Prospect of Implementation of Biometric Verification for Secure Credit Card Transactions

Akash S Rao and Deepak Albert
Department of Electronics and Communication Engineering, PES Institute of Technology, Bangalore South Campus, Karnataka-560 100, India
Email: akash1994@gmail.com

***Abstract*—In the modern day world, majority of transactions are made using credit cards, but the security techniques used for security in credit cards is far outdated and is being broadly misused by fraudsters. Fraud is cumulating into billions of dollars per year hence a new method of security must be brought into place. In this light, biometric verification is the brightest prospect as it is superior and accurate compared to other methods of providing security the reference copies of the finger prints can be stored on the card itself. This method is practical, reliable and feasible .Hence it should be put into place to secure transactions. Implementation of this method is a one time investment and is beneficial to all saving billions of dollars in the years to come**

***Index Terms*—biometrics, credit cards, fraud, secured, transactions**

I. Introduction

Bought something new? How did you pay for it? cash? cheque? of course not. Credit card? Sounds more like the answer, right? Are you sure your transaction was safe? Sure that no one has cloned your credit card and is committing fraud and is using it to deplete you of your wealth right this moment? No. The way to be sure that you and only you can make transactions using your credit card is through biometric verification at the time of the transaction. That is the way for the future of credit cards.

In the modern day world, almost every large purchase carried out by us online or in a store is payed for using a credit card. But the concept of a credit card is that of the 1920's and first implemented in September 1958, when the Bank of America launched the BankAmericard in Fresno, California. However, the credit card itself has barely evolved since its first appearance into the market as compared to other technologies. The only improvement in credit cards has been from magnetic strips to smart cards i.e: integrated circuit cards(icc) widely know as Europay, MasterCard and Visa (EMV) (a global standard for inter-operation of integrated circuit cards) technology which in terms of security hasn't been as big as an improvement as thought to have been earlier. Criminals have made much more technological advancements in ways to steal and clone credit card information and seem to always be a step ahead [1], [2].

As regards magnetic strip credit cards, it is extremely simple to clone using card skimmers. The technology itself is more than 40 years old which at the present rate of technological advancements is prehistoric. Hand held battery operated card skimmers are widely used by criminals, it is cheap and compact. These skimmers can copy the data of a mag-strip credit card within seconds and a new card with exactly the same data can be created with which criminals can carry out fraudulent transactions [3].

As for EMV cards which is also around 20 years old (ancient compared to rate of technological progress) it has been found that the security provided by integrated circuit chips too can be cloned / hacked into / completely bypassed by the following processes as listed out by a research carried out at Cambridge University

A. Attack Variants

A few of the different attack variants are as listed below.

- Malware. There are already numerous cases of malware-infected automated teller machine (ATMs) operating in Eastern Europe.
- Supply chain attacks.
- Collusive merchant. A merchant might maliciously modify their EMV stack to be vulnerable.
- Terminal cut-out. Is where the transaction stream between the merchant terminal and the acquirer is hacked to misreport the unpredictable number when triggered by a particular signal.
- UN modification in the network.

Perhaps the main takeaway message is that an attacker who can subvert a merchant's premises, get access to his terminal equipment (even before it is purchased), or get control of his network connection, can do transactions that are indistinguishable from card cloning to the bank that issued the EMV card – even if full card cloning is physically impossible. The EMV attack surface is a bit bigger than one might think, especially once crooks learn how to manipulate the protocol [4].

According to Forbes, "Merchants in the United States are losing approximately $190 billion a year to credit card fraud – much of it online, Banks lose $11 billion and customers lose about 4.8 billion, so merchants lose

Manuscript received June 6, 2013; revised December 1, 2013

doi: 10.12720/ijeee.1.4.291-294

almost twenty times as much as banks. And this is in the United States alone [5].

Year by year the number of frauds too is increasing by an average of 15%.

Hence, there is clear evidence that the current security provided for credit cards is negligible, outdated and very easily bypassed and there is a definite need to bring in stronger security measures for credit card transactions which will benefit banks, merchants as well as consumers. The technology thats needs to be implemented is discussed in the next section.

II. Related Work

A. Technology for the Next Level of Security:

As we have seen in the previous section, there is definitely a need for added security in the field of digital financial transaction so as to save billions of dollars. But how do we do so? What is the next step forward? Here is what is proposed:

To make financial transactions more secure in the future we must use a form of biometric authentication. What better way to know your transactions are safe than having the authentication factor being a part of you. You yourself will be the authentication. Your own physical features which cannot be replicated would be the only way to go forward with the transaction hence making sure no one else can misuse your credit card.

There are many forms of biometric verification- retinal, fingerprint, voice recognition etc. just to name a few. Of these, fingerprint verification is the best combination for reliability as well as feasibility and practicality as retinal scan would be non feasible and voice recognition not completely reliable. Hence fingerprint verification would be the perfect form of security.

It is an universally accepted fact that at any given point of time, no two people on earth possess exactly the same fingerprint. Hence the chances of a fraud criminal having the same fingerprint as the person whose credit card he has duplicated is nil.

"Biometrics is certainly the most secure form of authentication. It's the hardest to imitate and duplicate. " ~ Avivah Litan

How does fingerprint verification work with credit cards:

B. Fingerprint Recognition System:

1) Acquisition of fingerprints-

The optical fingerprint recognition sensor consists of a light source, a prism, a lens, and an image acquisition device charge-coupled device (CCD). The input light from the light source creates the image of the fingerprint on the prism, and delivers it to the CCD.

2) Derivation of characteristics

Character points and special points of fingerprints are derived through the process of improving the quality of the fingerprint image to read the ridges, finding the directions of each ridge, separating the ridges and the valleys, and making the ridges into 1-pixel thick lines.

3) Matching

Matching is a process of measuring the degree of similarity between two fingerprints. Scores are calculated on the correspondence of characteristics, and the scores have to be higher than a certain level in order to determine that two fingerprints match. Character points of fingerprint images are derived, and compared with those stored in a database to calculate the matching scores [6]-[8].

The different types of finger prints are as shown in the figure below [9].

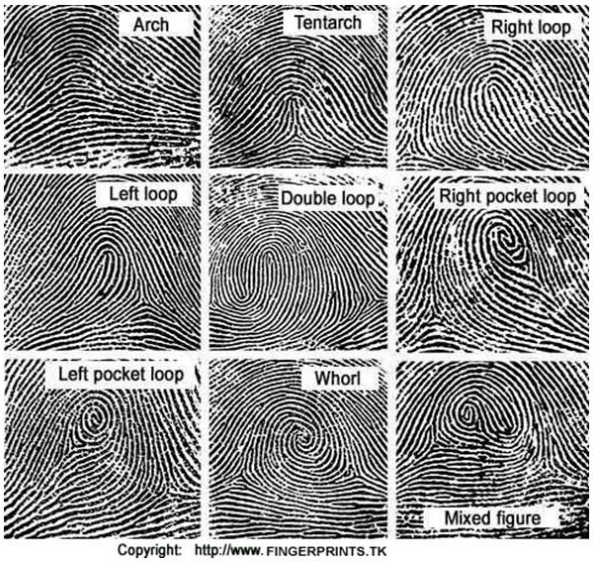

Figure 1. Types of finger prints.

C. How Can it be used for Credit Card Transactions

At the time of issue of the credit card to the customer, the fingers of the customer are scanned and a copy of the fingerprints is stored on the EMV chip of the card. These are the reference copies which are to be matched at the time of a transaction.

Now, when a customer is to make a transaction, he inserts his card into the machine and after the amount and other details are entered, before the transaction is processed the customer must place his finger on the optical finger print reader so as to read his fingerprint and match it with the reference copy contained on his card. The transaction proceeds if and only if the fingerprints match. If there is even the slightest of doubts over the matching of the prints, the customer must be asked to enter his 4 or 6 digit pin. In addition, a combination of multiple fingerprints taken singularly can also be used and the finger prints required may be changed on a monthly basis. An example would be January - index finger first followed by middle finger. February - ring finger first followed by thumb. March - middle finger first followed by index finger and so on. This gives numerous permutations thus making duplication an even harder process. This method is extremely safe as it requires the fingerprint when the credit card is in the machine and matches the prints there and then, leaving no scope for credit card fraud. Storing a reference copy of the finger prints on the chip of the card itself does away with the need to make a large data base of fingerprints hence saving storage space. Applying this method also reduces the time required to match the required prints.

The same principle can be used for online transactions too. Before the secure page goes through on making a transaction, the fingerprint must match. For this purpose, an online data base of fingerprints can be created too with the fingerprint of each customer stored agains his credit card number. This principle can be used in ATM machines especially for large value transactions [10], [11].

In case of damage of the fingerprints of the customer, he/she is to report it to the company so as to change the reference fingerprints on the card to the fingers of the customer in which the fingerprint can be read with clarity.

For the implementation of this technology, there is no physical change that needs to take place to the credit card. The EMV credit cards in current use themselves may be used with the only change being more data being stored on the chip and modification to the software on the chip to accommodate a secure reference copy of the customers fingerprint and proceed with the transaction only if a match is made with the machine i.e. the reference copy and the scanned fingerprints match.

At the merchants end though, the credit card machines must be upgraded to be compatible with the following requirements:

- To read the customers fingerprint i.e. addition on an optical fingerprint scanner.
- Updated software to match the fingerprint of the customer with the reference copy on the card and only then (when the prints are matched) go ahead and process the transaction.

Considering the huge jump in the level of security provided by this technique of authentication, the changes required are minimal, practical and completely cost effective.

Let us now look more into detail as to how fingerprint authentication out shines other present forms of security and future ideas in terms of practicality, reliability and feasibility. With reference to the first section we aware of the loopholes of the present security provided to our precious wealth during the course of this section we shall see why me must use fingerprint verification as the most viable and secure means for authentication of our credit card transactions.

The following table compares some of the biometric systems used lately, from the point of view of accuracy, cost, devices required and social acceptability.

TABLE I. COMPARISON OF BIOMETRIC SYSTEMS [12]

Biometric Technology	Accuracy	Cost	Device Required	Social Acceptability
Fingerprint	High	Medium	Scanner	Medium
Iris recognition	High	High	Camera	Low
Signature recognition	Low	Medium	Optic pen, touch panel	High
Voice recognition	Medium	Medium	Microphone, telephone	High
Facial recognition	Low	Medium	Camera	High

D. Fingerprint Vs. Retinal Scan

Retinal scan known to be the king of biometric verification due to its reliability is a very good idea for verification since it is almost impossible to impersonate. But it has one too many a draw back. Whilst in terms of reliability it scores over fingerprint verification the draw backs are as follows.

The environment required for a retinal scan is hard to replicate due to size and requirements of the scanner. It is also extremely expensive. Many a lay man has the conception that it is intrusive and harmful to the eye hence it could be serious costumers resistance and the idea would be turned down. Additionally the storage of templates takes a lot of memory and matching of templates too takes up to 10 seconds. Thus it looses out to fingerprint verifications whose advantages will be discussed in the coming paragraphs.

E. Fingerprint Vs. Voice Recognition:

Voice recognition is quirky ,cheap and high on cost efficiency but it loses out majorly when it comes to reliability as it is prone to being by passed easily by playing back the voice of the original owner hence cannot be used as a secure form of verification [13].

F. Advantages of Fingerprint Verification:

a) Very high accuracy.
b) Is the most economical biometric PC user authentication technique.
c) It is one of the most developed biometrics
d) Easy to use.
e) Small storage space required for the biometric template, reducing the size of the database memory required
f) It is standardized.

G. Disadvantages of Fingerprint Scanner:

The fingerprint scanner does not cater to physical changes in a person's finger. When there is change in the fingerprint of a person due to injury or other reasons, the person must report it to the respected bank and get a new set of fingerprints verified and stored in the smart card. People who do physical work with their hands may have a problem trying to use the finger-scan because their fingerprint may be altered from wear and tear regularly. This is not a big disadvantage because the population of people who use credit cards in developed nations who are susceptible to wear and tear makes up a very small percentage of the total population. In the under developed and developing countries , credit card users belong mainly to the non physical work category and hence credit card users would not be susceptible to this disadvantage [14].

Using the fingerprint scanner can lead to false rejections.

This biometric device does not always match an individuals fingerprint accurately, and could therefore refuse access. This problem can be solved by using a precision fingerprint scanner and in case of doubt, the user should be asked to enter the pin code given along with the smart card [15].

As seen above, fingerprint verification brings together the best of both reliability as well as practicality. Hence it out shines other forms of biometrics. Also it is a well known fact that biometrics is one of the best forms of security as you are the only one with the key. Hence fingerprint verification out shines all other forms of biometrics and it must be the technology implemented.

III. FEASIBILITY

The next obvious question would be how feasible is this new technology and wether it is worth the cost required to put into place all the new machines required to capture and match the fingerprints. Definitely. As compared to the money lost to criminals by fraud the one time cost of installing new machines is surely worth it. This comparison shall be analyzed in detail in this section.

As explained in the previous section to implement this technique there is a requirement to include finger print scanners into the credit card and A.T.M machines. A good quality finger print scanner machine costs about Rs.3500 or $70, but if ordered in bulk which in this case is the requirement would cost only about Rs.2000 or $40. The total amount of credit lost in fraud around the world in the year 2011 alone is about $19 billion! Of which the merchants loose about 40% i.e around $7.6 billion, hence it is evident that it is beneficiary for the merchants themselves if they install these machines as they would reduce their losses by a huge margin. Moreover, the installment of these machines is a one time investment as against the amount lost due to fraud which is cumulative year after year.

The other requirement for this type of security is the process of issuing of new credit cards to all the consumers. But this cost too is comparable to loose change compared to the credit lost by banks due to fraud which is about 40% totaling up to $7.6 billion. Hence, the banks too would only be covering up their losses by issuing new cards to their customers which is also a one time investment whilst ensuring high security against fraudulent transactions.

People have a tendency to resist change, particularly when additional expenditures are involved which may look exorbitant to them. However, this is easily overcome when they are made to realise that this one time expenditure is minute when compared to the colossal amounts lost due to fraudulent transactions and the high degree of security achieved to safeguard their assets in the years to come. Those who disagree just need to have a re-look at the cost figures for implementation of the system and the current losses due to frauds given earlier [16].

IV. CONCLUSION

We can conclude that, it is quite evident that we do in fact require a new norm of security to guard us against fraud and to protect our hard earned wealth from fraudsters. The present technology is out dated and open to exploitation. The technology required to make transactions secure is present and only needs to be implemented. This technology as stated in the article is reliable, practical and cost effective and is sure to benefit all in in the years to come, saving billions of dollars. The system will take some time for implementation but it is the right step forward and in due time can be implemented even in the remotest parts of the world and will become the norm. Once fully implemented, being a victim of credit card fraud will be a thing of the past as fraud then will almost completely be eliminated by implementation of this type of technology.

Hence, for the benefit of all fingerprint authentication must be implemented for all credit card and ATM transactions without any further a due for the benefit of all. Efforts are being made to produce a working prototype for the same.

REFERENCES

[1] D. Akers, J. Golter, B. Lamm, and M. Solt, "Overview of recent developments in the credit card industry," *FDIC Banking Review*, vol. 17, no. 3. Pp. 23-35, 2005.

[2] Encyclopaedia Britannica: Credit Card. [Online]. Available: http://www.britannica.com/EBchecked/topic/142321/credit-card

[3] An Article by Linda Musthaler Dated. (Jan 2012). [Online]. Available: http://www.securitybistro.com/blog/?p=811

[4] M. Bond, O. Choudary, S. J. Murdoch, S. Skorobogatov, and R. Anderson. Chip and skim: Cloning EMV cards with the pre-play attack. [Online]. Available: http://www.cl.cam.ac.uk/~rja14/Papers/unattack.pdf

[5] Forbes: MBA Without Bachelor. [Online]. Available: http://www.forbes.com/sites/haydnshaughnessy/2011/03/24/solving-the-190-billion-annual-fraud-scam-more-on-jumio/

[6] F. Alonso-Fernandez, J. Bigun, J. Fierrez, H. Fronthaler, K. Kollreider, and J. Ortega-Garcia, "Fingerprint recognition," in *Guide to Biometric Reference Systems and Performance Evaluation*, D. Petrovska-Delacrataz, G. Chollet, and B. Dorizzi, Eds, Springer, Heidelberg, 2009,ch. 4, pp. 51-90.

[7] R. Ayoub and C. Rodriguez, *A Best Practices Guide to Fingerprint Biometrics Ensuring a Successful Biometrics Implementation*, Frost & Sullivan.

[8] Howstuffworks: How Fingerprint Scanners Work. [Online]. Available: http://computer.howstuffworks.com/fingerprint-scanner5.html

[9] [Online]. Available: http://www.fingerprints.tk/

[10] L. Coventry, A. De Angeli, and G. Johnson, "Usability and Biometric Verification at the ATM Interface," in *Proc. SIGCHI Conference on Human Factors in Computing Systems*, Ft. Lauderdale, Florida, USA, April 5–10, 2003, pp. 153-160.

[11] M. Upmanyu, A. M. Namboodiri, K. Srinathan, and C. V. Jawahar. Efficient biometric verification in encrypted domain. [Online]. Available: http://cvit.iiit.ac.in/papers/Maneesh_ICB09.pdf

[12] A. K. Jain, S. Pankanti, and S. Prabhakar, "Biometric recognition: Security and privacy concerns," *IEEE Security & Privacy*, vol. 1, no. 2, pp. 33-42, March/April 2003.

[13] [Online]. Available: http://biometrics.pbworks.com/w/page/14811349/Advantages%20and%20disadvantages%20of%20technologies

[14] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *Appeared in IEEE Transactions on Circuits and Systems for Video Technology*, Special Issue on Image- and Video-Based Biometrics, vol. 14, no. 1, pp. 4-20, January 2004.

[15] [Online]. Available: http://www.nsa.gov/ia/_files/factsheets/I73-009R-007.pdf

[16] Biometrics for Identification and Authentication Advice on Product Selection–Issue 2.0

Akash S Rao born in Udupi-Karnataka, India on the 10th of May 1994. Currently pursuing a bachelors degree in the field of electronics and communication engineering in PESIT-BSC Bangalore, India. Current research interests include robotics, nano electronics, vlsi, microprocessors and micro controllers.

Deepak Albert born in Bangalore on March 8, 1994. Currently pursuing a bachelors degree in the field of electronics and communication engineering in PESIT-BSC Bangalore. Current research interests include microprocessors and micro controllers.