Full Length Research Paper

Security improvement of credit card online purchasing system

A. W. Naji[1]*, Anas S. Housain[1], B. B. Zaidan[2,3,4], A. A Zaidan[2,3,4] and Shihab A. Hameed[1]

[1]Electrical and Computer Engineering Department, Faculty of Engineering, International Islamic University, P.O. Box 10, 50728 Kuala Lumpur, Malaysia.
[2]Faculty of Engineering, Multimedia University, 63100, Selangor, Malaysia
[3]Predictive Intelligence Research Cluster, Sunway University, Selangor, Malaysia.
[4]Institute of Postgraduate Studies/ Research and Development Group / Al-Madinah International University.

The paper aims to improve the security of the credit card online purchasing with taking into account the time and cost issues. Since the current online purchasing system using credit card has security drawbacks, a security improvement is suggested in this work by implementing a model which integrates the current authentication system of credit card with the fingerprint authentication. Moreover, it complements with a technique for validating and transmitting the fingerprint features. The customer submits his or her credit card information through the internet together with a file containing the fingerprint features and a validation code. This technique makes the customer feels more secure, at the same time it makes credit card fraud more difficult. Credit card information, fingerprint transaction authorization code and fingerprint features were the main components of the model. The authorization code is able to handle the usage of the scanned fingerprint features for one time only and preventing the submission of old and expired features. In addition, a 'biometric and authorization code' file is presented in this work to increase the fingerprint features security. It has its own structure in terms of storing the authorization code and fingerprint features which is unknown for the attacker and known only for the matching program. The average processing time consumed by the model to match all the data is 2.47 s while the overall accuracy rate was 99.48% with 0.52% error rate.

Key words: Credit card, authentication, fingerprint and biometrics.

INTRODUCTION

The usage of 'credit cards' has become one of the most succession elements in the business world (Blackwell, 2008), because there is no doubt that the credit card played a big role in the rapid growing of the nowadays E-commerce. The usage of credit card in online purchasing eliminate physical paper in use like cash or checks (Kumar, 2008). Customers simply browse merchant website and choose their preferred goods, after one click they need to key in their credit card number and other related information on payment form and wait for their purchase to be shipped to them. The only things need to be passed between customer and merchant is the credit card number and other information such as card holder's name and credit card expiry date etc. The problem is: it is not that simple as it sounds. Many people have logical fears about passing their credit card information through the Internet. It is an open network and has no security features built in; therefore, data is traveled between customer and the other side insecurely. In addition, the card holder needs to pass only credit card information including the security code at the back of the card in the online purchasing. Another unauthorized person other than the legitimate customer may access the information and use it in online purchasing (Hannan, 2008). Due to these fears, many techniques were developed to make the online purchasing more secure and trustable such as the widely used SSL and S-HTTP protocols (Sahut, 2008; Yan, 2007). During the last few years, many researches were done to thwart the credit card fraud (Bella, 2003;

---

*Corresponding author. E-mail: ahmed@iium.edu.my. Tel: 006 - 03 - 6196 4560. Fax: 006 - 03 - 6196 4488.

Bo, 2004; Hannan, 2008; Raghuwanshi, 2009; Yingjiu, 2004, 2005). Using the digital signature based on the public key infrastructure (PKI) is the common way of authenticating a customer (Bella et al., 2003). This makes the task at the customer side impractical and inconvenient since it requires the customer to have a public key certificate before emerging an online purchasing, (Abomhara et al., 2010a; Abomhara et al., 2010b; Alam et al., 2010; Naji et al., 2010).

The online purchasing needs a strong authentication system to handle the security issues. The strongest authentication systems are based on biometrics. Biometric authentication is based on something you are. It can provide a high level of authentication and ensure the person identity (Alanazi et al., 2010a; Alanazi et al., 2010b). Integrating the credit card online purchasing system with biometrics will ensure that no one can use the credit card except the authorized customer. This will protect both customers and merchants from credit card fraud and denial of service (Kumar et al., 2008). This paper presents an improved secure model for credit card online purchasing based on fingerprint verification. Fingerprint verification is based on minutia extraction algorithm. The model is employing three programs to handle the enrolling, capturing and matching for the fingerprint features. We also present a new technique to validate the fingerprint features by proposing the fingerprint transaction authorization code (FP-TAC) and biometrics and authorization code (BAC) file. Customer should submit this code along with his fingerprint features through a BAC file to the server to be validated and verified. The model also includes web pages to generate the FP-TAC and verifies the credit card (CC) information (Ahmed et al, 2010; Al-Frajat et al., 2010).

Related work

To enhance the security of online purchasing system, a new system is proposed to use automated handwritten signature verification for online purchasing system (Trevathan, 2009). This system is employing the static and dynamic features of the signature to make a judgment about the signature identity through a combination of complementary statistical models to analyze them. However, the system is consuming very long time in processing the handwritten signature and extracting their features. In addition, the system needs a long time to match the signature and has an error rate that reached 2.1% in the best cases. Another solution was proposed by Kim and Chang to integrate the credit card payment system with biometrics. They propose a method to employ the strength of fingerprint verification in credit card payment (Woong-Sik, 2006). The method was developed to apply in stores and point-of-sale (POS). The POS system is responsible of all the verification process. It requests the customer information and fingerprint image from the bank's database and verify them at the

POS. Nevertheless, this method is risking the customer's credit card information and his fingerprint image by requesting it from the database and verifying them at the POS. It also needs to install the verification server on each brand store which increase the cost and decrease the reliability (Zaidan et al, 2010a; Zaidan et al, 2010b).. Another system was proposed to enhance the security of online purchasing using credit card by employing biometrics and steganography at the same time (Ihmaidi, 2006; Zaidan et al, 2010c; Zaidan et al, 2010d). This system is hiding the card sensitive information into an image called electronic internet shopping card (EISC) using a fragile steganography algorithm (Hmood et al., 2010a; Hmood et al., 2010b; Hmood et al, 2010c; Zaidan et al., 2010e; Zaidan et al., 2010f).

This image is created by software given to the customer which is accessible only by the customer fingerprint. However, this system is taking much time in creating the EISC which affects the user acceptability for the system. Also, the fingerprint matching is done on the client side which is risky while the verification on the server side is done only on the credit card information.

MODEL OVERVIEW

The integrated authentication model (IAM) is integrating the current online purchasing system with biometric authentication. The model uses a two factor authentication. The first factor is the secret information that the customer has such as card security code, passwords and etc. the second factor used in this model is biometric. Since it provides a high level of security and it can be used in everyday life. The model uses the fingerprint authentication as it is one of the most usable type of biometric authentication (Kumar et al., 2008). Fingerprint authentication is low to medium cost and medium level of accuracy. The model is employing the commercial fingerprint readers to capture and enroll the fingerprint features since most of the computers nowadays have a built in fingerprint reader. Moreover, customers with no fingerprint reader built in their computer can get an external USB reader for a very low price (Shihab et al., 2010).

Model components and diagram

The proposed model consists of four components which are independent and work together to provide an effective and efficient validation. The four components are illustrated in Figure 1:

User (customer and employee)

An individual uses the model either to register a new customer or purchase through the Internet.
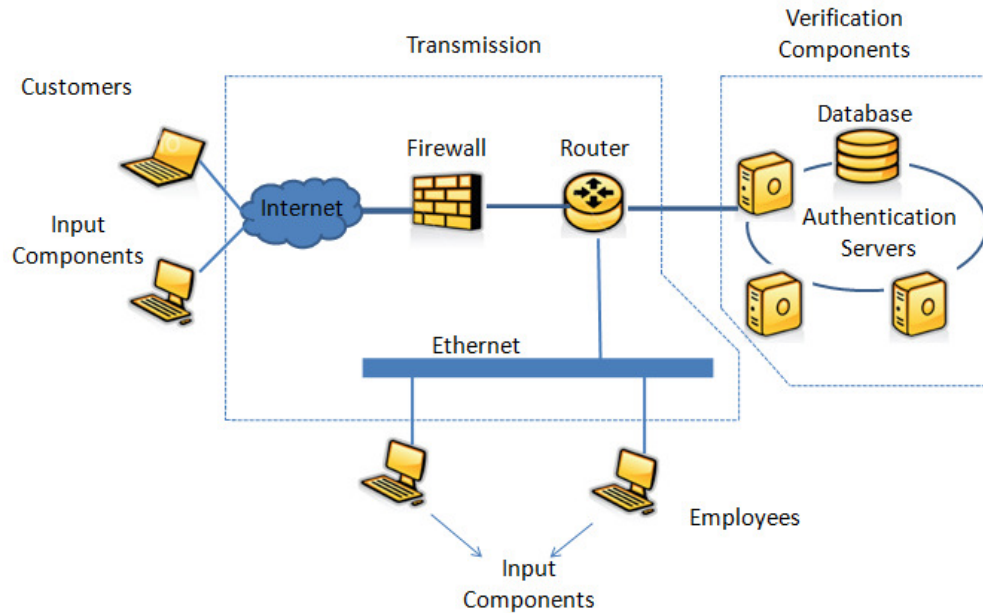
Figure 1. Model's diagram.

Input components

The proposed model used two different types of authentication components. These components are performing as an interface between user and the proposed model. The two components as follows:

Keyboards: The user needs this component to enter the CC information such as CC number and credit security code etc.

Fingerprint scanners: This component is taking part in registration part and capturing part so the user can enroll fingerprint features into database and capture it to be sent for verification.

Transmission

This part is responsible for transfer data between the input components and the verification component which is responsible of confirming the customer identity. Data may transfer through a public network and can be protected by transferring protocols. However, data transfer may take place in a local network (Medani et al., 2010; Nabi et al., 2010; Zaidan et al., 2011).

Verification component

This component is responsible for confirming the user-supplied identity against its database. The database is hosted on an authentication server. It contains a copy of CC information and fingerprint features of each customer.

The verification component also contains the fingerprint verification program to validate the fingerprint features. The proposed model can be applied on current online purchasing systems. The only need to be available in current systems is the input components and the fingerprint verification program. Therefore, there is no need to do major changes on current system to apply the proposed model.

Model's security elements

In order to enhance the security, the IAM proposes a two security elements which can raise the security level for the online purchasing process. The two elements are FP-TAC and BAC file. In the following, a detailed explanation about each element is presented:

Fingerprint transaction authorization code

The fingerprint features is a very crucial element in the IAM and needs a lot of concentration concerning its security, since it is traveled on an open network and managed by the customer. The fingerprint features is containing a data that can be used by matching program to match two fingerprints. The fingerprint image cannot be built from the fingerprint features, but the purchasing process can be done through submitting an old fingerprint features which is acquired by an old scan or hacked form the network or the customer's computer. The IAM proposed the FP-TAC which decreases the importance of the fingerprint features by making it useless without a valid generated code from the payment page. The IAM
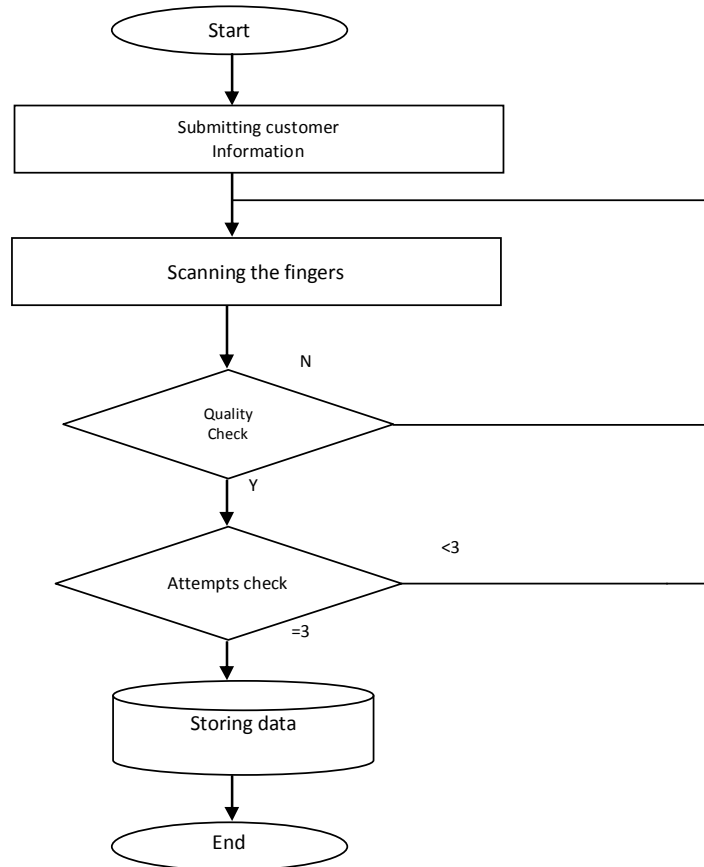
Figure 2. Registration part's flowchart.

employs the English alphabet (lower case) and numbers (0 to 9) to generate the four digits FP-TAC. Since it is generated randomly, the combination of both English lower case alphabet and numbers from 0 to 9 gives a probability of (4)36 random code. This huge number of codes is making the mission of submitting a fingerprint features with old or used FP-TAC is almost impossible.

Biometric and authorization code file

The BAC file is a binary file that is used by IAM to accommodate the fingerprint features data and FP-TAC. On the server side, the BAC file is used to store the fingerprint features data only. While the BAC file on the client side, is containing the fingerprint features data and FP-TAC together. The BAC file has a very small size that makes it travel rapidly and reliably during the data transmission between client and server. The BAC file's size is varying between 150 and 350 bytes depending on the scanned finger size and how much details contained. The BAC file has I unique proposed structure which makes the task of detecting the fingerprint features data or FP-TAC by an attacker a very hard task to obtain. Only the matching program has information about the BAC

file's structure and has the ability of extracting the FP-TAC and fingerprint features. Using the BAC file helps in decreasing the processing time for the IAM since it does not consume a lot of time for traveling through the transmission link (Sameer et al., 2011).

Model design

The proposed model is consisting of three major parts. First part (registration) is responsible of registering the customer and perform on the server side, while part two and three (verification and capturing) are working together to perform the online purchasing with fingerprint authentication.

Registration

The customer submits his information through an application form to a bank employee to register him and issue the credit card. The employee should ask the customer to scan his ten fingers Figure 2. Each scan should pass the quality check which checks the fingerprint image quality otherwise the customer would be
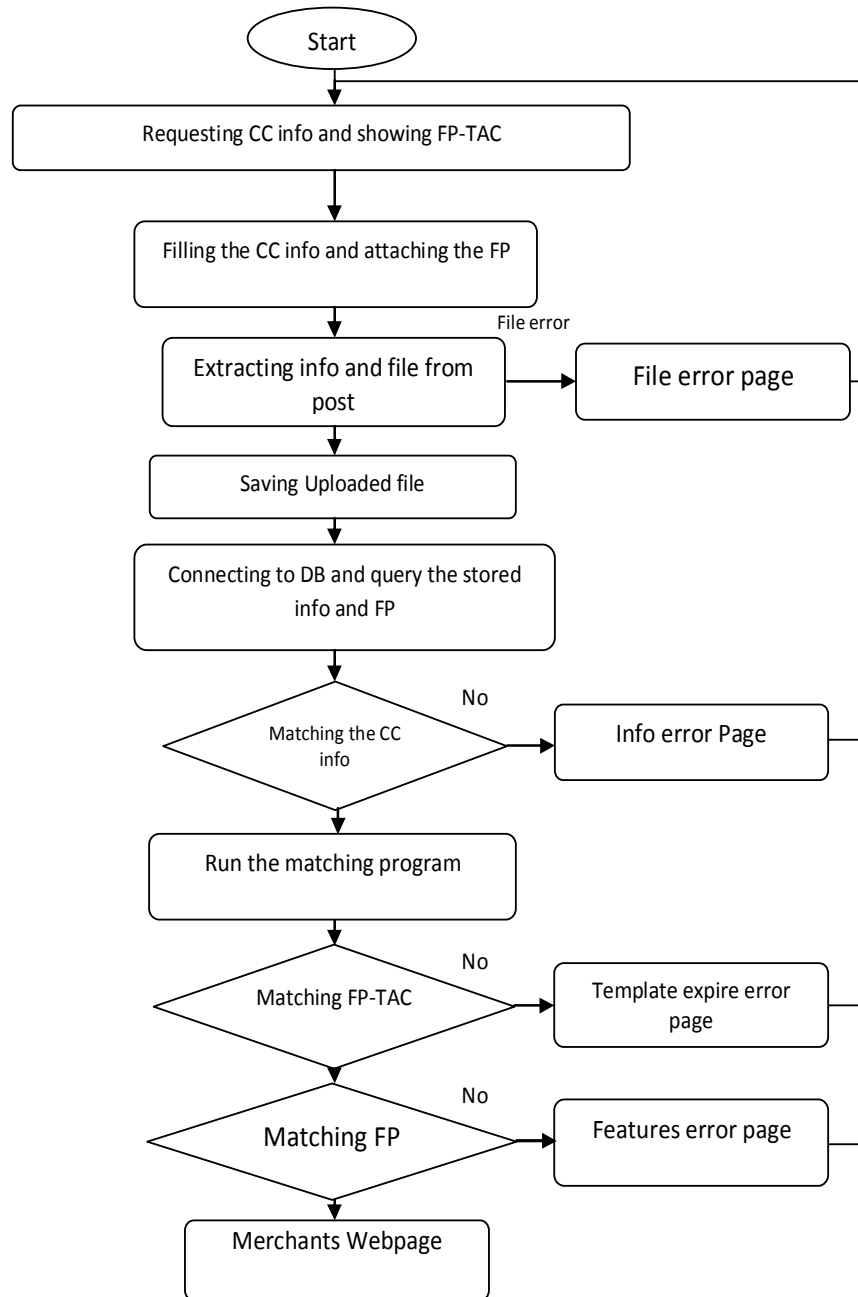
```
                              ┌─────────┐
                              │  Start  │
                              └─────────┘
                                   │
              ┌────────────────────────────────────────────┐
              │  Requesting CC info and showing FP-TAC      │
              └────────────────────────────────────────────┘
                                   │
              ┌────────────────────────────────────────────┐
              │  Filling the CC info and attaching the FP   │
              └────────────────────────────────────────────┘
                                   │           File error
              ┌─────────────────────────┐      ┌──────────────────────┐
              │  Extracting info and     │─────▶│   File error page    │
              │  file from post          │      └──────────────────────┘
              └─────────────────────────┘
                                   │
              ┌─────────────────────────┐
              │  Saving Uploaded file    │
              └─────────────────────────┘
                                   │
              ┌─────────────────────────┐
              │  Connecting to DB and    │
              │  query the stored        │
              │  info and FP             │
              └─────────────────────────┘
                                   │              No
                        ◇ Matching the CC ◇──────────▶ ┌──────────────────────┐
                        ◇      info       ◇            │   Info error Page    │
                                   │                   └──────────────────────┘
              ┌─────────────────────────┐
              │  Run the matching program│
              └─────────────────────────┘
                                   │              No
                        ◇  Matching FP-TAC ◇─────────▶ ┌──────────────────────┐
                                   │                   │ Template expire error│
                                   │                   │        page          │
                                   │                   └──────────────────────┘
                                   │              No
                        ◇   Matching FP    ◇─────────▶ ┌──────────────────────┐
                                   │                   │  Features error page │
                                   │                   └──────────────────────┘
              ┌─────────────────────────┐
              │   Merchants Webpage      │
              └─────────────────────────┘
```

Figure 3. Capturing and verification flowchart.

asked to rescan his finger. Next, the model should checks the number of attempts since it needs three attempts to approve the fingerprint features. After scanning the ten fingers, the employee starts to enroll the customer into database and assigns the primary key to CC number.

Verification and capturing

These two parts are representing the hard core of the proposed CC online purchasing model. When the customer is purchasing through the Internet and after selecting the goods to buy, the two parts take action to authenticate the customer and approve the money transaction Figure 3. First the customer will be directed to model's home page which shows the FP-TAC and ask the customer to provide the CC information and scan his fingerprint with attaching the FP-TAC within the scanning process. Now the model should move to another page which responsible of verification process. First, the data is

extracted and the received file is stored in a temporally location. Next, the page connects with database and queries the stored information based on CC number. It stores the stored fingerprint features in the same location where the received one stored. The page first matches the received CC information and the stored one. The page should move to next stage if result was positive, otherwise the page will redirect the customer to an error page. If the received CC information were correct, the page lunches the verification program. The program extracts the FP-TAC from the received fingerprint features. Next it matches the two fingerprint features and deletes the features permanently from the temporary location on server hard disk. After this task, the program returns the matching result and FP-TAC and terminates itself. Now the page is starting to do the crucial part. First it matches the received FP-TAC with the generated FP-TAC and validates the received fingerprint features. The customer will be directed to an error page if the FP-TAC is expired. Otherwise, the page should move down to next stage. This stage is examining the received matching result from the verification program.

It is a very crucial stage since the transaction status relies on it. The transaction is approved if the matching result was positive and the customer will be directed to merchant's webpage. However, customer will be directed to an error page if the matching result was negative.

Model implementation

The prototype is built on three essentials foundations. The foundations are fingerprint programs, web pages and database. Fingerprint programs consist of three programs to manage the enrollment, capturing and matching of the fingerprint features. On the other hand, web pages consist of three essential pages and several error pages. Meanwhile, database is storing the user CC information and the ten fingerprint features.

Implementation environment

The model is carried out by using three different programming languages. The fingerprint verification, enrollment and capturing programs have been built by using C programming language and BSAPI 3.0 for Linux SDK. SQL statements were used to build the database and execute the web page queries. The web pages were developed by using PHP script language and a little of JAVA script. The model employs a commercial fingerprint reader to capture and enroll the fingerprint features. The reader is Eikon digital privacy manager USB fingerprint reader, UPEK brand. The prototype is performed on two different personal computers with different specification. The server is hosted on a desktop PC with the following specification: Intel Core 2 Duo CPU, 2.66GHz processor.

3.5 GB RAM.

1) 500 GB hard disk.

2) Linux, Ubuntu 9.04 environment.

For user, a notebook PC with the following specification is used:

1) Pentium dual-core CPU, 1.6 GHz processor.
2) 2 GB RAM.
3) 120 GB hard disk.
4) Linux, Ubuntu 9.04 environment.

Model testing

A real time implementation is done for the proposed model. The implementation is done within two local networks which are connected through a router device. The server is hosted on a desktop personal computer running Apache server and it is located on the first network. The user uses a notebook personal computer and it is located on the second network. Both computers are connected to the router by wire. The real time implementation is divided into two parts. The first part is implemented with correct data and valid fingerprint features. This part is implemented to check the ability of the proposed model to verify the CC information and examine the fingerprint matching process. In the second part, deliberate mistakes were done through the purchasing process to check the proposed model ability of detecting the errors and examining the error pages. Throughout the two parts, the server computer is turned on and the server is ready to receive any request from the user. The user starts the model with requesting the IAM's home page, assuming that the user is directed from the merchant web page to complete the payment process.

Correct data

This experiment is started by loading the home page on the user's web browser. The page shows the empty fields in addition to the generated FP-TAC and requests the user to submit the CC information and attach the BAC file. User starts to fill in the CC information as it appears on the CC and chooses the finger that will be scanned later Figure 4. After entering the information, the user turns to capturing program and runs the application. The program starts with requesting the FP-TAC and then, the user starts to enter the code that appears on the Home page. Then, the user scans his finger upon the program request and waits for the scanning status. After approving the scan process, the BAC file with fingerprint features and FP-TAC is stored on user's computer and

Figure 4. Home page with correct CC information.

ready to be sent Figure 5. Now the user turns back to the Home page and attaches the BAC file. At this point, the user is ready to click the submit button and wait for the transaction status. Since all the CC information is correct and the fingerprint features is valid, the model approves the transaction and directs the user to 'transaction status' page. Now the user is allowed to quit the capturing program. By this action, the program removes the BAC file permanently and terminates itself. The model shows a reliable performance and a very fast response during the experiment (Figure 6).

False data

This part consists of several experiments since there are several error scenarios. The errors are categorized under four categories: file upload error, CC information error, FP-TAC error and fingerprint features matching error. The four following cases examine the model ability of detecting and handling the various errors:

File upload's error experiment (case one)

In this experiment, the user makes a mistake on purpose Concerning the file uploading. First mistake, the user

uploads a file exceeding the size limits. The model checks the file size and notices an error concerning its size. The model stops processing the data and directs the user to uploading error page (Figure 7). The second mistake is done by the user is submitting the CC information without attaching the BAC file. The model also notices the error and directs the user to uploading error page.

CC information's error experiment (case two)

There are several error scenarios applicable for this experiment. Any mistake with any of the submitted CC information can cause an error. The user in this experiment makes a mistake with the expiry date and submits the data. The model checks the CC information and notices an error with the expiry date. The model stops the processing process and directs the user to the information error page. This experiment is repeated several times; in each experiment a different mistake is taken (Figure 8). The model shows a good result in identifying the error and handling it.

FP-TAC's error experiment (case three)
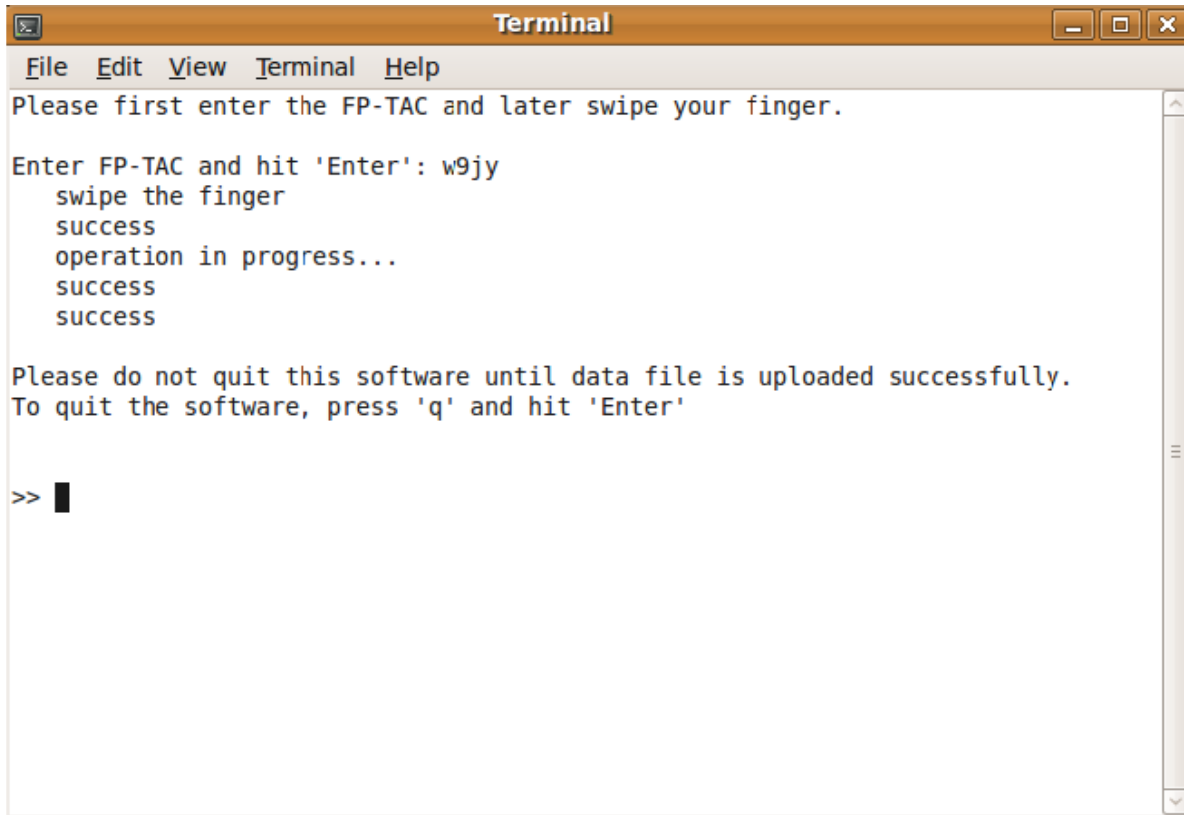
This error happens when the user submits a BAC file with

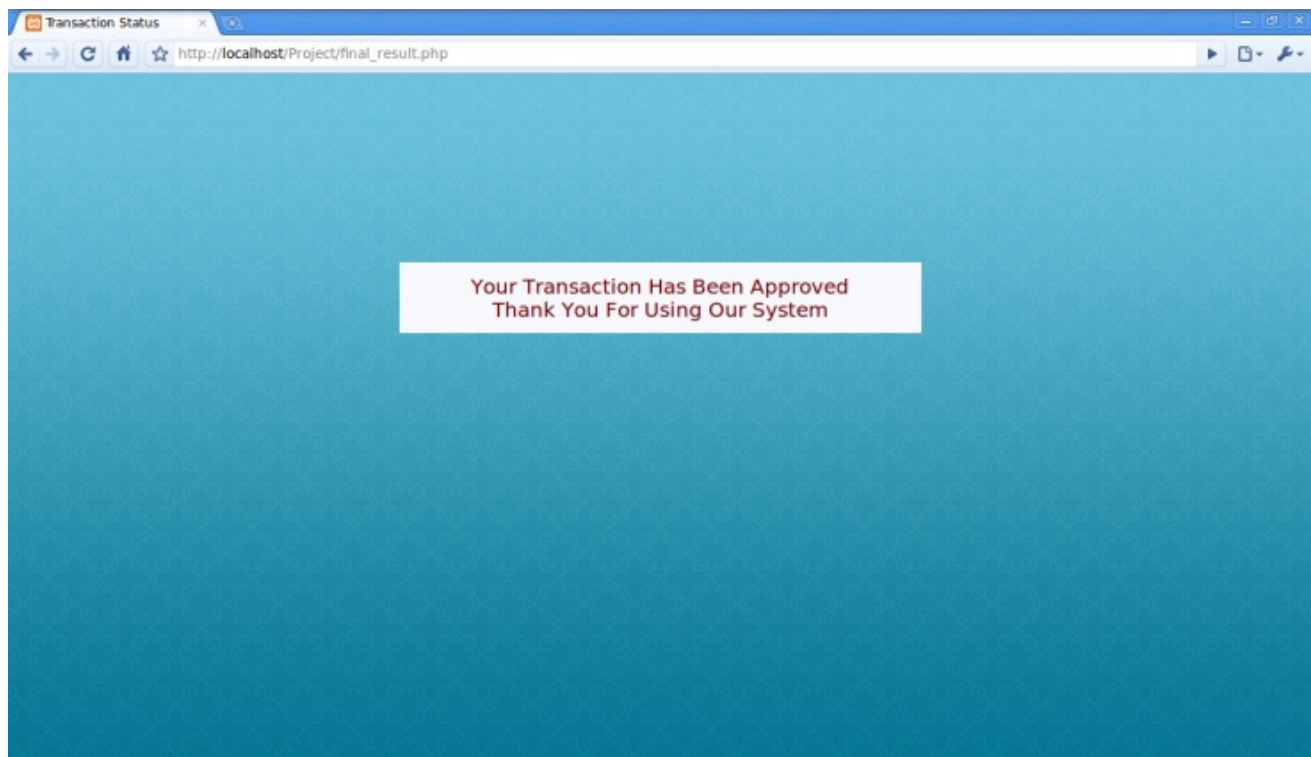**Figure 5.** User enters the right FP-TAC and scans the correct finger.
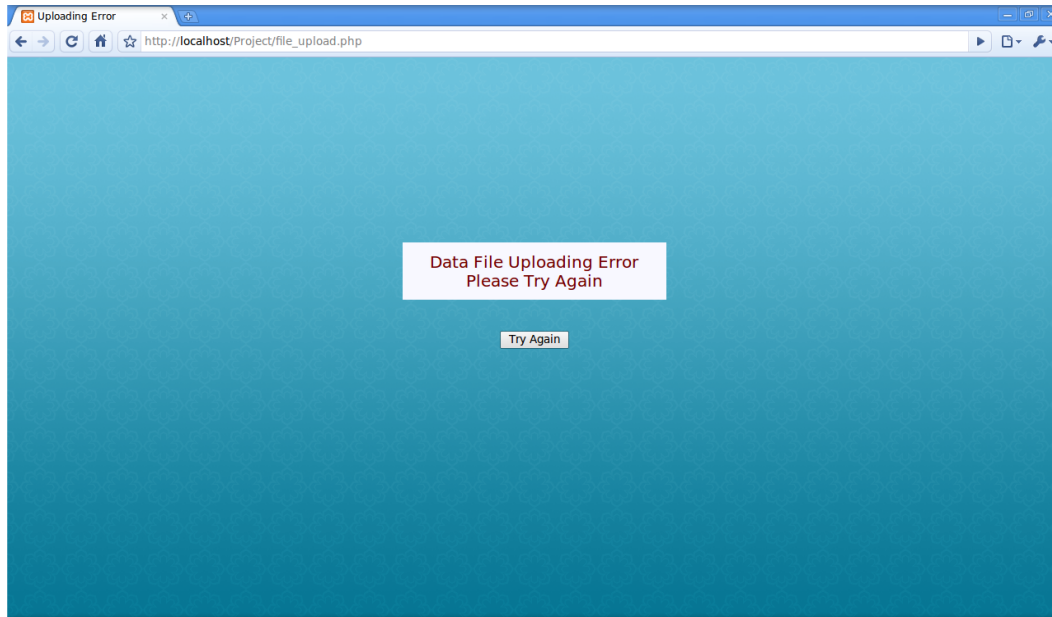

Figure 6. Model approves the transaction.
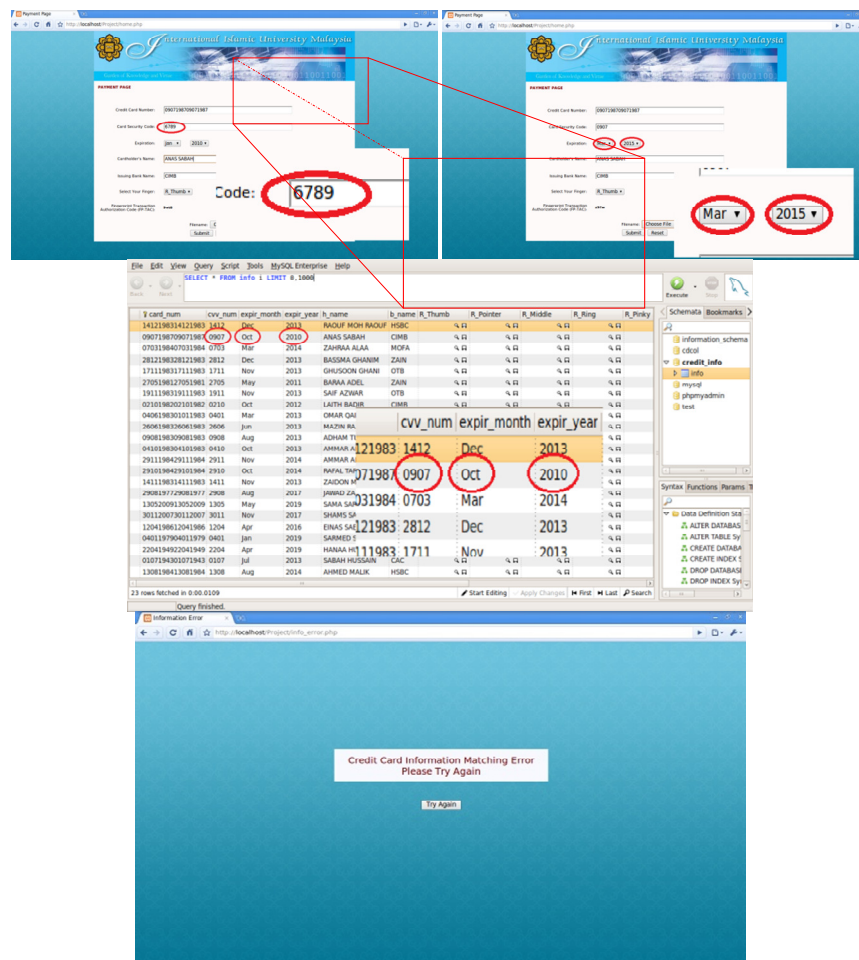
Figure 7. Uploading error page.
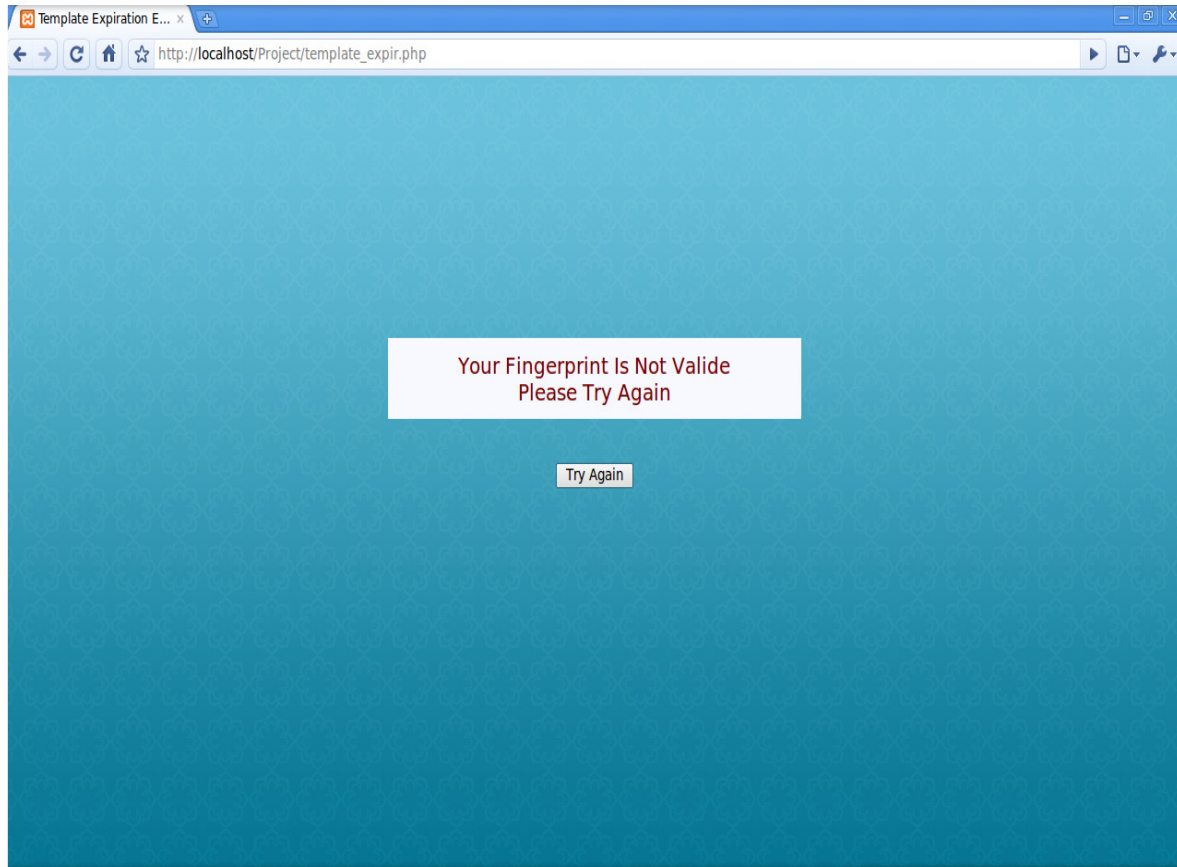

Figure 8. Information error scenarios.

Figure 9. Features expiration error page.

either wrong or old FP-TAC. Also, it happens when the user submits an old BAC file. In this experiment, the user makes a mistake by entering a different FP-TAC than the one that appears on the 'home page'. The model matches the received and generated FP-TAC and notices the error. The model leaves the 'processing page' and directs the user to features 'expiration error page' (Figure 9). The experiment is repeated by submitting an old BAC file and then the model responses by detecting the error and directing the user to the error page. The model shows a reliable performance in identifying and detecting the error.

Fingerprint matching's error experiment (case four)

Throughout this experiment, two scenarios were tested. In the first scenario, the user scans a different finger than what he selects in the home page. The other scenario is that unauthorized user scans his finger and claiming the identity of an authorized user. At both scenarios, the matching program detects the fingerprint features error and notifies the processing page. The processing page stops the matching process and directs the user to the 'fingerprint matching error page' (Figure 10). The IAM shows a very good result in detecting the false and faked

fingerprint features.

RESULT ANALYSIS

In the following, we will go through the result acquired from the two implementation parts: correct data with valid fingerprint and false data with invalid fingerprint. In addition, a demonstration of the model's processing time and each part of it is presented.

Correct data results

The database file consists of twenty five records for candidates who volunteered to participate in model evaluation. Each candidate tests the model by submitting the correct CC information and a valid BAC file with correct right selection of the scanned finger and valid FP-TAC as shown in Table 1. This process is repeated ten times for each candidate to examine the ten fingerprints. The total testing number for the model with correct CC information and valid BAC file was 250 times with 248 successful and 2 failures. The two failures were due to connection errors between client and server. The
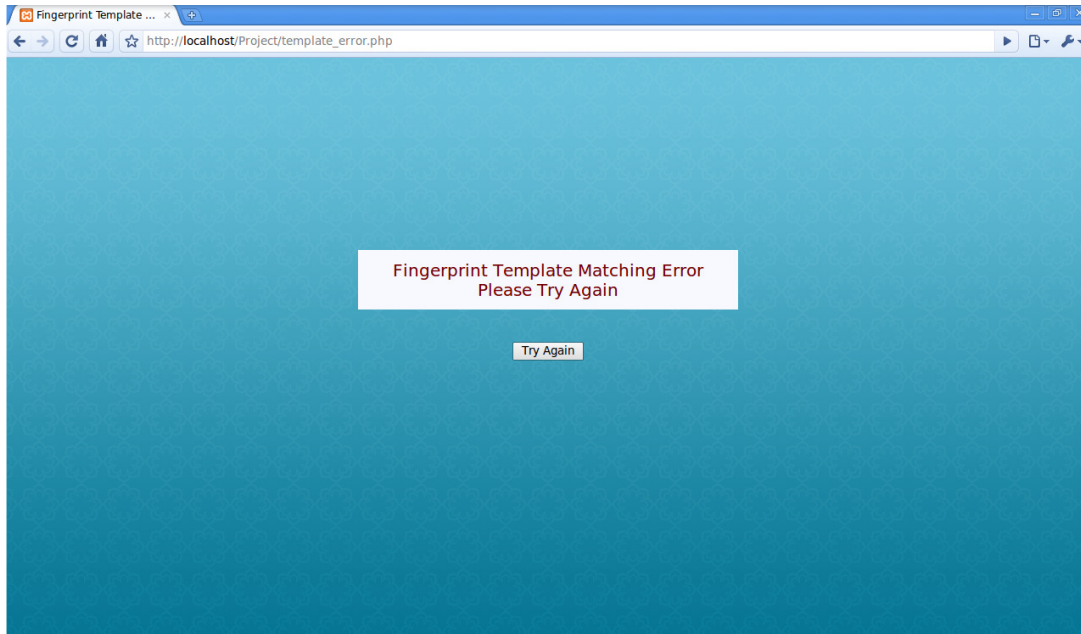
Figure 10. Fingerprint matching error.

Table 1. Model results with correct data.

Total testing attempts	Success	Failure	Accuracy rate	Error rate
250	248	2	99.2%	0.8%

Table 2. File upload's error results.

Error type	Attempts	Success	Failure	Accuracy rate	Error rate
Size > 500 bytes	20	20	0	100%	0%
No uploaded file	20	20	0	100%	0%

accuracy rate for the model was 99.2% while the error rate was 0.8%. The FRR for the fingerprint matching program is less than 0.1% when the FAR is 0.01%.

False data results

This part is divided into four sections based on the expected error scenarios:

File upload's error experiment results

This experiment were tested 40 times, 20 times for uploading file with a size exceeding the 500 bytes and other 20 for submitting the CC information without uploading any BAC file. During all the experiments, the model was able to detect the errors efficiently. The

accuracy rate was 100% while the error rate was zero as shown in Table 2.

CC information's error experiment results

This experiment was repeated 100 times to examine the model ability of detecting the errors with the CC information. First we chose to make a deliberate mistake with single information and test the model 10 times. Since we have six information representing the CC information, the experiment was repeated 60 times. The model was successfully able to detect the errors and give a 100% accuracy rate and 0 error rate as shown in Table 3. Next, we started to test the model by making double mistakes with two selected information and repeated 10 times. The selected information were: CC's number with 'card security code', 'expiry month with expiry year' and 'card

Table 3. Information's error results.

Error type	Attempts number	Successful	Failure	Accuracy rate (%)	Error rate (%)
CC number	10	10	0		
Card security code	10	10	0		
Expiry month	10	10	0	100	0
Expiry year	10	10	0		
Holder's name	10	10	0		
Bank's name	10	10	0		
CC # & CSC	10	10	0		
Expiry month and year	10	10	0	96.6	3.4
Holder' name and bank's name	10	9	1		
All Info	10	10	0	100	0
Total	100	99	1	99	1

Table 4. FP-TAC's error results.

Testing attempts	Success	Failure	Accuracy rate (%)	Error rate (%)
20	20	0	100	0

holder's name' with 'bank's name'. The model was tested 30 times and scored 29 successful attempts and 1 failure. The accuracy rate was 96.6% while the error rate was 3.3%. Finally, the model was tested by setting all the information wrongly and repeated 10 times. The model was efficiently able to notice the errors and gave a 100% accuracy rate and 0 errors rate. The overall evaluation is 99% accuracy rate with 1% errors rate. The total repeating number for this experiment was 100 with 99 successful and 1 failure, the failure was due to a connection error between the client and server.

FP-TAC's error experiment results

This experiment was tested by sending a BAC file with different FP-TAC than that generated on the home page and correct fingerprint features. This experiment was repeated 20 times with different candidates. The model was able to validate the BAC file and detect the false FP-TAC. The accuracy rate was 100% while the error rate was 0% as shown in Table 4.

Fingerprint matching's error experiment results

In this experiment, each candidate tested the model 10 times. The candidate tested the model by submitting his correct CC information and different fingerprint. Five of the ten attempts were by submitting a different fingerprint than that selected during the purchasing process for the same candidate. For instance, the candidate selects the right hand thumb and submits the right hand pointer. The other five were performed by submitting a fingerprint for a different candidate than the one whom performed the purchasing process. The experiment was repeated 250 times since the number of candidate is 25. The model detected the false fingerprints and scored 250 successful errors detection out of 250. The accuracy rate was 100% and the error rate was 0% while the FRR for the matching program was 0.1% when the FAR was 0.01% as shown in Table 5.

Processing time

The processing time of all fingerprint programs and web pages of the model were measured throughout the experiments. The average processing time for the capturing program is 1.83 s. The capturing program consists of two parts. The first part is the average time for processing the fingerprint image and produces the fingerprint features. The second part is the average time for creating a BAC file and storing the FP-TAC and fingerprint features inside it. The first part is taking 0.71 s while the second part takes 1.12 s in average. The enrollment program has the same parts as the capturing program excepting that the first part is repeated three

Table 5. Fingerprint matching's error result.

Error type	Attempts	Success	Failure	Accuracy rate (%)	Error rate (%)
Same candidate, different finger	125	125	0	100	0
Different candidate	125	125	0	100	0
Total	250	250	0	100	100

Table 6. A subjective benchmark table.

Author	Year	Technology used	Time	Cost	Error rate	Acceptability
Ihmaidi et al.	2006	Biometric-Fingerprint	High	medium	N/A	Medium
Kim andChang	2006	Biometric-Fingerprint	Medium	High	N/A	Medium
Vankataramani and Gopalan	2007	RFID Cards	N/A	High	N/A	Medium
Lu et al.	2007	Biometric-Iris	Medium	N/A	N/A	Low
Trevathan et al.	2009	Biometric-Handwritten Signature	High	N/A	2.1%	Medium
Yildiz and Gokturk	2010	Biometric	N/A	High	N/A	Low
IAM	2010	Biometric-Fingerprint	Low	Low	0.52%	Medium

times and the second part stores only the fingerprint features without the FP-TAC. The average time for the enrollment program is 3.32 s. The first part takes 2.21 s while the second part takes 1.11 s on average. The average time for the processing page to take decision is 2.47 s including the matching program processing time. The matching program takes 0.87 s while the processing page takes 1.6 s to connect to database and match all the data. The test done in a local network, a further test using internet recommendation and it would be more appreciated.

RESULT DISCUSSION

From the model testing, matching program exhibits a great performance in matching the fingerprint features rapidly and reliably. Throughout all the experiment, the matching program score 100% accuracy rate and 0% error rate in terms of verifying the correct features and detecting the false ones. The average processing time for the matching program gave the desired result and scored 0.87 s to match the features and pass the result. The model accuracy rate for the correct data case was 99.2% while the error rate was 0.8%. In addition, the overall accuracy rate for the false data case was 99.75% with 0.25% error rate. In both cases, the errors were due to connection error between the router and client computer, in other words, the errors is caused by transmission link and not by IAM's verification elements. The average time for processing and matching the entire data was 2.47 s, which means that our target of keeping the processing time as low as possible is achieved. The overall evaluation for IAM gave a 99.48% accuracy rate and 0.52% error rate. Table 6 is illustrating a comparison to

benchmark the IAM with some related work since the papers did not provide too much data.

CONCLUSION

Credit card security is based on the physical security of a plastic card and the privacy of the credit card number. Hence, security is potentially compromised whenever a person other than the cardholder has access to the card or its number. Current authentication system for online purchasing using credit card is based on information located on the credit card. That information provides a certain level of security but not a high level as it is needed for this type of online money transaction. Also, that information is vulnerable to loss and theft. In this paper, an integrated authentication model for credit card online purchasing (IAM) is proposed. This model is proposed to improve the security of the online purchasing system and it is based on fingerprint authentication technique. In this model, computer programs are developed to perform the capturing, enrolling and matching of fingerprint features. Also, a group of web pages and database are created to handle the online data matching and verification. The overall performance evaluation for the prototype shows a good overcomes that encouraged to continue investigation in this field.

REFRENCES

Abomhara M, Khalifa OO, Zakaria O, Zaidan AA, Zaidan BB, Alanazi HO (2010a). Suitability of Using Symmetric Key to Secure Multimedia Data: An Overview. J. Appl. Sci., 10(15): 1656-1661.
Abomhara M, Khalifa OO, Zakaria O, Zaidan AA, Zaidan BB, Rame A (2010b). Video Compression Techniques: An Overview. J. Appl. Sci., 10(16): 1812-5654.
Ahmed MA, Kiah MLM, Zaidan BB, Zaidan AA (2010). A Novel

Embedding Method to Increase Capacity and Robustness of Low-bit Encoding Audio Steganography Technique Using Noise Gate Software Logic Algorithm, J. Appl. Sci., 10(1): 59-64.

Alam GM, Kiah MLM, Zaidan BB, Zaidan AA , Alanazi HO (2010). Using the features of mosaic image and AES cryptosystem to implement an extremely high rate and high secure data hidden: Analytical study, Sci. Res. Essays. 5(21): 3254-3260.

Alanazi HO, Jalab HA, Alam GM, Zaidan BB, Zaidan AA (2010a). Securing electronic medical records transmissions over unsecured communications: An overview for better medical governance. J. Med. Plants Res., 4(19): 2059-2074 .

Alanizi HO, Kiah MLM, Zaidan BB, Zaidan AA, Alam GM (2010b). Secure topology for electronic medical record transmissions, Int. J. Pharmacol., 6 (6): 954-958.

Al-Frajat AK, Jalab HA, Kasirun ZM, Zaidan AA, Zaidan BB (2010). Hiding Data in Video File: An Overview, J. Appl. Sci., 10(15): 1644-1649.

Bella G, Massacci F, Paulson LC (2003). Verifying the SET registration protocols. IEEE J. Sel. Areas Commun., 21: 77-87.

Blackwell C (2008). The management of online credit card data using the Payment Card Industry Data Security Standard, Proceedings of the 3rd International Conference on Digital Information Management,Nov. 13-16, London, United Kingdom, pp. 1-13.

Bo M, Qianxing X (2004). SOCPT: a secure online card payment protocol, Proceedings The 8th International Conference on Computer Supported Cooperative Work in Design, 2004, 2: 679-684.

Hannan X, Christianson B, Ying Z (2008). A Purchase Protocol with Live Cardholder Authentication for Online Credit Card Payment, Fourth International Conference on Information Assurance and Security, 2008. ISIAS '08, IEEE Computer Society Washington, DC, USA, Pp. 15-20.

Hmood AK, Jalab HA, Kasirun ZM, Zaidan AA, Zaidan BB (2010a). On the Capacity and Security of Steganography Approaches: An Overview., J. Appl. Sci. 10(16): 1825-1833.

Hmood AK, Jalab HA, Kasirun ZM, Zaidan AA, Zaidan BB (2010b). On the accuracy of hiding information metrics: Counterfeit protection for education and important certificates", Int. J. Phys. Sci. 5(7): 1054-1062.

Hmood AK, Zaidan BB, Zaidan AA, Jalab HA (2010c). An overview on hiding information technique in images. J. Appl. Sci., 10(18): 2094-2100.

Ihmaidi HUDA, Al-Jaber A, Hudaib (2006). A Securing Online Shopping using Biometric Personal Authentication and Steganography, International conference on Information and Communication Technologies, 2006. ICTTA '06. 2nd, pp. 233-238.

Kumar D, Yeonseung R, Dongseop K (2008). A survey on biometric fingerprints: The cardless payment system, International Symposium on Biometrics and Security Technologies. ISBAST 2008. pp. 1-6.

Medani A, Gani A, Zakaria O, Zaidan AA, Zaidan BB (2011). Review of Mobile SMS Security Issues and Techniques towards the Solution, Sci. Res. Essays, 6(6): 1147-1165.

Nabi MSA, Kiah MLM, Zaidan BB, Zaidan AA, Alam GM (2010). Suitability of Using SOAP Protocol to Secure Electronic Medical Record Databases Transmission, Int. J. Pharmacol., 6 (6): 959-964.

Naji AW, Zaidan AA, Zaidan BB (2009). Challenges of Hidden Data in the Unused Area Two within Executable Files. J. Comput. Sci., 5 (11): 890-897.

Raghuwanshi S, Pateria RK, Singh RP (2009). A new protocol model for verification of payment order information integrity in online E payment system, World Congress on Nature & Biologically Inspired Computing, 2009. NaBIC 2009, pp. 1665-1668.

Sahut JM (2008). Security and Adoption of Internet Payment, Second International Conference on Emerging Security Information Systems and Technologies, 2008. SECURWARE '08. pp. 218-223.

Sameer HAI, Mat Kiah ML, Zaidan AA, Zaidan BB, Alam GM (2011). Securing Peer-to-Peer Mobile Communications Using Public Key Cryptography': New security strategy, Int. J. Phys. Sci., 6(4): 930-938.

Shihab AH, Zaidan BB, Zaidan AA, Naji AW, Omar F (2010). Accurate Method to Measure Three Dimensional Skull Bio-Metric, J. Appl. Sci., 10 (2):145-150.

Trevathan J, McCabe A, Read W (2009). Online Payments Using Handwritten Signature Verification, Sixth International Conference on Information Technology: New Generations, 2009. ITNG '09, pp. 901-907.

Woong-Sik K, Byung-Ik K, Yun-Seung C (2006). An Credit Card Verification System by Biometric Method, Proceedings of the 9th International Conference on the Control, Automation, Robotics and Vision, ICARCV '06. Dec. 5-8, Singapore, 10.1109/ICARCV. Pp. 1 – 4.

Yan WNY, Chiu DKW (2007). Enhancing E-Commerce Processes with Alerts and Web Services: A Case Study on Online Credit Card Payment Notification, International Conference on Machine Learning and Cybernetics, 2007, 10.1109/ICMLC.2007. pp. 3831-3837.

Yingjiu L, Xinwen Z (2004). A security-enhanced one-time payment scheme for credit card, Proceedings 14th International Workshop on Research Issues on Data Engineering: Web Services for e-Commerce and e-Government Applications, 2004, pp. 40-47.

Yingjiu XZ, Li Z (2005). Securing credit card transactions with one-time payment scheme. Electronic Commerce Research and Applications 4: 413-426.

Zaidan AA, Zaidan BB, Al-Fraja AK, Jalab HA (2010a). Investigate the Capability of Applying Hidden Data in Text File: An Overview, J. Appl. Sci., 10(17): 1916-1922.

Zaidan AA, Zaidan BB, Al-Frajat AK, Jalab HA (2010b). An overview: Theoretical and mathematical perspectives for advance encryption standard/rijndael. J. Appl. Sci., 10(18): 2161-2167.

Zaidan AA, Zaidan BB, Alanazi HO, Gani A, Zakaria O, Alam GM (2010c). Novel approach for high (secure and rate) data hidden within triplex space for executable file, Sci. Res. Essays, 5(15):1965–1977.

Zaidan AA, Zaidan BB, Taqa AY, Mustafa KMS, Alam GM, Jalab HA (2010d). Novel multi-cover steganography using remote sensing image and general recursion neural cryptosystem, Int. J. Phys. Sci. 5(21): 3254-3260.

Zaidan BB, Zaidan AA, Al-Frajat AK, Jalab HA (2010e). On the Differences between Hiding Information and Cryptography Techniques: An Overview, J. Appl. Sci., 10(15): 1650-1655.

Zaidan BB, Zaidan AA, Taqa A, Alam GM, Kiah MLM, Jalab HA (2010f). StegoMos: A secure novel approach of high rate data hidden using mosaic image and ANN-BMP cryptosystem, Int. J. Phys. Sci. 5(11): 1796-1806.

Zaidan BB, Zaidan AA, Mat Kiah ML (2011). Impact of Data Privacy and Confidentiality on Developing Telemedicine Applications: Review, Participates Opinion and Expert Concerns, Int. J. Pharmacol., 7(3): 382-387.