

Multi-Factor Authentication and Fingerprint-based Debit Card System

Mubarak Adetunji Ojewale¹, Patrick Meumeu Yomsi²




¹CISTER Research Centre, ISEP, Polytechnic Institute of Porto (IPP), Rua Alfredo Allen, 535, 4200-135 Porto, Portugal (mkaoe@isep.ipp.pt); Department of Electrical and Computer Engineering, Faculty of Engineering, University of Porto, Rua Dr. Roberto Frias, 4200-465 PORTO, Portugal (up201809172@fe.up.pt) ORCID [0000-0003-3861-1782](https://orcid.org/0000-0003-3861-1782); ²CISTER Research Centre, ISEP, Polytechnic Institute of Porto (IPP), Rua Alfredo Allen, 535, 4200-135 Porto, Portugal (pamy@isep.ipp.pt) ORCID [0000-0003-0473-1559](https://orcid.org/0000-0003-0473-1559)

Abstract

One thing can be said to be common to all forms of debit card fraud – authentication bypass. This implies that a secure debit card transaction system can only be guaranteed by a safe and reliable authentication system. Many approaches have been adopted to ensure a secure authentication system, but often, these approaches are either focused on the Automated Teller Machines (ATM)/Point of Sales (POS) terminals or Online/e-commerce transactions, thus not providing full security on both fronts. In this work, we address this problem by adopting a multi-factor debit card system that uses a combination of the traditional Personal Identification Number code (PIN) and the mobile-phone delivered One-Time Password (OTP) with a biometric authentication option (fingerprint). We demonstrate that this approach ensures the security of both online and terminal transactions. The fingerprint option makes it easy to use by people who find memorizing PINs difficult.

Author Keywords. Debit Cards, Authentication, Fingerprint, OTP.

Type: Research Article

 Open Access  Peer Reviewed  CC BY

1. Introduction

The use of electronic payment methods is not only widely accepted in developed societies but has become the norm. The increasing number of people with bank accounts has been accompanied by an increase in the use of debit cards – now being widely used by current and savings account holders at the point-of-sale and at Automated Teller Machines (ATMs) worldwide. The growth in retail banking accounts, together with widespread consolidation in the industry and the merging of smaller banks into larger entities, have been highly beneficial trends for both banks and their customers. But just like every other forms of payment, cards are exposed to security vulnerabilities. While traditional forms of card payment frauds (stolen card fraud, card-not-present transaction, etc.) are still an important threat, fraud due to unauthorized access to customer's payment data appears to be on the rise (Sullivan 2010). If someone, say B, steals A's card or gains access to A's card number, then B can potentially deplete funds from A's account. And, at the end of several unauthorized transactions, this can result in overdraft fees, bounced checks or even bankruptcy for A, in cases whereby the bank is not liable for any fraudulent transactions made from one's debit card.

The security of a debit card system depends greatly on a secure and reliable authentication system. Many approaches have been adopted to ensure a secure authentication system in the state-of-the-art. However, most of these approaches are focused either on the ATM/POS

terminals or Online/e-commerce transactions only. Furthermore, they do not consider customers with a low level of education who finds it hard to remember complex PINs. There is, therefore, a need for a robust and user-friendly system that guarantees debit cards transaction security both at terminals (ATM and POS) and in online transaction environment. This work fills this gap by providing a new system that features the following characteristics:

- Is highly secure for both terminal and online transactions;
- Provides tighter security measures than the existing system;
- Is User-friendly especially for people who find it difficult to remember complex PINs.

The work tackles the authentication problems of the debit card system as a whole. It proposes two authentication pathways which are the biometric authentication with fingerprint and the PIN with One Time Password (OTP). While the fingerprint authentication is more suitable in terminal transactions, the PIN with OTP is advisable for online transactions although the two can be used on any transaction platform.

2. Background

The single factor authentication (e.g. passwords or PIN) is no longer considered secure in the debit card world today because of the many attacks on systems with this authentication method (Aloul, Zahidi, and El-Hajj 2009). In order to circumvent this hurdle, two-factor authentication methods have recently been introduced to meet the demand of organizations for providing stronger authentication options (Aloul, Zahidi, and El-Hajj 2009; Parameswari and José 2011; Saha and Sanyal 2014). In most cases, a hardware token is given to each user for each account. But the increasing number of carried tokens and the cost of manufacturing and maintenance those has become a burden on both the client and organization. An alternative is to install software tokens on the clients' mobile phones, since most clients, if not all, carry mobile phones today at all times (Gupta 2013) and to use a biometric technique for verification along with existing PIN. However, in rural areas, people find it sometimes challenging to remember complicated PINs (Bachas et al. 2017). For this specific class of people, the use of only biometric verification can help them access any ATM in an easier manner and hence increase its popularity among rural masses as well increase security. Our approach, which combines the two features mentioned above (two-way authentication and biometric authentication), ensures a debit card system that is secure, inclusive, reliable and user-friendly even for those who find it difficult to understand complicated PINs.

2.1. Review of debit card attacks

The concept of attacking debit cards is a situation in which someone, say B, is attempting an unauthorized use of someone else's, say A, debit card in order to obtain goods of value on the internet, ATM or POS terminal. Such attacks include counterfeiting cards, using lost or stolen cards and fraudulently acquiring debit card numbers through the mail. Here, the fraudster uses a physical card, but physical possession is not essential. A typical case is the "cardholder-not-present" fraud, where only the card details are given (e.g. over the phone) (Gossett and Hyland 1999). There are various ways by which fraudsters attack Debit cards. But most, if not all, can be grouped under one of the three following groups: (1) phishing, (2) skimming or (3) identity theft.

2.1.1. Phishing

Phishing attacks are one of the fastest growing fraud trends for both large and small financial institutions (Andronova et al. 2018). Apart from sounding like 'fishing', both concepts share the same mode of operation. Specifically, whereby a fisher trolls in a boat on the river and uses bait to catch the fish, criminals who perpetuate phishing also troll the Internet by using

any communication method (email or websites for example). In phishing emails, for example, phishers use bait to convince the user and steal his credentials such as card number, Social Security (SS) number, and/or passwords (Andronova et al. 2018). Phishing e-mails appear to come from a known individual or an organization - with which the victim may or may not have an account- and ask for victims' personal information. This results in identity theft, fraud, and possible account hijacking. On phishing websites, victims are tricked into clicking on some links, which redirects to malicious websites that request the victim's sensitive information. If the victim is not well educated about this type of attack, he can divulge this information, which may then be used to gain unauthorized access to the victim's debit card.

2.1.2. Skimming

Card skimming is an alternative way for fraudsters to steal cardholder's identity and use it to commit fraud, i.e. to borrow money and/or take out loans in victim's name (Rizou 2010). It usually occurs at payment terminals – ATM and POS terminals. The perpetrator makes use of special devices, called skimmers. These are hidden devices attached to legitimate payment terminals by fraudsters to illicitly capture account information (Scaife, Peeters, and Traynor 2018). Some skimmers can store large volumes of track information while some others do not store data but transmit it to a scammer. Once criminals have skimmed the card, they are able to create a fake or 'cloned' card with the victim details. Then, they run up charges on the victim account.

2.1.3. Identity theft

Identity theft consists of using information (e.g. name, address, SS number) related to the identity of one person to gain unauthorized access to something (Manap, Abdul Rahim, and Taji 2015). These types of records make it easier for criminals to get control over accounts in the victim's name and assume his identity. Here, perpetrators observe directly a victim from a nearby location, such as looking over someone's shoulder to extract valuable information. It is especially effective in crowded places and/or when the victim keys in his PIN at an ATM or a POS terminal, public internet facilities, public and university libraries or airport kiosks. Shoulder surfing can also be accomplished at a distance using binoculars or other vision-enhancing devices. Inexpensive, miniature closed-circuit television cameras are yet other options. They can be concealed in ceilings, walls or fixtures to observe data entry. Criminals can also go through the victims' garbage cans or a communal dumpster or trash bin to obtain sensitive information.

3. Multi-Factor Authentication and Fingerprint-based Debit Card System

Multi-factor authentication allows more than one means of authentication in a single system (Saha and Sanyal 2014). This drastically reduces the risk of a system being compromised because the chance of more than one authentication factors being broken or lost at the same time is very limited. Also, the application of multifactor authentication increases the number of mediums in which a Debit card system can be deployed. Note that the withdrawal of money from an ATM machine utilizes a two-factor authentication; the user must (1) possess the ATM card, i.e. what he has, and must (2) know a unique PIN, i.e. what he knows. Despite this additional level of security, two-factor authentication of terminal transactions can be easily bypassed. So, adding a third factor like a One-Time-Password (OTP) delivered to customer's mobile phone will make the system much more secure and more difficult, if not impossible, to bypass (Parameswari and José 2011). An OTP behaves exactly as its name indicates: It is used exactly once; after which it is no longer valid. This provides a very strong defense against eavesdroppers, compromised telnet commands, and even publication of login sessions.

3.1. Authentication with fingerprint

Obiano (2009) blamed the menace of ATM frauds on indiscriminate issuance of ATM cards by financial institutions without giving due consideration to the customer's literacy level. According to this author, one of the frequent causes of fraud is when customers are careless with their cards and PIN numbers as well as their response to unsolicited email and text messages to provide their card details. Using a biometric information like the fingerprint in place of a PIN, which can be accessed by various dubious means discussed above, is more secure (Oko and Oruh 2012). On the other hand, fingerprint technologies have also advanced so much that synthetic fingerprints can be detected from real ones. In addition, people who find memorizing the PIN difficult will no longer stand such risks as being careless with their (written down) PIN or telling unscrupulous individuals their PIN to transact on their behalf. This will drastically reduce the rate at which the less educated people suffer from fraudsters due to their inability to deal with numerical complexities such as PIN.

3.2. The multi factor approach

In the system proposed in this work, the user can choose between using the fingerprint authentication or the PIN system associated to a randomly generated 3-digit number, which will be sent to his mobile phone (the phone number is the one registered with the debit card). We propose that this choice be available for both online and terminal transactions. For PIN based transaction, the system will prompt the user to key in a 3-digit OTP generated for the transaction that is being processed. The transaction can only be completed upon successful entry of a valid OTP – together with a valid PIN. The 3-digit validation is meant to timeout after a short period to prevent a deadlock situation in case there is a problem with the SMS gateway. Algorithm 1 (see following page) describes the pseudocode of the operations.

4. Implementation

To demonstrate the performance of the proposed approach, an ATM machine simulation was developed using the Java programming Language, Microsoft Access database, VeriFinger free fingerprint Software Development Kit (SDK) (Neurotechnology 2010) and Nesmo SMS gateway (Nexmo 2017) to deliver the OTP. Figure 1 shows the start page of the system interface provides the two proposed authentication methods.

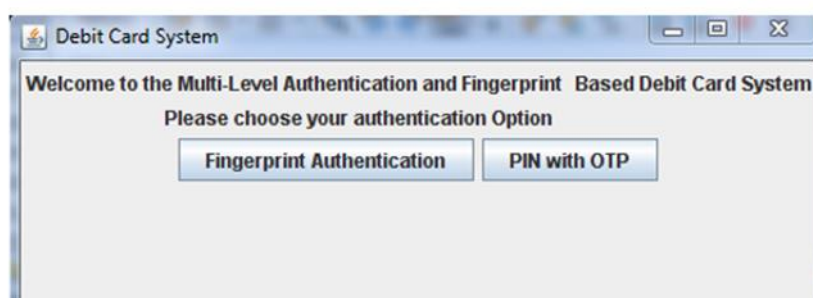


Figure 1: The landing page of the debit card terminal

If the user chooses the fingerprint option, he gets a prompt to thumbprint the fingerprint scanner after which he will be authenticated or rejected if his fingerprint does not match. Upon successful authentication, the user is directed to the landing page where he can perform transactions. If the user opts for fingerprint authentication, he will not need an OTP to complete transactions.

```
Begin  
Read card details           #user inserts card/card details  
Read authentication option  #user selects authentication option  
if (authentication_option == fingerprint)  
    Scan fingerprint        #Scans user fingerprint  
    if (fingerprint match)  
        Proceed to transaction  
    else  
        Reject card and deny transaction  
    end if  
else if (authentication_option == PIN with OTP)  
    attempts = 0  
    while (attempts < 3)  
        Read PIN             #user keys in his/her PIN  
        Read transaction details  
        Send OTP to users' phone  
        Read OTP             #user keys in the OTP sent to his/her mobile phone  
        if (OTP is correct and PIN is correct)  
            Proceed to transaction  
        else  
            Reject card and deny transaction  
        End if  
        Attempt+=1  
        if (attempt ==3)  
            Block card  
        end while  
    end if  
end
```

Algorithm 1: Multi-Factor Authentication with Fingerprint and OTP

Figure 2 shows a fingerprint mismatch error reported by the system.



Figure 2: Fingerprint mismatch - authentication denied

On the other hand, if the user chooses the “PIN with OTP” option, a prompt will appear for the user to login with his PIN (simulating the usual process of inserting the cards and entering the 4-digit PIN or entering the card number in online transaction). The system has a maximum number of permitted login attempts before the debit card is flagged for fraud protection and the card is disabled for some days. Figure 3 shows a prompt where the system informs the user about the remaining login attempts before the card is disabled.

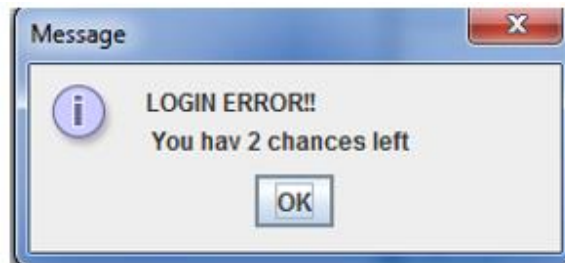


Figure 3: PIN login error, the card will be blocked after 2 more unsuccessful attempts

Upon successful authentication, the user is directed to the transaction page where he can perform transactions. The home page of the debit card system, modelled after an ATM machine interface, is shown in Figure 4.

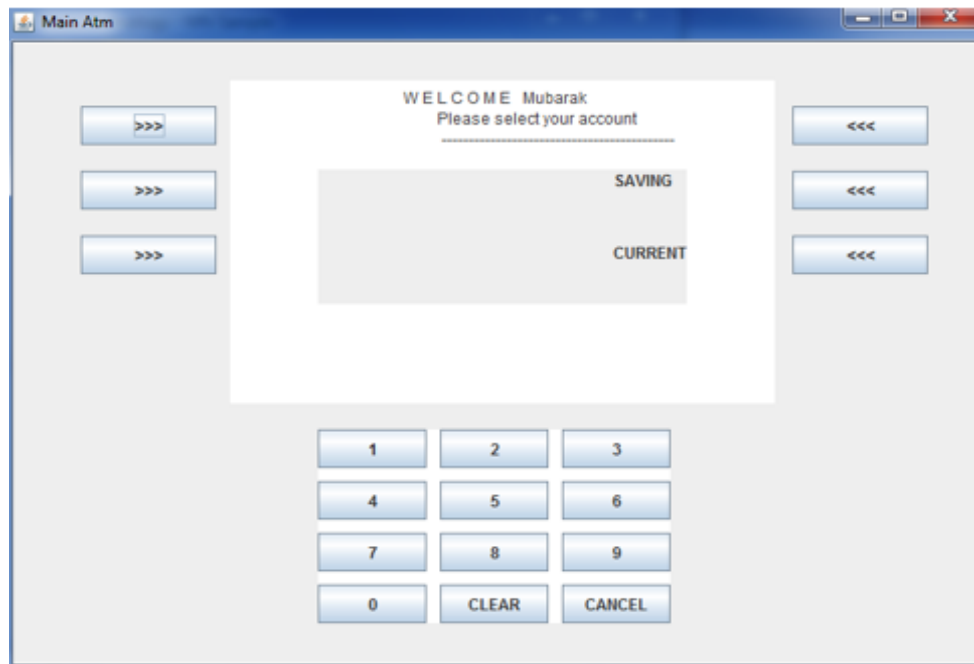


Figure 4: transaction page

The user will need an OTP to complete transactions under this authentication option. After entering the transaction details, a 3-digit OTP will be sent to the user’s mobile phone and he

will be prompted to enter these digits. Once a valid OTP is entered, the user can perform the transaction. Figure 5 shows an interface prompting the user to key-in the OTP while a display showing the confirmation message from the system is shown in Figure 6.



Figure 5: Prompt for OTP to continue transaction

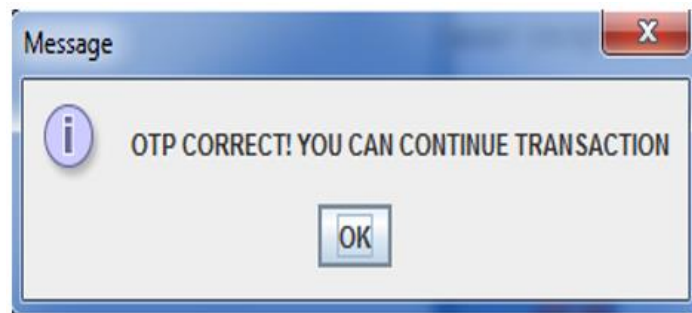


Figure 6: OTP confirmation

The two-factor authentication methods give users secure authentication choices within the debit card system. These authentication methods are suitable for both terminal and online debit card transactions.

5. Literature Review

Authentication is as old as the crime of impersonation and identity theft. Since these crimes have been detected, man has been using different means to assert that a person's claim to a thing is genuine. The oldest and the most basic of these methods is verbally asking the parties involved for verbal clarification. This seems to be the most reliable but at the same time the most inefficient method by far. There are other common means developed over time which includes signatures, seals and the evolving electronic authentication. Our focus is, however, on debit card authentication methods, and, below, we present a review of previous works on debit card authentication.

5.1. Two-factor authentication

Aloul, Zahidi, and El-Hajj (2009) addressed the problem of carrying out secure authentication via mobile devices. They proposed the use of a two-factor method of authentication, which makes use of something you have (mobile phone) and something you know (one-time password). The method involves the use of a mobile phone for the generation of a one-time password (OTP), or the use of SMS in retrieving a remotely generated OTP from a server. Results showed this two-factor authentication method to be a more secure form of verifying users than traditional password systems. They also showed how this method can be used to eliminate the problems that one actor authentication methods (e.g. passwords) face. Their method provides a cheaper alternative to current two-factor authenticating systems (tokens, cards) widely used today. It does this by making use of the users' mobile phone for OTP generation, therefore eliminating the extra cost involved in purchasing additional tokens and cards. The work, however, still requires users to memorize PINs and the solution is not robust enough to accommodate people who find it difficult to recall their PINs.

5.2. Single-sign-on systems

When a user has several accounts with different service providers, he needs to remember and use different user-ids and passwords while connecting to those accounts. The single sign-on (SSO) mechanism relieves users from having to undergo unnecessary multiple authentications for each service. [Ying, Yao, and Hua \(2009\)](#) pointed out that systems that have a single sign-on experience, assign the same level of security to each service providers within a distributed network. But, according to the authors, this is not secure. Typically, if one of the services provided within the distributed network becomes compromised, then the single sign-on experience will tend to pose a threat to other service providers that require a higher level of security. The authors proposed a multi-level authentication mechanism (MLASSO), in which different security levels that are required by different service providers can be automatically analysed and assigned by a server. This improves the flexibility, performance and security of the network.

5.3. Strong authentication

[Van Thanh et al. \(2009\)](#) introduced the concept of using the mobile phone device as a token for authentication instead of a traditional hardware token. The overall cost of using an additional device to carry out authentication is very high for organizations that must maintain thousands of tokens. Also, users will have to carry around hardware tokens whenever they need to carry out authentication on the fly. The authors proposed the use of mobile phones as a replacement for hardware tokens.

5.4. Social authentication

[Soleymani and Maheswaran \(2009\)](#) suggested that social authentication factor (someone you know), should be highly dependent on the social network the individual belongs to. That is, every individual who uses a mobile device as an authenticator needs to belong to a social network. In the case when a member of that network has lost his secret credentials or the mobile device, that person will require someone to vouch for him. During the process of vouching for someone, the secret credential is not sent to the voucher but to the individual who needs to be vouched for. This maintains the secrecy and privacy of the credentials and thus, adds an additional level of security to the already existing system. A downside to this is that the compromise of anyone on the network puts every other person on the social network at risk.

5.5. Biometric authentication

Person's identification is crucially significant in many applications and the hike in debit card fraud and identity theft in recent years indicates that this is an issue of major concern in wider society. Because passwords are known to be one of the easiest targets of hackers, biometrics-based authentication offers several advantages over other authentication techniques. It is a rapidly advancing field that is concerned with identifying a person based on his physiological or behavioural characteristics ([Oko and Oruh 2012](#)). Biometric authentication has grown in popularity to provide personal identification.

6. Conclusion

This paper provides a robust solution to debit card authentication problems by adopting a multi-factor approach with two authentication pathways. The two pathways are biometric authentication with fingerprint and PIN combined with OTP. With its flexibility of offering different authentication options, users can now enjoy a variety of not only secure but also easy authentication process. In this context, the fingerprint authentication comes as a big

relief to people who find it hard to deal with complicated PIN. Living in a world with growing e-commerce and online transaction activities, we strongly believe that this approach would be very helpful in many domains.

References

- Aloul, F., S. Zahidi, and W. El-Hajj. 2009. "Two factor authentication using mobile phones". In *The 7th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA-2009)*, 641-44. <https://doi.org/10.1109/AICCSA.2009.5069395>.
- Andronova, I. V., I. N. Belova, M. V. Ganeeva, and Yu N. Moseykin. 2018. "Scientific technical cooperation within the EAEU as a key factor of the loyalty of the participating countries' population to the integration and of its attractiveness for new members". *RUDN Journal of Sociology* 18, no. 1: 117-30. <https://doi.org/10.22363/2313-2272-2018-18-1-117-130>.
- Bachas, P., P. Gertler, S. Higgins, and E. Seira. 2017. *How debit cards enable the poor to save more*. NBER Working Paper Series: Working Paper 23252. <https://doi.org/10.3386/w23252>.
- Gossett, P., and M. Hyland. 1999. "Classification, detection and prosecution of fraud on mobile networks". *Proceedings of ACTS Mobile Summit*, no. 1: 2-4. <http://www.chrismitchell.net/ASPeCT/CD%20Data/Papers/P31.PDF>
- Gupta, S. 2013. "The mobile banking and payment revolution". *European Financial Review* (february - march): 3-6. <https://www.hbs.edu/faculty/Pages/item.aspx?num=44356>.
- Manap, N. A., A. Abdul Rahim, and H. Taji. 2015. "Cyberspace identity theft: An overview". *Mediterranean Journal of Social Sciences* 6, no. 4S3 (august): 290-99. <https://doi.org/10.5901/mjss.2015.v6n4s3p290>.
- Neurotechnology. 2010. "Free fingerprint verification SDK". <https://www.neurotechnology.com/free-fingerprint-verification-sdk.html>.
- Nexmo. 2017. "Convoso: Leading provider of cloud-based contact center software relies on Nexmo SMS to enable enhanced customer communications". <https://www.nexmo.com/customers/convoso>.
- Obiano, W., 2009. "How to fight ATM fraud". *Online Nigeria Daily News*, june 21, 2012.
- Oko, S., and J. Oruh. 2012. "Enhanced ATM security system using biometrics". *IJCSI International Journal of Computer Science Issues* 9, no. 5 (september): 352-57. <https://www.ijcsi.org/papers/IJCSI-9-5-3-352-357.pdf>.
- Parameswari, D., and L. José. 2011. "SET with SMS OTP using two factor authentication". *Journal of Computer Applications (JCA)* IV, no. 4: 109-12. <https://www.semanticscholar.org/paper/SET-with-SMS-OTP-using-Two-Factor-Authentication-Parameswari-José/07997f7ac77c6ce976f9abfa4fb4c888122ef727>.
- Rizou, A. 2010. "Analysis of fraud detection". Master's thesis, Athens Information Technology – Center of Excellence for Research and Graduate Education, Athens, Greece. https://www.academia.edu/4655404/Analysis_Fraud.
- Saha, A. and S. Sanyal. 2014. "Survey of strong authentication approaches for mobile proximity and remote wallet applications - Challenges and evolution". *International Journal of Computer Applications* 108, no. 8 (december): 10-15. <https://www.ijcaonline.org/archives/volume108/number8/18930-0319>.
- Scaife, N., C. Peeters, and P. Traynor. 2018. "Fear the reaper: Characterization and fast detection of card skimmers". Paper presented at the 27th USENIX Security Symposium Security '18. <https://www.usenix.org/conference/usenixsecurity18/presentation/scaife>.

- Soleymani, B., and M. Maheswaran. 2009. "Social authentication protocol for mobile phones". In *Proceedings - 12th IEEE International Conference on Computational Science and Engineering, CSE 2009*, 436-41. <https://doi.org/10.1109/CSE.2009.390>.
- Sullivan, R. 2010. "The changing nature of US card payment fraud: Issues for industry and public policy". Paper presentend at the 2010 Workshop on the Economics of Information Security - WEIS 2010. https://www.econinfosec.org/archive/weis2010/papers/panel/weis2010_sullivan.pdf.
- Van Thanh, D., I. Jørstad, T. Jønvik, and D. Van Thuan. 2009. "Strong authentication with mobile phone as security token". In *2009 IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, MASS '09*, 777-82: Article number 5336918. <https://doi.org/10.1109/MOBHOC.2009.5336918>.
- Ying, N., Z. Yao, and Z. Hua. 2009. "The study of multi-level authentication-based single sign-on system". In *Proceedings of 2009 2nd IEEE International Conference on Broadband Network and Multimedia Technology, IEEE IC-BNMT2009*, 448-52. <https://doi.org/10.1109/ICBNMT.2009.5348533>.