International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 5 | ISSN : 2456-3307

A Review on Dynamics Authentication in Touchscreen Mobile

M. F. Gaikwad*[1], Puja Kumbharde[2]
[1]Department of Information Technology, MCOERC ,University of Pune, Nashik,India
[2]Dr. D.Y. Patil College of Engineering, Pune, Nashik, India

ABSTRACT

This paper based on user interaction with touchscreens of mobile which is based on swipe gestures for personal authentication. There is an comparions of existing systems (based on SVM and GMM using selected features from the literature) exploiting independent processing of the swipes according to their orientation.By analysising the database user always sliding one finger on the screeen which having various behavioral patterns.Owing to the widespread use of touchscreen mobile devices, it is need for us to study the different techniques and their effectiveness in the area of touch dynamics biometrics. This paper provide some comparative analysis in the topic area with additional data acquisition protocols,data representation and decision making techniques.so we can understand differnet challenging issues.

Keywords: Active authentication, biometrics, smartphone, touchscreen, human computer interaction

I. INTRODUCTION

As Technology growing day by day in computing and communicational devices,the use of device shift from traditional desktop computers to mobile devicesAS usage of smart phone inceses it directly implies the increaseing of important of data base. The portability of mobile devices is responsible for vulnerable to theft.Data leakage and misuse of mobile device are potentially more valuable than device itself .There are some Knowledge-based authentication methods, like as pass- words, PINs or pattern locks which are some primary methods which are used for authentication of device.

All of thses methods are vulnerable to various of security threats or attacks, with addition brute force attacks , shoulder surfing , and smudge attacks.Higher level of authentication tends to decrese usability so to balance these conflict between security factor and usability, measures such as the delayed authen- tication.Still there is an issue to enhance done by physiological or behavioral characteristics like such as fingerprint, facial characteristics, and iris pattern.Behavioral biometrics acquired data from human behavior or habits like signature, voice, gait and keystroke dynamics. Authentication through Biometrics provides more security than other authentication methods as it cannot be lost or stolen as well it is hard to be forged. To make these methods more effective it should be secure as well as stable. As survey reports that Iris and voice biometrics authentication are more secure but gives less usability. That means these type of authentication gives either more security or usability. According to the survey results placed by **De Luca et al. (2015)**,important factor is which method is choice by person for mobile device for authentication which is the usability factor.There are some isuue related with biometrics authentication method first is low authentication speed and inconvenience and second is social awkwardness In first case of face biometrics, participants felt that it was difficult and time consuming to align the face correctly in front of the device's camera. In the case of fingerprint biometrics,

the par- ticipants felt that it was hard to scan a fingerprint properly when the fingers were too oily or dry, or when the device was covered with a protective casing. For the second issue (i.e. social awkwardness), for example, participants felt that it was awkward to hold a device in front of a face to perform an au- thentication task in a public area. This is more case in terms of mobile devices, because is used in public area mostly.

Touch dynamics is a behavioral biometrics, which cap- tures the way a person touches on a touchscreen device.like other biometrics data, touch dynamics biometrics can be used to identify a person/user, and can be used combination with a passcode which increse security in user authentication as well mobile devices. These methos is more cheaper than other biometrics authentication which gives feasibility to Owing to important person for usage of mobile activity **(Shen et al., 2016).** of touch dynamics biometrics, there have been increasing research efforts in this topic area, as shown in Fig. 1.

This paper discussing their major contributions and identifying issues for further research.The main contributions of this paper are Firstly, it presents a comprehensive survey of published works in the topic area of touch dynamics biometrics high- lighting their contributions and technological advances in the topic area. Secondly, it critically analyzes these related works from a range of perspectives, leading to the identification of knowledge gaps and issues for further research. Finally, the ref- erences cited in this paper provide a useful lead into this topic area.

In detail, the structure of the paper is as follows. Section 2 provides an overview of touch dynamics biometrics in general. Sections 3–8, respectively, compare the related works in terms of their experimental designs, data acquisition methods, feature selection strategies, decision making techniques, fusion approaches, and data adaptation approaches. Their performances are discussed in Section 9. The identified knowledge gaps and issues for further research are outlined in Section 10. Finally, Section 11 concludes the paper. To the best of our knowledge, there has not been a similar paper published in literature at the time of this writing.

II. TOUCH DYNAMICS BIOMETRICS

2.1. Overview

Touch dynamics biometrics is the process of measuring and assessing human being touch rhythm on touchscreen mobile devices (e.g. smartphones and digital tablets)When human interact with these devices a form of digital signatures is generated.These signatures are said to be discriminative and unique for each one,so it can be called as personal identifier. In the 1860s, telegraph method used for long distance communication, operators "identified" each other through telegraph keys (Bryan and Harter, 1897). Today, instead of telegraph keys we used computer keyboards, mobile keypads, and virtual keyboards. Late 20th century Computer keyboards used as common input device. And the human key board typing patterns are unique so it used as personal identifier.

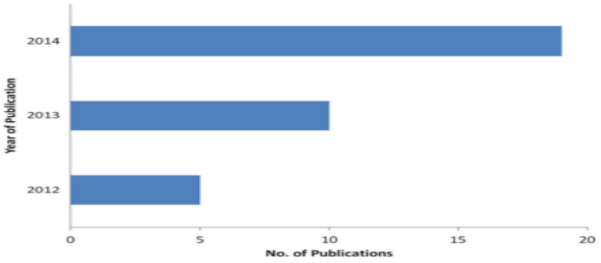

Figure 1. The increasing trend of research works on touch dynamics biometrics.

In 1980 Gaines et al.research on Keystroke dynamics authentication. They experiment to recognize 6 professional secretaries by analyzing the way they typed three passages of texts consisting of 300 to 400 words each. Crawford, Karnan et al. And Teh et al. have, independently, written surveys of the published works on keystroke dynamics authentication (Crawford, 2010; Karnan et al., 2011;

Teh et al., 2013). However, these early works largely focused on keystroke dynamics authentication on computer keyboards. as mobile communication technologies are growing ,more recent research focused on mobile devices with physical keypads (Campisi et al., 2009; Clarke and Furnell, 2007; McLoughlin and Naidu, 2009). Recently more reasearch going on touchscreen mobile devices. Fig. 2 summarizes the timelines of the touch dynamics biometrics research as influenced by technological developments in the sector.

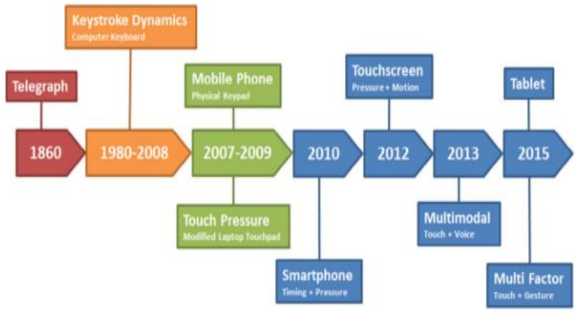

Figure 2. The evolution of touch dynamics biometrics research.

Touch dynamics biometrics having uniquness about its features but it having some challenging issues. The sections below summarize the merits and the challenging issues.

2.2. Features

A touch dynamics authentication system have some useful features as compare to the other types of biometrics authentication system. These are the following.

Distinctiveness: Touch dynamics patterns are capable of generating multi-dimensional features, such as timing, spatial and motion features. These multi-dimensional features can be measured up to a precision level that is significantly which is higher than human perception (Zheng et al., 2014).which makes difficult to replicate consistently, so can be used for authentication.

Enhanced Security: Excluding weakness feature, passcodes method mostly used for authentication (Schlöglhofer and Sametinger, 2012). By integrating touch dynamics biometricsmethos with passcode the overall assurance level can be increased.

Continuous Monitoring: Touch dynamics biometrics can be used for authenticity of a user as compare to previous authentication by constantly monitoring the user touch dynamics patterns. In other words, user reauthentication can be performed easily and non-intrusively throughout an active login session. In this way, security protection goes beyond initial login without compromising usability.

Revocability: In an event when a pass code associated with a touch dynamics template is compromised, a new touch dynamics template can easily be generated when a new pass code is created. This is not the case for other physiological biometrics. For example, with iris or face biometrics, once it is created, can't change it similarly for fingerprint once we generated can change maximum ten times. so there is an limited for updatation.

Non-dependency: A mobile device usually operates in an on-the-go manner, so the surrounding noise level continuously changing. So as comparison with other biometrics features, face and voice biometrics, more sensitive to environmental factors as compare to touch biometrics methods.so it is feasible to deployed into mobile device.

Transparency: For acquiring and processing of touch dynamics patterns there shopuild be littel or more additional interventions from a mobile device user while the user is using the device. Users may not be aware that their touch dynamics patterns are being captured,and this process happen periodically or they are protected by an extra layer of authentication. This is in a stark contrast to other biometrics authentication systems that usually require explicit alignment of a biometrics feature to a specific sensor.In the case of iris authentication, a user is required to look straight into a camera to take an iris

image, and in the case of fingerprint authentication, a user needs to put one of his/her fingers on the fingerprint sensor.

Familiarity: The process of authentication must be user friendly so the data so the data acquisition process have a gentler leraning curve with a higher usability level than other biometrics data acquisition cases.

Cost Effectivenes: iris and fingerprint biometrics methods required specialized hardware where touch dynamics authentication system only uses builtin mobile sensors. So it reduce the device cost so can deploy in arge scale.

2.3. Challenging issues

The design of a touch dynamics authentication system have a number of challenging issues as follows.

Minimizing Computation and Communication Costs: Computational capabilities of desktop computer are higher than mobile devices. Some criteria such as algorithm complexity, communication cost, and authentication delay these are important factors should be considered while designing touch dynamics authentication .we can say that algorithm and communication costs factors are responsible for deploying authentication in miminimal cost.

Minimizing Energy Consumption: Mobile devices are operated by batteries. The less the energy consumes, the device life increases. Communication process consume more battery(Perrucci et al., 2009),The number and usage frequencies of various sensors embedded in a mobile device, also effect on battery consumption. Power consumption of mobile device can be reducing by reducing the sample rate.

Maximizing Accuracy: The accuracy performance of touch dynamics authentication system is relatively low in comparison to other physiological biometrics authentication system (e.g. fingerprint and iris). This is because touch dynamics biometrics features (or feature data) acquired at different occasions are likely to exhibit a certain degree of variations due to external factors such as fatigue, mood, or distraction.

Adaptation Capability: Human behavioral characteristics change with time, and they usually change more frequently than physiological characteristics. So, touch dynamics patterns gradually change as the user more familiar with the passcode, input method, device, and other external factors. A touch dynamics authentication system adapt with changes in a user's touch dynamics pattern.

2.4. Operational process

A general touch dynamics authentication system is illustrated in Fig. 3. From the figure, we can see that the operation of this system can largely be captured in three major phases:

I. User Enrollment, where touch dynamics data (or samples) are capture, processed, and stored as a smaple.
II. User Authentication, where a touch dynamics test sample is compared against the stored reference template(s) to determine the similarity or dissimilarity
III. Data Retraining, where referncing sample updated by storing the latest touch dynamics data. The three operational phases are accomplished by a number of functional blocks (i.e. architectural components), each of which performs a well-defined function, and these components and their respective functions are described below.

2.4.1. Data acquisition

It's a first step in which raw touch dynamics data are acquired. This data set of no.of times input samples acquired periodically. Devices commonly used for data acquisition are commercial off-the-shelf smartphones (Buschek et al., 2015; Trojahn et al., 2013; Zheng et al., 2014) or, in some cases, digital tablets (Saravanan et al., 2014).

2.4.2. Data preprocessing

Data preprocessing is carried out to remove outliers in the raw data, improving data quality and accuracy performance. Techniques used in this operation include outlier detection and removal (Zheng et al., 2014). A dimension reduction technique may also be used to ensure that raw data remain small yet representable, for the sake of computational efficiency on resource limited mobile devices (de Mendizabal-Vazquez et al., 2014).

24.3. Feature extraction

Feature extraction is a mandatory operation that is carried out in both user enrollment and authentication phases. The main

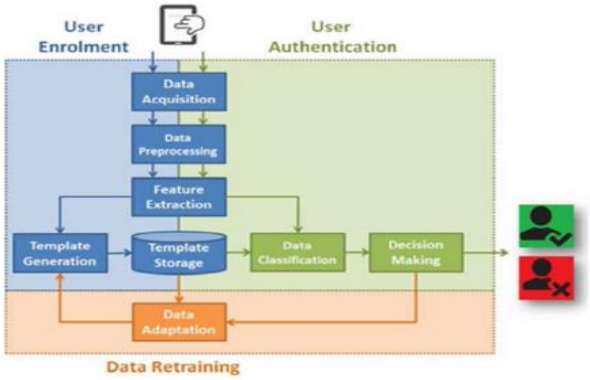

Figure 3. A touch dynamics authentication framework.

task of this operation is to identify and extract distinctive features common to a user from the acquired raw data. These features will be later used for template generation. Possible features extracted from human touch dynamics data can be categorized into three broad categories, namely timing, spatial and motion features.

2.4.4. Template generation

Template generation is an operation which represents outline of the user's touch dynamics characteristic.Normally, several different types of features are concatenated into a sequence of n-dimensional feature vectors, where n is the number of feature elements (Cai et al., 2013; Serwadda et al., 2013). These unique reference templates are then stored for user authentication or data retraining purpose.

2.4.5. Data classification

In Data classification data are categorized and compared against reference templates. The outcome of this phase is normally associated with a matching score used for decision making. Data classification is usually carried out using machine learning techniques.

2.4.6. Decision making

Decision making is an operation carried out to determine if the touch dynamics data submitted by a user are indeed originated from the target user. This decision is made by comparing the similarity or dissimilarity score generated from a machine learning technique against a predefined threshold (Bo et al., 2014; Kolly et al., 2012). Before the final decision is made, a fusion approach may be applied to combine either the information from multiple features (Buschek et al., 2015; Jeanjaitrong and Bhattarakosol, 2013) or to combine the matching scores from different machine learning techniques (Samura et al., 2014), to increase accuracy performance.

2.4.7. Data adaptation

Data adaptation is an operation update the sample template with the latest touch dynamics patterns from a user. because a user's touch dynamics patterns always change with time, causing the initially enrolled reference template to deviate from the most recent touch dynamics patterns from the same user. By adding an adaption component that performs the data adaptation operation after each successful authentication, these gradual changes can be captured and taken into account (Crawford et al., 2013).

2.5. Evaluation criteria

A touch dynamics authentication system chaving two modes a verification (or authentication) mode

and an identification (or recognition) mode. Each mode having different purposes and usage. The verification mode is used to verify a claimed identity. It is used to answer the question "is this person whom he/she claims to be". This mode is fit for authentication of a mobile user or a mobile device where identification mode is used to classify and identify some unknown identity. It is used to answer questions such as "who is this person" or "is this person in the database". This mode is typically used for forensic investigations or intrusion detections. As shown in Fig. 4, the fundamental difference between the two modes is that, in the verification mode, the checking between the touch dynamics data submitted by a user and the reference template is 1-to- 1, whereas, in the identification mode, this checking is 1-to many. According to our literature survey, the number of papers published on the study of the verification mode (74%) is much higher than the identification mode (26%). The focus of this paper is on authentication using touch dynamic biometrics, so hereafter our analysis is on the verification mode. To assess the suitability of a biometrics authentication method to real-world applications, three major criteria should be used to evaluate the system. These are verification accuracy, system efficiency, and system usability.

2.5.1. Verification accuracy

The metrics that are commonly used to evaluate the verification accuracy of a biometrics authentication method are the false rejection rate (FRR), false acceptance rate (FAR) and equal error rate (EER). The relationship among these metrics is shown in Fig. 5 and their definitions are given below.

2.5.1.1. False rejection rate (FRR).

This is the percentage ratio of the number of legitimate users who are falsely rejected against the total number of legitimate user trials. A lower FRR value indicates fewer legitimate users being falsely rejected. It also means that the system usability level is higher. FRR is also referred to as a false alarm rate, false negative rate, false non-match rate, or Type II error.

2.5.1.2. False acceptance rate (FAR).

This is the percentage ratio of the number of illegitimate users who are falsely accepted against the total number of illegitimate user trials. FAR reflects the ability of a non-authorized user to access the system, whether via zero-effort access attempts or deliberate spoofing or any other method of circumvention

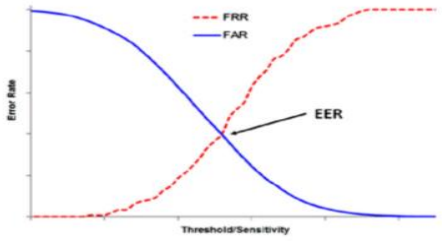

Figure 4. The relationship between the FRR, FAR, and EER.

Again, a lower FAR value indicates fewer illegitimate users being falsely accepted, and this also indicates that the system has a higher security level. FAR is also referred to as miss alarm rate, false positive rate, false match rate, or Type I error.

2.5.1.3. Equal error rate (EER).

EER is a single-number performance metric, which is commonly used to measure and compare the overall accuracy level of different biometrics authentication method. It is sometimes also referred to as crossover error rate (CER). EER can be obtained by finding the interception point of two graphs, one for FRR and the other for FAR. Typically, the lower the FRR and the FAR values, the lower the EER value, which in turn indicates a better accuracy performance of a biometrics authentication method. However, FRR and FAR are negatively correlated, so it is not possible to lower both FRR and FAR values at the same time. Therefore, in real-life applications, FRR and FAR are usually adjusted and determined based on the security and usability requirements of the applications. In some literature, the term "accuracy", rather than EER, is used as an accuracy performance

metric. It is worth noting that "accuracy" and EER are actually the same; "accuracy" is defined as the inverse of EER. In other words, a higher "accuracy" value indicates a better accuracy performance of a biometrics authentication method.

Figure 5. The ROC curves of three performance scenarios.

The accuracy performance can also be graphically visualized by using the receiver operating characteristic (ROC) curve as shown in Fig. 6. This graph is obtained by plotting genuine acceptance rate (GAR) against FAR at different matching threshold values. GAR is the percentage ratio between the correctly accepted legitimate users against the total number of legitimate user trials. It is also referred to as the inverse of FRR (100 FRR), true positive rate, or true match rate. A larger area under the curve (nearer the curve towards the top left corner of the graph) indicates a better performance.

2.5.2. System efficiency

The system efficiency refers to the computational cost or the authentication delays imposed by a biometrics authentica tion method. Satisfying this criterion is particularly important for computational resource-limited mobile devices. A complex authentication method may impose a higher level of computational overhead, increasing authentication delays and reducing system usability. Therefore, it is important to design authentication methods that introduce as low computational overhead as possible.

2.5.3. System usability

The system usability (or user acceptance) of an authentication system is also an important factor to the successful deployment of a new authentication method. Users will eventually abandon or reluctant to use any system that is tedious or slow to use, even if it can offer a higher level of security protection. Therefore, an authentication system should offer a good level of system usability and this can be achieved by (i) reducing the workload imposed on a user as much as possible, (ii) requiring users' intervention as less as possible, and (iii) making authentication delays as short as possible.

III. DECISION MAKING

Decision making is an operation carried out to determine if the touch dynamics patterns submitted by a subject have indeed originated from the target subject. This decision is made by comparing the similarity or dissimilarity score generated from a machine learning technique against a predefined threshold. A number of such techniques have been used in a touch dynamics research reported in literature, namely: (i) Probabilistic Modelling, (ii) Cluster Analysis, (iii) Decision Tree, (iv) Support Vector Machine, (v) Neural Network, (vi) Distance Measure, and (vii) Statistical. Fig. 15 summarizes the machine learning techniques against the number of papers that adopted them in touch dynamics research.

3.1Probabilistic modeling (PM)

The main idea behind the probabilistic modeling technique is to predict the likelihood of a given test sample belonging to a

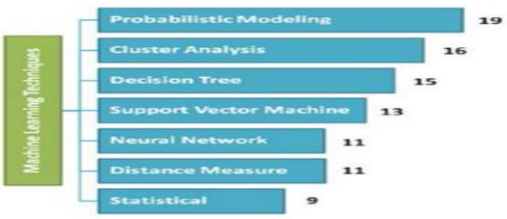

Figure 6. Machine learning techniques vs the number of papers that employed them.

particular subject using the prior probability calculated from training samples (touch dynamics data acquired during user enrollment phase). One widely used probabilistic modeling technique is the Bayesian Network. It uses an acyclic graph model to find the probabilistic relationship between parent and child node . For example, feature data from a reference template will be used as the parent node and the associated subject identity as a child node. Then, given a test sample (touch dynamics data acquired during user authentication phase), the intended child node is determined by the probability of the parent node. Other variants of the probabilistic modeling technique include the Naive Bayes and the Gaussian Probability Density Function.

Cluster analysis (CA)

The cluster analysis technique assumes that samples belonging to the same subject have similar properties . The goal is to group sample with similar properties to form a homogeneous cluster. Then the label of a test sample is decided by the degree of proximity toward a cluster . Samples from different clusters are highly dissimilar but very similar among the samples in the same cluster. There are variants of the cluster analysis technique, including the K-means K-Star and k-Nearest Neighbors (k-NN).

Decision tree (DT)

The decision tree technique is popular and used in many areas. It is well known for its low computational complexity . This technique is particularly suitable for classification problems that involve a small number of output labels. For example, in the case of touch dynamics authentication, it
is often used to check whether a test sample is legitimate or not. The main objective of these techniques is to create a tree-like model that predicts the class label of a given test sample based on previously known training samples. A decision tree is constructed by continuously splitting feature data into subsets so that the information gain ratio at each node of the tree is maximized. This iterative process stops when a node has only a single label, or when further splitting a tree node no longer provides additional information gain. The RF differs from the J48 in that it adds a randomized procedure in the process of splitting each tree node The experimental results reported in Feng et al. (2013) and Serwadda et al. (2013) show that the RF performs better than the J48 in classifying subject touch dynamics patterns. However, it requires a longer time to formulate a decision tree .When using a decision tree technique, considerations should be given to prevent over-fitting the tree, which could result in a higher level of computational complexity and a lower level of performance.

Support vector machine (SVM)

The support vector machine is another technique commonly used in many biometrics studies. The fundamental concept of this technique is to first determine how two classes of feature data differ from each other and then create a boundary that best separate them. Having this boundary, subsequent test samples can be classified as either legitimate or illegitimate according to which side of the boundary they are located. The search for this boundary can be performed within a 2-dimensional hyperplane using a linear kernel (separating) function. However, distinguishing the touch dynamics patterns between legitimate and illegitimate subjects are non-linear in nature (Xu et al., 2014). A non-linear kernel function such as Radial Basis Function can be used to map feature data onto a higher dimensional feature space to create more complex boundaries that can optimally split both classes (i.e. legitimate and illegitimate). As a result, it can more accurately determine which side of the feature space a test sample belongs.

Neural network (NN)

The neural network technique simulates the information processing structure of biological neurons. Typically, a neural network architecture consists of three interconnected layers (the input,

hidden and output layer). To start with, the feature data from all subjects are fed into the input layer of the network

as a set of neurons. An activation function is used to assign weights to each neuron. Then the information of the activated neurons is passed from one to another within the hidden layer. This process iterates until an output is produced. Finally, based on the output values, a learning process is used to update the weights of each neuron in the hidden layer to improve the network. Some commonly used neural network techniques are Radial Basis Function networks (RBFN) and Multi-Layer Perceptron (MLP) neural network generally produces a higher level of accuracy in identifying a subject but is more computationally expensive (Draffin et al., 2014) and more time consuming to be used (de Mendizabal-Vazquez et al., 2014). According to Kambourakis et al. (2014), it is impractical to run on mobile devices with less than 512MB of memory.

Distance measure (DM)

The distance measure technique calculates a dissimilarity or similarity score between a test sample and the training sample of a given subject. The score is then compared against a threshold to determine if the test sample belongs to the target subject.

Statistical (ST)

There are several statistical techniques that have been used in biometrics research. These techniques include the mean and standard deviation and the deviation tolerance.There are a number of advantages associated with these techniques. For example, in comparison with the techniques discussed above, they are less complex and easy to implement, cost less computational time, and consume less resource such as battery power. These advantages are important for resource-limited mobile devices.

IV. FUSION

Fusion is an approach used to combine information from multiple sources to improve the accuracy performance of a biometrics authentication method. The multiple sources may be from multiple features or by using multiple machine learning techniques. The information from these sources may be combined at three different stages, which are, respectively, referred to as (i) feature level fusion, (ii) score level fusion, and (iii) decision level fusion.

4.1.Feature level fusion (FLF)

The feature level fusion is the most used fusion approach in touch dynamics research. The fusion approach involves concatenating more than one feature data into a single feature vector and is performed before the template generation or the data classification operation. Fusion may be performed on feature data acquired from the same or different sensors . Although feature level fusion is simple to implement and it enables the utilization of additional properties of multiple feature data, it can result in an overly large joint feature vector known as the curse of dimensionality. Some machine learning techniques, such as decision tree, may not work well with a high dimensional feature vector. Therefore, the number of feature data fused may influence the selection of machine learning technique.

4.2. Score level fusion (SLF)

The score level fusion, unlike the feature level fusion, is performed after the data classification operation. For example, in Samura et al. (2014), two different machine learning techniques (the Weighted Euclidean Distance and the Array Disorder) were used independently on one set of feature data, resulting in two matching scores, one from each machine learning technique. The two scores are then combined into a single score for decision making. Methods such as the sum, weightedsum, or product rules are commonly used to combine multiple scores . If the scores from different machine learning

techniques are no1t comparable, they will need to be normalized prior to fusion

4.3 Decision level fusion (DLF)

The decision level fusion is the least complex among the three fusion approaches. It requires minimum changes being applied to the internal structure of each data classification algorithm. Fusion is performed by combining decisions (accept or reject) made by multiple machine learning techniques using voting rules, such as the AND or OR rules .

V. DATA ADAPTATION

Human touch dynamics, unlike physiological biometrics (e.g. fingerprint or iris), are not permanent and are likely to evolve over time. After some time, a subject's reference template (generated using samples acquired during enrolment phase) may no longer reflect the subject's most recent touch dynamics patterns. One way to deal with this issue is by introducing an adaptation component. The component uses the most recent touch dynamics patterns to update the reference template of the subject, allowing gradual adjustment of the reference template based on the touch dynamics pattern changes. To control unintended or unnecessary changes imposed on a reference template, two different policies can be used (Crawford et al., 2013), e.g., selecting samples from different input instances or mixing the most recent samples with a portion of the existing template samples. These policies can reduce the effect of short-term pattern changes of the legitimate subjects or prevent unauthorized modifications made to reference template by the illegitimate subjects. Although the adaptation component requires additional computation time and resource, if implemented correctly, it may not degrade device performance, reduce battery life span or affect usage experience. For example, an adaptation module can be executed during the period when the execution of the component have the least effect on a device.

VI. CONCLUSIONS

Touch dynamics biometrics have promising potentials to strengthen the security of mobile devices or on-line services accessible via mobile devices without additional hardware requirements. The availability of various sensors in recent mobile devices provides added opportunities for such potentials to be explored. This paper gives a comprehensive review of the re search work or efforts made on touch dynamics biometrics on mobile devices. The paper first provides an overview, outlines the primary operational process and defines a set of criteria for the evaluation, of a touch dynamics authentication system. Then it presents detailed implementations, experimental settings, and approaches of each of the process, namely, data acquisition, feature extraction, and decision making. Next, the performances reported in published work have been discussed. Finally, it discusses open issues in the topic area and recommends areas for further research. The review presented in this paper may provide a roadmap and stimulate further research in this area.

VII. REFERENCES

[1]. Prof. Abdulsalam H, Skillicorn DB, Martin P. Classification using streaming random forests. IEEE Trans Knowl Data Eng 2011;23:22–36. doi:10.1109/TKDE.2010.36.

[2]. Alghamdi SJ, Elrefaei LA. 2015. Dynamic user verification using touch keystroke based on medians vector proximity. Presented at the 2015 7th International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN), pp. 121–6. doi:10.1109/CICSyN.2015.31.

[3]. Alotaibi N, Bruno EP, Coakley M, Gazarov A, Monaco V, Winard S, et al., 2014. Text input biometric system design for handheld devices. Proceedings of Student-Faculty Research Day. pp. B7.1–8.

[4]. Antal M, Szabó LZ. 2014. Keystroke dynamics on Android platform. Proceedings of the 8th International Conference Interdisciplinarity in Engineering, INTER-ENG 2014, Romania, pp. 131–6.

[5]. Antal M, Szabó Z-L. 2015. An evaluation of one-class and two class classification algorithms for keystroke dynamics authentication on mobile devices. doi:10.1109/CSCS.2015.16.

[6]. Aviv AJ, Sapp B, Blaze M, Smith JM. 2012. Practicality of accelerometer side channels on smartphones. Proceedings of the 28th Annual Computer Security Applications Conference, ACSAC '12. ACM, New York, NY, USA, pp. 41–50. doi:10.1145/ 2420950.2420957.

[7]. Babaeizadeh M, Bakhtiari M, Maarof MA. Authentication method through keystrokes measurement of mobile users in cloud environment. Int J Adv Soft Comput Appl 2014;6:94–112.

[8]. Bartlow N, Cukic B. 2006. Evaluating the reliability of credential hardening through keystroke dynamics. 17th International Symposium on Software Reliability Engineering, 2006, pp. 117–26. doi:10.1109/ISSRE.2006.25.

[9]. Bellinger C, Sharma S, Japkowicz N. 2012. One-class versus binary classification: which and When? Presented at the 2012 11th International Conference on Machine Learning and Applications (ICMLA), pp. 102–6. doi:10.1109/ICMLA.2012.212.

[10]. Bo C, Zhang L, Jung T, Han J, Li X-Y, Wang Y. 2014. Continuous user identification via touch and movement behavioral biometrics. IEEE International Performance Computing and Communications Conference (IPCCC), 2014, pp. 1–8. doi:10.1109/PCCC.2014.7017067.

[11]. Bond WF, Ahmed Awad EA. 2015. Touch-based static authentication using a virtual grid. Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security, IH&MMSec '15. ACM, New York,NY,USA,pp.129–34.doi:10.1145/2756601.2756602.