TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 2698 - 2709

Three Way Access Control Using Biometrics and Data Mining Algorithm

D.Venkata Subramanian[1] , C.K.Keerthana[2] ,A.Shivapriyadharshini[3] ,Shree gayathiri[41]
Adjunct Professor, Department Of Computer Science and Engineering, Velammal Institute of Technology[2,3,4]
Undergraduate Student, Department Of Computer Science and Engineering, Velammal Institute of Technology[1]

Article Info
Volume 82
Page Number: 2698 - 2709
Publication Issue:
January-February 2020

Article History
Article Received: *14 March 2019*
Revised: *27 May 2019*
Accepted: *16 October 2019*
Publication: *18 January 2020*

Abstract:
In recent years, security and privacy are very important to keep our data safely. The normal cryptographic key generation for encryption and decryption is not highly secured in this modern world. This work introduced biometric concept for cryptography key generation for authentication process. Behavioral and physical characteristics are measured to identify individuals by biometrics. As every individual has a unique identity like IRIS, finger prints, palm prints, retinal, face, etc. It is difficult to strengthen the security process using single modality biometric system as it dealt with decision making. So, it is important to introduce multimodal biometric system which uses dual finger print, face and retina images for creating a multimodal template. This work also adopted SVM classifier for performing verification as well as validation. The given user biometric feature vector is verified using the existing binary digit of the individual personal key for acceptance or rejection. The multimodal template can be further used to generate the cryptography key. This proposed approach using weights can be helpful to simplify the key generation process but also increases the security of the data as well as privacy of users.

Keywords:*Support Vector Machine, Multi-Modal Biometrics.*

I. INTRODUCTION

Backbone of the modern security lies on Cryptography and cryptographic techniques for establishing security controls. The traditional and typical authentication which uses conventional cryptography purely depends on the secret codes such as passwords or token codes. These approaches may not be able to identify and validate the users in the real time effectively. Actual authentication of users could be carried out with the help of Biometrics like fingerprints, IRIS, retinal, and face recognitions. These techniques are more powerful compared to traditional authentication methods. Biometric data provides numerous preferences when compared with normal frameworks as these can't be speculated and overlooked [2]. Cryptography [4] signifies "secret writing". It is utilized for not only to provide exclusive privacy information in addition to that it is aimed to give answers for different issues like information honesty, confirmation, non-disavowal, Access control, and Availability of the pertinent security information. The plaintext is Original information, which is decipherable either by an individual or by a PC. While the cipher text, which is muddled, without the best possible figure to unscramble it. The way toward encoding the plaintext into cipher text is considered as encryption. Whereas inverting of unraveling cipher text to plaintext is called Decryption. So the generation process requires calculation and key for both encryption and decryption. Key assumes an imperative job in cryptography in light of the fact that the calculation legitimately relies upon it. The data encryption is classified into two unique classes namely symmetric and asymmetric encryption which is represented in Figure 1.1.

TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 2698 - 2709

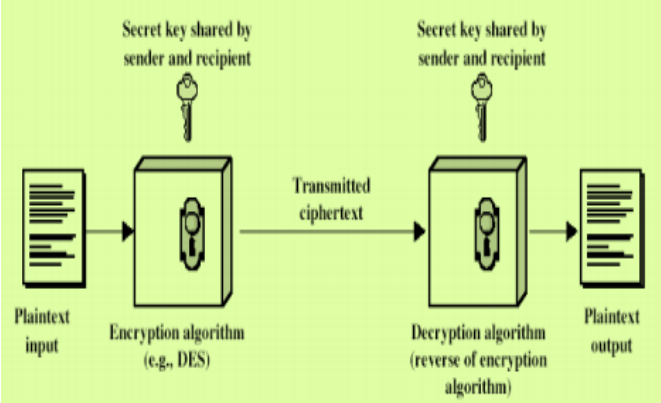

Figure 1.1: Symmetrical Encryption Model

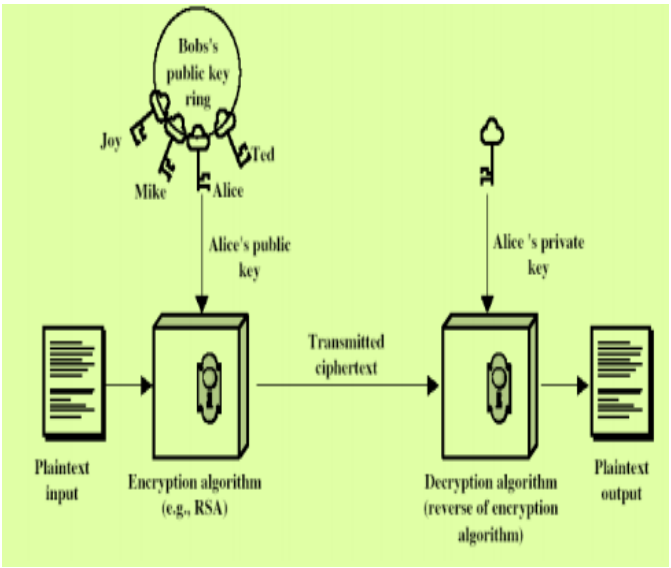

Figure 1.2: Asymmetric Encryption Model

The key used for encryption is once again used in decryption in symmetric encryption. This technique is also called a regular or mystery key encryption. One of the fundamental focal points of utilizing the symmetric key encryption is that the computational intensity of this encryption system is little. Figure 1.1 depicts to the model for ordinary encryption. In asymmetric encryption scheme, distinguishing keys are utilized for unscrambling and encryption. It is otherwise called open key or public encryption. Figure 1.2 represent the model for Asymmetric Encryption.

Biometric is the estimation of biological information [7] and it is usually personal attribute of individual which is robust, measurable and distinctive. Biometric indicates and provides the confirmation of qualities through fingerprint, marks and other human attributes. Biometric aims to provide validation when compared with other cards, keys, passwords and frameworks. The recognizable proof of an individual usually end up in using secret keys and PINs [5]. To avoid the theft of card ids and observations of things by others, biometrics would be ideal as they resolve this type of issues. Additional security protection can be provided using different type or modal of biometrics like hand geometry, face, IRIS, retinal, voice and fingerprint. The biometric system which is represented in Figure 1.3 contains four major components namely Input Interface, Output Interface, Processing unit and data store.

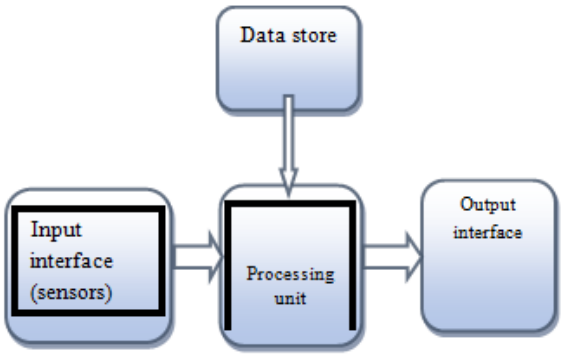

Figure 1.3: Components of Biometric System

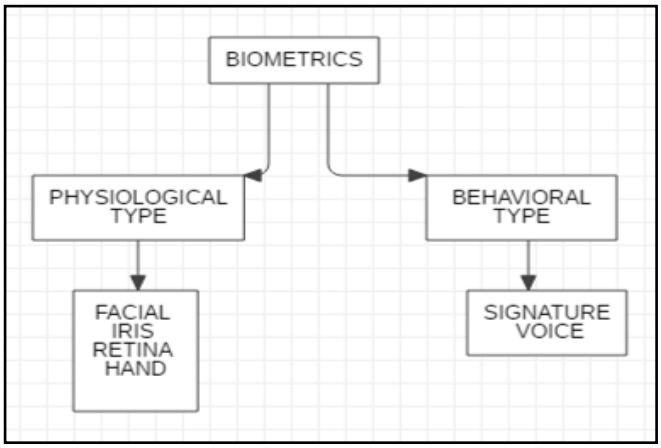

Figure 1.4: Classification of Biometric System

The first component is Input Interface which includes set of sensors which translate biological data of human aspects into digital data. Input interface includes sensor component for converting human biological data into digital data. CMOS and/or CCD will be used for IRIS, Retinal,

January - February 2020
ISSN: 0193 - 4120 Page No. 2698 - 2709

Fingerprint, and Face recognitions. For voice recognition microphone is used whereas for fingerprint optical sensors are used. In the processing unit of the biometric system either DSP or a capable small computer is used for data obtained from the input interfaces. The central part of the biometric system performs the processing of the images such as normalization, enhancements and feature extraction. Apart from that the processing component also performs the comparison of the samples in the database store. The storage component of database store is used for performing verification process. Either EPROM or RAM will be used for authentication proof and for a quick verification contactless or contact smart is utilized as a storage component. The output interface will enable access to the users through interfaces such as RS232 (Serial communication interface), USB, TCP/IP, Bluetooth or Wifi. The Biometrics systems are broadly classified as physiological and behavioral to determine the identity of the individual. For proper estimation, distinctive qualities of both were used. Image Scan of Retina, Hand, Finger, Face and IRIS were treated as physiological biometrics as they were aiming of the portion of the body directly for scanning and estimation. Mark outputs and voice sweep can be viewed as social biometrics as they directly depend on the information for the estimation. The time of the activity is very important for social biometrics for example what time the word was spoken or marked arrangement of words from starting point to end point. This type of classifications is very much helpful for further innovations for supporting specific factors and further enhancing security improvements. The distinctions from physiological and behavioral could help to identify artificial similarity and fake identities. Social biometrics are treated as extents to physiology, for example, skill of hands and fingers in mark check and state of the vocal lines in voice. It is important to pay attention to the conduct of the users or clients during the biometric processing for example, how they show a finger or how they take a glance at the camera [13]. Figure 1.4 contains the information about the classification of biometric.

The following sections discusses about the basic requirements for biometric methods for collecting Physical and Behavioral characteristics. These requirements could be practical and theoretical might be theoretical or practical.

A Biometric modal can be basically classified into two categories. They are Unimodal and Multimodal. Prior to adopting the right biometric technique, it is imperative to ask whether to choose unimodal or multimodal. There exist many challenges when deploying single or unimodal biometric system for large population. Susceptibility towards noisy or bad data is an important feature to be looked at for the sensors. The captured biometric feature can be distorted due to bad acquisition and the quality of the images can also be affected due to the environment conditions especially illumination. Lack of power and issues with power in the sensor environment can affect the quality of image, so it is important to have multiple images apart from taking one single image sample. The features retrieved from the image samples can be used to develop a biometric key for encryption of text messages.

The passwords being weak or enabled as compromised are the primary reasons for the common security incidences and data breaches. The main door or entry point for hacker is the password entry and even a strong password could not stop the attacks. Biometrics are less vulnerable compared to password based and other traditional mechanisms. Fingerprint Proper recognition of fingerprint checks for exclusive patterns of valleys and ridges in the user's fingerprint. Most of the times, these are unique for every person and therefore enable to identify the person from the large set of population. At the same time, single trait biometric does not provide better authentication and introduces many limitations and issues for attacks.

II. LITERATURE REVIEW

Rane et al (2013) reviewed different biometrics and referred secure biometric and biometric template

January - February 2020
ISSN: 0193 - 4120 Page No. 2698 - 2709

protection as a strategy for addressing different security issues. Biometrics assumes a significant job in personality confirmation and access control. Biometrics are appealing as individual characteristic or properties which always vary between person to person. Unlike passwords or tokens, these measures should not be recollected again and again and can't be lost. Biometrics are crucial and constantly shows slight varieties among the estimations [12].

Jadhav et al (2015) presented a computerized framework dependent on biometric unique finger impression verification. For this situation, fingerprints are valuable for the different administrations of government or association or business. Unique mark Matching calculations are utilized for correlation of recently put away formats of fingerprints with client fingerprints for the verification procedure. This work exhibited a sort of this sort of Fingerprint acknowledgment framework and this framework that can be effectively executed. In the meantime, the full execution of such a model will accomplish the goals like security, proficiency, dependability, and simple to-use by numerous individuals on the planet [6].

Kang and Park (2009) proposed a multi biometric framework dependent on unique mark and mark recognition. They proposed another multimodal biometric acknowledgment dependent on the combination of finger vein and finger geometry. This examination demonstrates three curiosities contrasted with past works. In the first place, this is the principal way to deal with join the finger vein and finger geometry data in the meantime. Second, the proposed strategy incorporates another finger geometry acknowledgment dependent on the consecutive deviation estimations of finger thickness extricated from a solitary finger. Third, coordinate finger vein and finger geometry by a score-level combination strategy dependent on a help vector machine. Results demonstrate that acknowledgment exactness is essentially improved utilizing the proposed technique [8].

Tayal et al (2009) suggested a multi-modal biometric framework that consolidates iris features and speaker distinguishing proof framework utilizing the vitality compaction in addition to time-recurrence goals of wavelet examination. The uniqueness of the iris design and the strength of speaker recognizable proof dependent on pitch period estimation supplement each other in the proposed framework. This work likewise basically breaks down the execution of Daubechies wavelets (Db3 and Db4) in the investigation of iris and discourse tests with an undertaking to have a high achievement rate with ideal computational intricacy [14].

Kumar and Zhang (2009) presented exhibited another technique for individual verification utilizing face and palm print pictures. The face, finger prints and palm print pictures can be at the same time obtained by using a couple of computerized images and they are implemented to achieve high level assurance in close to home verification. This strategy uses the creditable personality of clients as a factor of combination. Subsequently the required loads and predisposition on individual biometric coordinating scores are consequently processed to accomplish the most ideal presentation. The test results additionally show that additional computation principles for accomplishing improvements in execution. The technique proposed in this work can be stretched out for any multimodal validation framework to accomplish higher execution [9].

Kumar and Farik (2016) concentrated on multimodal biometric confirmation frameworks being used today. The point is to inspire the best blend of verification factors for multimodal use. They contemplate the qualities and shortcoming of chose biometric instruments and prescribe novel answers for incorporate into multimodal biometric frameworks to enhance the current biometric downsides. The creator trusted this work will furnish security specialists with some valuable knowledge while structuring better biometric frameworks. As confirmation is the way toward approving the personality of an individual dependent on certain info that the individual gives. Confirmation has

January - February 2020
ISSN: 0193 - 4120 Page No. 2698 - 2709

turned into a noteworthy subject of research because of the expanding number of assaults on computer networks far and wide [10].

Parkavi et al (2017) provided staggered verification for the frameworks using multimodal biometrics for recognizing the people. Multimodal confirmation gives more dimensions or views for the purpose of verification when compared with single biometric like palm print or face or unique mark with a user. This work applied unique mark and IRIS of an individual for the programmed distinguishing proof of a person by consolidating unique mark and the IRIS of an individual. Edge discovery and minutiae coordination were applied and utilized. Both FRR and FAR were evaluated and shown ways to control precision by limiting FAR [11].
Asha and Chellappan (2008) proposed a validation framework with multi-biometrics to help different administrations in e-Learning where client confirmation is important. E-learning frameworks speak to another type of learning and are winding up increasingly well-known each day. Security in e-Learning has turned into a major necessity. So to validate an e-student particularly if there should be an occurrence of e-tests is a noteworthy test in an e-learning condition. Client validation techniques can be arranged into three classifications: (1) strategies dependent on human memory, for example, passwords, (2) strategies dependent on physical gadgets, for example, attractive or Integrated Circuit (IC) cards, and (3) strategies dependent on biometrics, for example, unique mark, iris, and so on., Hence, Multi-modular biometric improves the unwavering quality of confirmation as single biometric verification innovation can't fulfill a required dependability level [3].

Besbes et al. [1] proposed a multi-modal biometric system which produced recognition accuracy and population coverage by using iris and fingerprint templates. Shahin et al. [2] presented a biometric security profile by fusing hand veins, hand geometry and fingerprint. Kumar and Ravikanth [3] suggested an identity authenticator using both finger geometry and dorsal finger knuckle surface features provides excellent person authentication. Chandran et al. [4] worked and proposed a method to improve the efficiency by integrating the features of iris and fingerprint. Chin et al. [5] suggested a proposal at which combines the features of palm print and fingerprint and a series of steps are applied on palm and finger print to increase performance and for feature extraction of 2D by implementing Gabor filter at feature level. Sheetal Chaudhary and RajenderNath proposed a system by integrating palm print, fingerprint and face based on score level fusion [6]. Fan Yang and Baofeng Ma proposed a method to build an identity by combining different features like fingerprint, hand geometry, palm print comparison score fusion [7]. Muhammad Imran Razzaket. al. [8] proposed a multi-modal recognition system using the biometric traits like face and finger vein. This system effectively reducing the error rates like FAR (False Acceptance Rate) and thereby increases AAR (Authentic Acceptance Rate).

Gidudu Anthony, Hulley Greg and MarwalaTshilidzi (2007) proposed a simple image classification technique using Support Vector Machine (SVM). They compared the implementation of SVM using One-Against-One (1A1) and One-Against-All (1AA) techniques and evaluated their results in the field of remote sensing and land mapping.
Seyyed et al. [26] insisted Automatic MRI image threshold using Support Vector Machines. The number of thresholds in the segmented image determines the classification accuracy.
Vasta et al. [27] came up with an intelligent 2v-support vector machine-based match score fusion algorithm. The proposed method combines the quality of images in order to improve the recognition performance of face and iris features. A face and iris based multimodal biometric system that uses matching score level fusion with the help of support vector machine (SVM).

January - February 2020
ISSN: 0193 - 4120 Page No. 2698 - 2709

III. CRYPTOGRAPHIC KEY GENERATION PROCESS DESIGN

There are many novice users doesn't even use the lock code or secured mechanism to either access or protect their confidential data. So, if the phones are stolen the saved account and password information can be used to mishandle the concerned bank accounts or their confidential data [3]. Many smartphone users store the email id and password and hence the access codes or messages retrieved in the emails can be easily used for accessing the bank and/or other web sites or applications. In this paper, to overcome these issues, cryptographic key generation using multimodal biometric authentication for the security of mobile phones is proposed. The following has the proposed algorithm using weight based authentication for three different images.

Step 1: The fingerprint database (fin_db1), face database (fac_db2) and retinal database (ret_db3) are the inputs to this algorithm.

Step 2: The weight for fingerprint (w1), face (w2), and retinal image (w3) is initialized to 33.33 i.e., w1←33.33, w2 ← 33.33 and w3 ← 33.33.

Step 3: The image match score threshold is set as 0.6(or 60%) i.e., match_threshold← 0.6

Step 4: Capture the real-time fingerprint, face, and retina images of the user.

Step 5: Apply SVM classifier algorithm to classify the image type.

Step 6: Search the image type in the image type in the image stores fin_db1, fac_db2, andret_db3 using binary search.

Step 7: If (match1 and match2 and match3) found then

Step 7.1: If (fin_img_match_score>= match_threshold and fac_img_match_score>=match_threshold and ret_img_match_score>= match_threshold) then generate the fused key from the three image templates.

Step 7.2 else Calculate minimum match scores for finger, face, and retina images as

fin_min_match_score←w1*fin_img_match_score,

fac_min_match_score←w2*fac_img_match_score

andret_min_match_score←w3*ret_ing_match_score

.

Step8:If(fin_min_match_score+fac_min_match_score+ret_min_match_score >= 0.45)

Then, the user is authenticated, and a unique key is created from 3 image templates.

Else, User authentication fails and a user record is created in the failure database.

Step 9: Train the SVM model to give different weights based on failure count and thebiometric modal probability.

In this concept, the processed images collected from the biometric sensors are stored in different databases. A template is created for each user in the database with specific labels. For example, the fingerprint images extracted are stored in the fingerprint database with a label in case of multiple user system. Similarly every behavioral or physiological traits recorded are stored in their respective databases. Each template of a user comprises of his fingerprints, facial features under different conditions and iris images. These preprocessed templates are given as an input to our algorithm.

Since our concept compares the images and generates the desired key based on the weights calculated dynamically on certain conditions, it is mandatory to initialize the weights of each dataset at the beginning. As our concept deals with three datasets namely fingerprint, iris and face, the weight is equally divided and assigned to each feature. For example, 33.33 (100/3=33.33 approx.) is assigned as the weight of each data in fingerprint database and so on.

January - February 2020
ISSN: 0193 - 4120 Page No. 2698 - 2709

The main critical part of the algorithm is setting a threshold value. The threshold score plays a major role in comparison and thereby determining the credibility of the user. There exists many factors that resists 100 percent matching score like lighting, emotions of user, dust in the atmosphere, quality of sensors or camera used etc., therefore our image match score threshold is fixed as 0.6 (i.e. 60%) to avoid false rejection rate.

After initializing the parameters in the proposed algorithm, the real time biometric features of an individual is collected and processed to train the machine to deliver desired output. The aim of this proposed work is to eliminate false acceptance rate and false rejection rate.

Support Vector Machine (SVM) Support is a supervised machine learning algorithm which can be used for solving both classification and regression problems. However, it is mostly used in classification problems. Using SVM algorithm, we plot each data item as a point in n-dimensional space (where n is number of features used in the system) with the value of each feature being the value of a particular coordinate. Then, we perform classification by finding the hyper-plane that differentiate the two classes very well.

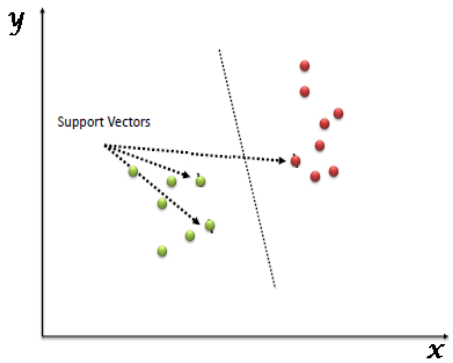

Fig 1.5: Visualization of Svm

Fig 1.5 depicts that Support Vectors are simply the co-ordinates of individual observation. Support Vector Machine is a frontier which best segregates the two classes effectively. This enables the machine to classify two closely related features as two different distinct features. As SVM is a supervised machine learning algorithm, we train the machine beforehand about the input image types. Based on the previous knowledge, the machine reads the input data provided and classifies the input images into their corresponding type. Search for the matching templates of fingerprint, face, and retina images in the image template databases such as fin_db1, fac_db2, and ret_db3 using their respective matching algorithms.

In this concept, the SVM is used to classify the real time images as distinct features namely fingerprint, face or iris thereby increases the efficiency by decreasing the time wasted in searching for a matching image in all three databases.

As proposed earlier, once the image is classified as specific type, using binary search algorithm, the matching image is searched in the already available databases using their respective matching algorithms. The templates that matches with the real time images is selected and matching score is calculated for each image that matches with the existing template.

If all three features extracted matches with the images on the template then, one of the following methods is carried out.

CASE I

If the matching score calculated for each individual biometric feature, matches with the threshold score (i.e. 0.6) then the fused key is generated from three image templates. The fused key enables the user to decrypt the information stored in his device.

CASE II

If the match score fails to equal the threshold value, then minimum match score is calculated for each template using the weight allocated earlier. The minimum match score for each feature is given by multiplying its weight by the calculated image matching score.

fin_min_match_score as w1 * fin_img_match_score
fac_min_match_score as w2 * fac_img_match_score
ret_min_match_score as w3 * ret_img_match_score.

If the minimum weight calculated for each model after calculations is greater than or equal to 0.45 (45%) then the user is authenticated, and a unique

January - February 2020
ISSN: 0193 - 4120 Page No. 2698 - 2709

key is generated from the image templates else, the authentication fails and the user record is created in failure database.

Based on number of cases that fails to achieve the threshold value, the weight of the particular feature will be altered. For example, if the facial feature always fails to reach the threshold value because of environmental factors or technical difficulties then the weight allocated for the particular feature will be incremented by a value which will be decremented from the most successful result producing features.

These failure data are trained by the machine so that it could work efficiently under abnormal situations. This model ensures that the machine will analyze and produce better results saving time and reducing false rejection rate. The proposed model is trained using the failed data to provide different weights to each feature based on its failure count as mentioned earlier.

IV. IMPLEMENTATION AND RESULT ANALYSIS

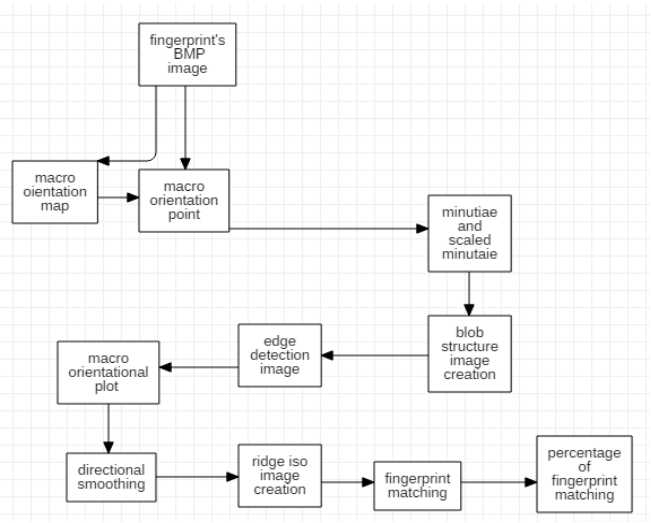

Fig 1.6:Feature extraction –Finger print

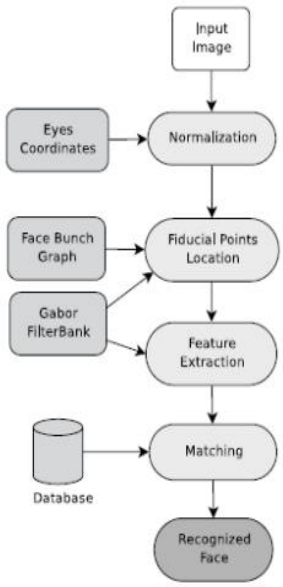

Fig 1.7:Feature extarction -Face

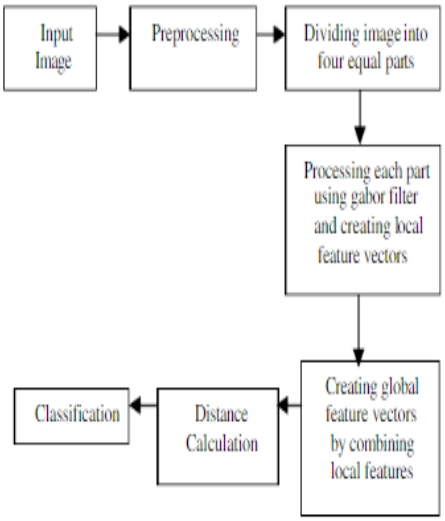

Fig 1.8:Feature extraction –Iris

Fig 1.6, Fig 1.7., Fig 1.8 depicts various techniques used in the feature extraction procedure of Finger print, Face and Iris respectively. This is a crucial step as it makes the image detection and other image processing techniques easier.

IMAGE TYPE CLASSIFICATION USING SVM:

frompathlib import Path
importmatplotlib.pyplot as plt
importnumpy as np

January - February 2020
ISSN: 0193 - 4120 Page No. 2698 - 2709

```
fromsklearn import svm, metrics, datasets
fromsklearn.utils import Bunch
fromsklearn.model_selection import GridSearchCV, train_test_split
from skimage.io import imread
fromskimage.transform import resize
defload_dir(container_path, dimension=(64, 64,3)):
image_dir = Path(container_path)
folders = [directory for directory in image_dir.iterdir() if directory.is_dir()]
categories = [fo.name for fo in folders]
descr = "A image classification dataset"
images = []
flat_data = []
target = []
fori, direc in enumerate(folders):
for file in direc.iterdir():
img = imread(file)
img_resized = resize(img, dimension, anti_aliasing=True, mode='reflect')
flat_data.append(img_resized.flatten())
images.append(img_resized)
target.append(i)
flat_data = np.array(flat_data)
target = np.array(target)
images = np.array(images)
return Bunch(data=flat_data,
target=target,
target_names=categories,
images=images,
            DESCR=descr)
df = load_dir("imgs/")
X_train, X_test, y_train, y_test = train_test_split(
df.data, df.target, test_size=0.8,random_state=None)

fromsklearn.preprocessing import StandardScaler
sc = StandardScaler()
X_train = sc.fit_transform(X_train)
X_test = sc.transform(X_test)

param_grid = [
  {'C': [1, 10, 100, 1000], 'kernel': ['linear']},
  {'C': [1, 10, 100, 1000], 'gamma': [0.001, 0.0001], 'kernel': ['rbf']},
 ]
svc = svm.SVC()
clf = GridSearchCV(svc, param_grid)
clf.fit(X_train, y_train)
y_pred = clf.predict(X_test)
print("Classification report for - \n{}:\n{}\n".format(
clf, metrics.classification_report(y_test, y_pred)))
out=[]
str1="face"
str2="finger"
str3="iris"
fori in y_pred:
ifi==0:
out.append(str1)
elifi==1:
out.append(str2)
else:
out.append(str3)
fromsklearn.metrics import accuracy_score
print(accuracy_score(y_pred,y_test))
```

```
Classification report for -
GridSearchCV(cv='warn', error_score='raise-deprecating',
       estimator=SVC(C=1.0, cache_size=200, class_weight=None, coef0=0.0,
  decision_function_shape='ovr', degree=3, gamma='auto_deprecated',
  kernel='rbf', max_iter=-1, probability=False, random_state=None,
  shrinking=True, tol=0.001, verbose=False),
       fit_params=None, iid='warn', n_jobs=None,
       param_grid=[{'C': [1, 10, 100, 1000], 'kernel': ['linear']}, {'C': [1, 10, 100, 1000], 'gamma': [0.001, 0.0001], 'kernel': ['rbf']}],
       pre_dispatch='2*n_jobs', refit=True, return_train_score='warn',
       scoring=None, verbose=0):
              precision    recall  f1-score   support

           0       1.00      0.99      0.99        90
           1       0.98      1.00      0.99        62
           2       1.00      1.00      1.00        82

   micro avg       1.00      1.00      1.00       234
   macro avg       0.99      1.00      1.00       234
weighted avg       1.00      1.00      1.00       234


accuracy_score is:
0.9957264957264957
```

Fig 1.9:Output of Svm Classifier with prediction accuracy

A. INFERENCE – SVM IMPLEMENTATION

The Fig 1.9 shows how the Svm is made to find the image type of image. Support vector machine is a supervised learning algorithm which is being used efficiently in the field of image classification. The load_dir function is used to load the directory

TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 2698 - 2709

containing the image folders of face, finger print and iris respectively. As soon as the image directory is loaded , the dataset is sliced into test data and train data using a package known as sklearn.model_selection.train_test_split .The train and test data are feature scaled for better performance and simplicity. The SVM function is called with the 'c', 'gamma' and type of kernel for training the train data. The c parameter is a list of 10 multiples and the gamma parameter is also a list of decimal values. These values are provided as list so that the efficient combination of c and gamma can be found from all possible combinations. The type of kernel used is the radial basis function or linear function as it can be tuned easily. The train data is classified with the gridsearchcv function performs an exhaustive search for the optimization of the parameters. The parameters used in this function are optimized by cross-validating grid search over a parameter grid. Once the training of data is over, the test data is classified and the result is stored in y_pred variable as an array. The classified data consists of images types labeled as 0, 1 and 2. These are labeled as face, finger print and iris respectively using a simple for loop for readability .Finally, the prediction results are compared with the test results for percentage of accuracy using the sklearn.metrics.accuracy_score package.

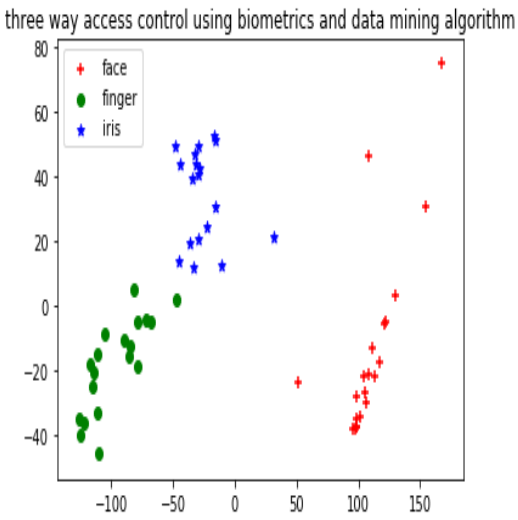

Fig 1.10: Scatter plot for train data

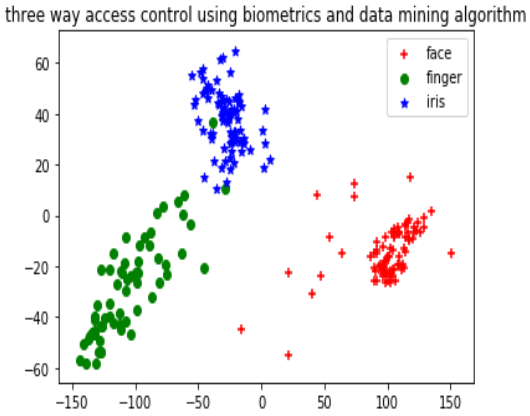

Fig 1.11: Scatter plot for predicted data

Fig 1.10 and fig 1.11 shows the two similar scatter plots for the train and test data in image classification program. It can be understood from these images that the machine gets well trained even for a small set of train data which has a positive impact on correctly predicting a large set of test data.

V. CONCLUSION

This work investigated the benefits as well as the security and privacy risks associated with the use of biometrics as an authentication mechanism for both smart phones and WSNs. In recent times the use of sensors has increased at an enormous rate in our day-to-day lives. An effective scheme is truly depending on multimodal biometrics for generating the cryptographic key in a secured manner. The proposed scheme followed in the work has three components namely extraction of features, biometric template generation using multimodal and key generation using the template. As the normal key used for encryption and decryption is not secure in this hackers' world, this work included multimodal biometric images. In the Multimodal biometric template generation consists of five major steps: pre-processing, feature extraction, feature fusion, biometric template creation. Based on the case studies and different evaluation exercises, this work shows that the proposed schema provides higher security.

January - February 2020
ISSN: 0193 - 4120 Page No. 2698 - 2709

VI. FUTURE DIRECTIONS

There is possibility to improve the existing system to identity the genuine users or intruders from the collections of multimodal biometric template existing in the database. The data mining and deep learning technique can be used to detect the structures and the failure patterns. The proposed model with real time sensors can be implemented to evaluate the performance and efficiency of the proposed methods. In order to improve the methods further, the WAM can be used to assign different weights for the biometric images generated from multimodal (fingerprints, retina and face) to classify effectively and process based on the quality preferences. The proposed system is works very well under defined image capturing system and biometric capturing systems. The proposed modal and algorithm can be further enhanced automatically to handle the distorted, partial and less quality images. This research can be further extended to generate biometric template and keys using other types of biometrics such as smile, hair color, skin color, and eye. There are other possible research avenues to handle the different facial expressions such as anger, surprise, sadness and others.

VII. REFERENCES

1. Agulla, E.G., Rúa, E.A., Castro, J.L.A., Jiménez, D.G. and Rifón, L.A., 2009, Multimodal biometrics-based student attendance measurement in learning management systems. In 11th IEEE International Symposium on Multimedia, pp. 699-704.
2. Al-Saidi, N.M., Said, M.R.M. and Othman, W.A.M., 2012. Password authentication based on fractal coding scheme. Journal of Applied Mathematics, vol. 2012, no. 340861, pp.1-16.
3. Asha, S. and Chellappan, C., 2008, Authentication of e-learners using multimodal biometric technology. In International Symposium on Biometrics and Security Technologies, pp. 1-6.
4. Chang, Y.J., Zhang, W. and Chen, T., 2004, Biometrics-based cryptographic key generation. In IEEE International Conference on Multimedia and Expo (ICME) (IEEE Cat. No. 04TH8763), Vol. 3, pp. 2203-2206.
5. Daugman, J., 2007. New methods in iris recognition. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics) 37, no.5, pp.1167-1175.
6. Jadhav, V.V., Patil, R.R., Jadhav, R.C. and Magikar, A.N., 2015. Proposed E-payment System using Biometrics. International Journal of Computer Science and Information Technologies Skin, Vol.6, no.6, pp. 4957-4960.
7. Jaiswal, S., Bhadauria, S.S. and Jadon, R.S., 2011. Biometric: case study. Journal of Global Research in Computer Science, vol.2, no.10, pp.19-48.
8. Kang, B.J. and Park, K.R., 2009. Multimodal biometric authentication based on the fusion of finger vein and finger geometry. Optical Engineering, vol.48, no.9, p.090501.
9. Kumar, A. and Zhang, D., 2009. User authentication using fusion of face and palmprint. International journal of Image and Graphics, vol.9, no.02, pp.251-270.
10. Kumar, K. and Farik, M., 2016. A review of multimodal biometric authentication systems. International Journal of Scientific & Technology Research, vol.5, pp.5-9.
11. Parkavi, R., Babu, K.C. and Kumar, J.A., 2017, Multimodal biometrics for user authentication. In 11th International Conference on Intelligent Systems and Control (ISCO) ,pp. 501-505.
12. Rane, S., Wang, Y., Draper, S.C. and Ishwar, P., 2013. Secure biometrics: Concepts, authentication architectures, and challenges. IEEE Signal Processing Magazine, vol.30, no.5, pp. 51-64.
13. Sharma, A.K., Raghuwanshi, A. and Sharma, V.K., Biometric System-A Review.International Journal of Computer Science and Information Technologies, vol. 6,no.5 , 2015, 4616-4619.
14. Tayal, A., Balasubramaniam, R., Kumar, A., Bahattacharjee, A. and Saggi, M., 2009, A multimodal biometric authentication system using decision theory, iris and speech recognition. In 2nd International Workshop on Nonlinear Dynamics and Synchronization, pp. 1-8.

January - February 2020
ISSN: 0193 - 4120 Page No. 2698 - 2709

15. Parkavi, R., Babu, K.C. and Kumar, J.A., 2017, Multimodal biometrics for user authentication. In 11th International Conference on Intelligent Systems and Control (ISCO) ,pp. 501-505.
16. Besbes, F, Trichili, H. ;Solaiman, B. Multimodal Biometric System Based on Fingerprint Identification and Iris Recognition Information and Communication Technologies: From Theory to Applications, 3rd International Conference ICTTA 2008.
17. Shahin MK, Badawi AM, Rasmy, A Multimodal Hand Vein,Hand Geometry and Fingerprint Prototype design for High Security Biometrics, CIBEC'08 (2008)
18. Kumar, A, Ravikanth C, Personal Authentication Using Finger Knuckle Surface, Information Forensics and Security, IEEE Transactions on (Volume:4 ,Issue: 1) , 2009
19. Chandran GC, Rajesh RS, Performance Analysis of Multimodal Biometric System Authentication, Int. J. Computer. Sci. Network Security, (2009) 9: 3
20. Chin YJ, Ong TS, Goh MKO, Hiew BY (2009). Integrating Palmprint and Fingerprint for Identity Verification, Third International Conference on Network and System Security
21. SheetalChaudhary ,RajenderNath. A Multimodal Biometric Recognition System Based on Fusion of Palmprint, Fingerprint and Face. International Conference on Advances in Recent Technologies in Communication and Computing, IEEE (978-0-7695- 3845-7) in the year 2009.
22. Fan Yang, Baofeng Ma. A New Mixed Mode Biometric Information Fusion on Fingerprint, Hand-geometry and Palm Print, IEEE published in the IV International Conference on Image and Graphics-2007.
23. Muhammad Imran Razzak, Muhammad Khurram Khan, et.al. Multimodal Biometric Recognition Based on Fusion of Low Resolution Face and Finger Veins ISSN 1349- 4198, pp. 4679–4689, ICIC International conducted in 2011.
24. P. S. Sanjekar , J. B. Patil, An Overview Of Multimodal Biometrics, Signal & Image Processing : An International Journal (SIPIJ) Vol.4, No.1, February 2013
25. Gidudu Anthony, Hulley Greg and MarwalaTshilidzi. "Classification of Images using support vector machines". arXiv: 0709.3967v1, Cornell University, Library, 2007.
26. Seyyed, M.H.; Javad, V.; and Seyyeddeh M.H. Automatic MRI Image Threshold using SVM. II International Conference on Knowledge-Based Engineering and Innovation, 207-210. (2015)
27. Vasta, M.; Singh, R.; Noore, A. Integrating image quality in 2V-SVM biometric Match Score Fusion. Int. J. Neural Syst in 2007
28. Minhas, Saadia & Javed, Muhammad. (2009). Iris feature extraction using gabor filter. 252-255.10.1109/ICET.2009.5353166.