ISSN: 2456-3463
International Journal of Innovations in Engineering and Science, Vol. 1, No.3, 2016

Authentication on Payment gateway using Face Recognition System

Rahul Kumar[1], Vishakha Sharawat[2], Ghevar Ram Dewasi[3], Rupesh Mahajan[4],

Department of Information Technology, DYPIET, PUNE-411018,INDIA

Abstract - *The threat of transaction timed-out or malicious software (malware)-based attacks or illegal use of technology is significant and growing; at the same time online banking gets more and more popular. Earlier during making any online payment or making any online banking related transactions, the method used to complete a transaction was with One-Time-Passwords as well as passwords, which were sent on the end users registered mobile number or email address which were linked with his bank account. Financial loss may be one of the consequences if credentials or credentials linked devices get stolen. In many protocols, the transaction information is not secured properly.*

The proposed "Authentication on Payment Gateway using Face Recognition" is based on the face recognition technique on payment gateway. This system eliminates the One-Time-Password & password based transactions with Face recognition system. When face recognition authentication is used spoofing or faking; of face comes into picture. As in face recognition faking can be done by displaying photograph (hardcopy) or video in front of the authenticating device. Considering these faking or spoofing techniques this system also uses Face spoofing algorithms to overcome these issues. Using this we can complete successful transaction by verified natural person in a way that it is proven to the executing party, that the transaction, as it is received, was in fact initiated and confirmed by an identified natural person.

Keyword: E-Commerce, Gateway, E-payment, Electronic Payment Gateway, Face recognition.

INTRODUCTION

The Gateway is called as Trusted Third Party or Entry point to any network. It is used in E-commerce system for more secure transaction. Online shopping allows customers to sit in their homes and buy goods from all over the world. Similarly allow Merchant to sell their products to all over the world from home. Most of the population will use online payment in near future. Most of the world's countries lagged behind in making a good Internet architecture.

There is need of a secure, fast and easy online payment gateway which is more reliable. On the basis of proposed architecture of e-payment system, this system gives an brief overview of e-payment gateway using face recognition. It also mentions the requirement of an e-payment gateway from customer and merchant's point of view. And on the basis of these facts and figures a new secure e-payment gateway has been designed and developed.

The payment gateway would provide secure and fast transactions. On the basis of proposed architecture of e-payment system and the requirements related to any electronic payment gateway, we design and develop a secure, reliable and efficient electronic payment gateway with face recognition. Nowadays, In India the concept of e-payment is getting more popular than earlier. The networks, run by banks and the government over high-speed phone lines, converge at just 10 secret data processing centres nationwide. They transmit everything from direct-deposit pay checks to utility bill payments to huge corporate transfers in the India and abroad. PayPal in the US, which was recently purchased by EBay, is one of the most frequently used e-payment gateway. In China payment gateway is the single biggest unmet demand because of lack of trusted and secure mechanism.

Turkey's payment gateway is difficult to use insecure and highly expensive. In Nepal there are around 3three banks that are offering Internet Banking Services, Etc. But wheresoever's and whichever Bank used for e-payment; first priority is always given to security as well as reliability of the transaction. On second priority speed of transactions comes. This proposed idea has a scope of developing such a system that will provide a secure, reliable and fast transaction processing using Face Recognition.

In Face recognition system, when a request is generated for transaction. Details of the payee are verified. If the details are legitimate i.e. payee is legitimate, then the facial details of payee are collected and simultaneously it is collected by the corresponding bank and compared with each other. Positive response of comparison will lead to successful transaction processing. Whereas, negative response will lead to termination of the transaction. And, If the user is not legitimate then the transaction processing is rolled back to merchant's website. This working of the system will eliminate the OTP based transaction processing as well as make the payment secure, efficient and faster.

PRELIMINARIES

Online customer:

A customer is an entity who will buy products by making payments in timely manner.

.

Merchants:

A merchant is a seller who will receive payments made by customer.

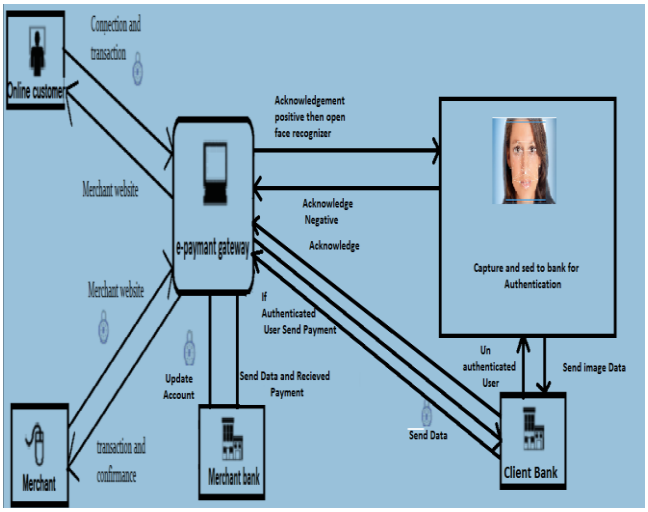


Fig 1-Framework Overview of Proposed Gateway Network

Banks:

Two banks involved are:-

1. Client bank
2. Merchant bank

Client bank:

Client's bank holds client's bank account details and validate customer during account registration.

Merchant bank:

Merchant bank holds merchant bank account details. It is responsible for management, fraud control etc. A merchant account is a type of bank account that allows businesses to accept payments by payment cards, typically debit or credit cards. A merchant account is established under an agreement between an acceptor and a merchant acquiring bank for the settlement of payment card transactions. In some cases a payment processor, independent sales organization (ISO), or merchant service provider (MSP) is also a party to the merchant agreement.

Payment Gateway:

A payment gateway is connected to all customers, merchants and banks through Internet and responsible for the speed, reliability and security of all transactions that take place. A payment gateway is an e-commerce service
that authorizes payments for e-businesses and online retailers. It is the equivalent of a physical POS (point-of-sale) terminal located in most retail outlets. A merchant account provider is typically a separate company from the payment gateway. Some merchant account providers have their own payment gateways but the majority of companies use 3rd party payment gateways.

The gateway usually has 2 components:

a) The virtual terminal that can allow for a merchant to securely login and key in credit card numbers

b) They have the website's shopping-cart connected to the gateway via an API to allow for real time processing from the merchant's website.

FRAMEWORK OVERVIEW

There are six interfaces:-

1. Customer Interface

2. Server (e-payment Gateway) Interface
3. Client Bank Interface
4. Face Recognition Interface
5. Merchant Bank Interface
6. Merchant Interface

Online Customer will connect to e-payment gateway through Internet. Gateway will connect to the Bank and check whether its bank accounts are enough to buy the required product. Online customer can also visit Merchant's website through Gateway. Secure Pay provides a payment gateway that facilitates electronic commerce,

By enabling merchants to accept credit cards and electronic checks as methods of payment for goods and services sold online.

The gateway acts as a bridge between the merchant's website and the financial institutions that process payment transactions. Payment data is collected online from the shopper and submitted to the gateway for real-time authorization. However, the payment gateway is targeted towards merchants that process Card-Not-Present transactions.

In a Card-Not-Present We proposed a model of electronic payment gateway using face recognition on the basis of facial details, such that transaction processing is done efficiently in a secure manner as fast as possible by eliminating OTP based transaction. All e-commerce and mail/telephone orders are Card-Not-Present transactions.

PRELIMINARY TERM

Privacy: It is necessary to assure privacy in the payments like bank accounts.

Naming: There should be a way of identifying the customer's bank accounts and the merchant bank accounts.

Security: In gateways security should provide to protect data of transactions.

Integrity: Data should be difficult to change.

Confirmation: When transaction took place customer must have notification and merchant must have confirmation

Confidentiality: Any third parties should not be able to access or view such payment.

FLOW DIAGRAM PROPOSED PAYMENT GATEWAY

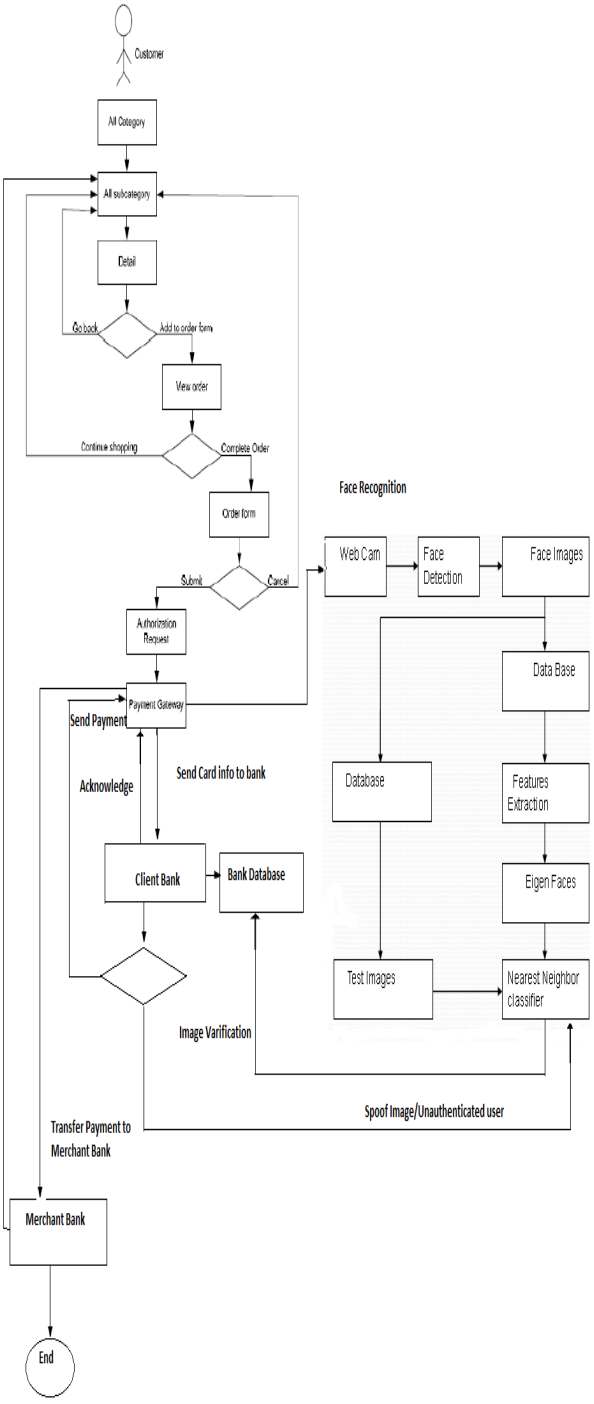


Fig 2-Flow diagram of proposed gateway

This system specially developed for encouraging e-payment for online shopping because of security issues. Here we use electronic gateway which is used for secure

transactions between client and merchant using Face recognition by eliminating OTP based transaction. If new user wants to do transaction then he/she should register Himself/herself first through registration form then browse merchant website using e-payment gateway.

Select item and encrypt payment request and send it to Server. Server receives encrypted message from sender, decrypt message, read, encrypt it using its own keys, encrypted facial details and send it to Client bank. Client bank first authenticates facial data which is received with the details available in database, and then the transfer of required amount is done to the merchant bank through secure network. After receiving the fund Merchant bank sends the payment.

TECHNIQUES & ALGORITHM

There are various algorithms on actions of client, merchant

1. **Algorithm of Client:**

   Client can browse merchant's website. After selection of items he can send payment order to e-payment server after filling required fields e.g. Credit card number, expiry date etc

   Steps: -

   a) Start and connect.
   b) Start Customer browse merchant website
   c) If select Category then
   d) Go to Item list of selected category
   e) If Select Item Then
   f) Show detail of selected item
   g) If Want to buy selected item Then
   h) Select Add to order form
   i) Else
   j) Go back to category
   k) If select add to order form
   l) Do Add To Order Sub Category Id
   m) go to Order form and fill required fields like credit card No., expiry Date, and telephone no, Address
   n) Select Submit
   o) Else continue shopping
   p) Else Cancel
   q) If select submit Display Authorization
   r) If Credit card no. Text is equal to Credit card no. display This Customer is Authorized From Bank.

2. **Payment gateway:**

   Steps: -

```
Start connection
If connected
Receive payment message
Else display Not Connected
If receive payment message
{Decrypt message
Split and send it to different textboxes
Add to database
Sent it to Client bank}
Else Cancel
If client bank is sending message
{Receive it
Send it to Face recognition Process}
If client bank is sending message
{Authorised User and Payment Receive
Send it to Merchant Bank}
Else wait
If merchant bank is sending message
{Receive it
Send it to Merchant}
```

Fig 3-Payment Gateway algorithm

3. **Algorithm of Client Bank:**

   Client bank receives payment message and verify client. Deduct amount from client bank and send that amount to payment gateway.

   Steps: -

   a) Start connection
   b) If connected
   c) Receive payment message including client's information.
   d) If client's info is present in database of bank
   e) Send message to server This customer is
   f) Authorized
   g) Else
   h) Send message This customer is not Authorized
   i) If customer is Authorized{Send request for Face Verification .Verify face with face present in bank Database}
   j) If customer is Authorized{Save payment request into database Deduct amount from Client bank Send that amount to Payment Gateway}
   k) Else
   l) Send message This customer is not Authorized

4. **Algorithm of Merchant Bank:** Merchant bank verifies merchant, receives payment message from

Client bank through payment server and add payment to Merchant's account.

Merchant Bank

Steps: -

a) Start connection
b) If connected
c) Receive payment message including merchant account no.
d) If merchant's account is present in database of bank {Receive payment Add payment to Merchant's account}
e) Else
f) Send message Invalid account no.

5. Algorithm of Merchant: Merchant makes and updates website and receives acknowledgement messages from payment gateway.

Merchant

Steps: -

a) Start connection
b) If connected {Make and update website}
c) If server is sending message Receive message and decrypt it}
d) Else
e) Retry to connect

FACE RECOGNITION AND SPOOFING TECHNIQUE

It has been shown that face recognition techniques are vulnerable to spoofing attacks. In a spoofing attempt, a person tries to masquerade as another person and thereby, tries to gain an access to the system. Numerous recognition approaches have been presented in face recognition topic, however the studies on face anti-spoofing methods are still very limited. Therefore, nowadays anti-spoofing is a popular topic for researchers to fill this gap. Aim is to develop non-intrusive methods without extra devices and human involvement. In this way they can be integrated into existing face recognition systems. Also, methods which are robust to pose and illumination changes are preferable.

1. Algorithm for feature extraction using PCA

The facial features are extracted using the PCA method. Let there are *R* face images in the training set and each image ***Xi*** is a 2dimensional array of size $m \times n$ of intensity values. An image ***Xi*** can be converted into a vector of *D* ($D = m \times n$) pixels, where, ***Xi*** = (xi1, xi2, ….,xiD). The rows of pixels of the image are placed one after another to form the vector. Define the training set of *R* images by $\boldsymbol{X} = (\boldsymbol{X}1, \boldsymbol{X}2, \ldots, \boldsymbol{X}R) \subset \Re D \times R$. The covariance matrix is defined as follows:

$$\Gamma = \frac{1}{R}\sum_{i=1}^{R}(X_i - \overline{X})(X_i - \overline{X})^T = \Phi\Phi^T$$

where $\Phi = (\Phi 1, \Phi 2, \ldots, \Phi R) \subset \Re D \times R$ and

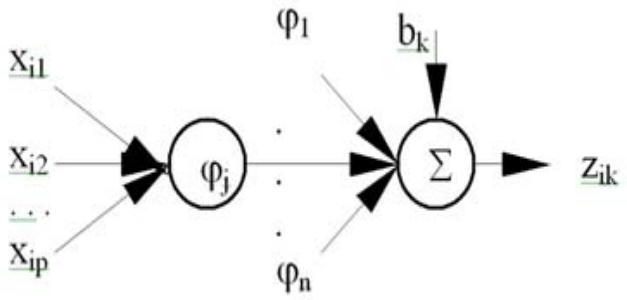
$$\overline{X} = \frac{1}{R}\sum_{i=1}^{R} X_i$$

which is the mean image of the training set. The dimension of the covariance matrix Γ is $D \times D$ .Then, the eigen values and eigenvectors are calculated from the covariance matrix Γ. Let $\mathbf{Q} = (\mathbf{Q}1, \mathbf{Q}2, \ldots, \mathbf{Q}r) \subset \Re D \times R$ ($r<R$) be the *r* eigenvectors corresponding to *r* largest non-zero eigen values. Each of the *r* eigenvectors is called an *eigenface*. Now, each of the face images of the training set **X**i is projected into the eigenface space to obtain its corresponding eigenface-based feature $Zi \subset \Re r \times R$, which is defined as follows:

$$\mathbf{Z}i = \mathbf{Q}T\mathbf{Y}i \text{ , } i = 1, 2, \ldots, R \quad \ldots\ldots\ldots\ldots\ldots (2)$$

where **Y**i is the mean-subtracted image of **X**i.

In order to recognize the test images, each of the test images is transformed into the eigenface space using the equation (2) and then fed to the RBF neural networks as inputs for classification.



2. Algorithm for spoofing using LBPV

LBPV is a simplified and efficient joint LBP and contrast distribution method . In LBP calculation, there is no information related with variance. Actually, the variance is also related to the texture feature and usually the high frequency texture regions have higher variances and contribute more to the discrimination of images. Since initially, DoG filtering is applied, the high frequency regions are all extracted after this step. Thereby, it is easier to discriminate captured and recaptured images by applying LBPV algorithm on these regions which are extracted by DoG filtering.

The contrast and pattern of a texture are complementary features. LBPV adds additional contrast measures to the pattern histogram and this provides significantly better results than LBP. This claim is verified by testing both LBP and LBPV using different textures in . These algorithms are also tested for our study.

The comparison result is given in 'Experimental Results' part of the paper. LBPV calculation is based completely on LBP calculation.

LBPP,R is calculated as follows:

$$LBP_{P,R} = \sum_{p=0}^{P-1} s(g_p - g_c)2^p, \qquad (1)$$

$$s(x) = \begin{cases} 1 & x \geq 0 \\ 0 & x < 0 \end{cases} \qquad (2)$$

LBPP,R is computed such that for a given central pixel in an image, a pattern number is computed by comparing its value with those of its neighbours. In Equation (1), gc is the gray value of the central pixel, gp is the value of its neighbours, P is the number of neighbours around a circle of radius R . To obtain LBP histogram of an X × Y image, the LBP pattern of each pixel (i, j) is used in calculation.

$$H(k) = \sum_{i=1}^{X}\sum_{j=1}^{Y} f(LBP_{P,R}(i,j),k), \quad k = [0\ K] \qquad (3)$$

$$f(x,y) = \begin{cases} 1 & x = y \\ 0 & else \end{cases} \qquad (4)$$

K is the maximal LBP pattern value in (3). In this histogram, each LBP pattern has weighting factor of 1.LBPV algorithm is used to add contrast information to this histogram. Variance is computed for the P sampling points around a circle of radius R using Eqs. (5) and (6).

$$Var_{P,R} = \frac{1}{P}\sum_{p=0}^{P-1}(g_p - u)^2 \qquad (5)$$

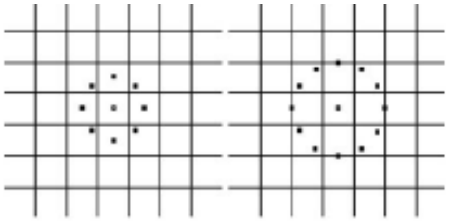
$$u = 1/P\sum_{p=0}^{P-1} g_p \qquad (6)$$

The LBPV computes the variance from a local region and accumulates it into the LBP bin as the weighting factors [10]. LBPV histogram is calculated using Eqs. (7) and (8).

$$LBPV_{P,R}(k) = \sum_{i=1}^{X}\sum_{j=1}^{Y} w(LBP_{P,R}(i,j),k), \quad k = [0\ K] \qquad (7)$$

$$w(LBP_{P,R}(i,j),k) = \begin{cases} \mathrm{var}_{P,R}(i,j) & LBP_{P,R}(i,j) = k \\ 0 & else \end{cases} \qquad (8)$$

The representations of two different selections for P and R values are shown in Fig. 2. When P and R values are increased, even better results are obtained; however
With a cost of increasing computational complexity as stated in.



(*P*=8,*R*=1.0) (*P*=12,*R*=1.5)

Fig 4- Circular representations of selections (P=8, R=1) and (P=12, R=1.5).

In the proposed approach, P and R values are selected as *P* = 8, *R* = 1, due to this computational complexity.
Instead of using all LBPV patterns, uniform patterns can be used as features in classification part. Uniform patterns are selected according to the U value which is defined as

$$U(LBP_{P,R}) = \left|s(g_{p-1} - g_c)\right| - \left|s(g_0 - g_c)\right| + \sum_{p=1}^{P-1}\left|s(g_p - g_c)\right| - \left|s(g_{P-1} - g_c)\right| \qquad (9)$$

There are both local and global rotation invariant algorithms in texture classification. In the proposed approach, a hybrid method, which is based on globally rotation invariant matching with locally variant LBPV texture features, is used to extract features for classification. Thereby, both global spatial information and local texture information are preserved in classification.

In our study, this global matching is implemented using exhaustive search scheme to find the minimal distance in all candidate orientations, which is a simple method. The LBPV histogram is reorganized and represented by a rotation variant histogram *Hrv*, and a rotation invariant histogram *Hri*. Then for two texture images, the matching distance is calculated as shown in Eq (10).

$$\begin{aligned} &D_{ES}(H_S, H_M) = D_{ri}(H_S^{ri}, H_M^{ri}) + D_{\min}(H_S^{rv}, H_M^{rv}) \\ &D_{ri}(H_S^{ri}, H_M^{ri}) = D(H_S^{ri}, H_M^{ri}) \\ &D_{\min}(H_S^{rv}, H_M^{rv}) = \min(D(H_S^{rv}, \overline{H_M^{rv}(j)})), j = 0,1,\ldots,7 \\ &\overline{H_M^{rv}(j)} = \left[h^M_{\mathrm{mod}(0-j,8)}, h^M_{\mathrm{mod}(1-j,8)}, \ldots, h^M_{\mathrm{mod}(7-j,8)}\right] \end{aligned} \quad (10)$$

In the proposed approach, chi-square distance is selected to be used as the dissimilarity metric, since for LBP based algorithms, it is recommended as dissimilarity metric in various studies. Chi-square distance between sample and model histograms is computed as

$$D(S, M) = \sum_{i=1}^{N} \frac{(S_i - M_i)^2}{S_i + M_i} \quad (11)$$

N is the number of bins and Si and Mi are, respectively,the values of the sample and model histograms at the nth bin. For each test image, matching by exhaustive search is applied using chi-square distance metric, and distances from each test sample to all samples (xi) in the client and impostor model sets are obtained. Then, quadratic means of distances are computed for client and impostor model sets, consecutively.N is the number of images in the model set and xi is the distance between test sample and model sample.

EXPERIMENTAL RESULTS

1. Graphical result of survey:

A survey was carried out of various users in three different areas for finding the reason that why people don't use ayment gateway and wrote it by compiling the average results of mentioned questions.

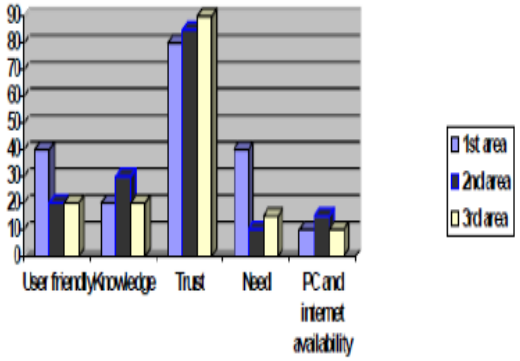


Fig 6 -Graphical Result Of Survey

a. User Friendly: People want a payment gateway which should be easy to use.

b. Knowledge: Some people don't know anything about payment gateway.

c. Trust: Mostly people don't use it because of lack of trust.

d. Need: Some people thinks there is no need of e-payment gateway.

e. PC and Internet availability: Limited access of PC and internet.

2. Graphical result of proposed gateway:

Graphical result of proposed gateway is following,As compare to other e-payment gateways our proposed system will be more secure and do transactions in less time as compare to other gateway. Proposed system will be inexpensive as compare to existing systems.

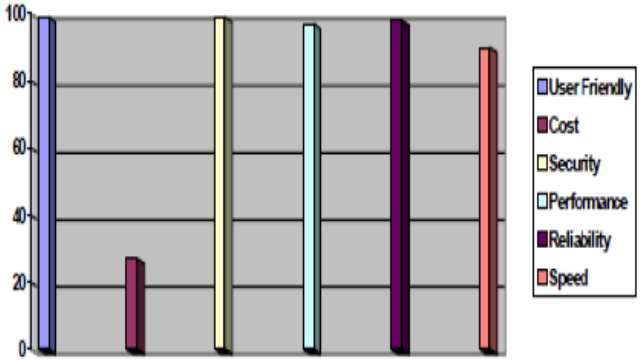


Fig 7 -Graphical Result Of Proposed Gateway

a. **Time**: Time of transaction
b. **Cost**: E-gateway's charges per transaction
c. **Availability**: The degree to which e-gateway is operable
d. **Security**: Overall security related to electronic gateway

FUTURE SCOPE

As the requirements of speedy processing of payment transaction is becoming the basic need for every area business. Therefore everybody is adapting technology for his or her business.

LIMITATIONS

- Computer cannot replace human judgment & Decision making.
- For transaction through E-Payment Gateway, user must have account in the bank which is registered on E-payment Gateway.
- The Availability of Gateway must be high to be used by online customers.
- Cost factor must be minimum so it can be afforded by customers.

CONCLUSION

The proposed Payment gateway is made secure by the implementation of secure e-transaction using face recognition. Because of this only authentic customers can do transactions. This payment gateway is made secure enough that any authorized customer can easily trust on it and fearlessly or confidently make payments over the Internet. At first it's checked if the customer is authorized one or not then the whole transaction takes place. E-payment gateway that fulfill their all requirements and provide security, privacy etc.

On the basis of these requirements and the local infrastructure, we propose an electronic payment gateway using face recognition for local environment.

REFRENCES

[1] *V. Athitsos, M. J. Swain, and C. Frankel, "Distinguishing Photographs and Graphics on the World Wide Web", in IEEE Workshop on Content-Based Access of Image and Video Libraries, pp. 10-17, June 1997.*

[2] *J. Friedman, T. Hastie, and R. Tibshirani, "Additive Logistic Regression: A Statistical View of Boosting", Technical Report, Stanford University, 1998.*

[3] *J. Huang, R. Kumar, and M. Mitra, "Image Indexing Using Color Correlograms", Proc. CVPR, pp. 762-768, 1997.*

[4] *R. Lienhart and A. Hartmann, "Classifying Images on the Web Automatically", Journal of Electronic Imaging, 11(4), pp. 445-454, 2002.*

[5] *T. T. Ng, S. F. Chang, and J. Hsu, "Physics-Motivated Features for Distinguishing Photographic Images and Computer Graphics", in proceedings of ACM conference on Multimedia, pp. 239-248, Singapore,2005.*

[6] *M. Stricker, and M. Orengo, "Similarity of color images", in Proceedings of SPIE Storage and Retrieval for image and Video Databases Conference, pp. 381-392, 199*

[7] *Belhumeur P. N., Hespanha J. P., and Kriegman D. J. 1997,"Eigenfaces versus fisher faces: recognition using class specific linear projection", IEEE Trans. Pattern Anal. Mach. Intell., vol. 23, no. 7,pp. 711-720.*

[8] *Chellapa R., Wilson C., Sirohey S. 1995, "Human and machine recognition of faces: a survey", Proc. of the IEEE, vol. 83, no. 5, pp. 705-741.*

[9] *Er M. J., Wu S., Lu J. and Toh H. L. 2002, "Face recognition with radial basis function (RBF) neural networks", IEEE Trans. Neural Networks, vol. 13, no. 3, pp. 697-710.*

[10] *Girosi F. and Poggio T. 1990, "Networks and the best appro--ximation property", Biol. Cybern., vol. 63, no. 3, pp. 169-176.*

[11] *Graham D. B and Allinson N. M. 1998, "Characterizing Virtual Eigen signatures for General Purpose Face Recognition", (in) Face Recognition: From Theory to Applications, NATO ASI Series F,Computer and Systems Sciences, vol. 163. H. Wechsler, P. J.Phillips, V. Bruce, F. Fogelman Soulie and T. S. Huang (eds), pp,446-456.*

[12] *Haykin S. 1999, Neural Networks a Comprehensive Foundation.Prentice-Hall Inc., 2nd Ed.*