IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue-15, May 2019 E-ISSN: 2347-2693

Internet Protocol Traceback Technique and Signature & Biometric Authentication for Financial Networks

Pawanraj S P [1*], Prasanna Kumar M [2]

[1] Department of Computer Science & Engineering, East West Institute of Technology, Bengaluru, India
[2] Department of Computer Science & Engineering, East West Institute of Technology, Bengaluru, India

DOI: https://doi.org/10.26438/ijcse/v7si15.349355 | Available online at: www.ijcseonline.org

***Abstract*—** Major bank hacking cases and bank robbery is reported constantly. The digital forensic evidence is the most important thing for incident response. Therefore, this paper proposes IP (Internet Protocol) traceback technique for better digital forensic.

The paper considers one of the most important components in the modern banking system, namely the direction related to ensuring the security of customer data. The number of bank cards is rapidly growing, and accordingly the network of automated teller machines (ATMs). There are smart cards, which provide higher reliability than cards with a magnetic line. This system allows the issuance of money to the client only when scanning his face. The explosive usage of mobile devices enables conducting electronic transactions involving direct signature on such devices. Thus, user signature verification becomes critical to ensure the success deployment of online transactions such as approving legal documents and authenticating financial transactions. This paper proposes a critical segment based online signature verification system to secure mobile transactions on multi-touch mobile devices.

The system extracts useful features from a user's signature that describe both the geometric layout of the signature as well as behavioral and physiological characteristics in the user's signing process. The experimental evaluation provide signature verification and robust to signature forging attacks.

***Keywords*—** *digital forensic,* IP traceback technique, *financial network, financial institutions; biometric ATMs,* online handwriting signatures, *signature authentication, signature verification,* critical segment.

I. INTRODUCTION

To achieve enhanced digital forensic, more information for incident is required. After the incident is identified, the environment is preserved and forensic experts perform data retrieval, data loss is hardly occurred. Most of data loss is due to not collecting data in usual situation. The data includes system information and network information. The system information can be collected through system logging and information volume is not much so it will be not a problem. But the volume of network information can be huge, so it is important collect efficient and effective information and after collecting information, analyzing huge volume of data is also can be a problem. Therefore this paper focuses on network information gathering and analyzing collected huge volume of data. For the network information gathering, IP traceback technique is suggested to collect attacker's information.

The financial institutions use the most advanced digital technologies in the field of security. In recent years, there has been testing of biometric ATMs that allow withdrawing money by scanning the customer's face and comparing its data with those in financial institutions' databases. Meanwhile, scanning is in 3-D format to ensure reliability in identifying the client's identity.

One of the important conditions for the introduction of innovative technologies is their economic efficiency. Therefore, the evaluation of the effectiveness of the introduction and use of biometric ATMs in relation to traditional ATMs is extremely relevant. That is why the study is promising both theoretically and practically.

As e-commerce related applications become more prevalent, more and more sensitive information, such as financial data and credit card information are sent through transactions using mobile devices.

User authentication therefore becomes vital to secure such sensitive information or mobile transactions on mobile devices. The digital signature techniques are effective for maintaining integrity and authentication of the data. However, such asymmetric cryptography-based methods are not appropriate to authenticate users.

© 2019, IJCSE All Rights Reserved

Online handwriting signatures, which consist of a series of complex finger strokes, typically contain personal traits and hence are unique among individuals. Due to its uniqueness and complexity, the online handwritten signature usually has its legal effect and is one of the socially accepted mechanisms used to authenticate users for supporting real time mobile transactions. When using his/her finger to sign on touch screens, each individual has an intrinsic signature signing behavior that has not been studied in the previous work. Such a signing behavior, if captured, could largely increase the accuracy of signature verification and effectively combat adversarial signature forging activities.

Toward this direction, a signature verification system is designed that has the capability to identify the critical segments in each individual user's signature and extract unique features to describe a person's intrinsic signing behavior.

The organization of this paper is as follows:
Section 1 explains enhanced IP traceback technique. Section 2 explains implementation of biometric authentication in ATM's. Section 3 explains signature verification for authentication and conclusions are made in section 4.

II. RELATED WORKS

A. IP Traceback Technique

The IP traceback is any method for reliably determining the origin of a packet on the Internet. Some IP traceback uses barely used IP field like an identification field, and others sends message like an ICMP (Internet Control Message Protocol) and observe reactions. Most of IP traceback processes are handled at router. Therefore major problem of IP traceback is bottleneck of router. To solve bottleneck problem, S. Savage et al.[4] proposed probabilistic model which marking only some of packets and A. Belenky and N. Ansari[5] proposed deterministic model which uses minimum numbers of routers. These methods still have bottleneck problem due to increasing network traffic. G. Yao et al.[20] proposed passive IP traceback which uses ICMP packet that generated some case of spoofed packet. G Yao method does not have bottleneck problem but it has restriction that detection of ICMP message is not always working. Therefore to solve classic IP traceback problem, we suggest different network structure with marking server that handles IP traceback process.

B. Biometric Authentication in ATM's

Existing methods for user authentication on mobile devices can be categorized into two major classes: schemes for unlocking mobile devices and schemes for continuous user authentication. To unlock screens, some mobile devices rely on manual entry of a secret password or PIN number. This method is insufficient as many people only go through this process once when the device is switched on [16]. There has also been active work in using biometric information for user authentication on mobile devices such as fingerprints [17]. However, such techniques are vulnerable to spoofing attacks and fingerprint scanners are also not always available on smart phones, making it less suitable for user authentication on mobile devices.

Several gesture based user authentication schemes have also been proposed [18]. The basic idea of these schemes is users can be authenticated by making a gesture in the air while holding the mobile phone. Such gesture is captured through the accelerometer embedded in the phone for user authentication. However, the gesture based authentication is vulnerable to replay attacks in which attackers can observe and replicate the authentication information. Along this direction, there is existing work employing users' finger gestures captured on touch screens for user authentication.

In [15], an authentication system named TouchIn has been proposed. The system asks users to draw curves on the touch screen using fingers, and then verify them based on the properties such as the curvature and acceleration of the drawing gestures. In slide-based user authentication approach [19], a series of customized finger slides are used to authenticate users jointly. However, all of the above schemes consider unique features in simple gestures for either unlocking mobile devices or performing user authentication, and they cannot be easily applied in signature verification scenario.

Furthermore, there are schemes on continuous user authentication systems relying on finger movements, finger taps or gait patterns. The purpose of such systems is to continuously authenticate users during the whole process of system execution. However, these behaviors did not happen frequently on mobile devices, because people hardly use mobile devices while walking or do heavy texting on them. Thus, it is difficult to collect a sufficient number of behavior traits for online transaction verification.

The approach in this paper focuses on the aspect of providing accurate online signature verification. Since signature is critical in many online transactions, several works have been proposed. In those papers, a user utilizes a stylus to sign his signature on the touch screen of mobile devices. The information of the signature is then captured and compared with a pre-constructed template. Moving forward, new development enables the user directly sign his signature using finger on touch screens without the requirement of a stylus pen. This approach captures attributes such as the first or second order derivative of coordinates derived from the online signature, and then represents them with a feature vector derived from attribute histograms for signature authentication. However, this system treats the user's signature as a whole and does not consider the intrinsic signing behavior of the user, which

© 2019, IJCSE All Rights Reserved

results in stable critical segments in signatures of the same user.

The work presented in this paper is different in that as it focuses on the development of a secure and robust online signature verification system by capturing the intrinsic user signing behaviors through identifying the segments which remain invariant within the user's signatures.

Moreover, the system verifies signatures not only based on the geometric layout of a signature but also based on the user's behavior and physiological characteristics. Additionally, signing signatures using multiple fingers (e.g., two fingers) are also considered to further improve the verification accuracy.

III. METHODOLOGY

A. IP Traceback
Digital Forensic Technique for Financial Network
In this section, we described IP traceback with marking server and their verification through network simulation.

To overcome bottleneck problem fundamentally, the technique introduces independent marking server. Therefore routers do not mark the packets anymore but send to marking server and marking server manages whole marking process.

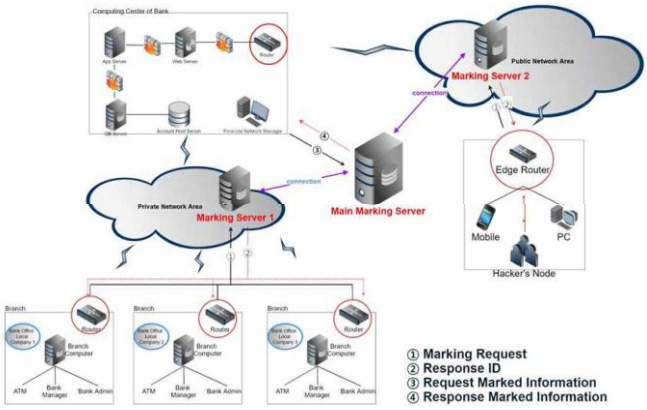

Fig. 1. Structure of IP marking server in financial network

For the marking field, IP protocol's identification field is used. The identification field is used to reassemble fragmented IP packets. But in the IP layer, fragmentation usage is about 0.25% because most of fragmentation occurs in the TCP (Transmission Control Protocol) layer. Therefore the IP protocol's identification field is selected and shows effectiveness. Fig. 1 shows structure of IP marking server in financial network. To verify IP backtrack structure with marking server, experiment is performed with simulation.

B. Evaluation of the economic efficiency of introduction and operation biometric ATMs

In the last few years, biometric ATM machines are being tested; they can recognize clients when scanning a face. Meanwhile, scanning is made in a 3-D format to ensure reliability when identifying a customer. In this case, you will not need to use a card identification system with a PIN code. Instead consider the costs of installing and maintaining one traditional ATM and a biometric one. Calculations will be made using the Total Cost of Ownership.

Capital investments for installing a traditional ATM can be estimated by the following formula:

$$K = K_1 + K_2 + K_3 + K_4 \quad (2)$$

Where
K1 - the cost of traditional ATM;
K2 – the cost of software;
K3 - the cost of installing an ATM;
K4 – the cost of connecting the alarm system;
Capital investments for installing one biometric ATM can be estimated by the following formula:

$$K = K_1 + K_2 + K_3 + K_4 + K_5 + K_6 \quad (3)$$

Where
K5 – the cost of the hardware component of the biometric system;
K6 – the cost of additional software for managing the biometric system

The costs of servicing the traditional and biometric ATMs can be determined using the following formula:

$$C = C_1 + C_2 + C_3 + C_4 \quad (4)$$

Where
C1 – maintenance expenses of the ATM;
C2 – the collection cost;
C3 - the cost of renting a place for an ATM;
C4 – the insurance cost of an ATM.

We will present the calculations using the TCO method in the graph form (Fig. 9).

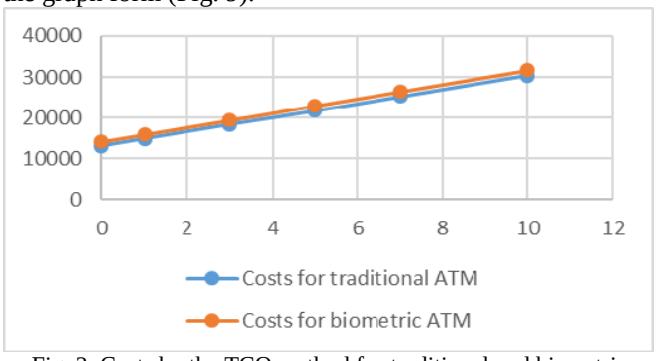

Fig. 2. Costs by the TCO method for traditional and biometric ATMs, dollars.

© 2019, IJCSE All Rights Reserved

System Overview

As shown in Figure 3, the system consists of five major components: *Signature Normalization and Interpolation*, *Feature Extraction*, *Signature Quality Evaluation*, *Critical Segment Extraction* and *Signature Comparison*.

Given a signature captured on the touch screen, the system first applies normalization and interpolation to deal with the signature geometric distortions caused by different writing sizes, orientations and locations on the touch screen under various signing conditions. In the feature extraction component, the system then extracts features from the normalized signatures to capture the geometric layout of the signature and the user's behavior and physiological characteristics. Signature quality evaluation designs a quality score to evaluate the quality of input signatures for the user profile construction during the user enrollment process.

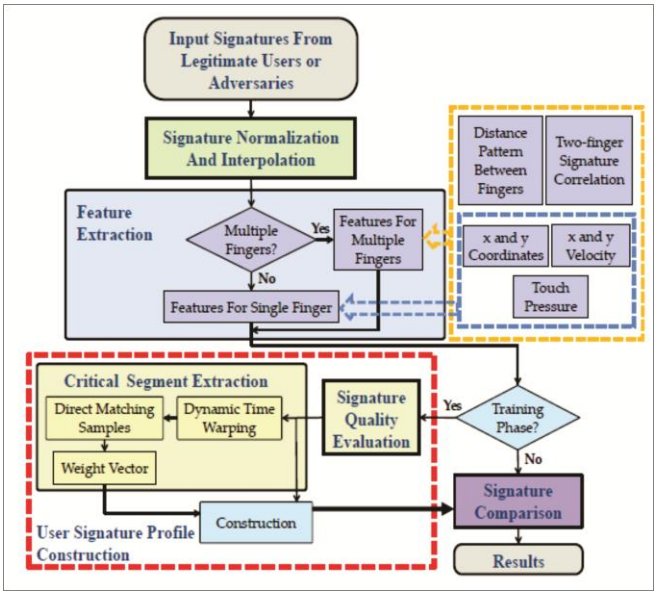

Fig. 3. Overview of our signature verification system

Such score considers the signatures' inconsistency (i.e., intra-user differences) and distinctiveness (i.e., inter-user differences) simultaneously to guarantee the user's signature quality. The problematic signature set is then discarded and the user is required to re-input a new signature set for user profile construction. Critical segments extraction is used to capture the user's intrinsic signing behaviors and identify the feature segments that remain stable within the user's signatures. The extracted critical segments are usually invariant in the presence of variations in the user's signatures, and hard for attackers to imitate. After that, the signature verification is performed by calculating a similarity score between the extracted features from the input signature and the pre-constructed user profile which is constructed when the user enrolls in the verification system. Based on the similarity score between the testing signature and the user profile, our system makes decision on whether to accept or reject the user.

Critical Segment Identification

A signature can be decomposed into several stroke segments. However, only a few of these decomposed segments are invariant across a set of signatures a user signs. Such segments reflect the user's intrinsic signing behavior, and we refer to them as *critical segments*. Existing work on signature verification did not consider capturing critical segments for signature verification. In this approach, critical segments that reflect the user's intrinsic signing behavior are extracted to increase the accuracy of signature verification and combat adversarial signature forging activities.

To identify the critical segments in a user's signature, an algorithm is developed by examining and comparing the user's genuine signatures. The algorithm takes a pair of signatures from the user as inputs and compares them using the dynamic time warping (DTW) technique.

DTW is chosen because it is a reliable and efficient to-implemented method that can calculate an optimal match between two temporal sequences with different lengths, and then measure the similarity between them. Specifically, given a feature sequence used to represent the signature (e.g., x and y coordinates of the signature, the signing pressure of the signature), the resulting coupling sequence from DTW denotes an optimal alignment between two feature sequences. The direct matching samples (DMSs) in the coupling sequence represent the segments without significant distortion between the two input signatures. Thus, the DMSs extracted from the coupling sequence can be utilized to derive a weight vector which denotes the similarity between two signatures.

To capture the invariance of the signatures, the above comparison is repeated between each pair of the user's genuine signatures in a signature pool, and then average over all the weight vectors to extract the critical segments as these segments have high similarity among a group of genuine signatures.

Critical Segment Identification Algorithm

To simplify the description of the critical segment extraction algorithm, assume a signature is already normalized and interpolated to a length L and five features (i.e., $f1$ to $f5$ including the coordinates, the velocities and touch pressure) are used for describing the signature.

Then assume $\{f_u^q ; 1 \le q \le D\}$ to be a set of the u-th features ($1 \le u \le 5$) extracted from D genuine signatures. Thus, the weight vector of the u-th feature from the pair of $q1$-th and $q2$-th signatures can be represented as: $w_u^{q1,q2}$ with $1 \le q1; q2 \le D$ and $q1 \neq q2$. Then use the coupling sequence

generated by the DTW algorithm to estimate the weight value. For each feature sequence (i.e. *u*-th feature), the dynamic warping procedure generates a coupling sequence $CS^{q1,q2}$ with a length of *K* as: $CS^{q1,q2} = \{(f_u^{q1}(i; jk);\ f_u^{q2}(i; j'k))\ ;\ 1 \le k \le K\}$, where $K \le 2L$ and $1 \le jk; j'k \le L$. The *i* denotes that the feature is extracted from the *i*-th finger in case multiple figures are used for signing signatures. A direct matching sample (DMS) in the coupling sequence is defined as a feature sample in the *q*1-th signature which has a one-toone coupling with a sample in the *q*2-th feature sequence. In other words, the matched sample $f_u^{q1}(i; jk)$ is a DMS if and only if both $f_u^{q1}(i; jk)$ and $f_u^{q2}(i; j'k)$ only appear once in the coupling sequence. The DMSs represent the signature region without significant distortion between two signature features. We thus define a weight sample $w_u^{q1,q2}(i; j)$ as:

$$w_u^{q1,q2}(i;\ j) = \begin{cases} 1, \text{if fq1; u (i; j) is DMS in } CS^{q1,q2} \\ 0, \ otherwise \end{cases} \quad (1)$$

To generalize the findings from each pair of signatures, our algorithm can examine a group of signatures from the same user and average the weight vectors over every pair of the signatures. Thus, the final weight vector of a particular feature for the user can be represented as:

$$\overline{W}_{u\,(i;\,j)} = \frac{\sum_{q1=1}^{D} \sum_{\substack{q2=1 \\ q2 \ne q1}}^{D} w_u^{q1,q2}(i,j)}{D \times (D-1)},\ 1 \le j \le L \quad (2)$$

Each average weight value $\overline{w}_{u\,(i;\,j)}$ which ranges from 0 to 1 indicates the stability of the *j*-th sample of the *u*-th feature of that user's signatures. Intuitively, a larger value denotes better stability. Our algorithm treats the samples with higher average weights more significantly during the signature comparison procedure as they can represent the user's intrinsic signing behaviors. The segments with larger average weight values are identified as critical segments of the user's signature.

IV. RESULTS AND DISCUSSION

A. IP Traceback Technique

TABLE I. PERFORMANCE ANALYSIS

	DFM [4]	**Proposed method**
Number Out	3,300	3,332
Total Time	1,716	1,655.50
Work in Process	33.1434	14.0894
Queue Waiting Time	33.39	0

Table 1 is a result of experimentation and it shows that the overhead increased by 1%, but the time was reduced by 3.5% and the process by the router was reduced by 57%. From these result, it can be said that the proposed method is suitable for gathering attacker's information in financial network traffic.

B. Biometric Authentication in ATM's

Along with the massive introduction of biometric systems, the cost of both hardware and software would be significantly reduced.

Then the capital investments for the introduction of biometric ATMs can be calculated using the following formula:

$$K = K_1 + K_2 + K_3 + K_4 + k_1 * K_5 + k_2 * K_6 \quad (5)$$

where

k1 - coefficient reflecting the decrease in the cost of the hardware component of the biometric system;

k2 - coefficient reflecting the reduction in the cost of the software component of the biometric system;

Coefficient k1 will be 0, 5 and coefficient k2 will be 0, 3 under massive introduction of biometric systems.

Then, if correction factors are taken into account, TCO capital investments for a biometric ATM will decrease.

The introduction of biometric ATMs is considered to reduce the risk of money theft from clients' accounts by almost 90%. If we take into account that the introduction and operation of the biometric ATM reduce the number of thefts from bank cards, that enables financial institutions not to spend money to pay customers, as well as raise the image in the field of the reliability of customer funds. Therefore, the saved money can be directed to decline costs on the implementation of biometric ATMs.

Then formula (4) can be represented in the following form:

$$C = C_1 + C_2 + C_3 + C_4 - Q_{stb} \quad (6)$$

Where

Q_{stb} – the volume of stolen funds saved during the introduction of biometric ATM.

The volume of stolen funds that can be saved when one biometric ATM is introduced estimates by the formula:

$$Q_{stb} = (Q_{stt1} + Q_{stt2}) / N \quad (7)$$

Where

Qstt1 – the volume of stolen funds nationwide at the initial time;

© 2019, IJCSE All Rights Reserved

Qstt2 – the volume of stolen funds nationwide at the final time;
N – the number of ATMs in the country.
The volume of stolen funds at the final time can be calculated by the formula:

$$Q_{stt2} = k_3 * Q_{stt2} \quad (8)$$

Where

k3 – coefficient reflecting a decrease in the volume of stolen funds from bank cards when introducing biometric ATMs, in this case, it is equal to 0,1.

The expenses of implementation according to the TCO method, given the fact that the cost reduction occurs evenly throughout the life of the operation are shown in Figure 10.

C. Signature Verification for Authentication
Performance Comparison with Existing Schemes
In the set of experiments, the effectiveness of our proposed signature verification system is evaluated by comparing it with two existing signature verification schemes: a histogram based signature verification system and TouchIn.

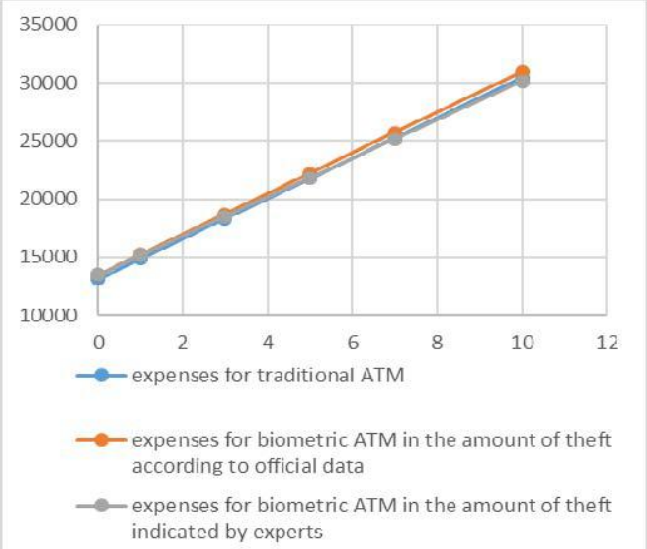

Fig. 5. Costs comparison of the introduction and operation of traditional and biometric ATMs taking into account the volume of stolen funds, dollars.

In Figure 6, we use "*Our scheme (single finger)*" and "*Our scheme (two fingers)*" to denote the results from our system using one and two fingers, respectively. The histogram based signature verification system captures the distribution of attributes such as the first or second order derivative of coordinates derived from the signature for verification, and we utilize the legend "*Histogram*" to denote it in the results.

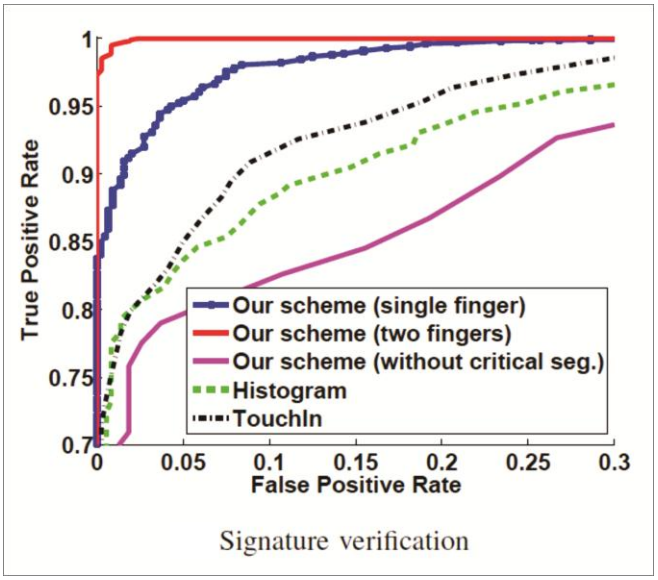

Fig. 6. Signal Verification

The TouchIn authentication system first asks a user to draw curves on the touch screen, and then verify the user based on the properties such as the curvature and acceleration of the drawing curves. To compare the performance of our system to Touchin, we apply Touchin to handle signatures instead of curves as originally proposed. And the results are denoted as "*TouchIn*".

Additionally, we evaluate our system performance when only using extracted features without considering the key technique, i.e., critical segments, for signature verification. This scenario is similar to the existing stylus-based online signature verification schemes which treat the user's signature as a whole.
We use the legend "*Our scheme (without critical seg.)*" to denote the results from such scenarios.

V. CONCLUSIONS

Financial network targeted cyber attacks are becoming more sophisticated and more critical, and major financial network hacking cases are reported constantly. Bank robbery cases show the importance of digital forensic evidence, therefore for the incidents response, effective digital forensic with sufficient information is necessary. For better digital forensic, IP traceback with marking server technique is suggested which make gathering attacker's information possible. Hope this technique can be used for enhancing incident response capability and for the future work; these techniques will be verified based on attack scenario.

The modern economic development is accompanied by a digital transformation of all industries. The introduction of information and communication technologies in the financial sector led to the creation of a new direction Fintech. It is

© 2019, IJCSE All Rights Reserved

based on the synthesis of the most advanced information and financial technologies, which contributes to the emergence of new business models of interaction with customers. Along with new directions in the financial sector, much attention is paid to the traditional areas of financial institutions development, in particular, the service using bank cards. The volume of cashless payments around the world is steadily growing. The volume of money stolen from bank cards is constantly growing.

In connection with the growth of stolen funds, financial institutions introduce the most advanced innovative forms of bank cards security. One of such forms is the biometric ATM, which allows identifying the customer when scanning his face in 3-D format.

This paper presents a critical segment based online signature verification system to secure mobile transactions on mobile devices. The proposed system identifies the critical segments, which remain invariant within a user's signature, to capture the user's intrinsic signing behavior. By leveraging the rich set of information enabled by touch screens, the system extracts useful features to describe both the geometric layout of the signature as well as a user's behavioral and physiological characteristics during the signing process. The system further utilizes a quality score to identify the problematic signature sets during user enrollment to achieve robust user signature profile construction. Moreover, the signature normalization and interpolation methods enable robust signature verification in the presence of signature geometric distortions caused by different writing sizes, orientations and locations on touch screens.

REFERENCES

[1]. Sungmoon Kwon, Jaehan Jeong, Taeshik Shon. Digital Forensic Readiness for Financial Network, 2019 International Conference on Platform Technology and Service (PlatCon), 2019 IEEE.

[2]. Alexey V. Bataev. The Model of Assessing Economic Efficiency of Biometric ATMs, 2019 IEEE, pp. 1365-1370.

[3]. Yanzhi Ren, Chen Wang, Yingying Chen. Signature Verification Using Critical Segments for Securing Mobile Transactions, 2018 IEEE, pp. 1536-1233

[4]. Stefan Savage, David Wetherall, Anna Karlin, Tom Anderson. Practical Network Support for IP Traceback, 2000

[5]. Andrey Belenky, Nirwan Ansari. IP Traceback With Deterministic Packet Marking, 2003 IEEE, pp. 62-64

[6]. Christiawan, Bayu Aji Sahar, Azel Fayyad Rahardian, Elvayandri Muchtar. Fingershield ATM – ATM Security System using Fingerprint Authentication.

[7]. Guang Yao, Jun Bi, Athanasios V. Vasilakos. Passive IP Traceback: Disclosing the Locations of IP Spoofers from Path Backscatter. 2014 IEEE

[8]. G. Renee Jebaline, S. Gomathi. A Novel Method to Enhance the Security of ATM using Biometrics, 2015 [ICCPCT]

[9]. H. Lasisi, A.A. Ajisafe. Development of Stripe Biometric based Fingerprint Authentications Systems in Automated Teller Machines, 2012 [ACTEA]

[10]. Akio Ogihara, Hiroyuki Matsumura, Akira Shiozaki. Biometric Verification Using Keystroke Motion and Key Press Timing for ATM User Authentication, 2016 [ISPACS]

[11]. Apurva Taralekar, Gopalsingh Chouhan, Rutuja Tangade, Nikhilkumar Shardoor. One Touch Multi-banking Transaction ATM System using Biometric and GSM Authentication. 2017 (BID)

[12]. Christian Gruber, Thiemo Gruber, Sebastian Krinninger, Bernhard Sick. Online Signature Verification With Support Vector Machines Based on LCSS Kernel Functions, 2009 IEEE

[13]. Donato Impedovo and Giuseppe Pirlo, Automatic Signature Verification: The State of the Art, 2008 IEEE

[14]. Napa Sae-Bae, Nasir Memon, Online Signature Verification on Mobile Devices, 2014 IEEE

[15]. J. Sun, R. Zhang, J. Zhang, Y. Zhang. Touchin: Sightless two factor authentication on multi-touch mobile devices, in Proceedings of CNS, 2014.

[16]. N. L. Clarke, S. Furnell. Authentication of users on mobile telephones - a survey of attitudes and practices, Computers and Security, 2005.

[17]. T. Clancy, N. Kiyavash, and D. Lin. Secure smartcard-based fingerprint authentication in Proceedings of the ACM SIGMM workshop on Biometrics methods and applications, 2003.

[18]. G. Bailador, C. Sanchez-Avila, J. Guerra-Casanova, A. de Santos Sierra. Analysis of pattern recognition techniques for in-air signature biometrics, Pattern Recognition, 2011.

[19]. M. Shahzad, A. X. Liu, A. Samuel. Secure unlocking of mobile touch screen devices by simple gestures: you can see it but you cannot do it, in Proceedings of ACM MobiCom, 2013.

[20]. Yao, Guang, Jun Bi, Athanasios V. Vasilakos. Passive IP traceback: Disclosing the locations of IP spoofers from path backscatter, IEEE Transactions on Information Forensics and Security 10.3 (2015): 471-484.

Authors Profile

Pawanraj S P: pursuing M.Tech in CSE (SCS), EWIT (VTU), Bengaluru. His areas of interest are Computer Security, Databases, Computer Networks, Storage Area Networks, Programming the Web, Software Engineering, Cloud Computing, Computer Graphics, etc.

Dr. Prasanna Kumar M: Associate Professor, Department of Computer Science & Engineering, East West Institute of Technology (VTU), Bengaluru. Qualification: B.E, M.Tech, Ph.D. His areas of interest & research are Software Engineering and Cloud Computing.

© 2019, IJCSE All Rights Reserved