# Smart AppStore: Expanding the Frontiers of Smartphone Ecosystems

**Félix Gómez Mármol**

*NEC Laboratories Europe*

**Gregor Rozinaj**

*Slovak University of Technology*

**Sebastian Schumann and Ondrej Lábaj**

*Slovak Telekom*

**Juraj Kačur**

*Slovak University of Technology*

***Smart AppStore offers five important features for today's smartphone users: biometric authentication, multilevel authorization, gesture recognition and navigation, user-tailored reputation scores, and identity management.***

Mobile ecosystems comprised of smartphones and tablets have experienced unprecedented growth in the past decade due to their permanent Internet connection, ease of use, and affordable prices. They are no longer mere devices for making and receiving calls and exchanging SMS messages: a plethora of applications have emerged, offering a broad range of services. The most common distribution channel for these apps are the so called 'appstores'. Until now, appstores belonged primarily to the smartphones' realm, but with the explosion of interconnected smart devices (such as smart TVs and other electrical appliances), the appstore customer base is expanding.

Within the context of HBB-Next (www.hbb-next.eu), a European research project aimed at taking the smart TV's user experience to a higher level, we investigated a new Smart AppStore model. In contrast to traditional appstores, which are usually tied to a specific platform or ecosystem, the applications offered through the Smart AppStore, which use the HBB-TV standard,[1] can run on any device able to launch a browser with CE-HTML capabilities. In this sense, the Smart AppStore is device-agnostic: it is irrelevant whether users consume applications through their smart TVs, smartphones, or tablets, regardless of the operating system. Moreover, the Smart AppStore is not bound to any specific vendor.

Traditional appstores have put considerable effort into blocking malware,[2,3] while many times neglecting aspects such as usability for users' authentication or applications' authorization rights, amongst others. We believe that proper attention to these commonly overlooked features is crucial for widespread acceptance of any appstore by end users, and this constitutes

a central Smart AppStore goal. A survey conducted by Katholieke Universiteit Leuven as part of HBB-Next validated this approach, finding that our Smart AppStore prototype beat out Xbox's current appstore in terms of ease of navigation and usability as well as perceived security.[4]

# Smart AppStore: A Novel User Experience

A simple example illustrates the Smart AppStore user experience.

In the comfort of their living room, Alice, Bob, and their young son Charlie simultaneously access the Smart AppStore to find some new apps to install and enjoy. Alice feels more comfortable using her smartphone, while Bob prefers their brand-new smart TV and Charlie his beloved tablet.

Since none of them is logged in the system so far, the Smart AppStore presents each app along with a generic reputation score that does not consider user preferences. As Figure 1 shows, a webcam (such as the one installed in Kinect) connected to the home gateway works in the background, recognizing the users in the room and creating a list of current active users or users' group profiles.

After a while, Alice finds an app that could help Charlie learn foreign languages while watching his favorite cartoons; the family decides to install it. To do so, they must first log in to Smart AppStore in one of two main ways:

- Follow the traditional username/password process. In this case, the family would face the tedious task of entering both a username and password for the selected profile (either individual or group) via the remote control. In the best case, they could use a keyboard paired with the smart TV, or even the tablet or smartphone. A written gesture recognition approach might work, too.[5]

- Enjoy Smart AppStore's biometric authentication. By making a simple gesture—such as waving his hand, which the webcam captures and the gesture recognition and navigation module in Smart AppStore analyzes—Bob triggers the process to display the previously generated list of active profiles. In this case, the Smart AppStore shows the individual profiles of Alice, Bob and Charlie, as well as the group profile "Family" (since all users comprising this group are present in the room).

Upon selection of the Family group profile, a combination of voice and 3D facial recognition mechanisms launch in parallel in the background. As soon as the system identifies both Alice, Bob and Charlie with a level of confidence determined by the multilevel authentication module, the Smart AppStore retrieves the required profile attributes from the identity management (IdM) module to complete the login process.

Once Alice, Bob, and Charlie are logged in with the Family group profile, the Smart AppStore updates the reputation scores associated with each app to present user-tailored values. The

system obtains these customized reputation scores by giving a higher weight to recommendations coming from other profiles (users or groups of users) similar to the Family one for preferences related to applications' price, usability, and so on.

According to the user-tailored reputation scores, the app that Alice selected is even better ranked, which reinforces the family's decision to install it. Should this be a free app, installation would happen immediately. However, the app for learning foreign languages while watching cartoons has an associated cost. In this case, a last authentication step consisting of entering a PIN is required to authorize the app's installation.

Once the app has been purchased and installed, Charlie can enjoy it while watching cartoons on the smartphone, tablet, or smart TV. Alice and Bob are quite satisfied with the app and decide to rate it, uploading their feedback into Smart AppStore either via the remote control or with the commodity of certain specific gestures (thumbs up, thumbs down). Smart AppStore stores the recommendation and uses it to update the app's reputation score.

# Biometric Authentication

The Smart AppStore's biometric authentication module recognizes several physical traits that are unique or distinctive to an individual. There is an obvious benefit in using biometric signals: there is no need to remember multiple access passwords, and usually a person's physical presence in front of sensors is sufficient. Depending on the features, the acquiring method might be more or less intrusive, demanding different levels of interaction. Each individual possesses many physical traits, so a good trait must be unique, stable, simple to acquire, robust against different types of noise, and limited to a feasible number. Today, the most common biometric modalities are iris images, 2D and 3D face images, fingerprints and speech. We focus here on speaker, face, and iris recognition.

## Speaker recognition

We can organize the general problem of speaker recognition into several categories: speaker identification versus speaker authentication, text-dependent and text-independent identification, level of extracted features, and the classification method used, just to name a few. Current systems usually achieve 90 to 95 percent accuracy rates for text-independent scenarios and 94 to 98 percent for text-dependent ones.

In real conditions, speech is prone to intersession variations (training and testing mismatches) and intrasession variations (changes in voice), and can be affected by the presence of ambient noise. To adjust for these factors, researchers use various compensation and normalization techniques such as cepstral mean subtraction, power normalization, Gaussianization, feature warping, and model mapping. Among the most popular classification techniques used in speaker recognition are *K*-nearest neighbors (KNN), which searches through all training samples and finds the best matches; the Gaussian mixture model (GMM), a generative classification method

that describes feature space in a probabilistic way; and the support vector machine (SVM), a discriminative approach that uses a hyperplane for optimal discrimination.[6]

## Face recognition

Face recognition is becoming more popular and is often used in authentication, surveillance, and database retrieval systems. Common 2D face recognition systems achieve roughly 90 percent accuracy rates in controlled environments, but this number rapidly drops in real-life conditions.[7]

Current systems apply several approaches that we can divide into three classes: local (local face features), holistic (whole faces), and hybrid methods (combination of both). The recognition process starts with a face localization that is usually followed by a preprocessing to eliminate any training–testing mismatches. Next, image features containing user identity are extracted, usually via Eigen vectors based on principal component analysis (PCA) and its variations such as block PCA, kernel PCA (KPCA), generalized linear discriminant analysis (GDA), and local binary patterns (LBPs). These features preserve person-specific information and suppress the training–testing mismatch. In the final stage of facial recognition, two discriminative classification methods are very successful, i.e. support vector machines in combination with kernels, and neural networks represented either by multilayer perceptron or radial basis functions.

3D facial recognition uses the depth *z*-axis to get complete geometrical information. Usually, the depth is acquired by measuring the reflected infrared light. Sometimes, the beam can absorbed or reflected, thus a hole-filling algorithm smoothes the final surface. The 3D processing is very similar to what happens in 2D systems, so the recognition process applies the same methods as in 2D case. Usually once the faces are localized, face-tracking algorithms are used in order to reduce a computational load,

## Iris recognition

The iris is one of the most discriminative traits as it fulfills two crucial requirements—uniqueness and stability. Iris-based identification consists of iris localization, feature extraction and classification. One of the most successful systems uses Gabor filters for feature extraction, with the filtrated signals quantized in two levels. This procedure leads to features that are strings of binary digits. Then, recognition is simply performed by matching the closest samples using the KNN method and a hamming distance. Although this approach achieves 100 percent accuracy in controlled environments the remaining work is in the localization and normalization phase for real life scenarios.

# Multilevel Authorization

Because multiple users can access Smart AppStore from one device or use more than one type of device, the system includes a multilevel authorization module that enforces adaptive access control rules with different levels of security for different users based on their profile. Paid apps

are linked with a higher authorization level that has more access rights. Thus, in our scenario Alice and Bob as parents are allowed to install applications, but Charlie is not. Moreover, depending on whether Charlie is present in the room, Smart AppStore can decide which sensitive data to show on the TV screen.

The multilevel authorization module deals with these varying confidentiality requirements through multiple biometric modalities in combination with password and PIN methods.[8] Whenever there is a request to access Smart AppStore or install a chosen app, it uses voice and face recognition to identify the user. Depending on the outcome of this process, it may allow access to Smart AppStore or request the person to enter certain information—for example, a username and password when installing free apps and a PIN when installing paid apps. In the future, iris recognition could replace the PIN method and thus improve security and the overall user experience.

Smart AppStore periodically checks whether a user it has authorized is still present, and if anyone else is in the room. If another identified person appears in front of the smart TV screen, for example, the authorization module will reevaluate access control rules based on the new person's relationship with the previously authorized user. Relations among users are important, especially when sensitive personal or payment data is being accessed from the TV screen and the system detects more than one user. If an unidentified person is in the room, the rules for logging in might be even stricter.

## Gesture Recognition and Navigation

Several gesture recognition and navigation applications have been developed within the context of HBB-Next. Here, we present the finger-observing method, which uses convexity defect detection around the palm area.

Finding the hand's coordinates using the algorithm implemented in Kinect is relatively inaccurate given the detection problems between the palm's opening and closing. Therefore, we developed a new method to find the middle point of the palm. Localization of the palm helps determine center contours, which are ultimately the center of the palm, no matter whether it is open or closed. The precise localization of the palm is a crucial point for finger detection.

To find and calculate convexity defects, we used a standard function. Finding the starting point, the deepest point, and the end point helps us localize convexity defects, which is important for open finger counting. By modifying this method with certain thresholds, we can eliminate false detections and obtain only finger detections rather than false convexity defects. For gesture recognition, we introduced three sets of gestures (static, dynamic, and swiped), based on our own developed original algorithms. We have integrated all three sets of gestures into one gesture environment. This fact results in an easier and better recognition of all gestures in a natural and convenient application.

# User-Tailored Reputation Scores

Whereas different website services commonly personalize their offerings, reputation scores computed by traditional appstores typically neglect users' individual tastes or preferences. Smart AppStore disrupts this outdated model and provides user-tailored reputation scores for each app.

By introducing HTML apps in smart TVs, HBB-TV fosters the proliferation of application repositories in this new environment. Moreover, as in many other ecosystems where appstores have existed for some time (smartphones, for instance), reputation management is an effective and powerful tool for discovering those apps that users find to be useful (or not) or contain suspicious or malicious code.

Those reputation engines integrated in appstores today are not flexible and provide the same scores to every user, regardless of individual preferences for usability, responsiveness, price, and so on. As part of HBB-Next, we developed a novel reputation computation engine[9] that addresses these shortcomings and offers user-tailored reputation scores. This customization is achieved by giving a higher weight to feedback from users with similar preferences for HBB-TV apps.

Specifically, we compute the customized reputation score of a given app $App_i$ for a particular user $u_k$ as follows:

$$Rep_{u_k}(App_i) = \frac{\sum_{j=1}^{n}\left(W_{u_j} \cdot sim_{u_i,u_j} \cdot feedback_{u_j}(App_i)\right)}{\sum_{j=1}^{n}\left(W_{u_j} \cdot sim_{u_i,u_j}\right)}$$

where $W_{u_j} \in [0,1]$ represents the reliability of user $u_j$ when providing feedback, $sim_{u_i,u_j} \in [0,1]$ represents the similarity between user $u_k$ and $u_j$ (measured as the similarity/deviation of their respective preferences), and $feedback_{u_j}(App_i) \in [0,1]$ represents the feedback value given by user $u_j$ to the application $App_i$.

# Identity Management

IdM is generally responsible for managing appstore users. The Smart AppStore's IdM module supports multidevice access and is able to manage users, devices and services. Identity information in current systems is often limited to single subscribers, but IdM in the Smart AppStore (developed within the HBB-Next project) contains basic information about all users, security credentials, and *contexts*—connections between users and their devices.

Besides being a user repository for the HBB-Next system architecture, the IdM module manages several contexts. Especially in a mobile environment, users want adaptive behavior, identification, and preferences based on various parameters for several contexts. Utilization of

the presented concept can be applied in evaluating parameters that describe these contexts, such as location, background noise etc. These frequently changing parameters can be gathered from technical user equipment, e.g., users' mobile phones. Other parameters that do not describe the user's world, but the technical environment (e.g. speed or means of network connectivity) can also contribute to describing the context.. The IdM module is also useful for interpreting the user's current environment by analyzing and relating parameters from multiple devices and having them act as implicit user identifiers and keys for relations (for example, "find all users in one location without prior connections between them").

The IdM module not only stores and manages identity information, but also interprets and enhances it, transforming itself from being a mere user database to an enabler. An example is the normalization process of multimodal probabilities that has been performed for the Smart AppStore of the HBB-Next project: The multimodal interface collects these values over a predefined time span, and the IdM module receives them, but also processes them and calculates an average.

The managed contexts are temporary and independent relations of users and devices, and act as an enabler for dynamic adaptive personalization. They represent groups of users that consume content or interact together with their HBB-Next devices. While the traditional HBB-TV model limits the use of contexts because of the static environment (for example, the living room), mobile environments that are location independent extend usability and thus the potential of a contextually aware IdM enabler. Contexts can not only be built by linking devices and users (as done in the HBB-Next project), but also by taking environmental parameters, such as location, surroundings or localization into account.

Contexts can exist over a long period of time, even without active users. Smart AppStore distinguishes defined contexts ("usual contexts") and contexts based on what is currently happening ("active contexts"). The number of users and devices in a context is not limited. A context is not made up of just users or devices, but instead is a user–device relation. Mobility introduces scenarios where various contexts have the same user–device relations, with minor differences in location, creating the need to adapt the data that the IdM module exposes differently for the same group of people.

Smart AppStore's IdM module normalizes the multimodal interface's parameters to determine a user's actual availability and thus define the current context. For interaction and integration with other enablers (for example, to store data with Smart AppStore or normalize recognition data with the multimodal interface), the IdM module provides a RESTful API.[10]

**D**espite the number of advanced features integrated in our Smart AppStore prototype, further research is required in the field of biometric authentication, specifically in noisy environments. Moreover, the latest biometric traits for mobile devices, such as typing speed and browsing patterns, also need further exploration. We are currently investigating a method to dynamically select the most suitable reputation computation engine based on current system conditions and

expected performance measurements.

The multilevel authorization module needs to be extended for biometric methods and to consider advanced solutions such as usage control for mobile devices.[11] Finally, we plan to extend the IdM module to handle anonymous users, who can both partake in a context as well as gather identity information that can be part of calculated group profiles.

## Acknowledgments

*We express our gratitude to Ginés Dólera Tormo, Michael Probst, and Diana Escribano Henarejos, who contributed to the success of this article. This research has been partially funded by the Next-Generation Hybrid Broadcast Broadband (HBBNEXT) EU research project, FP7-ICT-2011.1.5, grant no. 287848.*

## References

1. *ETSI TS 102 796 v1.2.1, Hybrid Broadcast Broadband TV*, European Telecommunications Standards Inst., 2012; www.etsi.org/deliver/etsi_ts/102700_102799/102796/01.02.01_60/ts_102796v010201p.pdf.
2. D. Damopoulos et al., "Exposing Mobile Malware from the Inside (or What Is Your Mobile App Really Doing?)," *Peer-to-Peer Networking and Applications*, Dec. 2012; doi: 10.1007/s12083-012-0179-x.
3. D. Damopoulos, G. Kambourakis, and S. Gritzalis, "iSAM: An iPhone Stealth Airborne Malware," *Proc. 26th IFIP TC 11 Int'l Information Security Conf.* (SEC 11), 2011, pp. 17–28; doi: 10.1007/978-3-642-21424-0_2.
4. J. Vanattenhoven and B. Stockleben, "D2.3.2: 2nd Report on User Validation Results," HBB-Next, 2013; http://ec.europa.eu/information_society/apps/projects/logos/8/287848/080/deliverables/001_HBBNEXTD232.pdf.
5. K.Jelemenská and P. Čičák, "Touch Screen Input Shapes Recognition in PN Designer," *Proc. World Conf. Educational Multimedia, Hypermedia & Telecommunications* (ED-MEDIA 12), 2012, pp. 1418–1423.
6. T. Kinnunen and H. Li, "An Overview of Text-Independent Speaker Recognition: From Features to Supervectors," *Speech Comm.*, vol. 52, no. 1, 2010, pp. 12–40.
7. M. Oravec et al., "Face Recognition in Ideal and Noisy Conditions Using Support Vector Machines, PCA and LDA," *Face Recognition*, M. Oravec, ed., InTech, 2010, pp. 125–150.
8. J. Matejka et al., "Security Aspects of Hybrid Broadband Broadcast Communication," *Proc. 55th Int'l Symp. ELMAR*, 2013, pp. 223–226.
9. G. Dólera Tormo, F. Gómez Mármol, and G. Martínez Pérez, "Towards the Integration of Reputation Management in OpenID," *Computer Standards & Interfaces*, vol. 36, no. 3, 2014, pp. 438–453; doi: 10.1016/j.csi.2013.08.018.
10. R. Thomas Fielding and R.N. Taylor, "Architectural Styles and the Design of Network-Based Software Architectures," PhD dissertation, Dept. Information and Computer Science, Univ. of California, Irvine, 2000.
11. G. Bai et al., "Context-Aware Usage Control for Android," *Proc. 6th Int'l ICST Conf.* (SecureComm 10), 2010, pp. 326–343.

***Félix Gómez Mármol*** *is a senior researcher in the Security Group at NEC Laboratories Europe, Heidelberg, Germany. His research interests include authorization, authentication, and trust management in distributed and heterogeneous systems; security management in mobile devices; and design and implementation of security solutions for mobile and heterogeneous environments. Gómez Mármol received a PhD in computer engineering from the University of Murcia, Spain. Contact him at felix.gomez-marmol@neclab.eu.*

***Gregor Rozinaj*** *is a lecturer in the Department of Telecommunications at Slovak University of Technology, Bratislava. Slovakia. His research interests include speech recognition, automatic ship control, and telecommunications. Rozinaj received a PhD and habilitation in telecommunications from Slovak University of Technology. He has received CEng from IET, United Kingdom. Contact him at gregor.rozinaj@stuba.sk.*

***Sebastian Schumann*** *is a senior designer working in the Application and Platform Innovation department at Slovak Telekom. His lead expertise is the evolution of communication services, with a focus on IP-based telecommunications platforms and their convergence within the ever-growing competitive service market. Schumann received a Dipl.-Inf. (FH) degree from the Deutsche Telekom University of Applied Sciences in Leipzig, Germany. Contact him at sebastian.schumann@telekom.sk.*

***Ondrej Lábaj*** *works as a solution architect in the Service Innovation department at Slovak Telekom. His responsibilities include technical design of multimedia platforms and services in fixed and mobile networks, with a focus on application security, identity and trust. Lábaj received a MSc in telecommunicationsfrom Slovak University of Technology. Contact him at ondrej.labaj@telekom.sk.*

***Juraj Kacur*** *is an assistant professor in the Department of Telecommunications at Slovak University of Technology. His research activities include digital speech processing, speech recognition, speech detection, speaker identification, high-order statistics, wavelet transformation, classification theory, neural networks, and hidden markov mdels. Kacur received a PhD in signal processing from Slovak University of Technology. Contact him at kacur@ktl.elf.stuba.sk.*