Credit Card Fraud and Identity Theft: A Case Study in Malaysia

Rozita Ahammad, Jeyraj Maran, AuliaSyahirah, Fadhil Ahmad, Kazim Raza Talpur, Suraya Yaacob*, Nilam Nur binti Amir Sjarif
Advanced Informatics School, Universiti Teknologi Malaysia
rozita.ahammad@gmail.com, dtgunited@gmail.com, aulia.syahirah93@gmail.com, fadhil.ahmad2323@gmail.com, suraya.yaacob@utm.my, nilamnur@utm.my,

Abstract
Credit card industry is one of the major components of financial institutions in Malaysia. The crimes related to credit card and identity theft of late is increasing drastically. Credit card theft varies in terms of techniques and methods used and it’s crucially important to review and improvise the existing prevention method to reduce the number of crimes related to credit card and identity theft. This study also aims to analyze the recent studies and their findings regarding credit card and identity theft. This article contains information about credit card and identity theft, impact of TN50 implementation and also other fraud prevention methods being practiced internationally. There are plenty of methods being practiced to prevent credit card related frauds which is issue specific and it needs appropriate availability of technology to implement it. The methods that are discussed and considered in this article will definitely play a vital role in terms of cost savings and time efficiency.

Keywords: credit card fraud, identity theft, identity fraud, biometric credit card, TN50

1. Introduction
Credit card fraud is where unfamiliar individuals have in their possession victims credit card number illegally by way of, stolen credit cards, phishing method through emails, or skimming method where attackers use a machine that duplicates the data from the original card to make another illegal copy of the card [1]. Identity theft is having access or misusing someone’s personal information for their personal gain [2]. Most commonly, a person’s date of birth are being used by attackers to commit financial fraud. Most of the attacker’s motive in doing such criminal acts is for their personal financial gain. These kinds of frauds can also happen in order to destroy one’s financial institution reputation or specific individual by respective competitors. Credit card and identity theft might start through phishing method when individual and/or institutions least expected. Phishing is a crime which happens when attackers send deceptive e-mails to prospective victims. Attacker’s main motive through phishing activity is to deceive victim to reveal his/her personal information without them realizing about the fatal consequences. The emails and messages sent would look as genuine as a bank or any authorized party valid transactions and that’s where the victim falls prey to. Phishing has become a favorite method for criminals as it is easy to trick the victim without much effort. It is difficult for victims
to differentiate either the email message is genuine or not as the bank logo and website link that perpetrators use looks very similar at first glance as against the original bank message [2].

According to [3], since 2011 total amount of credit card transactions in Malaysia were reported at RM320 million and the amount increased to RM360 million in 2015. From January to September 2017, 262 of identity theft cases have already been reported to CyberSecurity Malaysia [4]. Hence, it is critically important to mitigate the risk of credit card and identity theft fraud to reduce the crime rate in Malaysia. This paper proposes biometric solution as more viable enhancement to existing credit cards verification methods. Biometrics is very unique and it mostly impossible for someone to provide fake identification through biometrics. We have to implement biometrics solution immediately in order to overcome this issue.

2. Background

There are cases reported in Malaysia under credit card frauds and identity theft which created increasing awareness among citizens. A 44 year old IT Manager became a victim of identity fraud when fraudster used his Identity Card to apply six telephone lines and broadband service in 2016. He received an overdue bills from different telco, citing outstanding broadband and phone bills amounting to RM1,420. Another case is a 62 year old man from Gurun, Kedah was one of the victim who suffered a big loss which adds up to RM95,000. He received a call from a bank representative saying that he owes the bank a particular sum for his credit card payment and urged to make immediate payment. The victim then transferred the stated amount to the account number provided by the fake bank representative and later he found out that he had been cheated [5]. The same incident also happened to Foo Soon Wah whereby he has been instructed by fake officers from Bank Negara Malaysia to transfer a sum of RM4999.11 for his credit card usage in Johor. He denied that he owns the credit card but the officer gave him a fake Bank Negara number to contact for further enquiries. Foo transferred the amount without investigating further and he found out later that it was a scam [5].

There is existing collaboration by Malaysian government agencies and authorities to reduce identity theft and credit card fraud. For instance, in 1986, The Central Bank of Malaysia created the Special Investigations Unit (SIU) to control and analyze unauthorized financial transactions. Relevant information collected from witnesses have enable this Unit to conducts search and seizure operations towards successful prosecution against perpetrators. Serious action will be taken to the offenders’ wrongdoing after thorough investigation and successful prosecution. The bank collaborates with various enforcement agencies such as The Royal Malaysia Police, Securities Commission Malaysia, The Royal Customs of Malaysia, Malaysian Anti-Corruption Commission, Cooperatives Commission of Malaysia, Ministry of Domestic Trade, Cybersecurity Malaysia and Co-operatives and Consumerism. This collaboration proved to be one of the current productive actions taken by government to reduce identity theft and credit card fraud [6].
Figure 1: TN50 initiatives and contributing factors

Figure 1 shows the TN50 initiative, key drivers and contributing factors to our proposal. The solution that we have proposed which is a biometrics solution to mitigate credit card fraud and identity theft is very much relatable to the components of TN50. According to [7] TN50 is a government initiative to plan for the future of Malaysia from the 2020 till 2050. The components identified which relates to biometrics solutions for credit card transactions are big data analytics, cloud computing, cyber threats and also the government policy.
According to [8], big data analytics is the method of processing large and wide-ranging data sets which is commonly said as big data. It helps to discover hidden patterns, unknown correlations and also provide other information to increase productivity and efficiency in an organization. There will be millions of data sets created when we implement biometrics solution for credit card verification and all the data generated should be managed prudently to avoid the misuse of biometrics data by the data brokers.

As per discussed in [9], cloud computing is the technique of storing data over the server storage which is hosted on the internet compared to the traditional method of storing in a local server or a computer. A web-based user interface like web browser and mobile application are being used by cloud-based services to get accessed through. The biometric templates database and all other information gathered for cloud users are stored in a cloud server. Even though biometrics are unique, problems might arise and attackers have access to stored biometrics templates database.

Malaysian Government should enhance existing policies like ‘National Telecommunication Policy’ and also ‘Malaysian Public Sector ICT Strategic Plan’ [7] to embrace biometrics approach. Both of these policies should include biometrics solutions components as it would be one of the safest and genuine verification methods. Introducing the implementation of biometrics through these government policies will leave deep and meaningful impact for a larger society. People will be more aware of the changes and how biometrics solution works through government initiatives of awareness programs and advertisements.

3. Research Methodology

The objective of this research is to identify types of credit card fraud and identity theft and its’ impact to Malaysian card users together with the propose mitigation solutions. Some research questions have been formulated to collect information for instance “What is identity theft and credit card fraud?” , “What are current implementation by Malaysian agencies and authorities to prevent credit card fraud and identity?”, “What is the Malaysian Government future plan to mitigate the crimes?” and ”How informatics roles can prevent credit card and identity theft?”. Electronic journal databases such as IEEE Explorer, Scopus, Science Direct and World of Science are the main source for gathering general information. References such as websites, newspaper, and published report are the additional mediums use for collecting latest and up-to-date associated data. These processes are done by combining search strings used i.e. “credit card fraud”, “identity theft”, “cyber fraud awareness”, “biometric credit card”, “cyber law”, ”Transformasi Nasional 2050”, “implementation”, and “issues” with Boolean “OR” and “AND” applied to the title, keywords and abstract of publications from 2010 to 2018.

4. Informatic Roles

Informatic plays a dominant role in computational, cognitive and social aspects of everyday activities especially in current modern technological era where life, culture and technology collide. In this paper we specifically focus on four (4) informatic roles in combating credit card fraud and identity theft crimes.
4.1 Fingerprint verification for credit card transaction

Biometric traits contain essential features that are widely used in application that needs a person identification and verification. There are several biometric traits such as face, palm, retina, and iris recognition but fingerprint image is found to be the most reliable due to its uniqueness and it is also universal as everybody holds it and time-invariant throughout a person’s lifetime [10]. Biometrics authentication linked to credit card payment method makes pin number or security code no longer needed and as such will increase security, convenience and confident level among users [11]. It is reported by [12], Mastercard and Visa as the world’s two biggest card companies (with 500 million card holders for MasterCard alone) have launched biometric authentication for their major payment projects. Mastercard will provide remote transactions and contactless transactions that use biometric authentication as additional measures to existing PIN and password verification via mobile device. Apart from that, Visa with over 320 million users is running Visa Ready for Biometrics pilot project in Bank of Cyprus, and Mountain America Credit Union in the United States for fingerprint authentication contact and contactless payments. Taking into consideration of advantages derived from those initiatives, Malaysian Government and Financial Institution should welcome and embrace this technology and ensure that it is in their execution plan soonest possible once the technology start to embark in Asian Region. Figure 2 shows the flow chart of proposed fingerprint verification for credit card transaction authentication to prevent credit card fraud and identity theft.

![Flow chart of fingerprint verification for credit card transaction authentication](image)

**Figure 2:** Flow chart of fingerprint verification for credit card transaction authentication

Firstly, card holder will insert credit card into a card reader and place the enrolled fingertip on the fingerprint sensor of the card. Fingerprint sensor captures the digital image of the card holder’s fingerprint and compared with reference template earlier stored on the card to verify the
genuine user. If the matching calculation for both captured and stored image is successful, the verification process will be authenticated and the transaction will be accepted by the bank. To avoid from identity theft, new credit card user will need to enroll their fingerprints within the credit card issuer premises together with the inspection of the user’s original Identity Card.

4.1.1 Advantages of Biometrics authentication for credit card

According to [13], there are some advantages of using biometric for authentication such as:

i. Effective in fraud reduction as existing approaches like username, password and PIN can be acquired through observation, either manual or via electronic devices such as CCTV.

ii. More accurate and reliable

iii. User no longer need to remember password and PIN

iv. Less problem in impersonation of identity

Adapted from [13], other advantage of biometric authentication are listed as per table 1.

<table>
<thead>
<tr>
<th>Method</th>
<th>Examples</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Something unique about the user</td>
<td>Fingerprint, Face, Iris, Voice print</td>
<td>Not possible to share, Repudiation unlikely, Forging difficult, Cannot be lost or stolen</td>
</tr>
</tbody>
</table>

4.1.2 Fingerprint as credit card biometric traits

Among all biometric traits, it is much cost economical and more prudent for the card issuer to go with fingerprint biometrics as initial phase of credit card fraud prevention. According to [14], fingerprint feature are divided into three levels. Level 1 showing the macro level details such as ridge flow, level 2 describes minutiae point which have sufficient differentiating attributes for recognition and level 3 gives fingerprint pore both quantitative and qualitative examination that’s complement level 2 uniqueness features.

i. Minutia Based Technique

Minutia method is the most popular method of choice for fingerprint or biometric system execution because it more reliable and efficient technique for matching an authentication of users fingerprint to the system. Many of fingerprint scanning technology depend on minutia; this method is the backbone of current available fingerprint products. Minutia techniques compare unique fingerprint impression given by users against respective stored databases. [14]. This technique represents the local feature of fingerprint (termination sand bifurcation).
ii. Pattern Based
This method is also known as Ridge Feature Based Techniques. The advantage of Pattern Based techniques as compared to Minutia Extraction, is that minutia may be compromised. On the other hand Pattern Based technique is very sensitive and it uses the finger on the point or placement and is very storage-hungry. Basically, Pattern Based technique analyze the user impression by fingerprint patterns such as whorl, arch and loop in comparison to previously stored information in database [14].

iii. Imaged Based
In image-based technique, the fingerprint image used same reference and each points of image will compare user input fingerprint impression points collected by respective devices to image stored in database system. Image based technique works on whole full impression of finger image for matching and verifies it with database system together with user fingerprint impression [14]

iv. Correlation Based
The correlation-based technique for authentication system is efficient in dealing with low-quality of image. However, notable main drawbacks are this method is less capable in real time and reference matching method demands high-computational effort. This correlation-based fingerprint techniques is occasionally accepted on a few grounds such as non-straight twist, skin-condition and shine clear finger impression albeit this particular matching approach is highly costly [14]
4.2 Cashless payment method with biometric solution

Cashless payment method brings multiple benefits to many sectors such as Government, business owners and also customers [15]. Before the execution of cashless payment is enforced, it is vital to ensure that all data and transactions are secured and safe for the users to proceed to the next steps. The best solution for the issue is introducing biometric technology as it is one of the most effective technologies to help solve security breaches by providing convenient and effective payment transactions. Examples of cashless payment methods are Paypal, Aadhar enabled payment system, mobile wallets and UPI applications [16].

4.2.1 Benefits of cashless Economy

i. Illegally earned money or ‘black money’ is classified into a category when someone intentionally hides their income to prevent them from paying tax to the government. It is very much possible to track someone’s cash flow through cashless transaction where every expenditure has to be accounted for. All transactions will then be transparent and it will help in overcoming corruption in a full cashless transactions’ cycle [16].

ii. There will definitely be an increase in government’s revenue through tax incomes since there is no other way to hide illegally earned money other than going through established financial institutions where they store all records. The revenue through tax can be optimally used for the betterment of nation’s economy [16].

iii. There are many channels offering discounts for cashless payment such as PLUS, Lazada and Tesco. This makes it easy for both merchant and also customer whereby they don’t have to worry about giving the remaining change and they can pay the exact amount without much hassle [16].

4.2.2 Implementation of Biometrics in Cashless transactions.

Biometrics will play a vital role in the cashless transactions to prevent any fraudulent events to materialize. Biometrics is unique for every human being and it is almost impossible to fake someone’s biometrics to pass through the authentication processes. Examples of biometric solutions which can be applied to cashless transactions are fingerprint and retina scanner.

Transaction Authentication Code (TAC) can be replaced with fingerprint verification through the fingerprint sensor installed in the device [17]. Transaction will be more secure and it will also reduce the crime rate related to identity theft. Another traditional method used in shopping malls is authentication through PIN where it is very easy for attackers to guess victim’s pin. This
method can be replaced with retina scan machines where it is highly impossible for fraudulent events to take place.

4.3 Tighten the Policy and Law Enforcement

The advance technologies in internet has created cybercrime problems [18]. Cybercrime can affect people when they are using online transaction resulting in huge amount of money stolen. Internet has become useful things and makes our daily life better. That being said, any great things do come with drawback and it’s the same scenario for internet. There are irresponsible people who use internet as tools to scam others such as identity theft, credit card fraud, hacking and blackmail [19]. As this problem increase from day to day, Malaysian Government has legislated and regulated a few acts of law that can bring cybercrime criminal to justice.


In this paper, we are looking for act that can be used for identity theft, credit card fraud and fingerprint identification. Before we focus on Malaysian Government legislative law regarding cybercrime, it is very helpful to study how develop country such as United State and United Kingdom has legislative and regulate their law on cybercrime. In United State, they have Identity Theft and Assumption Deterrence Act 1998 to tackle identity theft crime which is applied when a person makes possession of any means of identification in order to transfer, possess or use without lawful authority alongside identification documents [21]. In United Kingdom scenario, they have Data Protection Act 1998 that can charge a person guilty when a person has obtained personal data of another illegally. This act is significance of identity theft [21].

It is also stated in [22] that in Malaysia, Penal Code is an act that could be used on identity theft to a certain extent. Specifically, it contains provisions on cheating by personation. Even though Penal Code is not cyber specific but it is still legit on one such as provision in Section 416. Cheating by personation here means pretending to be someone that they aren’t, substituting one person for another, pretending to be a person who has already deceased to gain something or to cheat. Section 416 stated whoever cheats by personating can be punished with imprisonment for seven years long, or with fine or both. The cheat definition is under Section 415 and contains two parts which are deceiving any person with the sole or main inducement; i) Deceive a person fraudulently to take any property or to have permission to own any property. ii) Intentionally deceive a person to commit something that they would not do if not deceived and in which actions is likely to cause damage to the person in term of mind, property or reputation or in short ‘cheating’.

In our case study on identity theft, the situation where the perpetrator has stolen and used victim’s identity to transact in activities such as changing phone number ownership, opening new account like bank account, social media account, changing credit card delivery, or induce the victim to reveal his personal information are relevant examples that falls within the definition of
cheating under Section 415 Penal Code. The perpetrator can be charged for an offense of cheating by personation.

Penal Code has explained how criminal can be punished due to identity theft and credit card fraud. Fingerprint identification is our proposed technique to overcome identity theft and credit card fraud. The law that could fortified the reliability of this technique is Personal Data Protection Act 2010. Personal Data Protection Act 2010 (PDPA) is an act to protect Malaysian citizens personal data from being trade, or misconduct on its ownership. However, this act is not applicable to federal or states and the case outside of Malaysia [23]. Personal data is any information of a person that capable of identifying the person and collected by any digital equipment. The particular information discussed here are name, address, IC numbers, phone numbers, email address and even banking details. In fingerprints identification case, PDPA can prevent the digital signature of a person from being trade or transfer without owner permission. A telco company or any bank or credit card provider should protect their customer’s fingerprint detail so that it cannot be manipulated by criminal in any ways.

4.5 Awareness Program to Credit Card User

Governments and business that proactively move towards virtual transactions will increase the risks of data fraud and theft where harmful and obstructive. People using technologies the wrong way to gain their own benefit such as cyber criminals and the identity thieves. Therefore, more and better security infrastructure needs to be enriched simultaneously with other efforts to prevent our data from being compromised. In order to overcome these criminal activities, Malaysian citizen should be well informed with the specific preventive action and spread the awareness programs.

When there are many cases such as multimillion-dollar bank theft, leaked of millions of usernames and passwords over the web, scam unprotected people are some indications leading to lack of proper cyber security that if properly implemented should be able to protect systems, processes or data and will avoid people from being exploited. In Malaysia, the national cyber security specialist agency is under the Ministry of Science, Technology and Innovation (MOSTI) authority control and its responsibility is to accomplish a safe and secure cyberspace environment by minimizing unprotected of ICT systems and networks and at the same time inculcate effective cyber security culture to Malaysians. Most Malaysians doesn’t really have a sound knowledge on how to protect their information from being victim of cybercrime or identity theft. Therefore, the awareness about cyber security needs to spread proactively among Malaysian people [7]

The awareness types are divided into two; self-awareness and public awareness. Self- awareness is holding an obvious recognition of your character, as well as advantages, weaknesses, opinion, faith, enthusiasm, and feeling. Self-Awareness enables somebody to perceive other people, how they think, what their point of view is and how they receive feedback in the moment. Public awareness campaigns (PACs) could be productive elements of an extensive plan to encourage adjustment at the level of the particular person, organization, society, or a group of people living together. A public awareness campaign has been described as an extensive attempt that involve several elements such as messaging, extent of reaching out the most basic level of an activity, mass communication connections, government concern and financial plan to assist in achieve a
particular aim. Usually, a campaign attempt to spread awareness about a main issue and persuading expression to emphasize a good behavior change.

To avoid fraud and identity theft, customer awareness is one of the activities that should be implemented by financial institution. Financial institutions in Malaysia have take respective actions on this particular matters and will continuously make an effort to educate their customers. Consumer awareness should be further measured periodically to decide if additional steps are needed. Management of the bank should implement customer awareness program and evaluate periodically to measure how was its effectiveness by using tracking method of number of customers that report fraudulent attempts to obtain their authentication credentials such as ID or password, the number of clicks on information security links on web sites, the number of statement enclosed or other direct mail communications and also the amount of money losses due to identity theft [24].

In order to detect fraud possibility, the key approach of controlling weakness is requires by examining how the fraudsters manipulate variables that may not work properly. Enforce the policies and standard operating procedures should be implemented by organizations to avoid leak of any information regarding organizational assets, employees personal and detects employees that does not follow the organization’s code and ethics. An organization must stay attached to its specific checks or audits of the entire assets in order to achieve business goals. Every person must understand and have security awareness and concern pertaining to information security including personal data protection [25].

5. Conclusion

In this paper, we have proposed four approaches to prevent credit card fraud and identity theft meant for solution and problem solving consideration for the case study discussed. Our proposal is aligned with TN50 megatrend for rapid urbanization. In 2050, every credit card user should feel secure and confident to do credit card transaction with the implementation of biometric solution. The security of this approach will be enhanced with four techniques of fingerprint recognition and verification as an alternative to other cashless payment method and offer more options to user to do their financial transactions. Since biometric solution for credit card transaction and cashless payment will take some time to be implemented in Malaysia, hence government authorities and private agencies should work closely together to organize awareness and outreach program to keep user aware on their responsibility in eradicating associated crimes and avoid from being victimized. At the same time, Malaysian Law Enforcement Body should revise related policies and Acts to make sure that the criminals of credit card fraud and identity theft will be punished worthy of the value of their wrong doings. We believe that with this problem solving proposal the security of credit card transaction will be enhanced and statistics of identity theft will decline tremendously in coming years.
6. References


[9] G.L. Masala1, P. Ruin2, A. Brunetti1, O. Terzo2, E. Grosso1, Biometric Authentication and Data Security in Cloud Computing, 1 Department of Political Science, Communication, Engineering and Information Technologies, Computer Vision Laboratory, University of Sassari, Sassari, ITALY. 2 IstitutoSuperiore Mario Boella (ISMB), Turin, ITALY.


