European Journal of Research Development and Sustainability (EJRDS)
Available Online at: https://www.scholarzest.com
Vol. 2 No. 5, May 2021,
ISSN: 2660-5570

MULTI-FACTOR AUTHENTICATION AND FINGERPRINT-BASED DEBIT CARD SYSTEM

O'rinov Nodirbek Toxirjonovich,
Teacher, Department of Information Technology, Andijan State University
E-mail:nodirbekurinov1@gmail.com
Saidova Nigora Kamiljonovna
Teacher, Department of Computer Engineering, Andijan State University
E-mail: nigora.sayidova2115@gmail.com

Article history:

Received: April 10th 2021
Accepted: April 22th2021
Published: May 19th 2021

Abstract:

One thing can be said to be common to all forms of debit card fraud - bypassing authentication. This means that a secure debit card transaction system can only be guaranteed by a secure and reliable authentication system. Many approaches have been adopted to provide a secure authentication system, but often these approaches focus on either automatic cash register (ATM) / point of sale (POS) terminals or online / e-commerce transactions, which does not provide complete security on both fronts. In this paper, we solve this problem by adopting a multi-factor debit card system that uses a combination of a traditional personal identification number (PIN) and one-time password (OTP) mobile phone with biometric authentication (fingerprint) option. We demonstrate that this approach ensures the security of both online and terminal transactions. The fingerprint option makes it easy for people who find it difficult to remember PINs.

Keywords: Debit Cards, Authentication, Fingerprint, OTP.

1. INTRODUCTION

The use of electronic payment methods is not only widely accepted in developed countries, but has also become the norm. The increase in the number of people with bank accounts has been accompanied by an increase in the use of debit cards, which are now widely used by current and savings account holders at points of sale and ATMs around the world. The rise in retail bank accounts, coupled with widespread industry consolidation and the merger of smaller banks into larger businesses, have been highly beneficial trends for both banks and their customers. But, like any other form of payment, cards are vulnerable to vulnerabilities. While traditional forms of payment card fraud (stolen card fraud, cardless transactions, etc.) continue to pose a significant threat, fraud due to unauthorized access to customer payment information appears to be on the rise (Sullivan 2010). If someone, say B, steals card A or gains access to card number A, then B could potentially run out of funds from account A. And, at the end of several unauthorized transactions, this could lead to overdraft fees, bounced checks, or even bankruptcy for A, in cases where the bank is not responsible for any fraudulent transactions made with its debit card.

The security of the debit card system relies heavily on a secure and reliable authentication system. Many approaches have been taken to provide a secure authentication system in the state of the art. However, most of these approaches target either ATM / POS terminals or online / e-commerce transactions only. In addition, they do not take into account low-educated clients who find it difficult to remember complex PIN codes. Therefore, there is a need for a reliable and user-friendly system that guarantees the security of debit card transactions both in terminals (ATMs and POS) and in an online transaction environment. This work fills this gap by providing a new system that has the following characteristics:

- High security for both terminal and online transactions;
- Provides more stringent security measures than the existing system;
- Easy to use, especially for people who find it difficult to remember complex PIN codes.

The work solves the problems of authentication of the debit card system as a whole. It offers two authentication methods: biometric fingerprint authentication and one-time password (OTP) PIN. While fingerprint authentication is more suitable for terminal transactions, PIN with OTP is recommended for online transactions, although both can be used on any transaction platform.

2. BACKGROUND INFORMATION

One-factor authentication (such as passwords or PIN) is no longer considered secure in the debit card world today due to numerous attacks on systems using this authentication method (Aloul, Zahidi, and El-Hajj 2009). To get

around this obstacle, two-factor authentication methods have recently been introduced to meet the needs of organizations to provide more secure authentication options (Aloul, Zahidi, and El-Hajj 2009; Parameswari and Jose 2011; Saha and Sanyal 2014). In most cases, a hardware token is issued to each user for each account. But the growing number of portable tokens, as well as the cost of producing and maintaining them, has become a burden for both the client and the organization. An alternative is to install software tokens on customers' mobile phones, as most, if not all, customers carry mobile phones with them today (Gupta 2013), and use biometric verification methods along with their existing PIN. However, in rural areas, people sometimes find it difficult to remember complex PIN codes (Bachas et al., 2017). For this special class of people, using only biometric verification can help them access any ATM in an easier way and therefore increase its popularity among the rural masses as well as improve security. Our approach, combining the two features mentioned above (two-way authentication and biometric authentication), provides a secure, inclusive, secure and user-friendly debit card system, even for those who have difficulty understanding complex PINs.

2.1. Debit Card Attacks Overview

The concept of a debit card attack is a situation in which someone, say B, is trying to unauthorized use someone else's, such as A's debit card, to receive valuable goods over the Internet, ATM or POS terminal. These attacks include counterfeiting cards, using lost or stolen cards, and fraudulently obtaining debit card numbers by mail. Here the fraudster is using a physical card, but physical possession is not required. A typical case is "no-presence cardholder" fraud, where only card details are provided (e.g. by telephone) (Gossett and Hyland 1999). There are various ways scammers attack debit cards. But most, if not all, can be grouped into one of the following three groups: (1) phishing, (2) skimming, or (3) identity theft.

2.1.1. Phishing

Phishing attacks are one of the fastest growing fraudulent trends for both large and small financial institutions (Andronova et al., 2018). Aside from sounding like "fishing", both concepts use the same operating mode. In particular, when a fisherman trolls in a boat on a river and uses bait to catch fish, criminals who perpetuate phishing also troll the Internet using any method of communication (such as email or websites). For example, in phishing emails, phishers use decoys to convince the user and steal their credentials, such as card number, social security number (SS), and / or passwords (Andronova et al., 2018). It looks like phishing emails come from a famous person or organization that the victim may or may not have an account with and ask for the victim's personal information. This leads to identity theft, fraud and possible account hijacking. On phishing websites, victims are tricked into following some links that redirect to malicious websites requesting the victim's confidential information. If the victim is not sufficiently aware of this type of attack, they can disclose this information, which can 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 the identity of the cardholder and use it to commit fraud, that is, to borrow money and / or obtain loans in the name of the victim (Rizou 2010). This usually happens in payment terminals - ATMs and POS terminals. The offender uses special devices - skimmers. These are hidden devices attached to legitimate payment terminals by fraudsters to illegally collect account information (Scaife, Peeters and Traynor, 2018). Some skimmers can store large amounts of track information, while others do not store data, but pass it on to a fraudster. After the criminals have scanned the map, they can create a fake or "cloned" map with the victim's data. They then charge the victim's account.

2.1.3. Identity theft

Identity theft is the use of information (e.g., name, address, SS number) associated with the identity of one person to gain unauthorized access to something (Manap, Abdul Rahim, and Taji 2015). These types of records allow criminals to take control of the accounts in the victim's name and accept their identity. Here, criminals directly observe the victim from a nearby location, for example, looking over someone's shoulder to extract valuable information. This is especially effective in crowded places and / or when the victim enters their PIN at an ATM or POS terminal, at public Internet centers, public and university libraries, or airport kiosks. Shoulder surfing can also be done from a distance using binoculars or other vision-enhancing devices. Inexpensive miniature CCTV cameras are another option. They can be hidden in ceilings, walls or luminaires to monitor data entry. Criminals can also go through victims' trash cans, communal trash bins or trash cans to obtain sensitive information.

3. MULTI-FACTOR AUTHENTICATION AND FINGERPRINT-BASED DEBIT CARD SYSTEM.

Multi-factor authentication allows more than one means of authentication to be used on the same system (Saha and Sanyal, 2014). This drastically reduces the risk of a compromised system, since the likelihood of a breach or loss of multiple authentication factors is very limited. In addition, the use of multi-factor authentication increases the number of media on which a debit card system can be deployed. Please note that when withdrawing money from an ATM, two-factor authentication is used; the user must (1) have an ATM card, that is, what he has, and must (2) know a unique PIN, that is, what he knows. Despite this additional layer of security, two-factor authentication for terminal transactions can be easily circumvented. Thus, adding a third factor, such as a one-time password (OTP), that is delivered to the customer's mobile phone, would make the system much more secure and more difficult, if not impossible, to circumvent (Parameswari and Jose 2011). OTP behaves exactly as its name indicates: it is used exactly

once; after which it is no longer valid. This provides very strong protection against eavesdroppers, compromised telnet commands, and even the publication of login sessions.

3.1. Fingerprint authentication

Obiano (2009) blamed the threat of ATM fraud for the indiscriminate issuance of ATM cards by financial institutions, with little regard for customer literacy. According to this author, one of the most common causes of fraud is customers' negligence with their cards and PIN numbers, as well as their response to unsolicited emails and text messages with their card details. Using biometric information, such as a fingerprint, instead of a PIN, which can be accessed in the various questionable ways described above, is more secure (Oko and Oruh 2012). On the other hand, fingerprint technology is so advanced that synthetic fingerprints can be detected in real life. In addition, people who find it difficult to remember the PIN will no longer be exposed to risks such as negligence with their (written down) PIN or giving unscrupulous people their PIN to conduct transactions on their behalf. This will drastically reduce the rate at which less educated people suffer from scams due to their inability to deal with numerical complexities like PIN.

3.2. Multifactorial approach

In the system proposed in this work, the user can choose between using fingerprint authentication or a PIN system associated with a randomly generated 3-digit number that will be sent to his mobile phone (the phone number is registered with a debit card). We suggest that this selection be available for both online transactions and terminal transactions. For a PIN-based transaction, the system will prompt the user to enter the three-digit OTP generated for the transaction that is being processed. The transaction can only be completed after successfully entering a valid OTP - along with a valid PIN. The three-digit check is designed to time out after a short period to prevent a deadlock situation in the event of a problem with the SMS gateway. Algorithm 1 (see next page) describes the pseudocode of operations

4. IMPLEMENTATION

To demonstrate the performance of the proposed approach, an ATM simulation was developed using the Java programming language, Microsoft Access database, VeriFinger software development kit (SDK) without fingerprints (Neurotechnology 2010) and Nesmo SMS gateway (Nexmo 2017) for OTP delivery. ... Figure 1 shows the home page of the system interface, which provides two suggested authentication methods.

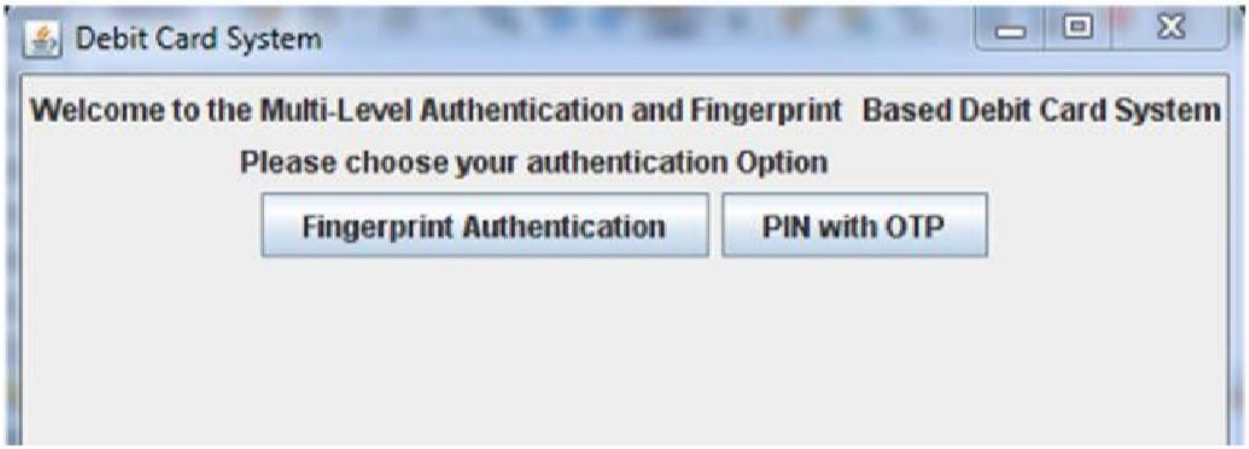

Figure 1. Terminal landing page for a debit card.

If the user selects the fingerprint option, they are prompted for a fingerprint on the fingerprint reader, after which they will be authenticated or rejected if their fingerprint does not match. After successful authentication, the user is directed to a landing page where they can perform transactions. If the user chooses fingerprint authentication, they will not need 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 Fingerprint Authentication and OTP

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

Figure 2: Fingerprint Mismatch - Authentication Denied

On the other hand, if the user selects the PIN with OTP option, the user will be prompted to log in with their PIN (mimicking the normal process of inserting cards and entering a 4-digit PIN or entering a card number. transactions). The system has a maximum number of allowed login attempts before the debit card is flagged for fraud protection and the card is disabled for several days. Figure 3 shows a prompt where the system informs the user of the remaining login attempts before the card is disabled.

Figure 3: Failure to enter the system using the PIN, the card will be blocked after 2 more unsuccessful attempts.
After successful authentication, the user is directed to the transaction page, where he can perform transactions. The home page of the debit card system, modeled on the ATM interface, is shown in Figure 4. the main objective

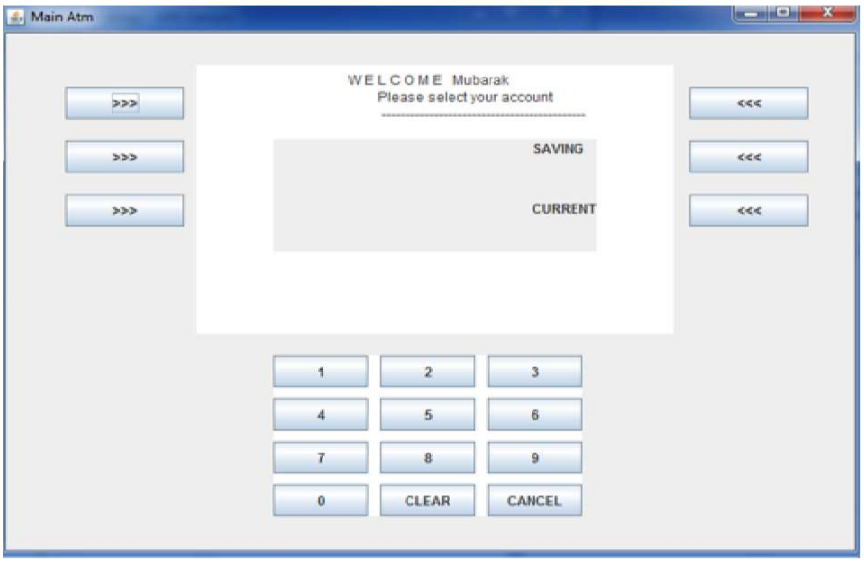

Figure 4: Transaction Page

The user will need OTP to complete transactions with this authentication option. After entering the details of the transaction, a three-digit OTP will be sent to the user's mobile phone, and he you will be prompted to enter these numbers. After entering a valid OTP, the user can complete the transaction. Figure 5 shows an interface prompting the user to enter a one-time password when displayed The display of the confirmation message from the system is shown in Figure 6.

Figure 5: Prompt for OTP to continue transaction

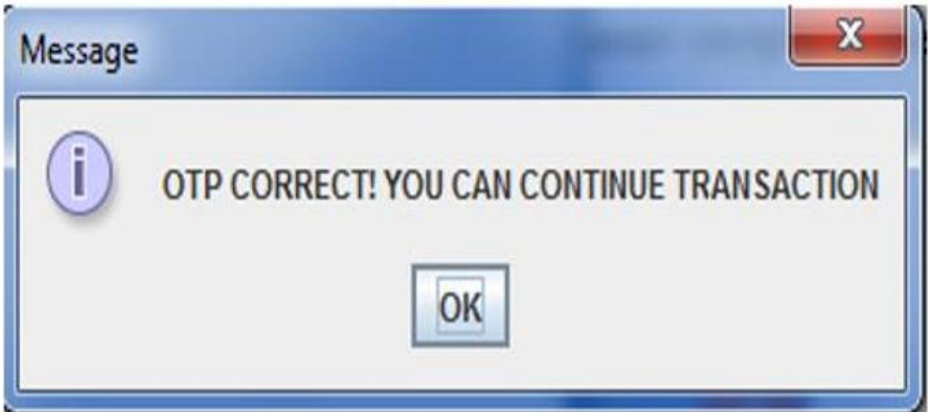

Figure 6: OTP confirmation

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 were uncovered, man has used various means to assert that a person's claim to a thing is genuine. The oldest and simplest of these methods is verbally asking the parties involved for an oral explanation. This seems to be the most reliable, but at the same time, the most ineffective method. Over time, other common means have been developed, including signatures, seals, and evolving electronic authentication. However, our focus is on debit card authentication methods, and below we provide an overview of previous work on debit card authentication.

5.1. Two-factor authentication

Alul, Zahidi and El-Hajj (2009) discussed the challenge of performing secure authentication using mobile devices. They suggested using a two-factor authentication method that uses what you have (mobile phone) and what you know (one-time password). The method involves using a mobile phone to generate a one-time password (OTP) or using SMS to receive a remotely generated OTP from a server. The results showed that this two-factor authentication method is a more secure form of user verification than traditional password systems. They also showed how this technique can be used to troubleshoot single-subject authentication methods (such as passwords). Their method represents a cheaper alternative to the existing two-factor authentication systems (tokens , cards) that are widely used today. This is achieved by using the users' mobile phone to generate one-time passwords, which eliminates the additional costs associated with purchasing additional tokens and cards. However, the job still requires users to remember their PINs, and the solution is not robust enough to accommodate people who find it difficult to remember their PINS codes.

5.2. Single sign-on systems

When a user has multiple accounts with different service providers, they need to remember and use different user IDs and passwords when connecting to those accounts. Single sign-on (SSO) eliminates the need for users to go through unnecessary multiple authentications for each service. Ying, Yao, and Hua (2009) pointed out that systems that have single sign-on capability assign the same level of security to each service provider in the WAN. But,

according to the authors, it is not safe. Typically, if one of the services provided on the WAN is compromised, then SSO will pose a threat to other service providers that require higher levels of security. The authors have proposed a Multi-Level Authentication Mechanism (MLASSO) in which the different levels of security required by different service providers can be automatically analyzed and assigned by the server. This improves the flexibility, performance, and security of the network

5.3. Strong Authentication

Wang Thanh et al. (2009) presented the concept of using a mobile phone as an authentication token instead of a traditional hardware token. The total cost of using an additional authentication device is very high for organizations that need to support thousands of tokens. Additionally, users will have to carry hardware tokens with them whenever they need to authenticate on the fly. The authors have proposed using mobile phones as a replacement for hardware tokens.

5.4. Social Authentication

Soleymani and Maheswaran (2009) suggested that the social authentication factor (of someone you know) should be highly dependent on the social network the person belongs to. That is, every person using a mobile device as an authenticator must belong to a social network. In the event that a member of this network has lost his secret credentials or mobile device, this person will require someone to vouch for him. In the process of assigning for someone, secret credentials are sent not to the voucher, but to the person for whom you need to vouch. This maintains the secrecy and confidentiality of credentials and thus adds an additional layer of security to an existing system. The downside to this is that compromising someone on the network puts any other person on the social network at risk.

5.5. Biometric Authentication

Identity identification is critical in many applications, and the rise in debit card fraud and identity theft in recent years indicates that this is a major public concern. Since passwords are known to be one of the easiest targets for hackers, biometric authentication offers several advantages over other authentication methods. It is a rapidly developing field that deals with human identification based on their physiological or behavioral characteristics (Oko and Oruh 2012). The popularity of biometric authentication for personal identification has increased.

6. CONCLUSION

This document provides a robust solution to debit card authentication problems by adopting a multi-factor approach with two authentication methods. The two paths are biometric fingerprint and PIN authentication combined with OTP. With the flexibility to offer multiple authentication options, users can now enjoy a variety of not only secure but also simple authentication processes. In this context, fingerprint authentication becomes a big relief for people who find it difficult to deal with a complex PIN. Living in a world of growing e-commerce and online transactions, we strongly believe that this approach will be very beneficial in many areas.

REFERENCES

1. 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.
2. 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.
3. 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.
4. Neurotechnology.2010."Free fingerprint verification SDK". https://www.neurotechnology.com/free-fingerprint-verification-sdk.html.
5. 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.
6. 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.
7. Parameswari, D., and L. Jose. 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-Jose/07997f7ac77c6ce976f9abfa4fb4c888122ef727.

8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. Van Thanh, D., I. J0rstad, T. J0nvik, 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.
14. 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.