A NOVEL SECURE M-TRANSACTION WITH BIOMETRIC SIGNATURE AND PARTIALLY ORDERED HIT RATE BASED KEY INPUT TECHNIQUES

[1]N.SINGARAVELAN, [2]B.RAJARAJESWARI, [3]K.SHANMUGAM.
P G Scholar, Assistant professor, Assistant professor.
AMACE, Kancheepuram, AMACE, Kancheepuram, VEC CHENNAI .

Abstract**:** This study focuses on an advanced mobile security system to provide rapid and highly secure human friendly M-commerce transaction. M-commerce transaction works in multistep process. The process involves User authentication, Merchant authentication, Message authentication and secure payment transaction. M-commerce provides availability, reliability and security in transaction phases. The proposed rank based *indirect virtual key input method*. Most virtual key inputs in the currently available mobile phones are *QWERTY* model virtual keys only. The proposed virtual keyboard regenerates the array of key PIN matrix periodically with *maximum hit rate as in the first two rows* and least used ones in the lower order rows. The use of all these together will strengthen the security in M-Commerce on a much larger scale. The achievable thing in the proposed model for avoiding shoulder surfing, screen shot attack and man in the middle attack.

Index Terms*— Rank oriented random generation, alpha numeric matrix, Pin distribution***.**

1 INTRODUCTION

1.1 OVERVIEW

M-commerce is defined as the delivery of electronic commerce capabilities directly into the hands, anywhere, via wireless technology and putting a retail outlet in the customer's hands anywhere [1]. There is much talk these days about the enormous potential of mobile commerce so m-commerce is in its infancy and meaning of m-commerce is a retail outlet in the customer's pocket [1] and [2]. It becomes the research hot spot gradually and dramatic growth in m-commerce and also consumers are still feeling their way with it [1] [3] and [4]. The requirements of the mobile commerce security focused on confidentiality, authentication, integrity, authorization, availability, and non repudiation must be rigorously enforced [4] and [5]. The M-commerce means purchase from everywhere and much easier than E-commerce. E-commerce means purchase from home/working place. E-Commerce needs Internet connectivity. M-commerce does not need any connectivity. Video conferencing can be done in M-Commerce, but not possible in E-commerce. Electricity not a main factor in M-commerce. But it is a main factor in E-Commerce. M-commerce and its related technologies offer many different application fields, such as Location Based services (LBS), Mobile ticketing, Mobile shopping, Mobile Financial services, Mobile Marketing and Mobile Entertainment. M-Commerce users can do multitasks at the same time. M-Commerce occurs through the use of wireless devices such as cell phones; pocket Personal Computer's (PC's), and Personal Data Assistant (PDAs.) It allows a user to purchase goods and services on the move, anytime, and anywhere.

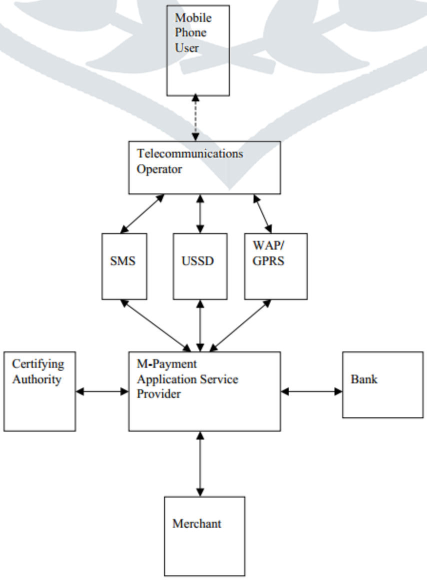

Mobile Phone User
Telecommunications Operator
SMS
USSD
WAP/ GPRS
Certifying Authority
M-Payment Application Service Provider
Bank
Merchant

Figure 1.2 Existing system of mobile PIN transaction

2 LITERATURE REVIEW

2.1 RELATED WORK AND CONTRIBUTION

There are many publications proposing how implementation can be done.

1 Drag-and-Type: A New Method for Typing with Virtual Keyboards on Small Touch screens T. KWON et.al. [15].

It developed unique *drag and tap and drag and drop model* in the mobile virtual keyboard with small flat touch screen enables those consumers to navigate various kinds of services and applications very easily, promptly, and intuitively with their fingers. The small touch screen is also changing the way of typing alphanumeric characters on those devices. Without a physical keyboard, today's smart phones popularly present virtual keyboards, aka software keyboards based on the high-resolution of small touch screens, e.g., 4.8″ 1280*720 pixels (306 ppi) and 3.5″ 640*960 pixels (326 ppi) in commodities. To input alphanumeric keys (PIN), for example, consumers may tap their fingers on the small virtual keyboard through the small touch screen but there exist at least two concerns that strongly motivate this study

The problem of drag and tap or drag and type with random key order would take too much time 20 to 30 sec on an average. It may lead to session time out and increased error rate while typing.

2 Secure OTP and Biometric Verification, Chang-Lung Tsai Chun-Jung Chen et al [7].

The proposed one time password (OTP) and personal biometric have been combined with personal identification and password for verification. M-banking may an extension of Internet banking. M-banking utilizing mobile terminal to perform those related banking transaction. Currently, mobile banking (also known as M-Banking, banking, or SMS Banking) could provide functions such as balance query, debit application, payment transaction etc. There are some popular service provided by M-banking such as announcement and notification, information providing, and business transaction. As adopting M-banking, there are some advantages as listed below following.

- **No restriction of location:** The user can perform banking anytime in any place as possible.
- **High penetration:** The popular utilization of mobile phones provides the sufficient assurance of the growth and utilization of M-banking.
- **Personalization:** Each of the mobile phones is dedicated to a specified user. Therefore, it increases the effectiveness of user authentication.

The detailed procedure of using the mobile phone for M-banking is depicted as the following.

Step 1: Enter the User login with their ID and password.

Step 2: Server side of M-banking verifies the validation of user ID and password. If the password is not correct, the server side will reject to provide service. If the ID and password of the user is correct, the user can browse the related restrict webpage and perform query process.

Step 3: As the user presents the business transaction request, the server side will then generate one time password OTP and transfer to the default receiving equipment, i.e. mobile phone of the user.

Step 4: The server side will request the user to key-in the valid OTP in specified time period.

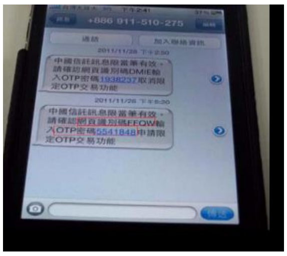
Step 5: The server side will perform the verification of OTP. If the input OTP is not correct, the server side will reject the request of business transaction and indicate OTP not valid and remind the user whether if the user needs to perform business transaction or not. If the user's answer is yes, the server side will then generate and transfer another new OTP for the user to register again. If the user does not need to perform the business transaction again, the process will retain on the privilege of browsing and query function.

Step 6: If the input OTP is correct, the user will be request to capture new biometric data. Then upload the captured data to the server side in real time with hash function process for authentication. This increases the security.

Step 7: The server side will compare and verify the uploaded biometric data if it is identical to the user. If the answer is "yes", the user then can perform those available business transaction services. Otherwise, the server side will reject the transaction process and request the user to Login again to prevent the possible defrauding.

Step 8: Logout and finish the M-banking activity.

Figure 2.1 is the OTP message received on the iPhone4 and Comparing
Of Traditional M-banking with proposed M-banking scheme is shown in table 2.1.



+886 911-510-275

2011/11/28 下午2:50

中國信託訊息限當筆有效，請確認網頁識別碼DMIE輸入OTP密碼1938237取消限定OTP交易功能

2011/11/28 下午8:36

中國信託訊息限當筆有效，請確認網頁識別碼FFOW輸入OTP密碼5541848申請限定OTP交易功能

Figure 2.1: Reading message from iPhone4

M-banking scheme

Item	***Traditional OTP verification scheme***	***Proposed OTP verification scheme***
Hash	NO	YES
OTP	Randomly generated	Randomly generated
Webpage verify	Randomly generated	Randomly generated
Password transfer via internet	Plaintext	Cipher
Bio verify	NO	YES

Table 2.1 value of comparison

It does not is not focus on which mechanism is captured the Biometric data and no secure encryption algorithm is provided to transmit the biometric fingerprint image to the server side. It also does not focus on the Fuzzy logic threshold level rules.

3 Pin Distribution Techniques, Arunprakash et al [8],

It presents the Pin distribution techniques. This proposed system tells about the Pin distribution process by using AES encryption. Customer details and Payment details (PIN) are sending by using WAP 1.0. Only, the Mutual authentication is main advantages of this system. WAP 1.0 is used because WAP 1.0 consists of one security problem, known as the “WAP gap,” is caused by the existence of a WAP gateway in a security session. Encryption, decryption time and throughput become low by using AES algorithm.

4 Biometric Authentications in M-commerce, existing biometric techniques [9].

It develops authentication is unique. User authentication is achieved by mobile device. The main advantage of this technique is as both users and service provider recognizes without an additional device. The merits of using *Elliptic curve cryptography (ecc)* for encryption methods are the process is small, efficient and requires low power.

The problem of Biometric techniques as it uses only encryption method for user and payment details for secure transfer of the data. By not using a security conversation mechanism like WAP gateway, data’s are not more secured. No Merchant authentication is available in this technique. Fingerprint verification and identification method is does not focused. Fingerprint Threshold level does not clearly analyzed.

3 SYSTEM DESIGN

To protect the password or Pin, the starting point (login PIN) itself considered as to be secure. In order to resist against the attacker (shoulder surfer), the keyboard of the mobile should have random keys for the attacker to guess the exact password and it should highly probable to type for the original user.

3.1.1 **Existing system in mobile virtual keyboard:**

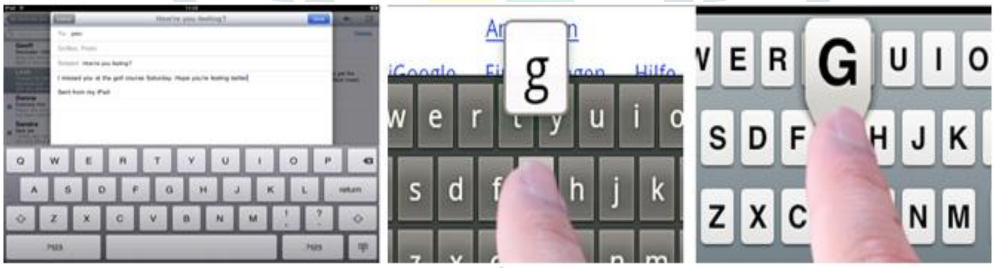


Figure 3.1.1 a. Ordinary key input (PIN) method b. Beep sound. c. Visual echo.

A smart phone is now becoming a part of electronics consumer’s lives and turns out to be one of the most popularly used consumer electronic devices. Its small flat touch screen enables those consumers to navigate various kinds of services and applications very easily, promptly, and intuitively with their fingers. The small touch screen is also changing the way of typing alphanumeric characters on those devices. Without a physical keyboard, today’s smart phones popularly present virtual keyboards, aka software keyboards based on the high-resolution of small touch screens, e.g., 4.8″ 1280*720 pixels (306 ppi) and 3.5″ 640*960 pixels (326 ppi) in commodities. To input alphanumeric keys, for example, consumers may tap their fingers on the small virtual keyboard through the small touch screen but there exist at least two concerns that strongly motivate this study [15].

First, the smart phone users are frequently experiencing difficulties and also many errors in typing alphanumeric keys (PIN) with their thick thumbs because a small virtual keyboard even with the reduced set of touchable keys can only provide tiny size keys to the users [16]. Although the higher resolution of touch screens can facilitate much smaller keys for constructing a full size keyboard layout, users may prefer a larger key so as to type characters with thumbs more easily. Unfortunately, such a larger key may only allow a partial keyboard layout having the reduced set of keys on the small touch screen, e.g., separate layouts for alphabets and numeric (and/or special) characters, and pop-up keys for rendering more characters on the keys at best. Note that the partial keyboard layout requires a number of switches between distinct layouts. As illustrated in Fig. 3.1.1-(a), even worse, a visual echo, i.e., the most widely used response method on the virtual keyboard, can be occluded and hidden under the thick thumb with blunt touch. This tendency could reduce the benefits from the recent and future advance in the high-resolution touch screens and hinder the consumers from being aware of the real key entry and eventually correct key entry on the touch screen. Second, the consumers are susceptible to malicious people nearby or spyware inside because they can capture the key input, particularly secret input such as a password, in mobile environments. As illustrated in Fig. 3.1.1-(b), when the visual echo is eminently shown bigger, the malicious people nearby can read what actually was entered by the consumer. This is called a shoulder-surfing attack that is more effective in a crowded place. Also, spyware can capture and exploit the T. Kwon et al.: Drag-and-Type: A New Method for Typing with Virtual Keyboards on Small Touch screens 99 touch events and its geometric data if a user types secret characters regardless of the visual echo [17]. In this paper, the two concerns regarding accuracy and security motivated the authors to develop a new style of typing method called Drag-and-Type, on the full layout of the virtual keyboard presented on the small touch screens. The Drag-and-Type method leverages the dragging action instead of direct taping on the touch screen to ease more accurate typing on the small virtual keyboard. In particular, two kinds of Drag-and-Type methods are proposed: Drag-and-Tap and Drag-and-Drop on the full layout of the virtual keyboard. The Drag-and-Tap method works with separate tapping actions on the full size keyboard, whereas the Drag-and-Drop method works with dragging actions only [17]. Although the typing speed is controversial in both methods, the consumers can choose the Drag-and-Type methods when an accurate typing is more required, for example, for a password entry that is quite more sensitive to erroneous key inputs. In that sense, the Drag-and-Drop method is further explored to secure the password entry against shoulder-surfing and spyware attacks well. The extended method is called Secure Drag-and-Type. Two user studies were conducted for both basic and secure methods, and it was found that the proposed method can particularly be used for accurate and secure typing on the small touch screen regarding security-sensitive consumer electronics applications.

Drawbacks of the Existing System (Random Keyboard with Drag and Drop):

a. Time taken to enter the password or PIN requires more than ordinary entry time.
b. Error rate while typing the password is too high.
c. Session time lapsed due to error and password entry.

Several existing works of mobile transaction security ensures only 100% verification of fingerprint password. It causes the unavailability of the password for the authenticated user because of some injury or small defect in the finger. The existing algorithm could not satisfy all the necessary conditions of creating strong encryption techniques.

The work done by Chang-Lung Tsai Chun-Jung Chen et al [7] has also introduced an interesting concept of biometric recognition after the bank secure password has been verified. It will create lot of complexity to the bank server. The reason for that is time for processing a client increasing drastically if every time the bank server checks the authenticity of the individual person.

Draw backs of the Existing System

- The entire PIN can be obtained if the external network is cracked.
- NO Mutual authentication and Merchant Authentication.
- Manageability problems due to limited resources.
- Suppose obtained finger print matches is partially true(60-99%),in this case which solution is considered?-not focused this case in existing techniques
- Existing technique uses only encryption method for user and payment details for secure transfer of the data. By not using a security conversation mechanism such as WAP gateway data are not more secured.
- Existing technique, using ECC for encryption but ECC consists of, difficulty in counting the number of points on the curve and generating suitable curves. ECC is not yet fully understood and relatively has slow signature verification.
- Attacks can be made over wireless network by means of sniffing.

3.1.3 PROPOSED SYSTEM OF HIGHEST HIT RATE KEY BASED PARIALLY ORDERED INPUT METHOD:

In the proposed structure, the key input PIN would be in random but the order of making shuffled keys is different. To make it partially ordered, by considering PARTIALLY ORDERED SET and LATICE structure of Hasse diagram to arrange the key according to the number of hits as shown in the figure 3.1.2.

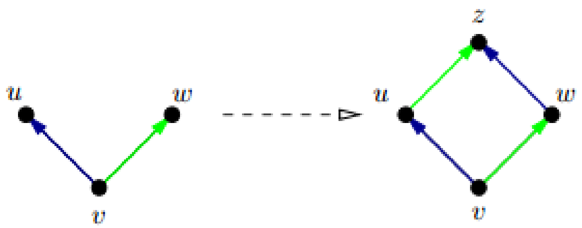


Figure 3.1.3 Hasse diagram and the arrangement of keys with relative partial ordering [18].

Let us consider the key inputs as u, v, w, and z. The simple logic in the "poset" (partially ordered set) is number of highest values get placed in the upper bound than the lower bound keys set [18]. From the above figure 3.1.3 mentioned, if the key z's hit is more than the hit rate of u, v which is in the middle order of the row in the virtual keyboard.

PROPOSED CONCEPT: HASSE LATTICE

Let X, Y is the lower and upper bound of the Hasse diagram and a_0, a1, a2, .a_{n-1} is the key inputs given as password PIN. According to lattice, the most high valued key input (let a_i<a_J) becomes at the top. This would ensure that the first and the next rows are arranged in accordance with the number of hit rates. The key board layout is composed of alphanumeric characters in random arrangement. Fig 3.1.3.1 shows the prototype design of *randomized highest hit rate virtual keyboard layou*t method. The characters of all keys are hidden when a user begins to drag a pointer on the touch screen. The keyboard layout remains blank until a character key is entered. After the character key is entered, the keyboard layout is rearranged in random sequences and the hidden keys reappear. These mechanisms enable *to prevent efficiently shoulder surfing and spyware attack* from stealing users' secret characters. A user can find out easily the location of own password, whereas it is hard for observers to identify it. Although adversaries may guess the secret characters, they could not find out exactly whole of them because of hiding promptly all keys in the keyboard layout

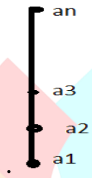


Figure 3.1.3.1 Arrangement of Highest Hit Rate Keys (Say A_n) at the Top Two Rows.

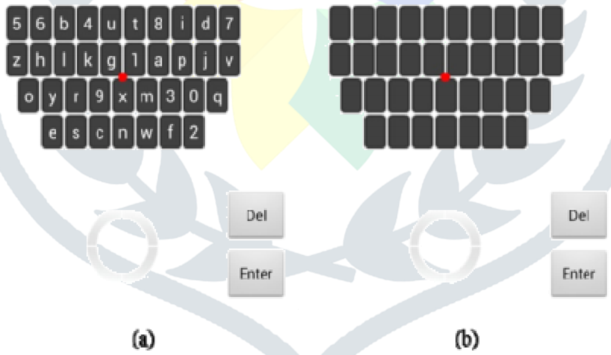


Figure 3.1.3.2. a) Randomized hit rate oriented key arrangement. b) Hidden keys to avoid screen shot attack.

C. Input Interface

Input interface differs from Drag-and-Drop in using without visual echo. However, it is possible to enter the character accurately with visual selected key echo and vibration feedback. A user has to verify the location of the target character keys before touching on the touch screen. When the touch event, e.g., ACTION_DOWN, is occurred, the proposed *keyboard hides all keys automatically without an additional action*, e.g., pressing the hide key button. So a user has no extra burden to enter the characters with this method.

D. Time complexity for the attacks:

Let us consider the 6*6 array matrix, alphabets (a, b, .z) are 26 letters and numeric values (0, 1,.9) are 10 numbers thus totally 36 alphanumeric keys with their input combination of 36!~O($n^{n)}$. Brute force attack needs O (36^{36}) unit time required to compute. If we want to consider the special characters, the array matrix increases accordingly to 7*7 matrixes etc. For the 6*6 matrix of keys, the password keys entered in the beginning stage is almost random and time taking process. Therefore it took more time to find the exact key input as shown in the figure 3.1.2.1.After one or two time entry level the upcoming regeneration are customer friendly because of lattice relation.

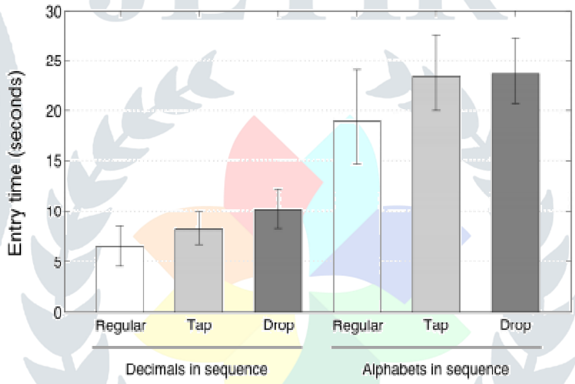
Array	C 0	C 1	C 2	C 3	C 4	C 5
R 0	7	A	X	6	M	K
R 1	D	J	0	5	F	L
R 2	9	4	B	Z	C	G
R 3	E	8	Y	N	V	H
R 4	O	T	R	P	1	3
R 5	Q	I	S	U	N	W
	SHIFT	TAB	SPL CHAR	CAPS	DEL	ENTER

Figure 3.1.3.3: the Array Matrix with Random order of keys.

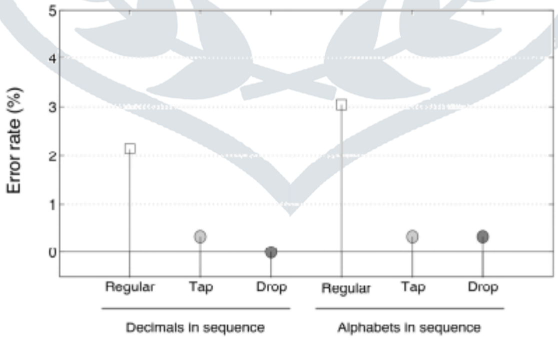
The input password given for the mobile transaction has been distributed all over the matrix. This would obviously take less time to type the password PIN. The advantage of this method is it prevents shoulder surfing, but increases the session time of the transaction. The customer can complete his individual transaction within time leads to *session timeout*. In order to increase the speed of the password entry time and completing the task within the given session, the password PIN should be easily identifiable for the customer only and not for the others.

In this matrix, the highlighted (red colored) letters be the PIN 7NSVL. The first letter would be 7 and so on. At the second time of the entry, the 7 key PIN would be at the first row but shuffled within that row in order to confuse the attacker. The same way all other keys also shuffled in the respective rows by their Partial order number and hits (RANK). During every hit of the touch screen, all the virtual keys getting hided and reshuffled within that row itself. This causes the adversary getting more complexity to find the correct and complete PIN.

TIME REQUIRED (AVERAGE) FOR TYPING USING DIFFERENT KEYBOARD METHODS [15]:

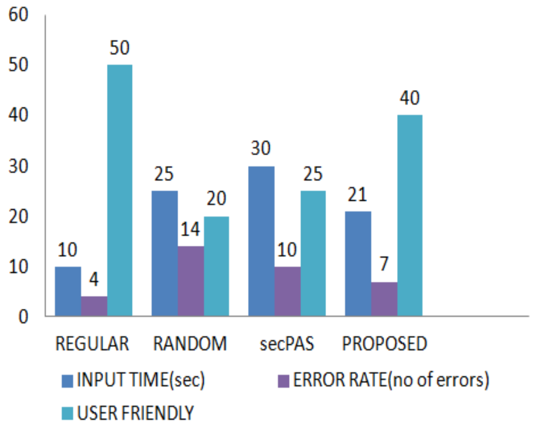


ERROR RATE COMPARISON IN DIFFERENT KEYBORDS [15]:



PROPOSED HIT RATED RANDOM KEY COMPARISON:

The experiment made with 10 people (men and women as well as literates and illiterates) between different keys with the reference to the previous results from T.kown et.al 2014, compared in the simulation mode. The results obtained shown in the graph 1.X-axis refers to the different virtual keyboard model/styles with certain constraints. The results corresponding to the input given as shown below.



CONCLUSION

This method was extended to its secure virtual keyboard version called Hit Rate virtual key to deal with shoulder surfing and spyware attacks. The Secure method was more efficient and/or more secure compared to the related authentication methods. The user studies and the attack experiments conducted in this paper confirm that it would be promising to adapt this user friendly random key access method. when a more accurate typing is preferred, and this method when a more accurate and securing typing is required on the consumer electronic devices. Specifically, a secure (and accurate) password entry can be achieved by the Secure input key method. The limitation is it can only resist a touch-based spyware attack. In the future study, a new method will be explored to resist an advanced spyware attack based on recording the whole interactions between consumer and electronic device through the small high-resolution touch screens.

REFERENCES

[1] T. Karygiannis, NIST, Computer Security Division, karygiannis, Wireless Network Security802.11, Bluetooth™, and Handheld Devices March 25, HPCC,2003

[2] *LI Xi, HU Han-ping* “A secure mobile payment system” Institute of Pattern Recognition and Artificial Intelligence, Huazhong University of Science and Technology, Wuhan 430074, China.

[3] Scarlet Schwiderski-Grosche, Heiko Knospe SECURE M-COMMERCE.

[4] Suresh Chari, Parviz Kermani, Sean Smith, Leandros Tassiulas. Security Issues in M-Commerce: A Usage-Based Taxonomy 2001.

[5] Jianqi Cui, DanLin Yao,” a new security solutions on WAP-based mobile e-business, computer application research”, September 2007, pp. 99-lOl

[6] S. Zhai, M. Hunter, and B. A. Smith, “Performance optimization of virtual keyboards,” Human-Computer Interaction, vol. 17, 2002.

[7] Arunprakash, et.al,” improved Pin distribution techniques in m-commerce”, science direct, GCSE 2011: 28-30 December 2011, Dubai, UAE.

[8] Chang-Lung Tsai Chun-Jung Chen, Deng-Jie Zhuang, “SECURE OTP and biometric verification scheme for mobile banking, 2012 IEEE.

[9] K. Go and L. Tsurumi, “Arranging touch screen software keyboard splitkeys based on contact surface,” in Proc. CHI’10 Extended Abstracts on Human Factors in Computing Systems, Atlanta, USA, ACM press, Apr. 2010.

[10] M. Klima and V. Slovacek, “Vector keyboard for touch screen devices,”in Proc. International Conference on Ergonomics and Health Aspects of Work with Computers, San Diego, USA, LNCS 5624, pp. 250-256, July 2009.

[11] S. Zhai and P. O. Kristensson, “Shorthand writing on stylus keyboard,” in Proc. SIGCHI Conference on Human Factors in Computing Systems, Lauderdale, USA, ACM press, pp. 97-104, Apr. 2003.

[12] D. S. Tan, P. Keyani, and M. Czerwinski, “Spy-Resistant Keyboard: More secure password entry on public touch screen displays,” in Proc. Australia Conference on Computer-Human Interaction, Canberra, Australia, Nov. 2005.

[13] X. Bai, W. Gu, S. Chellappan, X.Wang, D. Xuan, and B. Ma, “PAS: Predicate-based authentication services against powerful passive adversaries,” in Proc. IEEE Annual Computer Security Applications
Conference, Anaheim, USA, pp. 433-442, Dec. 2008.

[14] H. Zhao and X. Li, “S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme,” in Proc. IEEE International Conference on Advanced Information Networking and Applications Workshops, Niagara Falls, USA, vol. 2, pp. 467-472, May 2007.

[15] T. Kwon et al.: “Drag-and-Type: A New Method for Typing with Virtual Keyboards on Small Touchscreens” IEEE Transactions on Consumer Electronics, Vol. 60, No. 1, February 2014.

[16] M. Agarwal, M. Mehra, R. Pawar, and D. Shah, “Secure authentication using dynamic virtual keyboard layout,” in Proc. International Conference & Workshop on Emerging Trends in Technology, ACM press, pp. 288-291, Feb. 2011.

[17] Q. Yan, J. Han, Y. Li, and R. H. Deng, “On limitations of designing leakage-resilient password systems: Attacks, principles and usability,” in Proc. Network and Distributed System Security, San Diego, USA, Feb. 2012.

[18] http://uosis.mif.vu.lt/~valdas/PhD/Kursinis2/Sasao99/Chapter2.