DETECTING FRAUDULENT BEHAVIORS USING MULTI-VIEW BAGGING DEEP LEARNING IN SMART PHONE

Mr.E.Ramesh Reddy, Associate Professor, Dept of CSE, NECG
P. Hari Chandana, (17F11A0580), Dept of CSE, NECG.
S. Sreeja, (17F11A05A5), Dept of CSE, NECG.
N. Chandana, (17F11A0565), Dept of CSE, NECG.

Abstract – With the quick development in cell phone utilization, forestalling spillage of individual data and security has become a difficult errand. One significant result of such spillage is pantomime. This kind of illicit use is almost difficult to forestall as existing preventive systems (e.g., password and fingerprinting), are not prepared to do persistently checking utilization and deciding if the client is approved. When unapproved clients can overcome the underlying assurance instruments, they would have full admittance to the gadgets including utilizing put away passwords to get to high-esteem sites. We present KOLLECTOR, another structure to distinguish pantomime dependent on a multi-see stowing profound learning way to deal with catch successive tapping data on the PDA's console.
Index terms – Privacy; Deep learning; Multi view learning.

I. INTRODUCTION

The widespread adoption of smart-mobile devices has provided users with anytime, anywhere computing" capability. At the same time, such mobility has also lead to theft as these smart- mobile devices contain as much sensitive and private information as that contained in less mobile devices such as desktops and laptops. In 2013, over three millions Americans were the victims of smartphone theft. When stolen, electronic impersonation is often used to access personal data through these devices as if the actions are performed by the device's owner. Impersonation fraud is a serious problem that costs U.S. companies nearly $180 million between 2013 and 2014[1][2] .

While setting access codes can safeguard these devices, studies have shown that most owners choose very simple passwords or even no passwords to protect their mobile devices . Many studies have also shown that when passcodes are used, attackers can still reverse engineer passwords by observing screens for taps, fingerprints, and/or smudge patterns[3][4] . A key aspect of existing protection mechanisms is that they only try to prevent unauthorized users from unlocking devices. Once they are able to bypass these mechanisms, there are no additional mechanisms to continuously prevent them from using the device. As such, it is highly desirable to enhance the authentication mechanisms in smartphones to include additional defensive measures designed to be non-intrusive but which can continuously monitor the user activity such as web browsing or entering information to web applications to prevent unauthorized usage.

Currently, existing continuous monitoring approaches use a variety of standard smartphone sensors coupled with (shallow/traditional) machine learning techniques such as support vector machines (SVMs) to continuously authenticate the user. One notable aspect of much of this existing work is a "closed-world" model, wherein the device owner as well as all potential attackers are in the training set. This is clearly an unrealistic model. Furthermore, SVMs and other shallow machine learning techniques are unable to learn the complicated relationships inherent in sequential activities like typing. Despite this limitation, some systems combine several smartphone sensors in order to achieve high accuracy rates and low equal error rates. This additional sensor usage has been shown to degrade battery life . Furthermore, SVM based models have an additional problem in that they perform classification quite slowly.

The proposed system, KOLLECTOR, employs a deep learning approach to meet our aforementioned requirements. It continuously monitors and studies sequential tapping biometric behaviors while a user is typing. Our system can detect when an unauthorized user begins using the keyboard by collecting sequential tapping features including the duration of a tap and the horizontal and

vertical distances between successive taps. KOLLECTOR can protect the phone while user is holding or typing on the mobile. Unlike prior work that employ many sensors , our approach only uses one built-in sensor, the accelerometer, to record the position of the device as part of the continuous authentication process.

II. LITERATURE SURVEY

The problem of continuous identification lends itself well to machine learning[5][6]. Shallow machine learning algorithms are frequently used for behavioral biometrics. The most common technique is to construct a binary classifier (e.g., asking a question such as "Is the current user the owner of the device?"). Support vector machines (SVMs) and decision trees (DTs) are commonly used for this purpose. However, one major limitation of shallow machine learning is that it cannot capture the complex and hidden relationships between the features and sequential keystrokes. To the best of our knowledge, this is the first work to apply deep learning to tapping patterns in order to detect unauthorized users. Prior efforts in NLP and computer vision have shown that deep learning can produce accurate models that can achieve high detection rates.

Previous works use traditional—or shallow— machine learning techniques (e.g., SVM) which cannot capture the sequential information of keystrokes. To improve the classification performance, traditional machine learning must use more features by running more sensors background which leads to excessive energy consumption. Multi-view bagging (MVB) learning is an attempt to solve shortcomings in machine learning and deep learning by constructing multiple "views" of the same data and by focusing on a different set of features for each view. These views are analogous to views in a database. By using multiple views when we train a model, we can achieve higher classification accuracy than we could with a single view.

Bagging learning solves high variance problems by training multiple models and using a voting strategy for evaluation[7]. To the best of our knowledge, this work represents the first approach to use multi-view and bagging for continuous identification on smartphones.

In the next, we discuss our approach to capture sequential tapping information that our system uses to detect typing by unauthorized users. Our goal is to construct a deep learning system leveraging MVB models that can produce accurate identification with only a few taps on the keyboard.

III. PROPOSED SYSTEM

Propose KOLLECTOR, a multi-view bagging fraudulent usage detection framework via a deepstructure. The proposed framework contains three main steps to detect fraudulent usage. This process is illustrated in Figure 1 and summarized below:

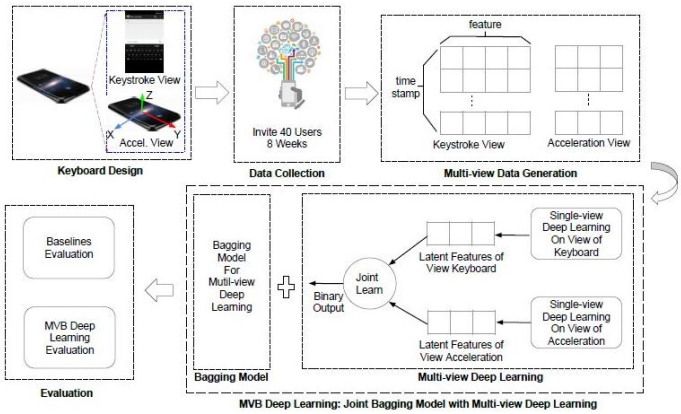

Fig. 1: Overview of KOLLECTOR.

1) In the first step, we create a custom software keyboard that can monitor and collect keyboard usage information. The new keyboard is then installed on smartphones that will be used in this study.

2) In the second step, the usage information is collected. The scale and scope of data collection can vary but in this study, we invited 40 volunteers to use smartphones equipped with the custom keyboard for 8 weeks. We retrieved the sequential tapping information from each phone in real time. We then process the collected data to build a multi-view version that can be used to detect fraudulent usage.

3) Once the data has been collected, we use the multi-view data and perform multi-view bagging (MVB) learning via a deep structure. To evaluate the effectiveness of MVB, we also compare the performance of the proposed approach with those of the traditional machine learning techniques to perform similar fraudulent usage detection. The techniques that we used to compare include support vector machine, decision tree and random forest.

Data Collection and Processing

To preserve user's privacy, we applied for IRB approval and was approved prior to any data collection. Data was collected and securely stored. The information was anonymized prior to processing.

We recruited 40 volunteers for this study, all of whom had extensive prior experience with smartphones. The volunteers ranged in age from 30 to 63. Out of the 40 volunteers, we find that 26 of them (17women and 9 men) used the provided phones at least 20 times in 8 weeks; the most active participant used the phone 4702 times while the least active participant only used the phone 29 times. Since deep learning requires more training data than traditional machine learning, we do not use any data from the volunteers who used the phone less than 20 times.

When collecting tapping data, not every tap has all of the features we use. For example, the distance from and time since the previous tap cannot be computed for the first tap in a typing session. In this case, we set a value of 0 for such features. All features are normalized to the range [0; 1].

Generating Training Models

To create two machine learning models to help detect fraudulent smartphone usage. First, we create a multi-view deep learning model to distinguish any two people in the data set based on their unique sequential tapping information. This enables us to validate that individual users really do have different sequential tapping behaviors that we can measure. Next, we create a multi-view bagging deep learning model which we use to distinguish a device's owner from an unauthorized user.

Instead of using early fusion to concatenate multiple views into one view, we decide to use multi-view deep learning with late fusion. First, we choose to model each view separately. Then, we use deep learning model to find the latent vector representation of each view. Last, we concatenate the latent vectors of each view for fraudulent activity prediction, which is named late fusion. Multi-view learning based on late fusion can avoid losing information as in the case when multiple views are combined to create single view. One key piece of information that we want to preserve is the sequence of keystrokes. By using multi-view, we are able to maintain each view separately but then use multiple views to make predictions.

In this manner, we develop a multi-view deep learning model. This model performs better than the single-view since it can better utilize the information from different views of the dataset. In our work, we generate the Multiview learning model to detect attackers when we can well separate one user with other users in our training dataset[8].

After generate the multi-view deep learning model for fraudulent usage detection in the training process, we apply a bagging policy in the testing process as shown in Figure 2. Generally, we use random initialization of an odd number m of the same dataset, and then choose to generate learning models for each initialization. Next, we use different trained models with one testing data set. Finally, we apply a majority voting strategy for the final output. For example, KOLLECTOR has three models for three random initializations in the training process. In testing process, for each input sample, we apply all three models on this sample to generate three detection results and output the majority result by the bagging policy.

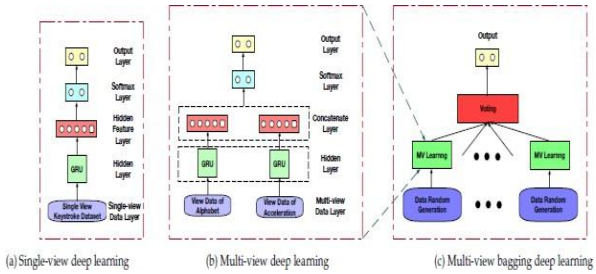

Fig. 2: A comparison of different learning frameworks.

IV. CONCLUSION

We propose KOLLECTOR, a new framework for continuous user identification. We use sequential tapping information to construct a powerful detector by using state-of-the-art learning methods. We also experiment with using only three keystrokes and find that the system still yields high accuracy while giving additional opportunities to make more decisions that can result in more accurate final decisions.

REFERENCES

[1] T. Mogg, "Study reveals americans lost $30 billion worth of mobile phones last year," Mar. 2012. [Online]. Available: http://www.digitaltrends.com/mobile/study- reveals-americans-lost-30-billion-of-mobile- phones-last-year/

[2] S. Watson, "Impostor fraud: A cyber risk management challenge," May 2015. [Online].Available: http://www.treasuryandrisk.com/2015/05/05/im postor-fraud-a-cyber-risk-management- challenge?slreturn=1485885396

[3] K. Knibbs, "Start memorizing your six-digit iPhone passcode," Sep. 2015. [Online]. Available:http://gizmodo.com/start- memorizing-your-six-digit-iphone-passcode- 1710072672

[4] Venkateswara Rao, P., Ramamohan Reddy, A., Sucharita, V.An approach of detecting white spot syndrome of peaneid SHRIMP using improved FCM with hybrid back propagation neural network, International Journal of Pharmacy and Technology, 2016, 8(4), pp. 22351–22363

[5] Sucharita, V., Venkateswara Rao, P., Bhattacharyya, D., Kim, T.-H. Classification penaeid prawn species using radial basis probabilistic neural networks and support vector machines International Journal of Bio-Science and Bio-Technology, 2016, 8(1), pp. 255–262

[6] Mandava Geetha Bhargava, Modugula TS Srinivasa Reddy, Shaik Shahbaz, P Venkateswara Rao, V Sucharita Potential of big data analytics in bio-medical and health care arena: An exploratory study, Global Journal of Computer Science and Technology 2017/8/5

[7] P. Venkateswara Rao , A. Ramamohan Reddy , V. Sucharita, Computer Aided Shrimp Disease Diagnosis in Aquaculture. International Journal for Research in Applied Science & Engineering Technology Volume 5 Issue II, February 2017 ISSN: 2321-9653

[8] D. Amitay, "Most common iPhone passcodes," Jun. 2011. [Online]. Available: http://danielamitay.com/blog/2011/6/13/most- common-iphone-passcodes