Volume 8, No. 3, March – April 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Implementing Levels of Security using Multimodal Architecture

Kinnri Sinha
Student, School of Computer Science and Engineering,
VIT University, Vellore
India

Prachi Kharge*
Student, School of Computer Science and Engineering,
VIT University, Vellore,
India

Ajit Pandey
Student, School of Computer Science and Engineering,
VIT University, Vellore
India

Sathyaraj R
Assistant Professor (Senior)
School of Computer Science and Engineering,
VIT University, Vellore
India

Abstract:Following the announcement of Demonetization in India, there has been a heightened need for online payments which calls for increased security measures. The following paper analyses the different techniques that Cn be used for user authentication before transactions. This includes the incorporation of barcodes/ QR codes, behavioural biometrics and physical biometrics in the security measures. It then proposes a multimodal security model which suggests a combination of these techniques to make transactions safer and more secure.

Keywords:Barcodes/ QR codes, behavioural biometrics, physical biometrics

I. INTRODUCTION

'Demonetisation' in India is an attempt to stop the black money which has been used to fund illegal activity and terrorism. It has pushed the people today to shift to complete digitization and what we call today, 'Cashless Transactions'. These transactions require authorization and call for additional security measures.
This paper surveys various types of safety measures that can be executed and suggests a model implementing various levels of security using a multimodal architecture to safeguard all online transactions and ensure protection having desired standards.

II. REVIEW

A)Quick ResponseCode:
A QR ("quick response") code comprises of 2-D barcode. Data is encrypted in several mini squares, in order to hold a bigger number of information than a customary barcode. Accessing a data can be done using a cellular phone's camera by taking a snapshot of the QR code which then scans the picture using a QR reader [1].
Quick Response Codes as of now have surpassed the traditional Barcode in fame in a few regions. A typical barcode can hold 20 digits at max, though a Quick Response Code can accommodate up to 4,296alphanumeric characters[2].

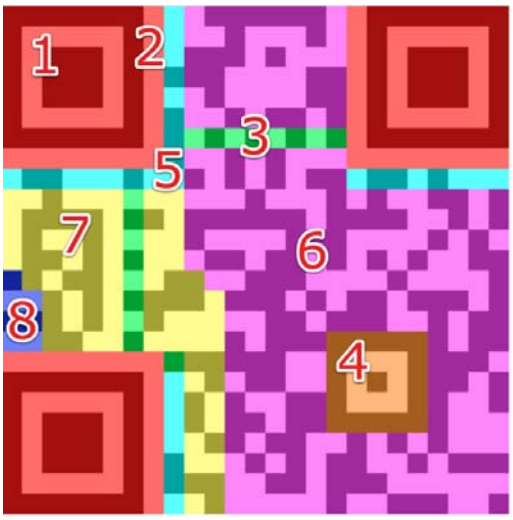

Figure 1: Structure of QR code [1]

Joined with the differing qualities and extendibility that makes the service of Quick Response Codes a great deal when contrasted with barcodes [1].
Mainstream utilization incorporate putting away URLs, address and different types of information on publications, signs, business cards, open transport vehicles, and so forth. In fact, it has countless applications [3,4,5,6,7].
Smart phone is popularised so much that QR code got incorporated in telecommunication industry [6, 8, 9]. QR Code can be printed and used as a medium to advertise online products [10].
Quick Response Codes comprise of various ranges that are saved for particular purposes.

- Quick response code have 3 big squares on top left, top right and bottom left which forms finder pattern. It is

non information component which is encompassed by dark modules encompassed by bright modules that are again encompassed by dark modules. Correct position and perception can be done using finder pattern[1].(Figure 1: 1st position)

- A separator can be found near the 3 finder pattern .The white separators segregates finder patters from the real information which is one pixel in thickness and enhance the conspicuousness of the finder patterns[1].(Figure 1: 2nd position)
- Varying between high contrastsmodules in order to get the thickness of solitary module can be achieved in timing design.[1].(Figure 1: 3rd position)
- Alignment patterns bolster the decoder programming in making up for direct picture bends. It is just like finder patterns but smaller in size and are set all through the code[1].(Figure 1: 4th position)
- There are strip of modules left near the separator to hold the format information. For top-left square, strip must be hold for right and below to the separator, for top-right strip must be hold for bottom to the separator and for bottom left strip must be hold towards the right of the separator [1].(Figure 1: 5th position)
- It helps scanner extract the information stored by the maker. These data packets or digitally encoded signals gets converted into binary formand gets secured in one code word in the data [1].(Figure 1: 6th position)
- Error rectification codes are one code word long which is useful when the code becomes messy or impair and we still want tore-establish the information [1].(Figure 1: 7th position)
- Error correction bits based on Reed-Solomon Codes [11] and Purge bits of data cannot be isolated into one code word without leftover portion. In that case, remainder bit will be empty[1]. It is also called BCH error correction code [12, 13].(Figure 1: 8th position)

B) Quick Response Codesas Attack Vectors

Attacks happen through Controlled Quick Response Codes. Contingent upon whether the peruser iscomputerized program or a human being[1].

1) Attack on Automated Process:

QR Codes are an institutionalized method for encrypting a data and it could be controlled keeping in mind the end goal to change the encrypted data. Attacks on peruser software and the backend are hypothetically conceivable irrespective of the automated process[1]. This could be beneficial by a foe for the following, non-comprehensive rundown of attacks [14].

- SQL Injection is a technique to hack website. A website comprises of two things html and database. Hackers attack on database to gain administrative privilege. The hacker needs to guess the position of username and password of the administrator inside the table of database. A query is needed in order to take the information from that position and download it into the hacker's system. Once the hacker will know the administrator's passwords, it will be his site and he will be the next administrator. This whole process is called SQL Injection[1].
- Another attack on web application architecture which needs an IP address and a system level in order to get to the system behind the web program known as command injection [1].
- It is used in deceiving the framework using different computerized framework to confer extortion for example, making the system trust that it is process shoddy item'A'while preparing the more costly item 'B'. is called a fraud [1].

2) Attack on Human Perception:

People cannot read the code without a peruser programming, the data put away inside the code is totally muddled. Be that as it may, by pursuing the controlled Quick Response code, a susceptibility in the peruser programming can happen or the program can also get activated[1].

- A fake website can be setup by an attacker with one purpose in mind to divert clients by altering the quick response code. The client will think that this site is genuine and he will continue his work without knowing that whatever information he is entering is retrieved by the attacker. This process is known as phishing [1].
- Quick response codes are frequently utilized as a part of notices to guide the intended interest group to extraordinary offers or extra information about particular items.The quick response code can be used to divert the client to a fake web site, an adversary will offer the requested item while never satisfy the agreement. The victim believes the promoting organization by taking after the connection. This method is known as fraud[1].
- Different software on PCs or mobile phones are vulnerable and can be attacked through buffer overflows or command injection. Once the attack gone successful, attacker will gain control over the whole cell phone, which includescontacts, e-mails etc. This method is the attack on reader software[1].
- Mix of click bait and phishing. In this method, client's psychology gets manipulated to retrieve his personal detail or the detail of his organisation. For example:Attacker can email the victim by making a fake email id and demand for some secret document to be given as soon as possible. This method is called social engineering attack [1].

For future study, 2D Codes like Data matrix [15] can be used to identify attack vectors and to find preventive measure.

C) Biometric:

The physical characteristics that can be used to identify humans are DNA, ear, hand vein thermograms, facial traits, and eyes (which includes the retina and iris), hand geometry and fingerprints, palm prints. Individuals also have personal traits which basically define things they do such as their handwriting, signatures, keystrokes, odour, voice, gait etc. These physical and personal features are included under Biometric recognition to differentiate between humans due to their uniqueness, universality, permanency and collectability [16]. A general biometric system follows three basic steps which are firstly, acquisition of the desired characteristic, secondly, acquiring the feature set from this data and thirdly, comparing it with a trained data set followed by recognition. Based on the application, biometric recognition can be categorised into 2 divisions, verification mode and identification mode.

Verification mode deals with evaluating the identity of the individual by comparing its characteristics with those stored

in the trained dataset. An example of this application is when a biometric is used to authenticate transactions. The acquired biometric is compared with stored values corresponding to that individual and the user's identity is thus verified to complete the transaction successfully.

This mode can be formulated as follows:

Let X be the characteristic acquired and I_x be the claimed identity. Let I_0, I_1, …, I_n be the identities in the dataset each belonging to a certain class. X is compared with the characteristics of the I_x from the data set and its class is verified. Since the biometric values acquired by an individual at different times may not be completely alike, the difference in compared values is allowed to exist up to a certain threshold.

The identification mode is when biometric is used to determine the identity of that particular individual. An example of this mode is in criminal investigations when a biometric of an unknown suspect is compared with values in the database and if a match is found, the corresponding person is recognised. Unlike traditional methods such as passwords, PINs and others, biometric is capable of negative recognition which disallows an individual from having multiple identities [17].

This mode can be expounded as follows:

Let x be in input biometric measurements, I_0, I_1, …, I_n be the identities in the database. The x value is compared with all other values present in the data set and if a match if found above the threshold value, the corresponding identity is of the required user. If not found, new identity is added to the database.

A biometric system process consists of four cardinal modules, they are, Sensor module which is responsible for acquiring the biometric data of the individual such as a fingerprint sensor, etc. The feature extraction module deals with processing and extracting elementary features from the acquired biometric data. For example, the orientation and location of ridges in the fingerprint image are determined in the feature extraction module. The Matcher module is used to compare the extracted features by the stored templates and generate matching scores. This also includes decision making module which can either be used for verification or identification of the user. The last module is System Database Module which is used to store the relevant information about the biometrics acquired from the user [17].

1) Types of Biometric

There are various kinds of characteristics that come under biometric and can be used in a unimodal biometric system. The choice of the biometric depends entirely on the requirements of the system. No single biometric is optimal or the best fit for all possible scenarios. Some examples of biometric based on physical characteristics are:

a) *DNA*:Deoxyribose Nucleic Acid (DNA) is the one-dimensional ultimate unique code for one's individuality. The only exception to this are twins who have the same DNA [17]. This biometric yields completely reliable and efficient results when used in forensic applications to confirm the identity of an individual but has a few disadvantages. It requires cumbersome chemical procedures to be performed to gain the results. DNA acquisition is very easy and such detailed information about an individual can thus be misused easily. Information about susceptibility of a person to a particular disease can be determined from a DNA and can be used for ulterior purpose.

b) *Ear:* Studies have shown that every individual has a unique shape of ear. But this biometric cannot be used to identify an individual as the differences are not distinctive enough.

c) *Face:* Facial characteristics are one of the very commonly used biometrics for identification. This process can vary from static to dynamic acquisitions. The common approaches used for facial recognition are by determining the location of various features on our face like eyes, nose, lips, etc. Another approach follow analysing the entire global outlook of the face and viewing it as a combination of various canonical faces. The major limitations faced by facial recognition include the dependency on the environment conditions. They sometimes require a particular background only or might produce a different image when taken with different illumination. An ideal facial recognition system should detect the presence of a face within the region of interest, locate it and be able to recognise it irrespective of the angle it is projected from [17].

d) *Fingerprint:*Fingerprints have been used for identification by the human race for many centuries as matching accuracy with this technique has proved to be very high [18]. Fingerprints are basically the impression left by the friction ridges of a human finger. Even identical twins have a different set of fingerprints. Fingerprint biometrics have been in use for many years to accurately identify and authorise individuals but it also has a few disadvantages. Fingerprint detection requires expensive scanners and plethora of resources. Finally, fingerprints of a minor segment of the population may be unfitting for automatic identification because of genetic factors, aging, environmental, or occupational reasons [17].

e) *Infrared Thermogram*: An infrared camera is used to acquire the patterns of the heat radiated by a human body. The recognition based on such characteristics does not necessitate human contact but cannot be carried out in environments where different uncontrollable sources of heat exist. Moreover, the equipment required is quite expensive which limits the use of such biometric.

f) *Hand and Finger Geometry:* Many features of a human hand like its shape, size, length and width of the finger can be utilised as biometrics. These are inexpensive and independent of the unreliable environment factors. But, the hand geometry of an individual is not substantially distinctive and cannot be used for a large population. Moreover, factors such as extra ornaments worn by individuals, invariant growth in children, diseases such as arthritis, etc. may limit the use of hand geometry for biometric recognition.

g) *Iris:* Iris is a circular structure in the eye which is responsible for determining the amount of light entering the eye and is unique for every individual, even twins. Research is still going on to make iris based recognition systems more user- friendly and affordable.

h) *Palm print:* Similar to fingerprint, palm prints are ridges and patterns present on the palm. Since palms cover more surface area as compared to fingerprints, they are further distinctive. Palm prints contain additional

features such as wrinkles and principle lines which can also be used to identify individuals. Palm scanners are expensive and bulkier but can acquire various biometric features such as hand geometry, fingerprint, palm prints at once whose results can later be combined to give more efficient results.

i) *Retinal Scan:* This biometric is known to be the most reliable biometric as it is distinct for each and every individual and every eye. The image acquisition procedure is tedious and needs to be carried out meticulously which requires the individual to cooperate. Moreover, retinal scan can reveal detailed medical condition of a person and thus, user acceptability for retinal scan systems for identification is limited.

Behavioural Biometrics involve determining measurable patterns in human activities in contrast to innate features under physical biometrics. Some examples of behavioural biometrics are:

j) *Gait:* Gait is a peculiar way in which a human moves. It is used in low security systems as it is insufficiently distinctive, and is adversely affected due to factors such as inebriation, injuries and changes over time.

k) *Keystrokes:* It is not necessarily distinct for every individual and researchers have been trying to develop more applications based on this biometric. However, keystrokes can give rudimentary level information to simply discriminate and permit identification of an individual.

l) *Odour:* Another behavioural characteristic of humans is the odour emitted by them which is known to be different for different individuals. A small segment of air near the object is subjected to few chemical sensors which determine the chemical compounds based on the aroma. These results can be used to identify an individual. Various studies are being conducted on the effect of deodorants and surroundings on such biometrics.

m) *Signature:* The way a person signs his or her own name can qualify as a distinctive representation of that person. Various government, banking, legal transactions use signature biometrics as a preliminary procedure to identify the individual. Identification based on Signature have various disadvantages such as varying style of signatures over time, dependency on emotional and physical state of individual, professional forgers who are able to copy any signature unmistakably.

n) *Voice:* Voice biometric is a combination of both physical and behavioural features. The physical features are determined by the vocal tracts, nasal cavities and the sound producing systems present in an individual. The behavioural characteristics depend on the mood of the individual, emotional conditions, medical conditions, etc. Voice can easily be faked and thus cannot be used for identification over a large population.

2) Errors in a Biometric System

A biometric acquired from a particular individual may vary when taken at different or location due to various factors such as noise, light variances, Difference in the behavioural or physical characteristic, user interaction and ambience. To tackle these errors, a matching factor is taken into consideration that evaluates the similarities between the stored template and the received bio metric inputs. The more the value of this matching factor, the more is the probability of two different templates coming from same human.

There are basically two types of errors, *False Match*, where two different persons are shown to have the same biometric features. *False Non- Match* is when the same person is shown to have two different identities. Both these scenarios are not probable and accounted as errors.

A biometric system is *unimodal* if it uses only a single biometric feature to perform the recognition process. There are many constraints in a unimodal biometric system, such as:

a) *Intra- Class Variations:* On incorrect interaction with the acquiring device, the user input can vary from that given at the time of enrolment to the time of recognition or authentication of the same characteristic.

b) *Noise:* Noisy, incorrect or unwanted data can also be an upshot of dirt accumulated on the sensors, environmental factors, ambience, maintenance, etc. A Fingerprint with a scar, is an example of noisy data. Noisy biometric data can lead to incorrect recognition of an individual.

c) *Non-universality:* While it is assumed that the single biometric characteristic in question will be available with every human but there can be exceptions to this presumption. For example: If we consider fingerprint image to identify individual, those who are physically disabled and cannot input a recognisable biometric won't be recognised by the system. den Os et al. [19] reports the Failure to Enroll problem in a speaker recognition system.

d) *Spoof attacks:* As technology is developing at a high rate and new applications are discovered day-by-day, it won't be surprising to notice that the number of ways one can fraudulently forge a biometric trait are also increasing. This makes a unimodal system very vulnerable and open to misuse of information.

e) *Distinctiveness:* As intra-class differences can increase, Inter-class differences can decrease and there may be noticeable number of similarities between characteristics of two different people [20].

f) *Collectability:* Characteristics must be measurable and obtaining them must be easy.

In order to overcome the constraints of a unimodal biometric system, a *multimodal* biometric system was introduced where in 2 or more biometric features are collected and integrated. The upshots of such a system are better performance, improved reliability and fulfilment of more strict requirements [21, 22]. The limitations of each of the single biometrics such as, non-universality of fingerprints, alteration of facial characteristics based on light conditions and many others, can be overcome by combing the outcomes of each feature.

D) Finger Print

Finger prints are one of the oldest biometric features used in identification and verification. Finger print identification is based on location of the ridges and the direction of the ridges. It can be carried out in two ways: minutiae-based matching, which is based on the finding the location and direction of each ridge present in the fingerprint, and pattern based matching, which simple matches two images for any existing similarities between them. The devices used to input the fingerprint images must be maintained properly as any discrepancies can lead to latent finger prints. The

devices are trained to differentiate between an actual 3D fingerprint and a 2D sample picture of one [23]. Once the fingerprint is acquired, Image enhancement techniques are performed on the images.

There are different types of Fingerprint Patterns:

a) Plain arch and Tented Arch
b) Radial Loops and Ulnar Loops
c) Plain Whorl
d) Central Packet Loop Whorl
e) Double loop whorl
f) Accidental whorl

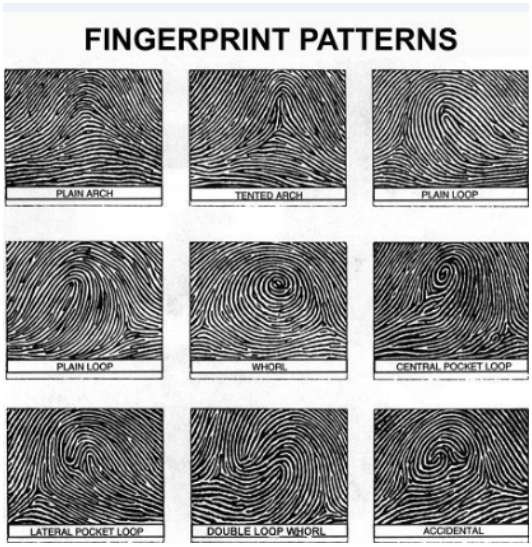

Figure 2: Types of Fingerprint Patterns [24].

The disadvantages of minutiae based matching is that they require high quality finger print images to locate the positions of the bifurcations, ridges, etc. and do not consider the global patterns present on the finger. Pattern matching is able to solve these limitations. However, it is affected by the rotation or any transformation in the images and requires the exact position of the registration points. In the final recognition process, the biometric system tries to determine a minutiae transformation between the current input and the stored template in the database. The matching decision then depends on the possibility and complexity of the necessary transformation [23].

One study [25] used fingerprint authentication for digital signing based on the X.509 certificate infrastructure. This research tried to add new features enabling the user to customise the protocols and algorithms used. Studies have been conducted to shift from fingerprint acquisition using traditional ink to more developed methods based on optical, silicon, thermal and ultrasonic factors.

E) Facial Recognition

The procedure of facial recognition in its most general form follows the steps of gray scaling to make the processing rapid and after using face detection, only the face part of the image is now our region of interest.

Once our region of interest is established, it is sub-divided into 3 images specifying features in each of the regions. A correlation is performed with the existing database images and the results are averaged to get a decision, whether the face is recognized (match exists) or not.

Before we begin to recognize a face, we need to detect the existence of a page to avoid overhead and comparison of images.

a) The image is received in the software after acquisition as the input for the forthcoming operations.
b) It is then converted from its color mode (RGB) to a gray scale mode followed by scaling of the image and resizing it.
c) Edges are then detected using calculations pertaining to the gradient of the image (Sobel Operator - binary mask is made with a threshold value which is the mean of all gray values in the image).
d) Now, some morphological operations are performed in the order: dilation -> filling -> combination of erosion and dilation techniques
e) Then the image is scaled back to its original size and finally a decision is made on whether or not a face has been detected in the image.

Following are the detailed steps for face recognition [26]:

*1) Lightning:*The image is first lightened to get a contrasting picture with the given difference as per the image.
2) *Scaling:* For image matching and recognition, the size of the image should be the same as the size of the images in the database. Hence, the face is initially detected, cropped and the resized to make comparison possible.
3) *Correlation:*The image is the correlated to each image in the database and a correlation coefficient is obtained. If the highest coefficient is greater than a selected threshold coefficient (0.9 or 0.5), a match is detected and the process is terminated with the result returned. In case we do not get a coefficient with a value big enough, we move to the next step if segmenting the images.
4) *Segmentation:* Here the face is sectioned into 3 parts, uppermost, middle and lowermost parts. Each of the parts is then correlated with the corresponding sections in the database images. The three correlation coefficients are averaged out and must fulfil a specific threshold criteria for the face to be successfully recognized.

F) Speaker Recognition Procedure

As mentioned before, the voice of an individual is dependent on both behavioural and physical aspects. The speech signal emitted by humans is rich with high dimensional features whose complexity must be lessened to add as much information as possible in the feature extracted.

a) *Signal Acquisition*: The voice of a user is first acquired using microphones and the analog signal is then digitized using an ADC, hence giving us a numeric vector representing the speech signal.
b) *Speech Signal Pre-processing*: The signal, a function x (n) is continuous and time-varying, but it is considered to be constant over extremely small time intervals. Generally, the signal is split into frames of 25 ms, each denoted byx_i (n). This division leads to discontinuities arising in the temporal domain, and to oscillations mainly in the frequency domain. To avoid this, a Hamming windows is used here.
c) *Feature Extraction*:Features are now extracted from the resulting signal after pre-processing which are most suited to the users and their type. These features have

the qualities of being robust and not subjected to variations sue to impersonation, sickness, etc.Short-term spectral features are used most often (MFCC: Mel-frequency cepstral coefficientsare found to bethe most efficient).

d) *Speaker Modelling*: Now that we have the feature vectors, a training phase follows. The VQ (vector quantization) method is used for this purpose[27]. It is based on the LBG (LindeBuzoGray) algorithm [26]. Following clustering, this method allows one to define a voice sample by a model vector having a predefined fixed size, whatever the initial length of the signal.

e) *Speaker recognition*: The above 4 steps enrol or register a user into the system. Coming to the recognition part of it, user authentication, the recognition question is answered by Euclidean distance computation between the reference template and the new captured template. Once a hit is found with distance less than a given thresholddistance, a match is obtained and the speaker is recognised.

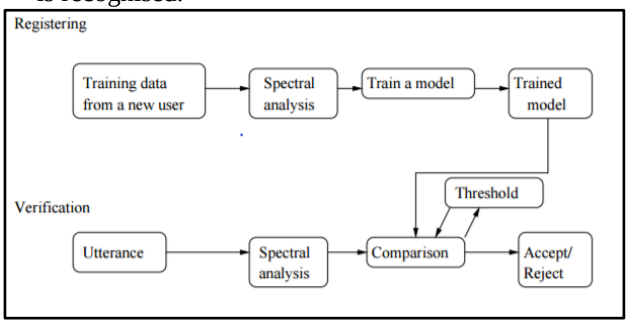

Figure 3: General Procedure for Speaker Recognition

G) Keystroke Recognition Procedure

Keystroke dynamics today are still in the experimental stages and cannot be used as an independent mode of verification as users may not be uniquely identified through these dynamics, but they can be classified into different subsets and matched accordingly.

The feature subset can be selected based on the following models, after which classification will follow:

a) Filter Method: Here a general subset of characteristics or features is considered without the application of a learning algorithm. This subset may or may not be the right subset of features for classification.

b) Wrapper Model: In this type of model, a learning algorithm is applied and over various iterations, the feature selection is improved manifold.

c) Hybrid Model: It uses the above to models at different stages and combine both their advantages. However, it is far more complex to implement.

After the subset is selected and features identified, the classification stage begins where the new sample is matched with previously available samples to the maximum accuracy. Methods of pattern matching are employed in the typing rates and rhythms of the user and his/her stored samples. If the samples have variations above a specified threshold, the user is denied access. While within the threshold, the identity of the user can be verified and authenticated to grant access.

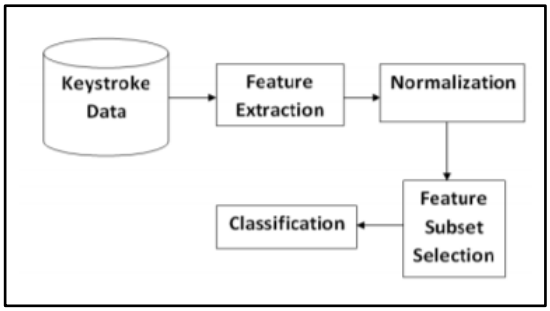

Figure 4: General Procedure for Keystroke Recognition [28]

III. SUGGESTED MODEL

Problem statement:Demonetisation in India has transported us into an era of digitised transactions. Dependency on cashless transactions has surged meteorically in the past few months. Citizens from all social strata are now forced to step up on the digital platform without complete cognizance of its risks. As a result, inexperienced people are more prone to cybercrimes and fraudulence.

Until recently, passwords or PINs were commonly used to secure transactions and authentication. These passwords can easily be hacked, decoded or guessed.Therefore, payment gateways must be made more secure. The existing system using RFID (Radio Frequency Identification) which incorporates a unique token based authentication system in a short wireless range, are often more expensive, can be unreliable and are less user friendly.

Objective: The aim of this paper is to propose a model for incorporation of multimodal biometric techniques in existing systems to enhance their security with respect to cashless transactions and minimize financial fraud. It uses the standard resources available on hand held devices and hence no added expenses are incurred. The establishment of this model will result in a more alert, responsible and safer society. It will bridge the gap between the technologically advanced and technological neophytes and reduce the potential risk to their finances.

Methodology: The user identifies the transaction he wants to make and all details like price, order, quantity, etc. are first obtained. When the user is ready to make the payment, the mode of payment (Net banking, Credit/Debit Cards, online wallets) is selected. A preregistered mode of authentication is then applied to validate the user's identity and complete the transaction. These modes of authentication can be:

1) Level 1: User defined Alphanumeric keys(Password, PIN) and Security questions.

2) Level 2: User Information encoded in Barcodes/QR Codes.

3) Level 3: Physical Biometric identification system
   a) Fingerprint
   b) Facial Recognition

4) Level 4: Behavioural Biometric Identification system
   a) Voice
   b) keystrokes

The level and extent of security measures will be incorporated as desired by the user. The user can select either unimodal (only one) security feature or multimodal (a combination of more than one) safety features to secure their accounts.

However, the system will analyse details such as average bank account balance, transaction rates and amounts, type of

account, etc. to suggest the most appropriate levels of security.

IV. CONCLUSION

This paper discusses the various types of identification and authentication techniques including basic QR Codes and Barcodes as well as unimodal and multimodal biometrics. Under biometrics, it covers both physical and behavioural categories, their procedures and the corresponding advantages and disadvantages in today's scenario. It then suggests a model implementing a combination of the above mentioned techniques, hence, introducing a multi-modal architecture with different levels of security to safeguard cashless transactions from fraudulent activities.

V. ACKNOWLEDGMENT

We would like to thank Prof.Sathyaraj R., Assistant Professor (Senior), Department of Software Systems (SCOPE), VIT University, Vellore for his constant support and assistance which helped us improve this manuscript. He boosted our confidence at each step to make this paper a possibility and we are forever grateful to him.

VI. REFERENCES

[1] Rieback, Melanie R., Bruno Crispo, and Andrew S. Tanenbaum. "Is your cat infected with a computer virus?." In *Pervasive Computing and Communications, 2006. PerCom 2006. Fourth Annual IEEE International Conference on*, pp. 10-pp. IEEE, 2006.

[2] ISO 18004:2006. QR Code bar code symbologyspeci_cation. ISO, Geneva, Switzerland.

[3] M. Canadi, W. Hopken, and M. Fuchs. Application of qr codes in online travel distribution. In ENTER, pages 137-148, 2010.

[4] Al-Khalifa, Hend S. "Utilizing QR code and mobile phones for blinds and visually impaired people." In *International Conference on Computers for Handicapped Persons*, pp. 1065-1069. Springer Berlin Heidelberg, 2008

[5] Alapetite, Alexandre. "Dynamic 2D-barcodes for multi-device Web session migration including mobile phones." *Personal and Ubiquitous Computing* 14, no. 1 (2010): 45-52.

[6] ISO 24778:2008. Aztec Code bar code symbologyspeci_cation. ISO, Geneva, Switzerland.

[7] Huang, Yo-Ping, Yueh-Tsun Chang, and FrodeEikaSandnes. "Ubiquitous information transfer across different platforms by qr codes." *Journal of Mobile Multimedia* 6, no. 1 (2010): 3-13

[8] Gao, Jerry, Vijay Kulkarni, HimanshuRanavat, Lee Chang, and Hsing Mei. "A 2D barcode-based mobile payment system." In *Multimedia and Ubiquitous Engineering, 2009. MUE'09. Third International Conference on*, pp. 320-329. IEEE, 2009.

[9] Gao, Jerry Zeyu, Lekshmi Prakash, and RajiniJagatesan. "Understanding 2d-barcode technology and applications in m-commerce-design and implementation of a 2d barcode processing solution." In *Computer Software and Applications Conference, 2007. COMPSAC 2007. 31st Annual International*, vol. 2, pp. 49-56. IEEE, 2007.

[10] Gao, Jerry Zeyu, HemaVeeraragavathatham, ShailashreeSavanur, and Jinchun Xia. "A 2D-barcode Based Mobile Advertising Solution." In *SEKE*, pp. 466-472. 2009

[11] Lisa, S., and G. Piersantelli. "Use of 2d barcode to access multimedia content and the web from a mobile handset." In *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, pp. 1-3. IEEE, 2008

[12] Bose, Raj Chandra, and Dwijendra K. Ray-Chaudhuri. "On a class of error correcting binary group codes." *Information and control* 3, no. 1 (1960): 68-79.

[13] Gaikwad, Shital Y., and Chandrakant S. Audhutwar. "Automatic Toll Collection by Using QR Code Capturing." *International Journal of Computer Science and Information Technologies* 5, no. 5 (2014).

[14] Reed, Irving S., and Gustave Solomon. "Polynomial codes over certain finite fields." *Journal of the society for industrial and applied mathematics* 8, no. 2 (1960): 300-304.

[15] ISO, BS. "IEC 18004: Information Technology-Automatic Identification and Data Capture Techniques-QR Code 2005 Bar Code Symbology Specification." *BS ISO/IEC* 18004 (2006).

[16] Kaschte, Birgit. "Biometric authentication systems today and in the future." *University of Auckland* (2005).

[17] Jain, Anil K., Arun Ross, and SalilPrabhakar. "An introduction to biometric recognition." *IEEE Transactions on circuits and systems for video technology* 14, no. 1 (2004): 4-20.

[18] den Os, Els, Hans Jongebloed, Alice Stijsiger, and Lou Boves. "Speaker verification as a user-friendly access for the visually impaired." In *EUROSPEECH*. 1999.

[19] Ribalda, Ricardo, Guillermo Glez de Rivera, Angel de Castro, and Javier Garrido. "A mobile biometric system-on-token system for signing digital transactions." *IEEE Security & Privacy* 8, no. 2 (2010): 13-19..

[20] Maio, Dario, DavideMaltoni, Raffaele Cappelli, James L. Wayman, and Anil K. Jain. "FVC2002: Second fingerprint verification competition." In *Pattern recognition, 2002. Proceedings. 16th international conference on*, vol. 3, pp. 811-814. IEEE, 2002.

[21] Hong, Lin, Anil K. Jain, and SharathPankanti. "Can multibiometrics improve performance?." In *Proceedings AutoID*, vol. 99, pp. 59-64. Citeseer, 1999.

[22] Kuncheva, Ludmila I., Christopher J. Whitaker, Catherine A. Shipp, and Robert PW Duin. "Is independence good for combining classifiers?." In *Pattern Recognition, 2000. Proceedings. 15th International Conference on*, vol. 2, pp. 168-171. IEEE, 2000.

[23] Owayjan, Michel, AmerDergham, Gerges Haber, Nidal Fakih, Ahmad Hamoush, and ElieAbdo. "Face Recognition Security System." In *New Trends in Networking, Computing, E-learning, Systems Sciences, and Engineering*, pp. 343-348. Springer International Publishing, 2015.

[24] Ayhan EMRE DenizBilimleriveMühendisliğiEnstitüsü, *Biometric Security Technologies.*

[25] Subban, Ravi, and Dattatreya P. Mankame. "A study of biometric approach using fingerprint recognition." *Lecture Notes on Software Engineering* 1, no. 2 (2013): 209.

[26] Brunet, K., K. Taam, E. Cherrier, N. Faye, and C. Rosenberger. "Speaker Recognition for Mobile User Authentication." *nd): n. pag* 25 (2013).

[27] Sajjadi, Sayyed Mohammad Sadegh, and BahareTajalli Pour. "Study of SQL Injection Attacks and Countermeasures." *International Journal of Computer and Communication Engineering* 2, no. 5 (2013): 539.

[28] Zhong, Yu, Yunbin Deng, and Anil K. Jain. "Keystroke dynamics for user authentication." In *Computer Vision and Pattern Recognition Workshops (CVPRW), 2012 IEEE Computer Society Conference on*, pp. 117-123. IEEE, 2012.