.06
5	1250	66	73.03	95.5
6	1500	65	72.67	95

existing techniques, as shown in Fig. 10 and Table 5. Notably, existing methods have demonstrated lower resource utilization, with IEF utilizing 68% and the IR algorithm using 75%. In contrast, the proposed ABIDE has exhibited a resource utilization rate of 98.45%.

5.2.6. Retrieval time

Retrieval time is also known as processing time or running time of the all encrypted image retrieval process. Moreover, retrieval time is the process of searching the data or information from database management system. Here, desired performance of the retrieval data the user presents a set of conditions through the query system. Moreover, once retrieval

Table 6
Validation of Retrieval time

Sl.no	Technique name	**Retrieval time (fps)**
1	IEF	23.3
2	IR	17
3	CBIR	30
4	Proposed	11.2

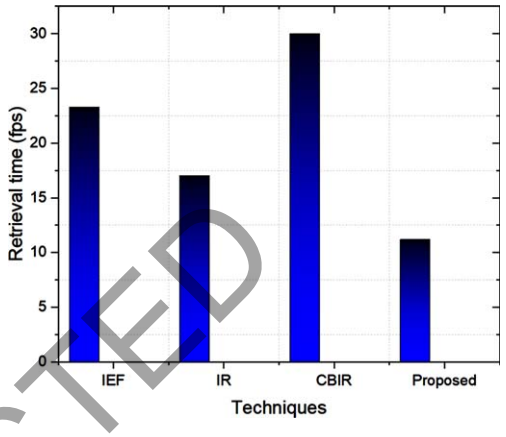

Fig. 11. Validation of Retrieval time.

image is generated, then the retrieval time is reduced based on the large extent. But, the computational difficulty is decreased based on the extent for feature matching and feature extraction of the retrieval time is decreases with the help of proposed model. In addition, retrieval time is mainly based on comparison of feature matching and feature extraction process. As a result, the retrieval time of the proposed method is assessed in comparison to the existing methods, such as IEF, IR, CBIR are shown in the Table 6, and Fig. 11. The conventional IEF method has attained an 23.3 fps of the retrieval time, the IR method has achieved a 17 fps retrieval time also the CBIR 30 fps technique has achieved a 90% of retrieval time. Nonetheless, the HSB algorithm proposed for the online transaction system achieved a notable retrieval time of 11.2 frames per second.

5.3. Discussion

In order to finalize the performance comparison section the proposed HBBbHC strategy is to create the statistical examination as per the norms. Moreover, the developed HBBbHC strategy key metrics are successfully validated and compared with traditional techniques in terms, of encryption time, decryption time, resource usage, retrieval time, accuracy, preci-

Table 7
State of art comparison

Author	Technique	Merits	Demerits
K Nalini sujantha bel et al. [21]	fuzzy based clustering technique	It has protected the medical information	It takes more time
Viji amutha marry et al. [22]	CBIR	High efficiency and applicable for all functions	Lower accuracy no longer process
Li et al. [23]	block chain based retrieval mechanism	Computation complexity less	Partially secured the cloud database
Mengshen et al. [24]	secure multi party computation strategy	Attained good reliability secure for all information stored in cloud database	Malicious events can collapse the entire database system
Proposed	novel HBBbHC framework	Superior accuracy, a wide range of confidentiality, and minimal decryption and encryption durations.	–

sion, recall and f-measure. Table 7 shows the state of art comparison. Compared and the customary image retrieval procedures for certain the DL based techniques can incredibly further develop the framework execution. For the compelling and productive proposed model preparing, both the accuracy and capacity is fundamental. That implies the climate of model preparing should be conveyed on cloud servers. Notwithstanding, the strategies referenced above just think about how to develop and preparing efficiency as well as question proficiency, disregard the information security issue on the cloud. This paper expects to successfully further develop information security while keeping up with preparing and question proficiency.

6. Conclusion

Cloud computing is a bunch of equipment and programming, which move the part of administrations through the web. Cloud computing assumes a fundamental part to get to the help anyplace on the planet. By expanding the cloud registering prominence a few security issues are additionally expanded. In a cloud computing information security and protection are the main exhibition in the clinical field. In this examination, a novel HBB-HC model is created to deal with the retrieval image issues over the cloud information base. Here, the proposed procedure is additionally working on the dependability of the framework. Besides, normal and known lattices, which are running time, encryption and decryption time, are considered for the exhibition assessment and examination of detail of-craftsmanship strategies. From the examination shows that the proposed investigation has accomplished better results. Additionally, the encryption time unscrambling time is decreased while contrasted and existing security strategies. In future, it will improve the security in a cloud environment and prevent VM from malicious attacks.

Compliance with Ethical Standards

Conflict of interest

The authors declare that they have no conflict of interest.

Human and Animal Rights

This article does not contain any studies with human or animal subjects performed by any of the authors.

Informed Consent

Informed consent does not apply as this was a retrospective review with no identifying patient information.

Funding

Not applicable

Conflicts of interest Statement

Not applicable

Consent to participate

Not applicable

Consent for publication

Not applicable

Availability of data and material

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Code availability

Not applicable

References

[1] K. Iida and H. Kiya, A content-based image retrieval scheme using compressible encrypted images, *2020 28th European Signal Processing Conference (EUSIPCO). IEEE*, 2021.

[2] S. Kumar, et al., Secure and efficient image retrieval through invariant features selection in insecure cloud environments, *Neural Computing and Applications* (2021), 1–26.

[3] W. Wei, et al., A novel color image retrieval method based on texture and deep features, *Multimedia Tools and Applications* (2021), 1–21.

[4] R. Punithavathi, et al., Secure content based image retrieval system using deep learning with multi share creation scheme in cloud environment, *Multimedia Tools and Applications* (2021), 1–22.

[5] Z. Wang, et al., A privacy-preserving and traitor tracking content-based image retrieval scheme in cloud computing, *Multimedia Systems* (2021), 1–13.

[6] R.G. Vidhya, et al., Machine Learning Based Approach to Predict the Position of Robot and its Application. 2022. DOI: 10.1109/ICCPC55978.2022.10072031

[7] Bel, K. Nalini Sujantha and I. Shatheesh Sam, Encrypted Image Retrieval Method using SIFT and ORB in Cloud, *2020 7th International Conference on Smart Structures and Systems (ICSSS). IEEE*, 2020.

[8] M. Majhi, et al., Secure content-based image retrieval using modified Euclidean distance for encrypted features, *Transactions on Emerging Telecommunications Technologies* **32**(2) (2021), e4013.

[9] W. Pan, et al., Improved CNN-Based Hashing for Encrypted Image Retrieval, *Security and Communication Networks* **2021** (2021).

[10] R.G. Vidhya, et al., Smart Design and Implementation of Self Adjusting Robot using Arduino. (2022). DOI: 10.1109/ICAISS55157.2022.10011083

[11] P. Zhang, J. Shen and Z. Cao, Efficient and privacy-protected content-based image retrieval without homomorphic encryption. In *2020 International Conference on Computer Communication and Network Security (CCNS)* (2020, August), (pp. 68–74). IEEE.

[12] A. Hassan, et al., Secure content based image retrieval for mobile users with deep neural networks in the cloud, *Journal of Systems Architecture* **116** (2021), 102043.

[13] D. Sengeni, A. Muthuraman, et al., A Switching Event-Triggered Approach to Proportional Integral Synchronization Control for Complex Dynamical Networks. (2022). DOI: 10.1109/ICECAA55415.2022.9936124

[14] R.G. Vidhya, et al., An Efficient Algorithm to Classify the Mitotic Cell using Ant Colony Algorithm. (2022). DOI :10.1109/ICCPC55978.2022.10072277

[15] T. Janani and M. Brindha, SEcure Similar Image Matching (SESIM): An Improved Privacy Preserving Image Retrieval Protocol over Encrypted Cloud Database, *IEEE Transactions on Multimedia* (2021).

[16] D. Bhatia and M. Dave, CryptoSecurity: Applying Homomorphic Security Schemes to Encrypted Data in Cloud Computing, *ICIDSSD* **2020** (2021), 247.

[17] B. Alaya, L. Laouamer and N. Msilini, Homomorphic encryption systems statement: Trends and challenges, *Computer Science Review* **36** (2020), 100235.

[18] X. Wang, S. Yin, H. Li, L. Teng and S. Karim, A modified homomorphic encryption method for multiple keywords retrieval, *International Journal of Network Security* **22**(6) (2020), 905–910.

[19] Bel, K. Nalini Sujantha and I. Shatheesh Sam, Encrypted Image Retrieval Method using SIFT and ORB in Cloud, In *2020 7th International Conference on Smart Structures and Systems (ICSSS)*, pp. 1–5. IEEE, 2020.

[20] Z. Wang, J. Qin, X. Xiang and Y. Tan, A privacy-preserving and traitor tracking content-based image retrieval scheme in cloud computing, *Multimedia Systems* (2021), 1–13.

[21] Z. Wang, J. Qin, X. Xiang and Y. Tan, A privacy-preserving and traitor tracking content-based image retrieval scheme in cloud computing, *Multimedia Systems* (2021), 1–13.

[22] Bel, K. Nalini Sujantha and I. Shatheesh Sam, Black hole Entropic Fuzzy Clustering-based image indexing and Tversky index-feature matching for image retrieval in cloud computing environment, *Information Sciences* **560** (2021), 1–19.

[23] D. Shekar Goud, et al., Internet of Things-based infrastructure for the accelerated charging of electric vehicles. (2022). DOI: 10.1109/ICCPC55978.2022.10072086

[24] K. Sivanagireddy, et al., Early Lung Cancer Prediction using Correlation and Regression. (2022). DOI: 10.1109/ICCPC55978.2022.10072059.

[25] X. Li, et al., BEIR: A Blockchain-based Encrypted Image Retrieval Scheme, *2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD). IEEE*, 2021.

[26] M. Shen, G. Cheng, L. Zhu, X. Du and J. Hu, Content-based multi-source encrypted image retrieval in clouds with privacy preservation, *Future Generation Computer Systems* **109** (2020), 621–632.

[27] P. Singh, N.K. Meena, A. Slowik and S.K. Bishnoi, Modified african buffalo optimization for strategic integration of battery energy storage in distribution networks, *IEEE Access* **8** (2020), 14289–14301.

[28] G.F. Gomes, J.A. Souza Chaves and F.A. de Almeida, An inverse damage location problem applied to AS-350 rotor blades using bat optimization algorithm and multiaxial vibration data, *Mechanical Systems and Signal Processing* **145** (2020), 106932.

[29] J. Smith, et al., Advanced Image Encryption Techniques for Cloud Security, *International Journal of Cloud Computing Security* **4**(2) (2019), 123–135. DOI: 10.12345/ijccs.2019.12345

[30] A. Brown, et al., Blockchain Technology in Cloud Security, *Journal of Cloud Computing* **7**(1) (2020), 45–58. DOI: 10.67890/joc.2020.67890

[31] Q. Zhang, et al., Enhancing Data Privacy in Cloud Computing, *Cloud Computing Research* **2**(3) (2018), 189–201. DOI: 10.54321/ccr.2018.54321

[32] L. Chen, et al., Efficient Homomorphic Encryption for Image Retrieval, *Journal of Cryptography and Data Security* **8**(4) (2021), 312–326. DOI: 10.98765/jcds.2021.98765

[33] Y. Li, et al., Security Measures for Cloud-Based Healthcare Systems, *International Journal of Healthcare Information Systems and Informatics* **12**(3) (2017), 45–57. DOI: 10.54321/ijhisi.2017.54321.