Abstract—Mobile devices nowadays contain a variety of personal or even business-related information that is worth being protected from unauthorized access. Owners of such devices should use a passcode or unlock pattern to secure such important assets, but since these techniques are being perceived as annoying barriers, locked devices are not standard. But even if such authentication mechanisms are used, they are very easy to circumvent. Biometric methods are promising applications to secure mobile devices in an user-friendly, discreet way. Based on embedded sensors like gyroscope, accelerometer or microphones, which are state-of-the-art sensors for mobile devices, behavioral biometric approaches appear even more attractive for user verification than physiological methods like fingerprints or face recognition. So far many biometric approaches have been presented. After a short overview of relevant representatives, we discuss these methods based on their applicability and limitations. Our findings are summarized and presented as a roadmap to provide a foundation for future research.

I. INTRODUCTION

Over the last decade, policies that allow employees to use their private (mobile) devices for accessing privileged and work-related assets have been adopted by a growing number of companies. These policies, also referred to as 'Bring your own device' (BYOD), are meant to increase the flexibility and productivity of the employees. While this might be the case in terms of infrastructure related investments and flexibility in general, these new paradigms come at a price: Incidents like e.g. the loss of mobile devices may include the loss of valuable privileged company information and - if the worst comes to the worst - unauthorized disclosure of the same. Common authentication methods like passcodes or visual patterns on mobile devices may be evaded by an attacker or may even not be in place at the time a device is lost or unattended. Moreover, these authentication methods are only performed once in a session, leaving mobile devices vulnerable to attackers who get intentionally unlocked units into their possession. Biometric authentication methods are becoming more popular as alternative or addition to passcodes. For example Apple takes advantage of biometrical approaches by using fingerprints as authenticators. Fingerprint scans are always with you, unique and easy to use. The Touch ID sensor under the Home button of the iPhone 5s [1] makes it possible to read fingerprints and automatically unlock the device. Physical biometric traits [2] based on anatomical or physiological characteristics of people also include iris or face recognition. Behavioral modalities [2] in contrast to fingerprint recognition require subjects to perform a specific activity over time, like gait or keystroke recognition. At the time of this writing, biometric systems available on the market are based almost exclusively on physiological biometric traits.

Modern mobile phones and tablets are equipped with a growing number of sensors [3] such as accelerometer, ambient light sensor, Bluetooth, camera, digital compass, gyroscope, GPS, proximity sensor, microphone, touchscreen or WiFi. Such sources are predestined for behavioral verification, as these sensors turn into gateways, allowing individuals to connect and interact with their devices [4]. Extracted data can be used for implicit user authentication, adding further protection against unauthorized access to sensitive information. Such approaches could provide continuous authentication and detect interaction attempts from unauthorized individuals. The advantage of this solution is that no additional biometric sensors are necessary and weaknesses of passcodes or patterns can be eliminated or at least mitigated.

The main contribution of this paper is to present an overview of biometric traits that can be used to secure mobile devices. The focus lies on new biometric methods, which act invisible and continuous in the background. Part of this work is the discussion and presentation of mobile device limitations as well as challenges that arise based on biometric traits and user performance. Possible approaches using embedded mobile device sensors are categorized and introduced. Finally our findings are summarized as a roadmap.

The remainder of this paper is structured as follows: We present biometric approaches used in combination with mobile devices in section II. In section III, existing limitations and considerations are discussed based on their category. Further, a representation of our roadmap is given. Section IV contains our findings as well as the conclusion and outlook of future work.

II. BIOMETRIC METHODS AND MOBILE DEVICES

In this section we describe continuous biometric methods used to authenticate authorized mobile device users. It should aim experts from academia, business and non-governmental organizations to broaden the knowledge-base of biometrics and mobile security. We are aware that our review cannot cover all work done in the area and thus, we aim at identifying major representatives in this research domain by our search process. In order to perform the search we decided to use the digital libraries of ACM, IEEE and Springerlink. Additionally we investigated the bibliography of existing literature for more taxonomies to establish the state-of-the-art.

Biometric research work is done in the area of face-,
fingerprints-, gait-, keystroke-, speaker-, gesture- and hand movement recognition. But when it comes to continuous authentication, behavioral features are used. In the opposite of physical biometric traits which involve anatomical or physiological characteristics like face-, fingerprint- or iris recognition rather than learned behavior, behavioral biometric modalities require subjects to be active. They must perform certain activities, which are learned and acquired over time like trait or keystroke dynamics. [2] In the following physiological biometric approaches are not discussed, the main focus lies on methods which can be applied to continuous verification. These methods can be divided into the following main-classes based on the sensors which collect the biometric features: Keyboard-based approaches, touchscreen-based approaches, accelerometer-based approaches, gyroscope-based approaches and hybrid approaches.

A. Keyboard-based Authentication

Saevanee et al [5], [6] introduce an approach to analyze the behavioral manners of users interacting with a Synaptic touchpad that is able to detect the fingerprint pressure and key stroke dynamics which can be divided into the inter-keytime (duration of interval between two successive keys) and hold-time. The results have shown that finger pressure is a discriminative information rich of content to authenticate users with an accuracy rate of 99%. Matching was performed with the k-NN analytical method based on data collected from 10 volunteers.

Differences between a 12-key and a QWERTZ-layout as an application for biometric authentication is discussed by Trojahn et al [7]. Features like the pressure during typing, size of the finger, the direct position of the finger to the key, orientation of the keyboard and angle of the device were extracted. Distance measures, neural networks and a Bayesian classifier were used for classification. During their experimental setup with 35 participants they focused on two different scenarios. One scenario is a numerical (PIN) and the other is an alphabetic (password) input for mobile phones. The average FAR (False Acceptance Rate)/FRR (False Rejection Rate) for numeric input with a 12 key-layout are 9.04% and 6.66%, with a QWERTZ 12.13% and 8.75%. The average FAR/FRR of the second scenario with a 12 key-layout are 8.31% and 5.26%, with a QWERTZ 9.53% and 5.88%.

Buchoux et al [8] implement a two-factor authentication based on PIN and an additional keystroke analysis during the login process. To achieve this, key events and inter-key latencies are captured. For classification, the Euclidean and Mahalanobis distance as well as the Feed-Forward Multi-Layered Perceptron (FF MLP) neural network are used. A group of 20 participants helped to evaluate the implementation. With statistical classifiers such an approach is adaptable for mobile devices, but a 4-digit PIN is too short to get reliable results.

Another method to authenticate users based on their keystroke behavior is presented by Zahid et al [9]. For identification features like the key hold time, digraph, and error rate are used. The key hold time defines the difference between pressing a key and releasing it, the digraph time the difference between releasing one key and pressing the next one. The error rate is the number of times the backspace key is pressed. For classification Particle Swarm Optimization (PSO) and Genetic Algorithms (GAs) are applied to adapt to the dynamically varying user keystroke behavior. In total, data of 25 phone users was collected and analyzed. Their proposed system achieved an average error rate of 2%. The error rate of rejecting authorized users has dropped to zero after PIN verification mode.

B. Touchscreen-based Authentication

De Luca et al [10] introduce an implicit biometric authentication approach that aims to enhance the Android login procedure. The way a user performs the password pattern or the unlock screen is used as an additional security feature. The authors developed an Android application with four different unlock screens (horizontal, vertical, vertical with two fingers, diagonal unlock) as well as password patterns to collect user data and evaluate their approach. Every 9 to 12 milliseconds, the application logged the following data available from the touchscreen: pressure, size, x/y coordinates and time. Feature analysis is done by dynamic time warping (DTW) to distinguish between different participants. The results show the feasibility of their approach. The authors conclusion is the more data points a data set consists of, the easier it is to make a valid decision. Better results were achieved by using password patterns with an average accuracy of 77%.

In [11] the authors present a novel multi-touch gesture-based authentication technique. Therefore, a comprehensive set of five-finger and palm touch gestures are extracted. An iPad application was developed which has the capability to track up to 5 points at a time. The x/y coordinates of the touch point trajectory, time stamp, touch order (of the different fingertips), touch sequence, and touch type are sequentially captured by the device. To verify the input of the user all the touch points need to be ordered in a consistent manner. After normalization of the fingertip trails or rather touch sequences a Dynamic Time Warping algorithm is used to compute the distance between the stored template and the captured multi-touch gesture. Finally, a dissimilarity score is calculated to accept or reject a user. The touch events are captured in the range of 20-30 per second. The authors achieved a 90% accuracy rate based on 34 participants with single gestures. Using multiple gestures, an improvement of 5% can be performed.

Angulo et al [12] developed an Android application to collect
Another accelerometer-based approach is described by Boyle et al [18], using wavelet transform to extract features from raw acceleration data. The data was classified using k-nearest-neighbor, achieving classification rates above 90%. They carried out 5 experiments using 2 to 4 test subjects who completed the training phase by walking at a constant pace in a controlled environment.

**D. Gyroscope-based Approaches**

Gyro-based approaches are based on the assumption that users have unique ways of holding their mobile devices in their hands while interacting with them. In their paper, Lin et al [19] propose an authentication method based on the collection of up-down flicks and left-right flicks retrieved from the gyroscope sensor. Their approach achieved an EER of about 6.85% using a test group of 20 participants. They extracted pitch (y-axis), roll (z-axis), azimuth (x-axis) and a combination of pitch and roll as their features and further applied statistical analysis (avg, max, min, range, std. deviation) to the following feature types: absolute coordinate, velocity and acceleration, resulting in a total count of 53 features.

**E. Hybrid Approaches**

In [20], [21], a notion of an implicit authentication approach is introduced. According to these publications, user models are generated based on recent behavior patterns. By means of a scoring algorithm, a measured score indicates the likelihood that the device is in the right hands. To validate their notion they performed experiments using the Blackberry platform. Amongst others following information was recorded during these experiments: emails, calls, SMSs, location, contacts, calendar, tasks, memos, alerts, battery level, power on/off, SD card removal/insertions, etc. For email activity, the following data is concerned to be worth further analysis: new email detection, opening/closing email messages, adding/removing email messages to/from folders, creation and sending of new email messages as well as types and file extensions of email attachments.

SenSec [22] is a mobile system framework using passive sensors like accelerometers, gyroscope, orientation sensors and magnetometer to construct a gesture model of users to provide user authentication and anomaly detection. Gesture patterns are modeled through a continuous n-gram language model. SenSec achieves an accuracy of 75% in users classification and 71.3% in detection non-owners. 20 participants from different demographic groups were recruited to evaluate the framework. The application produces 4 samples per second featuring 12 real valued readings, including Accelerometer (x, y, z), Orientation (Azimuth, Pitch, Roll), Compass (x, y, z), and Gyroscope (x, y, z). Each feature vector consists of statistical values including Root Mean-Square, Root Mean-Square error, minimum value, maximum value, average sample-by-sample change, number of local peaks, etc. to capture micro movements. This data is used in combination with a K-means clustering algorithm to classify people and to build behavioral n-gram model and a sureness score to enable user authentication.

SenGuard [23] is a mobile user identification management solution that provides continuous and implicit user authentication services on a mobile system based on voice, location, multitouch, and locomotion. Each modality happens at certain time and has its own specific duty cycles. For

---

Nickel et al [16] introduced a biometric gait recognition approach to authenticate users via their mobile phones accelerometer. The samples gathered from 36 test subjects were classified using k-nearest-neighbor. To extract the features, x-, y- and z-direction, as well as magnitude vectors were collected and transformed using statistical analysis. They showed that their algorithm performs well in a controlled environment while leaving open eventual external influences. The lowest EER/HTER was between 8.24 and 8.85%, based on 5 minutes of enrollment.

In [17], Tanviruzzaman et al propose an adaptive authentication process using gait recognition and location tracks. For the gait recognition part, Fast Dynamic Time Warping (FastDTW) was used to compute similarity scores between the samples. They further took data retrieved via Assisted Global Positioning System (A-GPS) into account in order to relate the extracted gait pattern to the geographical location of the user. References regarding the number of test subjects, recognition rates and features are not explicitly mentioned.

Another accelerometer-based approach is described by Boyle et al [13], Frank et al propose a set of 30 behavioral touch features like coordinates of two end-points, median velocity of the five last points, stroke duration or the length of trajectory. They designed an experiment to collect the touch behavior of 41 subjects to evaluate their proof-of-concept framework using a k-nearest neighbor and a Gaussian rbf kernel support vector machine as classifiers. Equal Error Rates between 0% and 4% were achieved.

FAST (Fingergestures Authentication System using Touch-screen) [14] is a novel touchscreen based authentication approach on Android mobile devices introduced by Feng et al. Besides extracting touch data from a touchscreen like above-mentioned approaches, FAST complements and validates this data using a digital sensor glove with IMU digital combo boards. The system gathers information like gesture type, x/y coordinates, directions of the finger motion, finger motion speed, pressure at each sampled touch point and the distance between multi-touch points. To classify the extracted data following classification algorithms are used: Decision Trees, Random Forest and Bayes Net Classifier. The evaluation process with 40 users achieves a False Accept Rate (FAR) of 4.66% and a False Reject Rate of 0.13% for continuous post-login user authentication.

A new biometric identification method for intelligent mobile devices is introduced in [15] by analyzing the users input patterns on touchscreen. Features which are extracted are finger touch duration, pressure level and the touching width of the finger. They implemented a Back Propagation Neural network (BPN) as learning algorithm which is a pattern recognition method that uses the Least Squares Method (LSM). For evaluation input pattern data of 50 individuals is used. The results show "that this method effectively identifies users with near a 100% rate of accuracy" [15].
example, accelerometer based user identification is triggered when user is walking, while voice based user identification is in place when human voice is detected around the phone. They pointed out that SenGuard is not designed to differentiate every person in the world. If SenGuard is insufficient, active user authentication is the last line of defense.

Saevane et al [24] investigate behavioral profiling, keystroke dynamics and linguistic profiling as biometric modalities for continuous authentication. Text messaging can be used to model an user profile. Therefore, information based on text log is used like receivers telephone number and location of texting. In the analytical process, Feed-Forward Multilayer Perception Neural Network was used for classification. For analysis of keystroke dynamics the hold time and in total five letters (e, t, a, o and n) were used. Inter-key time, the latency between five pair of letters: t, g, e, p, e, m, h, d and a m were calculated. Once again, Feed Forward Multilayer Perception Neural Network (FF-MLP) was used for classification. For linguistic profiling a total of 64 discriminating characteristics were extracted for example, average word length (number of characters), total number of sentences, total number of symbols etc. To create a user profile, t-test ranking measure were applied to rank input features according to their discriminative capability. For analysis, the Radial Basis function (RBF) neural network algorithm is used. Fusion experiments like simple sum and weight average are used based on data of 30 participants. "The results demonstrate the utility of using multimodal biometric systems for achieving better matching performance than single modal system" [24].

Conti et al [25] introduce the movement process which is performed from the moment initiating a call by pressing the phone button until holding the phone to the ear as a biometric feature using the accelerometer and orientation sensor of an Android phone. For similarity measurements Dynamic Time Warping Distance (DTW-D) and Dynamic Time Warping Similarity (DTW-S) are used. To test their application, data of 10 test users was collected. They applied DTW-D and DTW-S algorithms first on the collected accelerometer data and then on orientation data and obtained an Impostor Pass Rate (IPR) of 4.5% for a single method (i.e. DTW-D on orientation data), as well as a FAR of some 9.5%. Using combined methods based on boolean and normalized combinations they could observe an improvement of these rates, resulting in an IPR of 2.5%, and a FAR of about 8%, thus reducing again IPR by about 2% and FAR by 1.5%. The movement during phone calls has turned out to be a distinguishable feature.

III. RESEARCH AGENDA FOR CONTINUOUS BIOMETRIC AUTHENTICATION METHODS FOR MOBILE DEVICES

Despite differences between various modalities, biometric processes have much in common, starting with the initial enrollment and the biometric recognition mechanism for user verification. To develop new approaches, data has to be collected from participants first. Unique features have to be identified. Based on pattern recognition and classifiers, matching can be made. For implementing continuous biometric authentication approaches on mobile devices, a variety of additional challenges and limitations may occur.

A. Data Collection

Unfortunately, there are no databases of user samples available which contain data stored from accelerometer, gyroscope, touchscreen, keyboard and geomagnetic sensor, so it is necessary to collect data for this research purpose. Therefore, time should be spent for the user study design. One possibility to get data is to ask participants to perform a set of tasks like mobile web browsing or entering sentences using virtual touch keyboards over a predefined period of time. Before the experiment starts, it is possible to inform the subjects in detail or to maintain silence about the real purpose of the study to avoid affecting their natural behavior. Asking volunteers to perform a special way of acting in a controlled environment will also influence their behavior.

Another way of gathering data is to implement the invisible data collection processes on mobile phones. Such data will provide insights into the users everyday life over a period of time. In literature different periods of time are used for the collection process, 2 days [10] as well as 2 weeks [21] were mentioned. Furthermore, care should be taken to have different groups of the population properly represented by gender and age for data collection. The usage of mobile devices is highly dependent on exercise and handling this technology.
B. Architectural Structure

Continuous authentication almost always increases the power consumption of mobile devices. Background services that gather and analyze data, put additional load to the processor and storage, preventing them from taking advantage of built-in powersaving features when the device is in IDLE mode. Also, sensors that operate using wireless data transmission as e.g. GPS or WiFi are known to drain the battery as soon as they are activated, resulting in most users having such features turned off for the sake of extended battery life. One of the design goals of mobile applications, including continuous authentication services, should therefore be power efficiency if applicable.

To deal with power efficiency considerations, Wang et al [26] introduce an extended set of sensor parameters, including sensor sleeping duration (sensor offline time) and sensor sampling duration (sensor online time). This results in so called sensor duty cycles that effectively reduce the power consumption of these sensors while only providing periodic instead of "real" continuous sampling. Concluding their findings, periodic sensor sampling will provide a better user experience in terms of battery life, but it is up to developers and researchers to evaluate appropriate duty cycles to fit their respective biometric traits as well as eventual machine learning approaches.

To implement techniques like continuous authentication, an engine responsible for gathering and evaluating sensor data must be running even if the main application window has been backgrounded by the user. In Android this is achieved by running this code as a (background) service. When it comes to iOS, comparable programming models like services are not available. Apples’ iOS allows only specific app types to run in background without being suspended from the operating system, these apps are audio players and recorders, location based apps, Voice over Internet Protocol apps, download content regularly and apps which are connected to external accessories. [27] This restriction has been lifted with the introduction of the iPhone M7 motion co-processor, which polls all motion-related sensor input and provides a framework for fore- and background applications. Another advantage of the co-processor is the fact that other parts of the phone may stay in IDLE state while motion data is acquired, resulting in lower power consumption. Touchscreen related data is not covered by this framework.

Keystroke information, which could be collected from integrated virtual keyboards, is not directly accessible in iOS and Android. This can be circumvented by providing a third-party keyboard which collaborates with the continuous authentication service and delivers keystroke behavior to the same. Such data has to be stored and processed on the phone itself to protect valuable sensitive information. We insistently advise against processing such data in online environments as e.g. through cloud services, since this could leak sensitive information to unauthorized third parties and therefore would compromise the users security and privacy. Biometric templates should be stored within the (sandboxed) application storage area instead of shared storage (e.g. SD cards). This prevents other applications from accessing valuable information and mitigates the risk of an attacker replacing such reference templates by simply replacing external media.

An additional challenge which occurs is the accessibility of continuous features. For example in Androids’ Honeycomb and Ice Cream Sandwich an accessibility service was able to sense touch event locations in every application. Changes of API’s now prevent the access to this data.

C. Biometric Features and Classification

Through the possibility of running continuous authentication as a background service, user data can be gathered in an unconscious way. Generic features have to be identified to enable a platform independent usage of such services. For silent user identification Bo et al [28] introduce the SilentSense framework which combines touch behavior of an user and micro-movement of the device. A joint analysis of interacting features from both touching behavior (pressure, area, duration, position) and the reaction of the device (acceleration and rotation) makes the approach feasible for user verification. They highlight the challenges which arise through normal behavior changes like for example walking while typing. Therefore connections between single features have to be concerned. Different users have different mobility traces or interacting behavior depend on the environment (home or work), so it could be interesting to include sensory data such as GPS or device movements for more accuracy. Hybrid methods has shown to be more attractive for continuous user verification. The first authentication step after data collection is to interpolate raw data to a fixed sampling rate which is not given. Afterward a normalization step is necessary. To separate normalized data into parts for classifiers a sliding window approach with overlapping rectangular windows can be used.

For pattern recognition purpose different approaches could be identified in literature like Dynamic Time Warping, Random Forest machine learning classifier, Bayesian classifier, KNN or one-class SVM. For verification based on multiple biometric traits (gait, movement, touch, keystroke) a weighted multi-level classifier should be used instead of one single classifier to aggregate results from multiple sensors. Additionally it has to be mentioned that the system has to handle missing information because of sensor failure.

IV. Conclusion

In this paper we presented existing biometric approaches available for continuous verification on mobile devices. We discussed limitations and challenges which has to be handled during the development process. Further, architectural considerations have been explained in detail. For continuous verification it is important to develop an background service. Therefore, developers have to be aware that not every feature is available. For example touchscreen data outside an application is not available.

Furthermore, a combination of biometric traits like gait-, keystroke-, gesture- and hand movement appears very suitable for continuous verification. Therefore, the changing user behavior has to be considered. Feature selection and combination appears as the most challenging task. User behavior models which contain multiple features of user’s action and device reaction as well as the verification strategy should be planned very well.
ACKNOWLEDGMENT

This work has been supported by the Austrian Research Promotion Agency (FFG) under the Austrian Security Research Programme KIRAS.

REFERENCES