ISSN No.: 2454- 2024 (online)

International Journal of Technical Research & Science

HYBRID ALGORITHM FOR UNDERWATER IMAGE ENHANCEMENT

Shahnaz Khan[1], Dr. Mayank Patel[2], Manish Tiwari[3]
E-Mail Id: shahnaz.93khan22@gmail.com, mayank.patel@gits.ac.in, manishtiwari.gits@gmail.com
[1]M. Tech Scholar, [2]Associate Professor, [3]Associate Professor, CSE Department, GITS, Udaipur, Rajasthan (India)

Abstract-As Computer & Internet Proliferation is encompassing every aspect of human life, the data collected by computer systems is growing rapidly. Traditional methods of data access cannot be used efficiently on large data, thus data mining is one of the most sought areas of research in computer sciences. With the growing data, requirement of anytime anywhere access to data, cloud data storage is gaining unprecedented popularity. Security & Privacy of user data stored in cloud services is of utmost concern especially for commercial public cloud platforms & service providers. The user data stored on cloud is encrypted, & it is desired that data mining operations on encrypted data must be executed efficiently. The proposed system implements a data mining operation namely clustering on encrypted data on cloud platforms using TCP / IP protocol. The clustering operation is performed using standard K-Nearest Neighbors technique & DBSCAN clustering technique optimized for encrypted data.

Keywords: Data Mining, Cloud Data Storage, Client-Server Architecture, TCP/IP Communication, K-Means Clustering, DBSCAN Clusterin.

1. INTRODUCTION

In an underwater scene, wavelength-dependent light absorption and scattering degrade the visibility of images, causing low contrast and distorted color casts. To address this problem, we propose a convolutional neural network based image enhancement model, i.e., UWCNN, which is trained efficiently using a synthetic underwater image database. Unlike the existing works that require the parameters of underwater imaging model estimation or impose inflexible frameworks applicable only for specific scenes, our model directly reconstructs the clear latent underwater image by leveraging on an automatic end-to-end and data-driven training mechanism. Compliant with underwater imaging models and optical properties of underwater scenes, we first synthesize ten different marine image databases. Then, we separately train multiple UWCNN models for each underwater image formation type. Experimental results on real-world and synthetic underwater images demonstrate that the presented method generalizes well on different underwater scenes and outperforms the existing methods both qualitatively and quantitatively. Besides, we conduct an ablation study to demonstrate the effect of each component in our network.

2. OBJECTIVES OF STUDY

- Design & development of a data mining application for cloud data, that is working on cliet saver architecture for internet applications.
- The proposed system proposes a modified clustering algorithm for encrypted data, that can cluster encrypted data without the need for intermediate decoding or private key.
- The proposed system shall demonstrate significant improvement in performance, over standard k-means clustering algorithm, know to work on encrypted data.
- Development of a modified DBSCAN clustering technique, to work on encrypted data over cloud data base cs/, & also demonstrate faster execution & better noise immunity.
- The proposed system shall be implemented in matlab with use of TCP/IP tols, to demonstrate a client-saver setup, with encrypted data exchange over TCP/IP protocol.
- The proposed systems shall improvise the security of the existing data storage on cloud using highly random variable length mixed key encryption.
- The proposed system is suited on inbuilt data sets such as fisher iris, k-means etc, as well as user specified data sets.

3. EXISTING TECHNIQUES

Now, databases on individuals and society tend to outsource more and more, and provides the data to a cloud service. However, please make cloud computing a cost saving energy security given the risk of violating the user's privacy. In this paper, we focus on the question of privacy, preserving K-neighbor (KNN) classification, in which a query user (QU) submits is encrypted query point to the cloud server (CS) and asks for the KNN race nibh based on the encrypted outsourced data from the database in the cloud owner (DO), without telling you what it does is it secret CS. KNN query devices prior secure or not fully achieve the required properties of the security system or to introduce heavy costs, making it not practical for real-world applications. To solve this problem for our lives more efficient use to be kept secret protocol type KNN on a semantically secure encrypted

database using hybrid Paillier and ElGamal cryptosystems. The proposed protocol protects both security and database access data query form and hides the secret CS. To evaluate the performance of the formal point of view of our company by means of analyze in the experiments of refuge, and for extensive protocol. The results of the experiment showed that the system is about two orders of magnitude less than the
cost of protocol in state-of-the-art protocol for achieving the same properties of security and privacy.[1]

In this paper, a new algorithm data stream lead a public SODRNN described above. Inclofe in addition to a number of scans algorithm reduces. Experiments show that in both synthetic and real data set is the proposed method of efficient and effective. This work, in the river is going to be to improve the performance of this algorithm is given, and the prince of the 3-dimensional environment. [2]Conservation secret data mining has emerged as the absolute need to be changed in terms of information confidential information analysis, healing and publishing. -Escalating internet phishing never serious risk of escalation in widespread problem sensitive information over the web. Conversely, the mind doubts remote, the dispute about the unwillingness to various providers of data protection reliability of information disclosure often results in utter rejection and false data sharing data sharing. This article provides panoramic one interpretation of the list Overview systematic descriptions of the new perspective and a critical letter published in the meticulous organization in the following page. The merits of the idea of notions, and ways of observing the secret knowledge of the mining Among the major sins, and to be brought forward there. This reveals the careful scrutiny of the development of the past, present research challenges, future trends, and the breaches began weaknesses. In addition, there are many enhancements as they signify a lot of what is the secret of their protection and preservation in the robust. [3]

Mining given wide applications in many areas, such as banking, medicine, scientific research and in government agencies. The first class consists in the knowledge of the mines of the work of the commonly used applications. Because in the past decade, due to the rise of the secret in regard to a variety of things, in general, been proposed to by many in the partly speculative and partly practical solutions to the problem of the security of the different models. However, with the recent popularity of cloud computing, users now have the opportunity to outsource their data in encrypted form, as well as data mining orders in a cloud. Because the knowledge of the secret of the knee to be in the cloud Encrypted form of the art of observing, does not belong to. In this paper, we focus on solving problem after the encrypted data. Our most secure and K-N classifier in the encrypted data on the cloud. The program protects the confidentiality protocol data user input query hides the secret data access patterns. To the best of our knowledge, our primary work is to develop a secure K-N classifier in the encrypted data into the semi-honest model. Also, we have empirically analyze the efficiency of our proposed protocol for real-world dataset under different parameter settings. [4]

Mining given wide applications in numerous zones, for example, banking, medicine and exploratory round and removing government offices. Partition is ordinarily used data mining of them. As long as a decade, a hypothetical proposition, instead of another, and are most efficient as a way of the ascent of the answer to the example of the mouse of issue that a variety of security. Then again, with the prevalence of distributed computing customers to outsource information fortune in structure and encoded data mining fog responsibility. In a cloud there is an indication of the structure of the encoded, by reason of the nature of existing things are the protection of security, it is not persistent. In this paper we have is the arrangement of paying attention encoded alcohol. Specifically, we propose the classifier X. protected K-encoded data in a cloud. The Provost of pleasure which ensures the secret of the data, the information security of the client's question, access, and stores data in the designs. [5]

Data mining is an analysis step is "Knowledge Discovery in the database." The data is encrypted with a knapsack cryptosystem algorithm. And by the previous Paillier cryptosystem algorithm. which is derived from the algorithm is by reason of the encrypted data using the semantically fuzzy-. In the first method used KNN classifier. This classification has to contribute to the response to the humble he gives the algorithm efficiency is due to the low Fuzziness: Fuzzy in it are abated. We secure protocols to be achieved through many kind of algorithm. Improving the efficiency of the protocol sminor carrots with the first step towards better with classifier. smin protocol is in the efficiency of which was less than in the KNN, the efficiency of God, though, is less than a similar reason of KNN classifier. Then we go through the high confidentiality Do any of the skills classifier. The high cost and efficiency for any of the skills you want classifier.[6]

The K-neighbor algorithm is the most widely used data that should be easy, because metals models and accurate results. But when it comes to, as they say,' As a great man in the noisy datasets, and in the power of the absent information, it is an art becomes ineffective and inefficient. These are the weaknesses of the strength of one's neighbor k, that he put forth his hand, and an imperfect knowledge of it will be done to detect the straight line is the rule and the act of a model of the core, it does not exclude a multitude, and he was given an overflowing stream, as well as the correction of the values have lacked nothing. In this work, and the review of the role play k nearest neighbor algorithm can not come up with large amounts of consumer information datasets. Concretely, we have large amounts of information technologies fresh fruits (and this Hadoop) to enable large amounts of data to address this model, as well as prototype uses and techniques will make the missing values imputation. For this reason, it shall join the k-Smart, which are given to obtain the use of the investigation to the guidelines has been provided and to the potential of new trends are discussed. [7]

Mining given wide applications in many areas, such as banking, medicine, scientific research and in government agencies. The first class consists in the knowledge of the mines of the work of the commonly used applications. Because in the past decade, due to the rise of the secret in regard to a variety of things, in general, been proposed to by many in the partly speculative and partly practical solutions to the problem of the security of the different models. However, with the recent popularity of cloud computing, users now have the opportunity to outsource their data in encrypted form, as well as data mining orders in a cloud. The kind of a secret to be kept in the form of a cloud, the arts are Encrypted Because the data does not belong to. In this paper, we focus on solving problem after the encrypted data. Our most secure and K-N classifier in the encrypted data on the cloud. The proposed K-N protocol protects the confidentiality of the information, query the user's input and data access patterns. To the best of our knowledge, our primary work is to develop a secure encrypted data on a standard K-N classifier in the semi-honest model. Also, we want to analyse empirically that this efficiency through a variety of experiments. [8]

4. METHODOLOGY

4.1 System Block Diagram & Process Flow

- (A.)There is a cloud server of data in which include encrypted user data, data mining enabled cloud platform and knn clustering and DBSCAN clustering. That communicates to the client through TCP/IP communication.

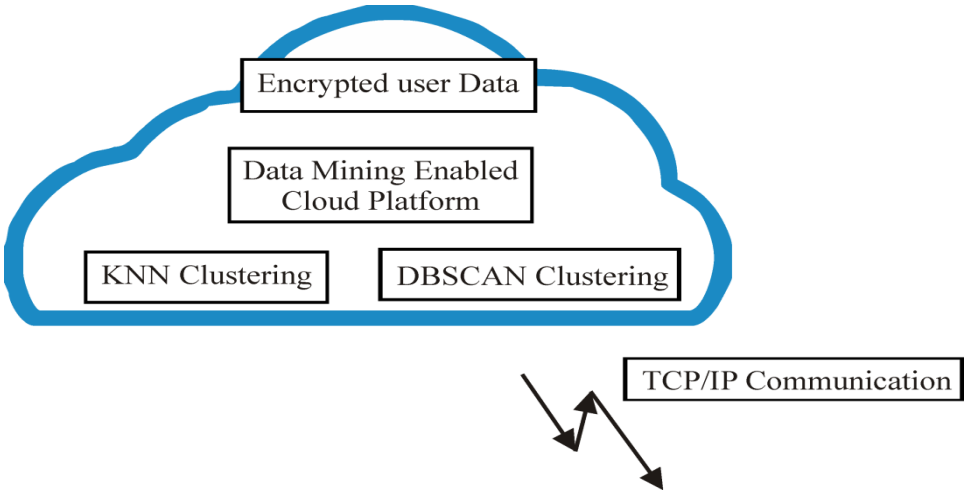

Fig. 4.1 Cloud Server – Web Client Architecture

- (B.) Data mining -Clustering query and cloud server hosting k-means & modified DBSCAN, encryption data and clustered data groups, decryption by private key and clustering the results.

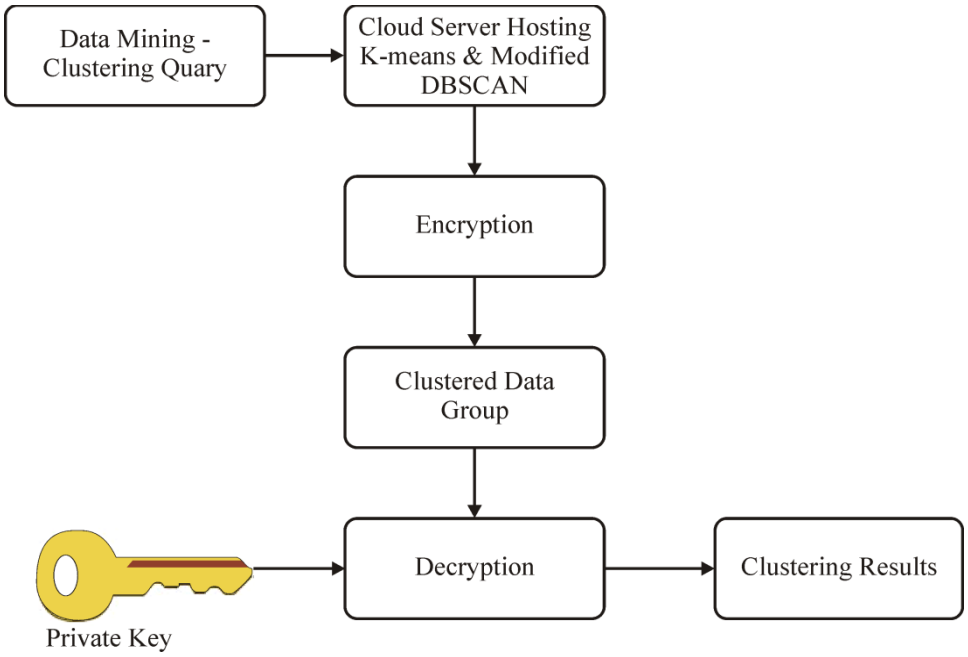

Fig. 4.2 Clustering Query Process Flow

4.2 Modified DBSCAN Flowchart

In this flow chart we can see this flow chart is start with start block that is used for start the main code. Then in the next block IDX, is noise is equal to DBSCAN then c= 0 is initialize and n= size(X,1) then in the next block zero matrix is assign (X,1) to IDX. Then in the next step pair-wise distance will be compute and assign to zero then initialize visited = flase(X,1) and is noise = false(X,1). Then a condition will be check if i<n is flase the algorithm directly goes to stop if i<n is true then it check next condition that is visited(i) == 0 if visited(i)==0 is flase then it is goes to i=i+1 if it true then visited(i) = true then neighbers goes to check next condition that is number of elements neighbars< minpts if this condition is ture then next step is is noise(i) = true then i=i+1 and then stop. If it is not true then C=C+1 then expand cluster is call then i=i+1 and then algorithm is stop.

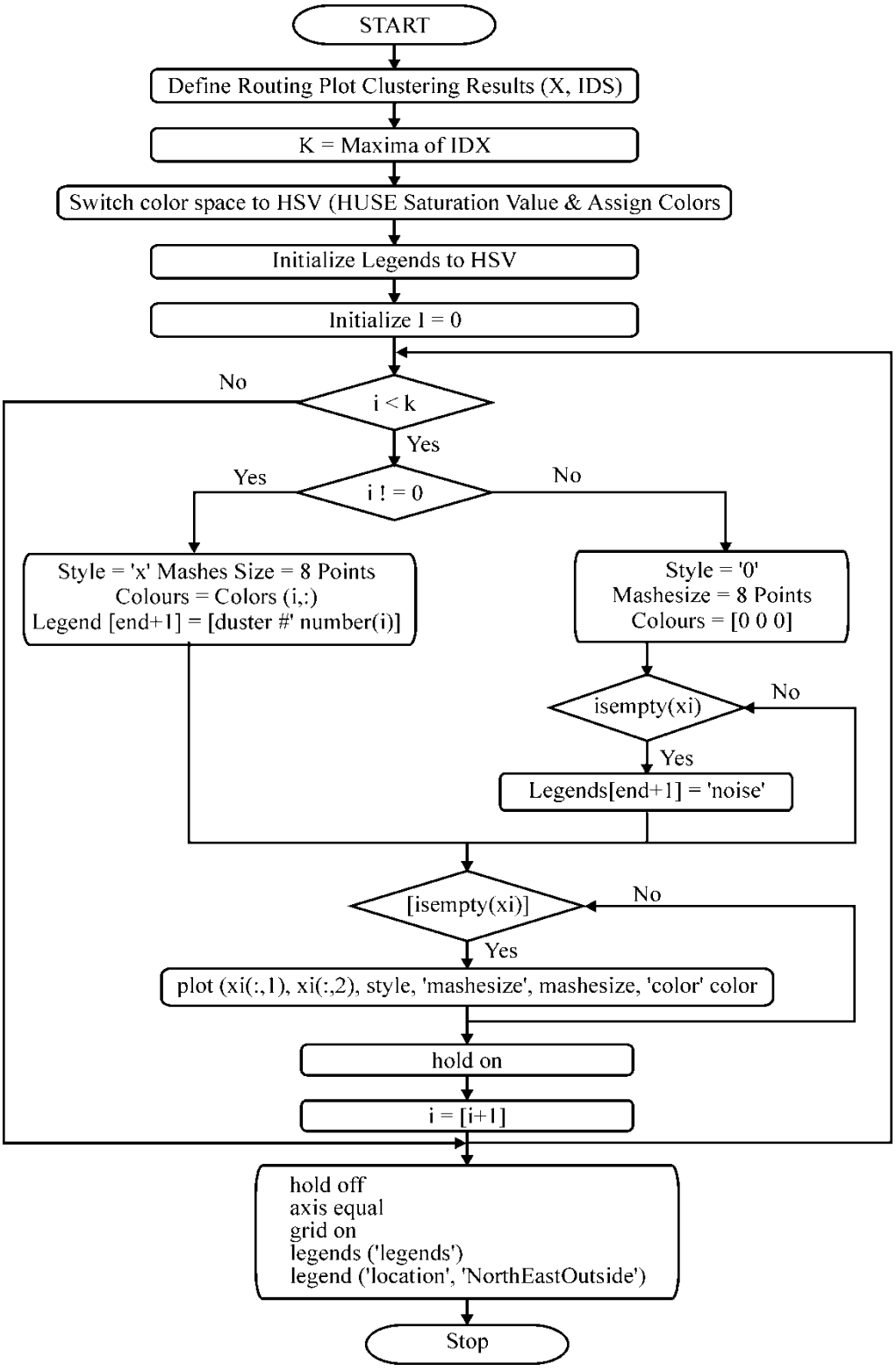

Fig. 4.3 Modified DBSCAN Flowchart

4.3 Function Plot Clustering Result

In this flow chart we can see this flow chart is start with start block that is used for run the main code file. After the run code routine plot clustering is define. Then next step is K is equal to maxima of IDX then next step is switch color space to HSV that is huse saturation value and assign colors. Then in the next step legends to HSV is initialize. Then in the next step i is equal to zero is initialize. Then next step is check condition i<k if this condition is false then algorithm directly goes to hold off block. If this condition is true then next step is check condition that is i ! = 0 if this condition is false then style = 0, mash size is equal to 8 points and color = [0 0 0] then is empty (xi) if it is yes then style 'X' mashes size is equal to 8 points colors = colors(i,:) then is empty (xi) then hold is off, axis is equal, grid is on, legends('legends') and legend ("location; north east outside") then algorithm is stop.

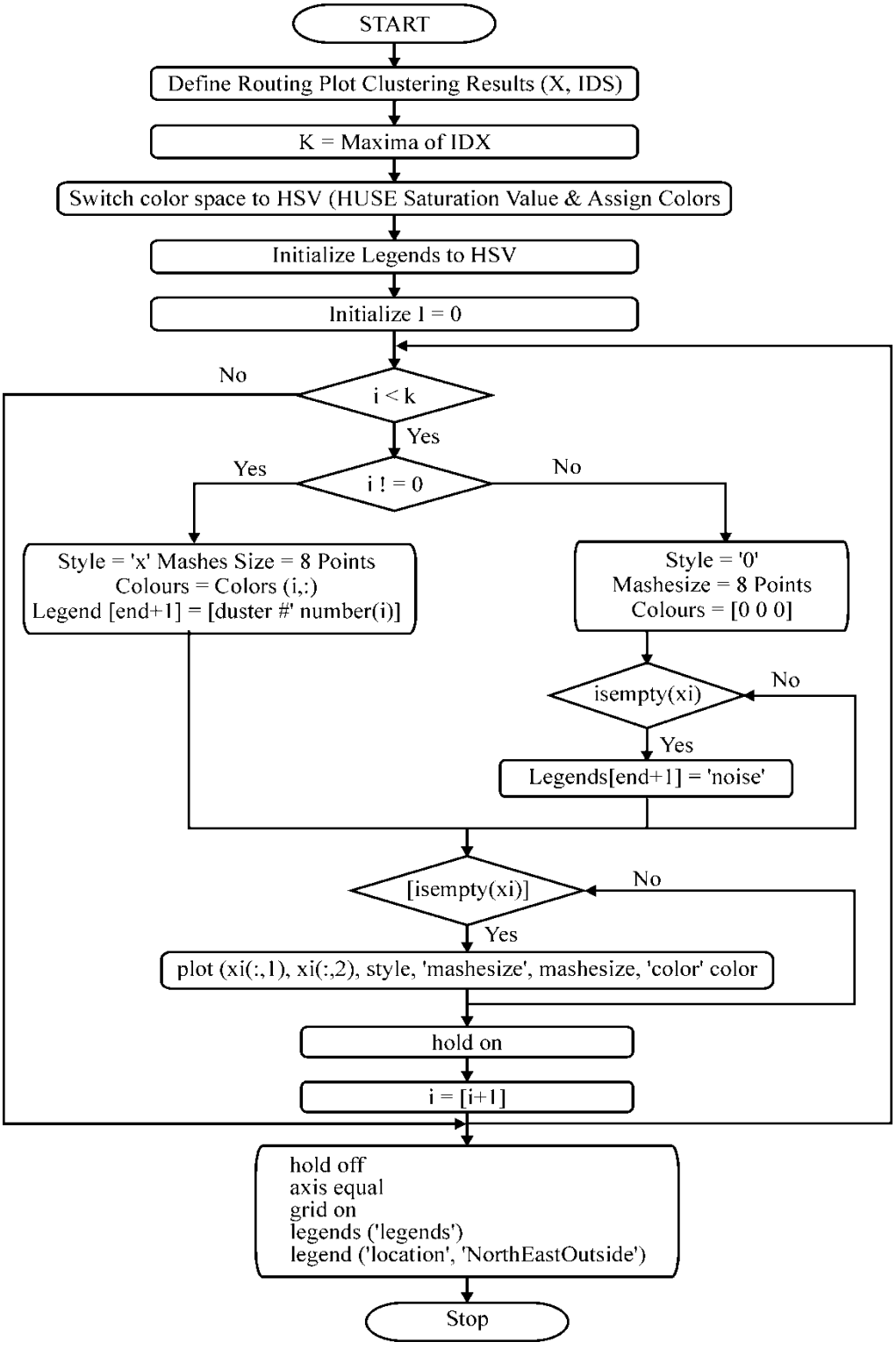

Fig. 4.4 Function Plot Clustering Result

5. RESULTS

5.1 Server Process

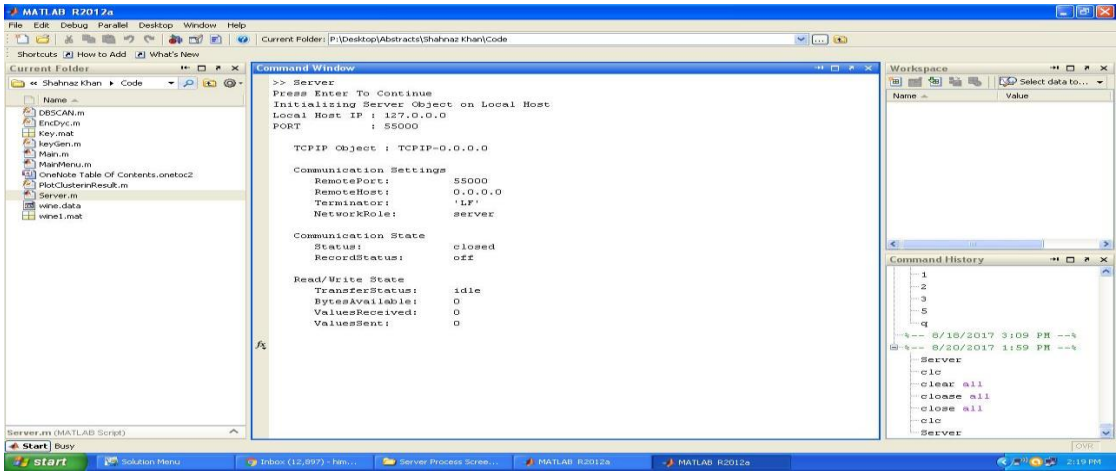

Fig. 5.1 Initializing Server Object on Local Host

The above fig. show that Initializing server object on local host, and we get local host IP 127.0.0.0 and port 55000.

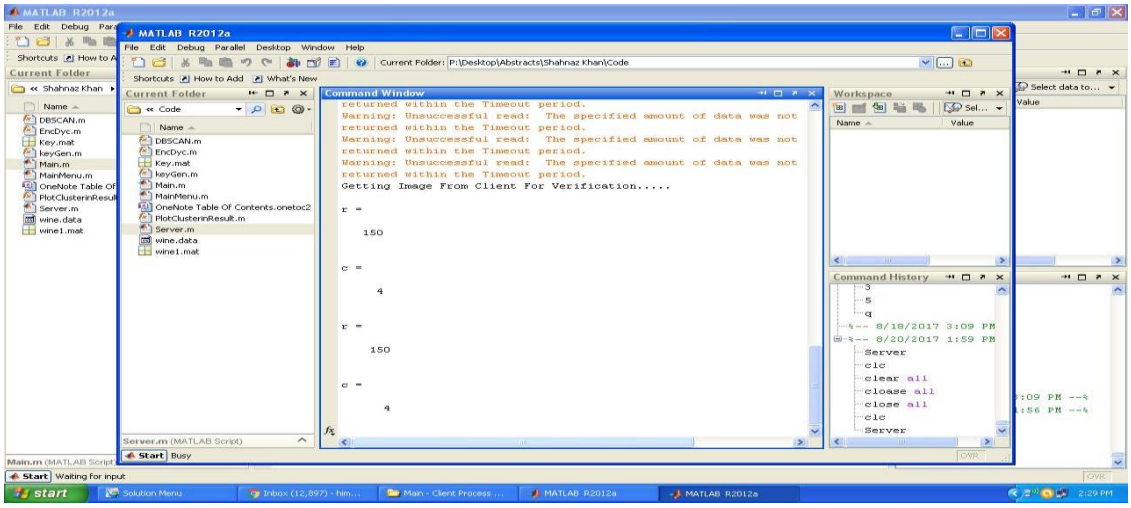

Fig. 5.2 Getting Image from Client for Verification

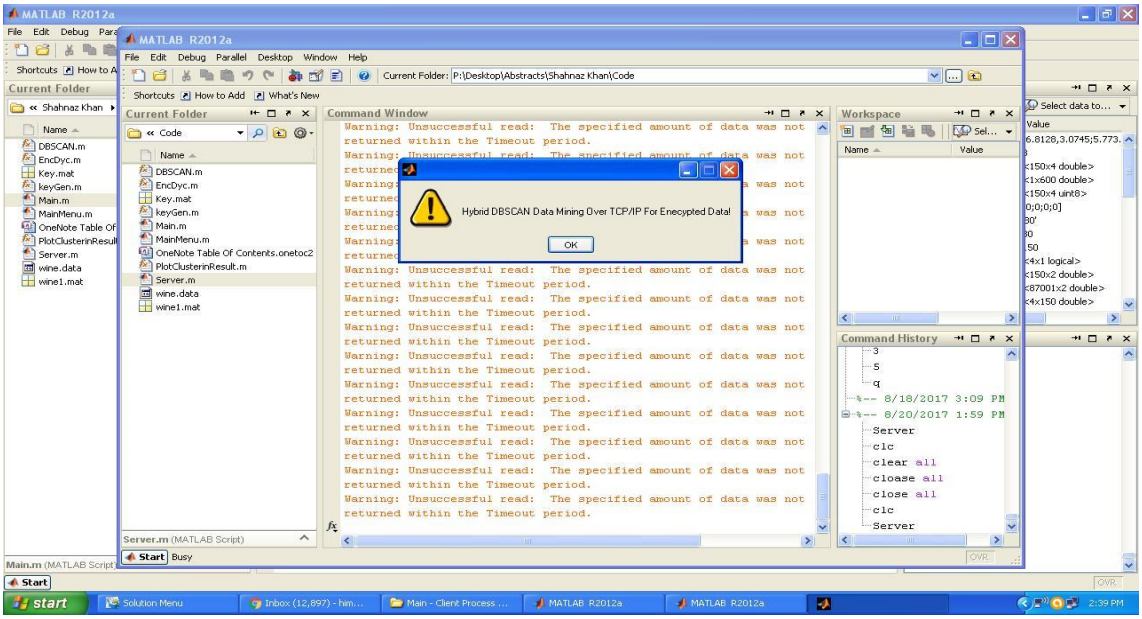

Fig. 5.3 Hybrid DBSCAN Data Mining over TCP/IP for Encrypted Data Loaded

Above figure show that Getting image from client for verification and Hybrid DBSCAN data mining over TCP/IP for encrypted data loaded.

5.2 Main Client Process

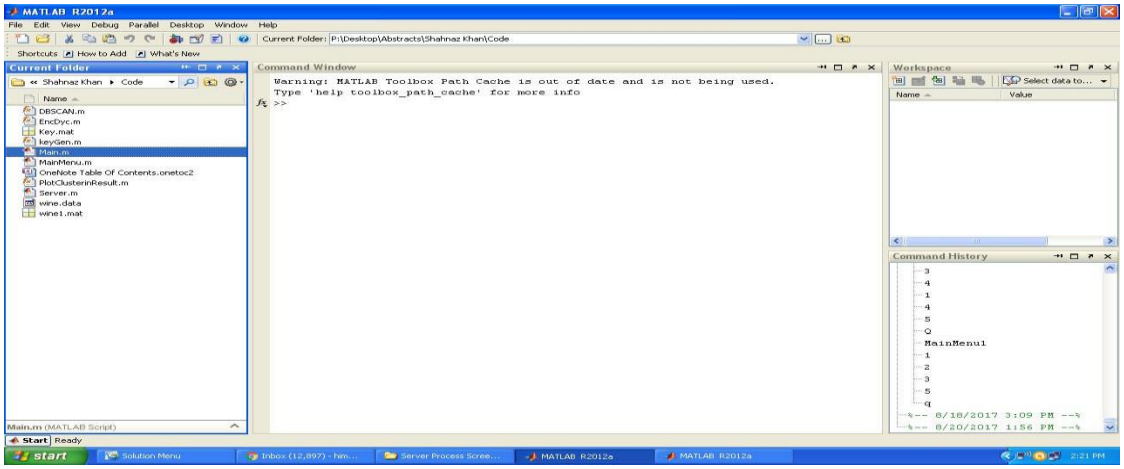

Fig. 5.4 Select Main M

In above figure we select the current folder and open main.m file

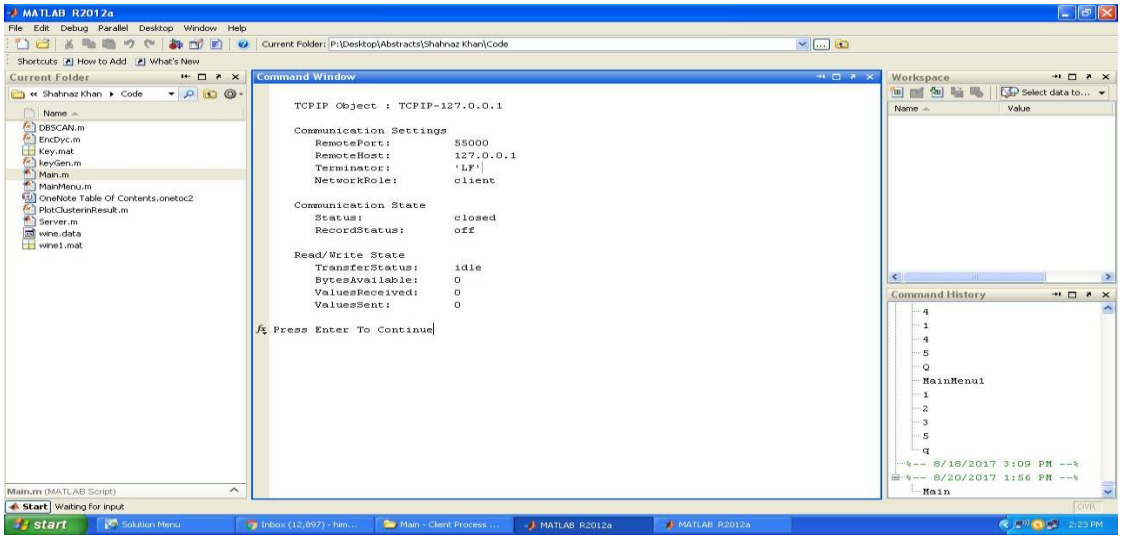

Fig. 5.5 TCPIP Object : TCPIP- 127.0.0.1

In above figure we get communication settings, communication state, read/write state.

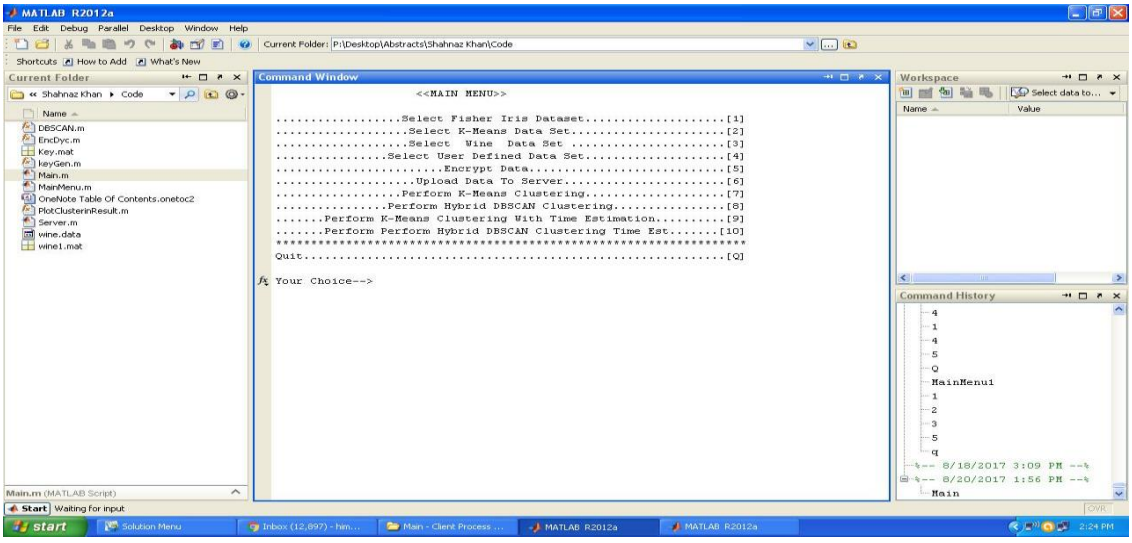

Fig. 5.6 Main Menu

Above figure show that we select fisher irish dataset, k-means dataset, wine dataset, user define dataset, encrypt data, upload data to server, perform k-means clustering, perfor hybrid dbscan clustering, perform k-means clustering with time estimation, perform perform hybrid dbscan clustering time estimation and quit.

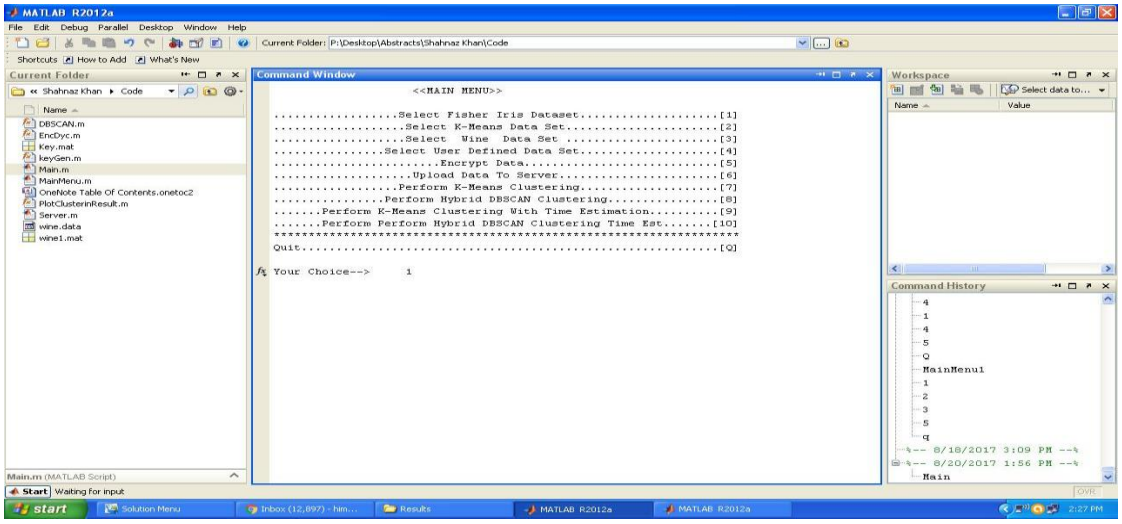

Fig. 5.7 Select Fisher Irish Dataset

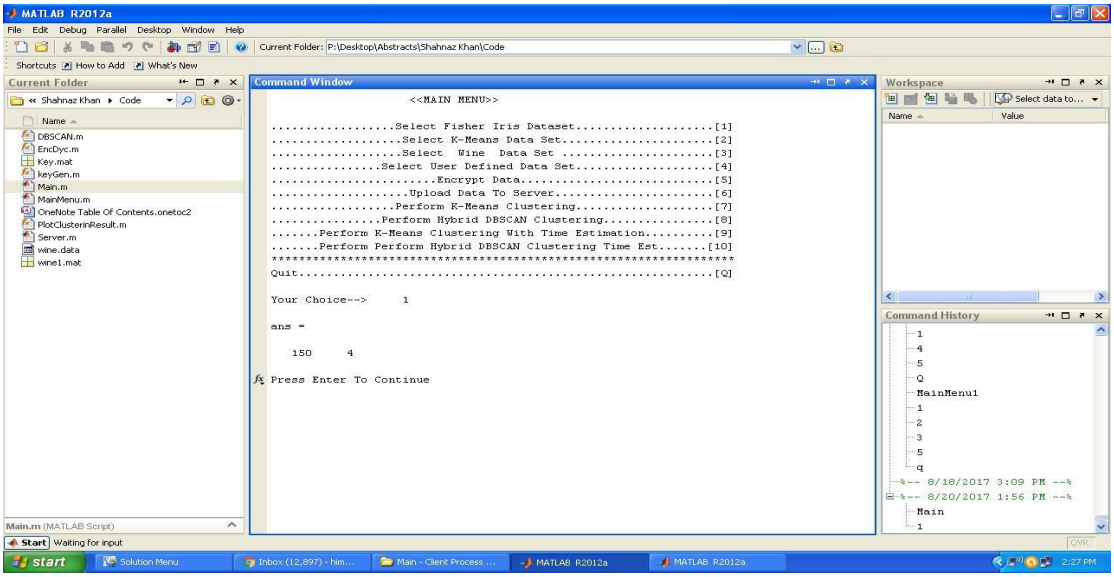

Fig. 5.8 Select Fisher Irish Dataset

In above figure we select fisher irish dataset and and we get 150x4 size of data set.

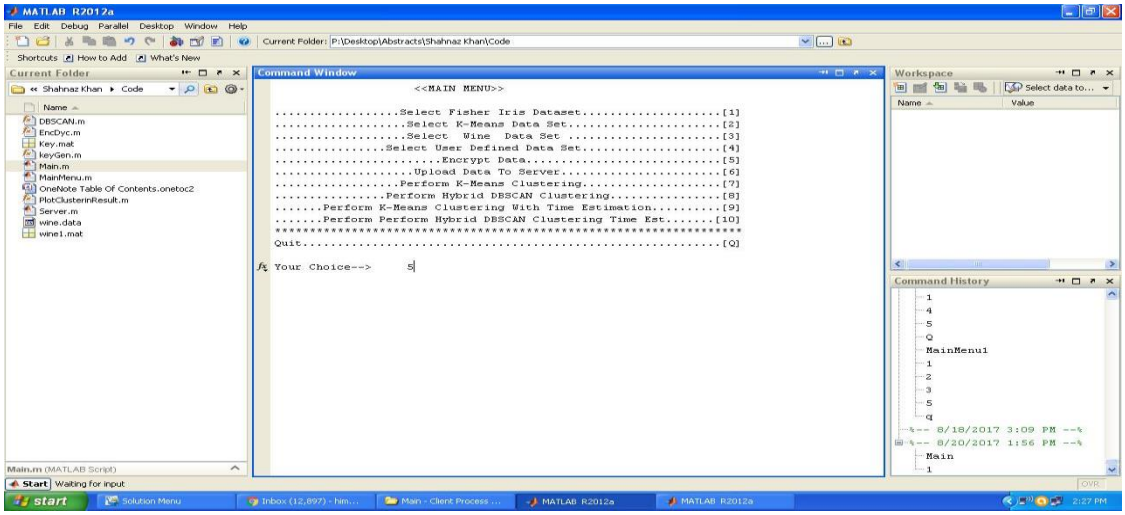

Fig. 5.9 Select Encrypt Data

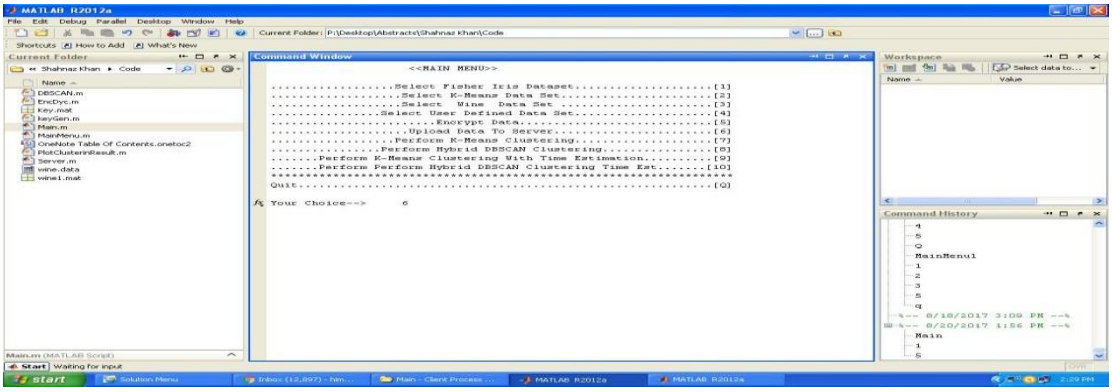

Fig. 5.10 Upload Data to Server

The above figure show that overall data we get upload to the server to perform another function.

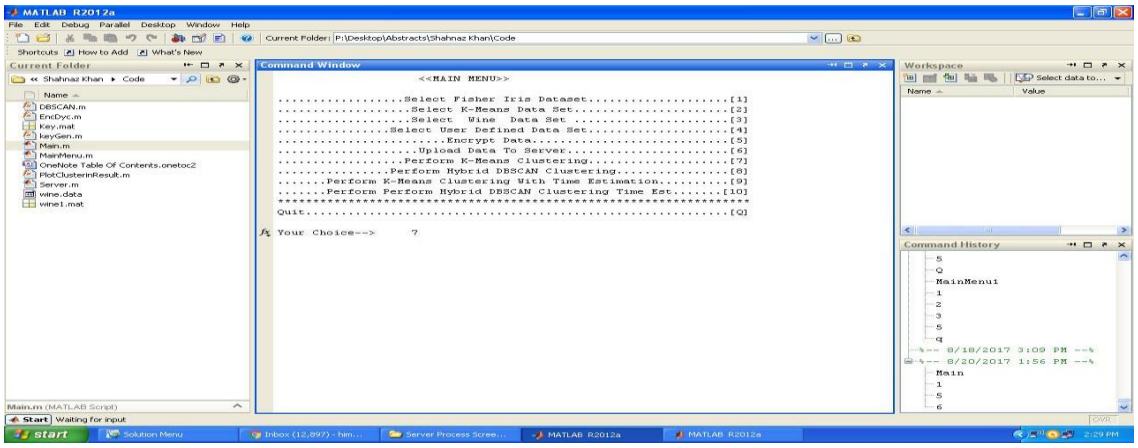

Fig. 5.11 Select Perform K-Means Clustering

The above figure show that first we got all data then we perform k-means clustering.

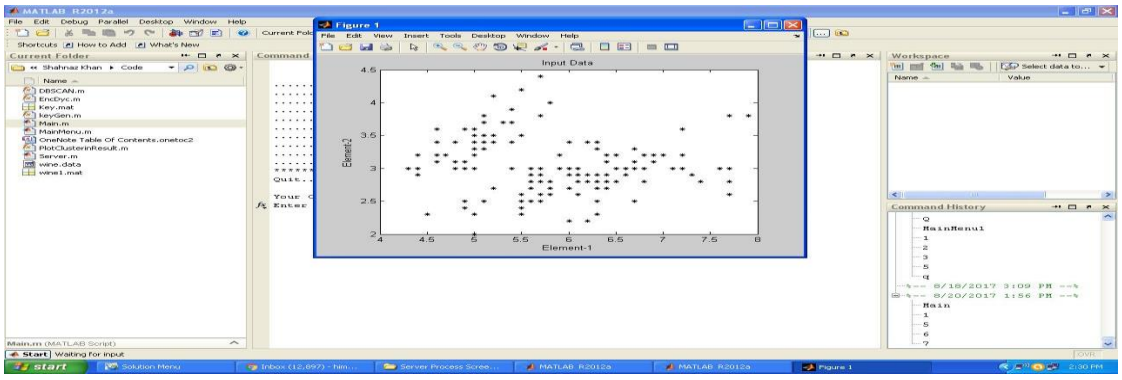

Fig. 5.12 Display the Data of K-Means Clustering

The above figure show thatwhen we select k-means clustering for data the clustered data graph display.

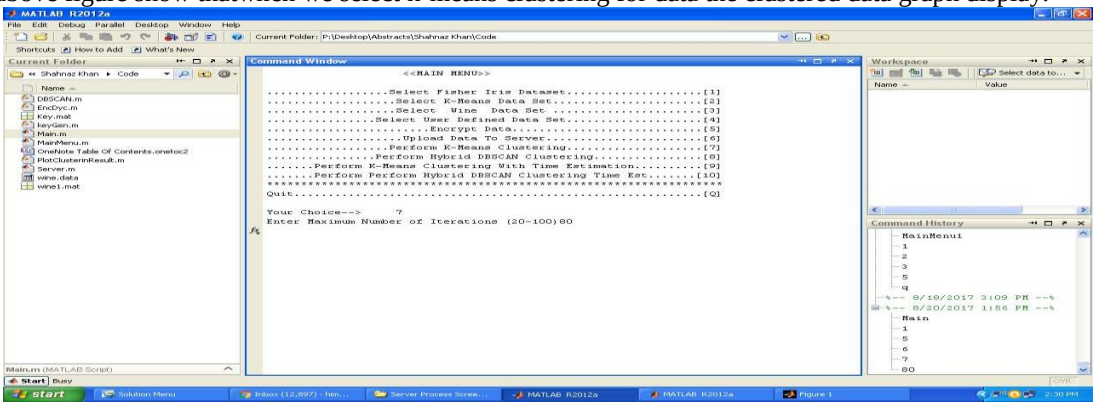

Fig. 5.13 Enter Maximum Number of Iteration

The above figure show that to perform k-means clustering we have to enter maximum number of iteration that is (20-100)80.

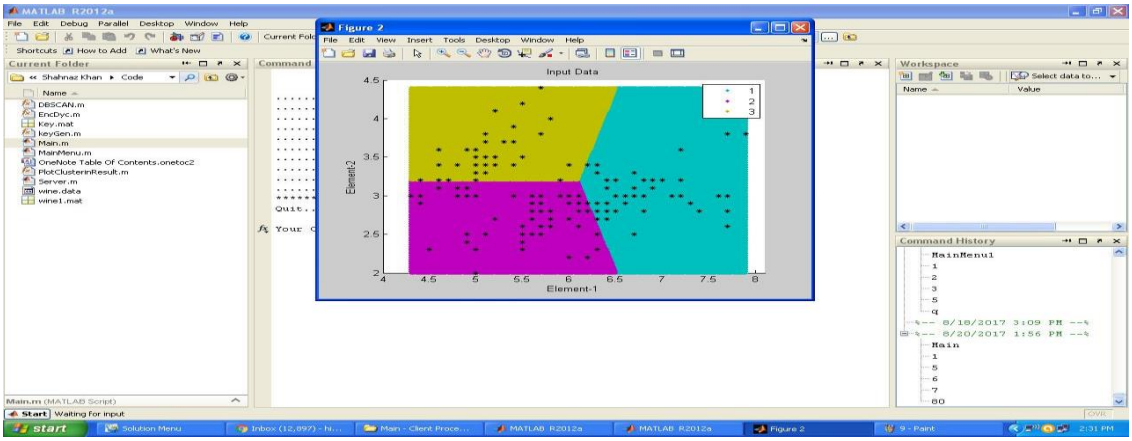

Fig. 5.14 Display the Input Data Clustering

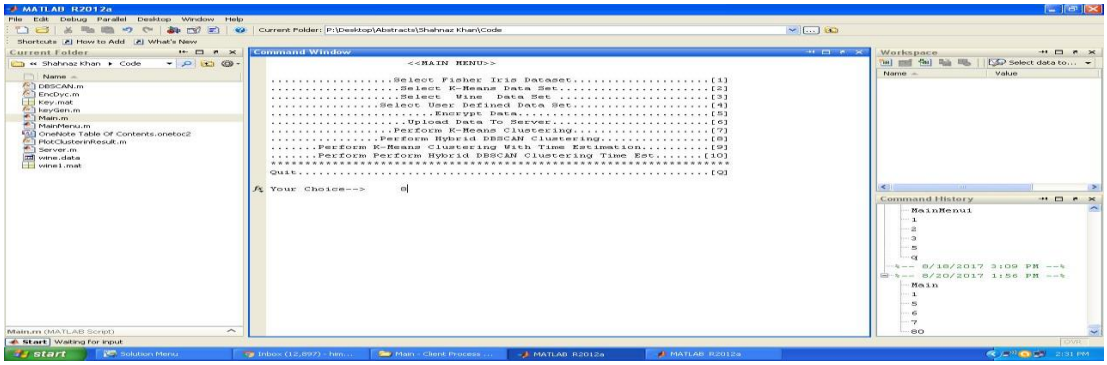

Fig. 5.15 Select Hybrid DBSCAN Clustering

In above figure after performing k-means clustering on data we select hybrid DBSCAN clustering.

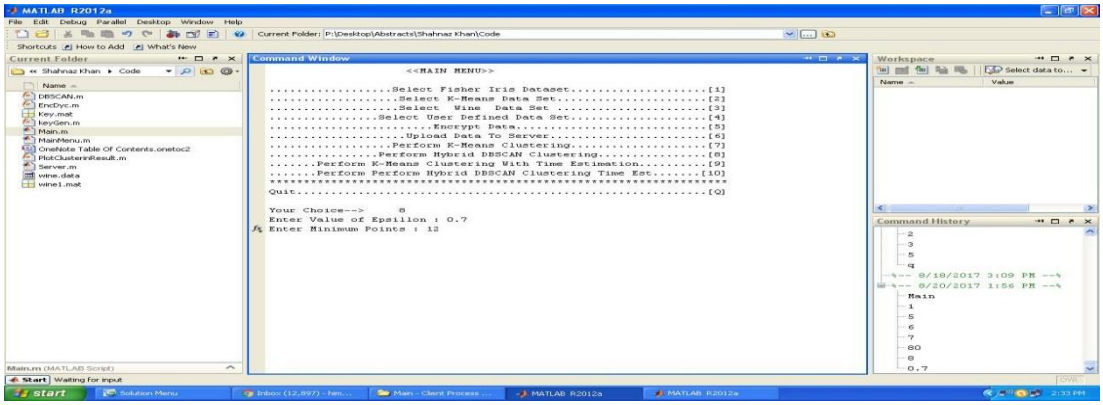

Fig. 5.16 Enter Values

In above figure to perform DBSCAN clustering we haveto enter the value of epsillon (0.7) and enter minimum point that is 12.

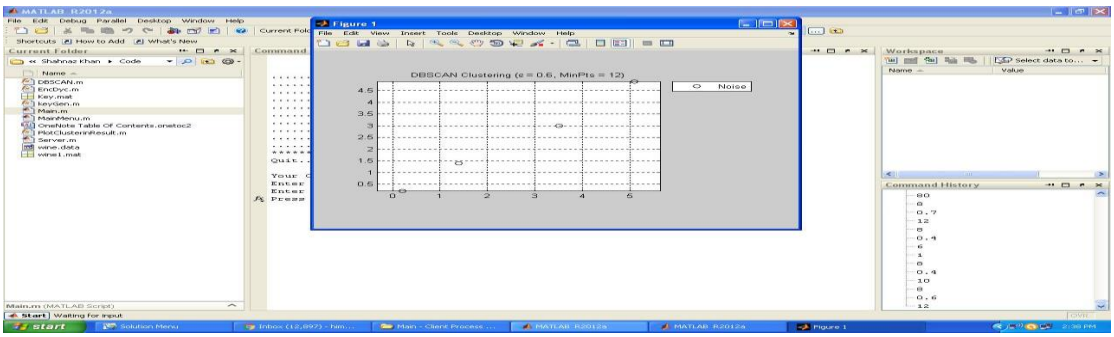

Fig. 5.17 Display the Graph Of DBSCAN Clustering

In above figure to perform DBSCAN clustering we haveto enter the value of epsillon (0.7) and enter minimum point that is 12. And display the graph of DBSCAN clustering.

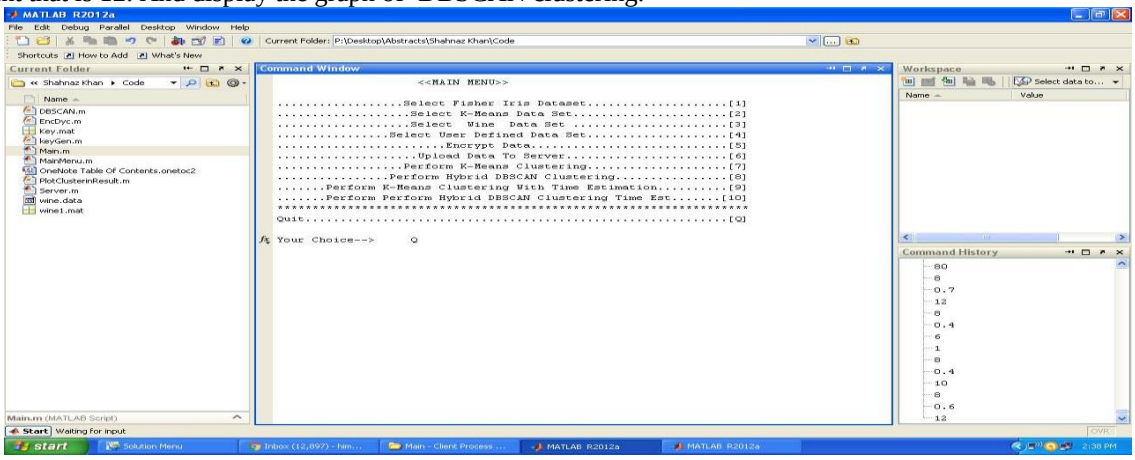

Fig. 5.17 Select To Quit the Server

CONCLUSIONS

In this work, we have presented an unique & efficient biometric authentication system with a high degree of template security using two modalities of iris (retina scan) we have used steganography or water matching to improve the security & reliabilities of the existing system. Also a unique method of enhancing security by converting an image into an audio signal is employed so as to decoy the unintended receiver will only intercept noise in the audio domain & thus we have been able to provide for a two tier security based biometric authentication system that demphonstate a high degree of reliability & flexibilities its operation which enhancing the privacy of the user & template misuse protection manifolds. Also the template matching system where recovered iris template from hand vein image are compared to iris template data using euclinder distance. Iris system also provides for variation of detection threshold to modify track off detection accuracy & rejection entries.

REFERENCES

[1] WEI WU , JIAN LIU, HONG RONG , HUIMEI WANG, AND MING XIAN, “Efficient k-Nearest Neighbor Classification Over Semantically Secure Hybrid Encrypted Cloud Database” IEEE July 25 2018.

[2] Lijun Caot, Xiyin Liu , Tiejun Zhou, Zhongping Zhang, Aiyong Liu, “BASED ON THE FLOW OF AN TI-K NEAREST NEIGHBORS ALGORITHM FOR DATA MINING OUTLIERS” IEEE 2010.

[3] Yousra Abdul Alsahib S. Aldeen, Mazleena Salleh and Mohammad Abdur Razzaque, “A comprehensive review on privacy preserving data mining” Aldeen et al. SpringerPlus (2015).

[4] Bharath K. Samanthula, Yousef Elmehdwi, and Wei Jiang, “k-Nearest Neighbor Classification over Semantically Secure Encrypted Relational Data” IEEE 2015.

[5] Akshay Dabi, Arslan Shaikh, Pranay Bamane, Vivek Thorat, Prof.Popat Borse. “K-NN CLASSIFICATION OVER SECURE ENCRYPTED RELATIONAL DATA IN OUTSOURCED ENVIRONMENT” Multidisciplinary Journal of Research in Engineering and Technology, Volume 2, Issue 4, 2015.

[6] V.Mohanapriyanka, N.Suguna, “FUZZY LOGIC CLASSIFICATION OVER SEMANTICALLY SECURED ENCRYPTED DATA” International Journal On Engineering Technology and Sciences, Volume II, Issue XI, November- 2015.

[7] Isaac Triguero, Jesús Maillo, Julián Luengo, Salvador García, and Francisco Herrera, “From Big data to Smart Data with the K-Nearest Neighbours algorithm” IEEE 2016.

[8] Chetan Wankhede, Nikhil Daundkar, Rohan Wadmare, Tushar Hinge, Prof. M.A.Ansari, “K-Nearest Neighbor Classification over Semantically Secure Encrypted Relational Data” International Journal of Innovative Research in Science, Engineering and Technology, Vol. 5, Issue 3, March 2016.

[9] Rashmi Sheshrao Kodane, Prof. Karuna Bagde, “A SURVEY ON PRIVACY PRESERVING TECHNIQUE USING K- NEAREST NEIGHBOR CLASSIFICATION” IJESRT march 2016.

[10] Ms. R. Poorvadevi, Ms. Mohana Priya, Bowshika.V and Bairavi.S, “A Secure Resource Exchangement Process for Cloud Clients by Using Access Control Technique” IJTRD Mar - Apr 2016.

[11] R.Mynavathi, V.Bhuvaneswari, T.Karthikeyan, C.Kavina, “K Nearest Neighbor Classifier over Secured Perturbed data” 2016 IEEE.