Face-based Passive Customer Identification Combined with Multimodal Context-aware Payment Authorization: Evaluation at Point of Sale

Adam Wójtowicz and Jacek Chmielewski

Department of Information Technology, Poznań University of Economics and Business,
al. Niepodległości 10, 61-875 Poznan, Poland

Keywords: Context-aware Authorization, Payment Authorization, Passive Identification, Multimodal Authorization, Face Recognition.

Abstract: In smart environments, fast passive transaction authorization is a key requirement for routine, recurring transactions. In our earlier work technical feasibility of multimodal multidevice system based on context-aware payment authorization model has been proved. Its main features are: passive user identification with face recognition followed by multi-criteria selection of transaction authorization methods, which jointly modify traditional customer service procedure. In the presented work, real-world evaluation of the new approach based on proposed multimodal payment authorization is described. Empirical tests at existing point of sale have been performed, the usage data have been collected, statistically analyzed and confronted with formulated research hypotheses. The research goal is to determine to what extent the approach simplifies payment process assuming the security level required for a given context is maintained. The evaluation confirms that proposed approach can be effective in a real environment.

1 INTRODUCTION

Nowadays a great percentage of payments is made online, without physical presence at a brick-and-mortar point of sale (PoS). However, there is still a need to perform in-person transactions as one moves through a city: a morning coffee on a way to work, a quick snack at a vending machine, products at a local grocery store, fuel at a gas station, etc. The most convenient payment method is payment with contactless card. For payments below a certain amount, the client only has to take out the card and hold it for a second above a terminal. However, this payment method has its drawbacks: for higher amounts it requires knowledge-based authorization – i.e. PIN, and the client still needs to find her wallet, take out the card and use it on the terminal. This inconvenience is especially significant for recurring transactions, where small annoyances add up over time. In this work recurring transaction is defined as a payment performed by a client multiple times in similar timespans (e.g. daily, specific days of a week), in the same place (particularly, authorizing multiple small orders during single visit) or at the same vendor (but at a different location), and for a similar amount.

In work presented in (Wójtowicz and Chmielewski, 2017) it is assumed that multiple devices (mobile or stationary, client's or seller's) can be used contextually to simplify the payment process as much as possible, optimally to make it fully passive, while maintaining the necessary security level. The system takes advantage of the ability to recognize the context in which users perform various transactions, which is unique to pervasive environments. In order to dynamically determine the optimal trade-off between security and convenience, context-based risk and trust assessment model has been developed. The focus is especially on routine, recurring transactions that constitute patterns of payments for transaction history of almost all users of pervasive environments. The simplification of the payment process concerns reducing the execution time of the process and minimizing the number of operations required to be performed by the client. The system potentially introduces added value for all actors of the process: payment operator (PO), seller (service provider), and the end-user.

By providing end-users and sellers with trusted and effective payment service, the PO reduces security concerns from all sides and can attract newcomers. The tool for dynamic assessment of the type of payment (routine / non-routine) goes beyond the model adopted for contactless payment cards (hard limit quota). By using the transaction context and dy-

Wójtowicz, A. and Chmielewski, J.
Face-based Passive Customer Identification Combined with Multimodal Context-aware Payment Authorization: Evaluation at Point of Sale.
DOI: 10.5220/0006798105550566
In *Proceedings of the 20th International Conference on Enterprise Information Systems (ICEIS 2018)*, pages 555-566
ISBN: 978-989-758-298-1

namically assessing payment risk level and trustworthiness of the participants, the system dynamically selects the most appropriate authorization methods of the payment. Rules for dynamic selection take into account the various authorization methods supported by client devices, as well as methods supported by other devices in the end-user environment, e.g. passive face recognition at a seller's location. It is possible to use multiple authorization methods simultaneously, which, if necessary, allows for greater authorization robustness. All this enables a controlled balance between security and convenience of payment for the client and the seller. On the other hand, contrary to proprietary approaches, the assumption of the openness is not violated in the proposed approach. The functionalities of sellers' and PO's services are not coupled together, thus competition between different sellers is possible which can leverage quality of services within the whole PO network.

From the point of view of the seller, the key advantage is the fact that the customer has to be identified for the purpose of payment at the beginning of the transaction. This information may be used to introduce improvements in the customer service process. By moving the moment of identification to the beginning of the service process and by providing the seller's sales / loyalty system with information about customer identification, it becomes possible to use a wide range of tools to support personalized service regardless of the knowledge and memory of individual employees serving clients.

Most of all, introducing the presented approach is beneficial for the end customer. She gains on every functional element of the system. Starting with fast and convenient realization of routine payments and the ability to use convenient authorization methods for non-routine payments, to full personalization of service and automation of loyalty procedures. In the routine payment scenario, the client orders products, receives the merchandise and leaves without having to search for any attribute necessary to authorize the payment.

This work focuses on the analysis of the customer benefits. The significant element of this work is the evaluation of the proposed approach with empirical tests in a real environment. The evaluation is based on a system for which technical feasibility, design and implementation is discussed in (Wójtowicz and Chmielewski, 2017). Evaluation scenario employs the system servicing regular transactions at PoS of existing retailer. In the data analysis activities, usage data are confronted with four research hypotheses related to security and convenience attributes of the approach.

The paper is composed of five main sections. Section 1 is an introduction to the research problem and proposed solution. Section 2 provides background information on existing payment solutions and on user identification based on face biometrics. Section 3 summarizes functionalities arising from the adopted business scenario, that guide the design of the proposed solution. Section 4 delivers details on the system evaluation, along with posed hypotheses and experiment design. Section 5 contains comprehensive evaluation results. The final Section 6 concludes the evaluation and the whole article.

2 RELATED WORK

2.1 Passive Payments in Pervasive Environments

Making user environment pervasive implies that it becomes aware of when and how its services are used. This enables supporting the users with automation of routine tasks and procedures. For example the smart city infrastructure can be used to identify citizen intentions and run operations such as user authentication in the background, even without explicit actions performed by the citizen. The presented research is focused on a particular type of background operations – automatic payments, which are a crucial feature of pervasive environments or smart cities. This feature will be increasingly used for billing users for the use of city infrastructure, goods or services. This includes services such as "smart parking", bridge toll collection, or public transport.

First "smart parking" systems were composed of parking stations broadcasting wireless signals to specialized transponders installed in cars (Hassett, 1994). The transponder had to be activated manually to start deducting an amount specified by the parking station periodically. It was not fully passive for a driver, however more convenient than cash payments at a parking station. With the growth of smart city infrastructure (e.g. an optical wireless sensor network (Chinrungrueng et al., 2007) or RFID-based solutions (Mainetti et al., 2015)) it is possible to automatically detect when a car stops at a particular parking spot and when it leaves, thus enabling full automation of parking payments.

Similar technologies are used for road toll collection. In such a case there is a need to identify a vehicle crossing a specific point. This identification can be done automatically with the use of RF identifiers installed in vehicles (Al-Ghawi et al., 2016) or by optical recognition of car plates (Ta et al., 2015). From the point of view of the driver, she simply drives through the toll collection point and her account is debited automatically. Such systems can be further enhanced with sensor fusion, for example to collect toll based on the number of occupants in the vehicle (Nakagawa, 2015a) or to become multi-purpose traffic management solutions (He et al., 2015).

The problem of enabling automatic payments becomes more complex, when there is a need to identify humans, not just objects such as car. An example of such case is public transport, where each passenger should be ticketed according to her travel. Many existing solutions require the use of contactless chip cards or smartphone applications – both of which require active participation of the passenger in the ticketing process (Nakagawa, 2015b). A fully passive ticketing solutions, so called implicit ticketing, is possible with BLE (Bluetooth Low Energy) technology, where the passenger only needs to carry a special BLE token or a capable smartphone and the payment is performed in the background (Narzt et al., 2015)(Narzt et al., 2016).

The concept of passive transactions can be exploited also in the context of citizens using city services not related directly to the city infrastructure, for example: ordering services or documents at a municipal office or buying products or services at a local retail store. One of notable examples of automatic payment systems in the retail domain is Google Hands Free (Google, 2015b) proposed by Google. The Hands Free application uses Bluetooth Low Energy, WiFi, location services, and other sensors on the user's device to detect user presence near PoS. This enables the user to pay hands-free, without getting out the smartphone or opening the application. During the transaction, verbal declaration of participation is required from the user (the system is not fully passive), and identity verification with initials and profile photo from the cashier. Google is also running early experiments using automated facial identification to further simplify the checkout process with in-store camera.

The payment system that is based on facial recognition to larger extent, called Zero-Effort Payments (ZEP), has been proposed recently in (Smowton et al., 2014), where authors interestingly discuss system evaluation results. The face identification results are promising, but the recognition is human assisted, i.e. a ranking of 5 most probable identities is presented to the human operator and he/she manually chooses the right one. The recognition process demands a heavy computational load since a number of faces are tracked at given moment. Also authors point out the low face recognition accuracy without supporting localization device. In their system BLE localization devices are used to significantly reduce the face recognition error rate. Therefore, it must be noticed that both Google Hands Free and ZEP are not deviceless systems, i.e. although a user does not need to manipulate with her device during the payment process, she needs to carry switched on device during identification and customer service.

Also Uniqul system (Anh Tran et al., 2016) has been deployed to provide fully deviceless payments authorized with user face image. However, it requires the user to type a PIN number when face identification has a low confidence level or tap the confirmation button on the in-shop tablet in the opposite case. Therefore, it cannot be considered as fully passive approach from the end-user perspective.

There are also payment systems based on face recognition that utilize end-user smartphone camera. MasterCard has proposed a simple to use mobile solution (Bowyer, 2015) that allows customers to authenticate their online purchases using their own face images. It refers to the selfie phenomenon, which is natural for a number of end-users. The application verifies image authenticity by detecting eyes blinking during image acquisition. MasterCard's approach is designed for online shopping, not brick-and-mortar trade. Contrarily, Lucova, using BLE technology proposes a system called FreshX (Lucnova, 2015) that also is based on selfie face image authorization, however it is dedicated for brick-and-mortar cafeterias. Such approaches, although natural, are neither deviceless nor passive, and security concerns can be serious.

There is a number of research and industry effort related to seamless payments focused on other biometrics than face, e.g. fingerprints, or palm recognition. For instance Liquid Pay(LiquidPay, 2015) identifies customers by their fingerprints and, for extra security, by veins and electrical signals emitted by the human body. It has been installed in restaurants, fitness clubs and theme parks. Payment systems based on the Fujitsu PalmSecure technology (Fujitsu, 2011) recognizing vein patterns in whole palm are being tested by (Biyo, 2014) or (Lee, 2015) in many cafeterias. However, those technologies, although deviceless, stable and relatively mature, cannot be perceived as passive.

Also, there are significant advancements in the field of NFC-based contactless payments for EMV smart cards that have become de facto standard (Alliance, 2012) for low-risk transaction authorization in brick-and-mortar retail trade. Nowadays, this technology migrates from smartcard to mobile device as a carrier. Mobile services and application such as Apple Pay (Apple, 2014), Samsung Pay (Samsung, 2015) or Android Pay (Google, 2015a) have been proposed to allow smartphone users for transaction authorization with their devices. However, these solutions mimic traditional card-based payments and are neither deviceless nor passive.

As a result of the research reported in (Wójtowicz and Chmielewski, 2017), a transaction system that is fully hands-free and does not require explicit user actions for routine payments has been proposed. Similarly to automatic toll collection where one just drives through a tunnel and her account is debited in the background one just places the order and leaves with the merchandise and the payment is performed in the background. All this in a deviceless manner – based on the optical recognition of customers using face biometrics. The goal of this work is to present the results of the quantitative evaluation of the proposed approach.

2.2 Face Biometrics for User Identification

Face biometrics gains popularity due to availability of high resolution cameras, increasing computational power of image processing devices and development of pattern recognition and machine learning algorithms. Because of its naturality face biometrics is more acceptable for end-users than many other biometric methods, but, on the other hand, the ability to collect face images without user acceptance may raise privacy concerns.

Generally, face recognition, as in the case of other biometric systems, consists of three main steps: acquisition of biometric data with a sensor, converting the data into a digital template, and comparison of the template with a reference template. In various approaches recognition can be based on a single image, image sequence, 3D image, or near-infrared / thermogram image.

Usually, face recognition is preceded by face detection and image segmentation, which are aimed at cropping face image from a larger image. Image segmentation can be performed automatically: either based on knowledge about specific image features that are common for human faces, or, in case of image sequences, based on human body movement features, that allow for detection of so called skeleton and face localization relative to the skeleton.

After segmentation, the face is recognized by comparison against an image base. Applying face recognition to user identification requires using less accurate one-to-many comparison model, as opposed to one-to-one model useful for user verification. In various approaches to face recognition, algorithms are based either on vectors describing whole face images or face geometry. In the former algorithm group, the reduction of face image representation to vectors is performed in order to preserve the information reflecting specific face features and to reject the noise resulting from e.g. variable lighting. Consequently, a face image is represented as a linear combination of simplified base images, namely Eigenfaces. These methods can be either global (indivisible face), or local (distinct representation for different face regions). In turn, the geometry-based algorithms from the latter group are able to represent geometrical relations between selected details (e.g. eyes and mouth) and to mutually compare whole details sets. Hybrid approaches combining both face features and face geometry are also developed.

There are three main groups of research challenges related to face recognition (Bolle et al., 2013), i.e. variation of face shape, variation of face acquisition geometry and variation of face acquisition conditions. Variation of face shape includes short-term variations related to speaking process or emotion expression, as well as long term variations related to ageing, putting on weight, injuries, make-up, facial hair, haircut and using wearables (glasses, hats). Variation of acquisition geometry results from variable distance (scale) and orientation of the face relative to the camera. Variation of face acquisition conditions is related to variable camera parameters (e.g. white balance, noise reduction, etc.) and also to variable environment conditions (variable or uneven lighting, occlusions).

3 PROPERTIES OF EVALUATED APPROACH

In the proposed approach, distributed architecture with components localized both at the client side and at the PO side, and to some extent also at the seller side, is assumed. On the client side BYOD model is assumed, so on this side only software that integrates with client devices is required. At the seller side hardware-software solution has been designed enabling the identification of clients and the use of a universal API for integration with sales/loyalty system of the seller. At the PO side there is a set of software modules that represent the main elements of the system logic. It is assumed that the software is running on infrastructure of the PO and is available remotely through a secured communication channel. Low-level description of components and technical feasibility of a system being an implementation of the presented approach, is presented in the work (Wójtowicz and Chmielewski, 2017).

3.1 Payment Automation

The idea of payment automation involves freeing the customer from the necessity of performing any active operations related to the payment and transferring decisions and handling of the payment process to the side of PO. Obviously, this should not deprive the customer of the control over her own resources, thus the automation should require prior approval from the customer. Payments automation requires interaction between the seller's and the PO's systems. The seller's system must inform the operator's system to initiate the payment (whom and how much to charge) and at the same time, the operator's system must properly inform the seller's system of acceptance or rejection of the payment. Detailed data flow model and communication protocol are elaborated in (Wójtowicz and Chmielewski, 2017). What is important, it should be possible to maintain the customer identification procedure on the side of the PO, which acts as a "trusted third-party" in the customer–seller relation.

The postulated payment automation should only be used for routine payments – i.e., recurring payments that meet certain patterns and seller-client trust requirements. In practice, the scope and characteristics of applicable patterns and requirements will be different for different POs – depending on their expectations and the data they process. There is no way to permanently define the thresholds for such requirements, because in practice they may be different for each customer-seller pair and also they may change over time. Therefore, it is assumed that values of parameters describing a payment, which include: level of seller's trust to the client, level of client's trust to the seller, and transaction risk level, are provided by external systems of the PO (fraud detection system, client profiling systems, etc.). Consequently, it is necessary to use a mechanism that will dynamically evaluate the parameters for a particular payment, and based on an extensible set of rules will determine whether the payment can be classified as routine or not, and if not, which authorization methods should be allowed to make sure the required security level is maintained. The mechanism takes into account various trust/risk requirements for biometric-based, possession-based and knowledge-based authorization methods, for active and passive methods, for methods based on client and seller infrastructure, and various convenience levels of the particular authorization methods.

3.2 Passive Customer Identification

To enable full payment automation it is necessary to use passive customer identification based on detection of the presence of a particular person at a particular location. Detection of the presence of a person may rely on what the person has (an object), or who she is (biometrics). The third option, based on what the person knows (the knowledge), is not applicable here, because it requires an active participation of the identified person. The passive identification based on objects can be performed, for example, by the use of radio identifiers (Bluetooth beacon technology). However, this approach assumes that the person identified will always have to carry a relevant object. Passive method of identification, which seems to be the best to use in the scenario under consideration, is therefore biometrics. Face recognition is the biometric method that can be utilized effectively without the active participation of the identified person. Method of this type does not require any specific action on the part of the customer. Just her mere presence in a particular place, in this case – on the seller premises, is sufficient. It is necessary, however, to equip the seller location with appropriate infrastructure and to register customer face images in a database. The assumed approach is to maintain the database on the PO side which is less burdensome for the customer. It requires only a one-time registration of face biometric controlled by the PO, which could offer the appropriate customer identification service for a number of vendors, e.g. city-wide. At the same time, it appears that this variant is easier to implement in practice because of the higher level of trust that customers have in POs.

For passive identification, face recognition based on a single image has a number of drawbacks. Apart from the risk of false matchings that would not be corrected automatically, such approach would require an additional effort from the seller side ("taking a photo") and would require active unnatural face presentation from the user. However, it can be assumed that there is short but continuous time period in which a user prepares to the transaction (e.g. walks over, looks through the offer). This few second period can produce several dozen of face images and this is the proposed timespan for the initial identification. As an element of the proposed system, rule-based heuristic algorithm has been developed in which final identification decision is a result of a number of face matchings calculated within given time period. Therefore, a low number of false matchings does not impact the final identification decision. If the data stream introduces a significant portion of new face matchings, the final identification is gradually improved and seamlessly updated on the seller device.

For a single-frame matchings standard Eigenfaces algorithm is used, c.f. Section 2.2. If a positive matching takes place, the identifier of the recognized user is returned along with recognition coefficient X. Since, as it has been mentioned, single recognitions can be erroneous, the heuristic algorithm has been introduced into the decision process and it is responsible for the final identification decision. It collects a number of faces N recently detected (not: recognized or matched to a template) with their X coefficients. The approach based on moving frame has been applied, i.e. in each iteration N last images are analyzed, even if in previous iteration some of them have already been analyzed. The size of the frame is limited not only by a number of images, but also by time period, i.e. images are excluded from the frame if they are too distant in time to be possibly related to the recognized user (e.g. one minute old).

Such sets of values describing detected/recognized faces are checked for compliance with three conditions:

1. $L_A > P_1 * N$ (correct recognitions number)
2. $L_A > P_2 * L_{NonA}$ (advantage of correct recognitions over misrecognitions)
3. $L_A^X > P_3 * L_A$ (correct recognitions quality)

Where:

L_A – number of images in the image sequence of N images, in which a user A has been recognized with the best coefficient;

L_{NonA} – number of images in the image sequence of N images, in which users that are not a user A have been recognized with the best coefficient; it does not include images in which no user has been recognized;

L_A^X – number of images in the image sequence of N images, in which a user A has been recognized with the best coefficient if the coefficient is less than or equal to X.

For user A in order to be recognized all three conditions must be fulfilled. Values of heuristic algorithm's parameters: N, P_1, P_2, P_3 and X have been calculated experimentally (40, 0.2, 1.0, 0.5 and 3700) – the single conditions are rather loose because of the conjunction logic of the approach.

Instead of Eigenfaces any other algorithm could operate underneath the proposed heuristic algorithm. Eigenfaces algorithm has been chosen to show that even for relatively simple and obsolete single-frame recognition algorithm, the proposed approach allows for fairly robust user identifications in practice. The key element is taking advantage of a long stream of individual recognitions, even if they can be ambiguous, in the manner described above in this section.

It is worth noting that as additional criteria improving the recognition accuracy, information obtained at the client side from sensor about face distance (too distant faces are uncertain), user attention (rotated faces are uncertain), or user mimics (images too different from neutral-mimics templates) can be taken into account. Improved recognition accuracy would reduce time delays related to unsuccessful data processing. Also scalability of the solution would be improved due to reduction of computational power requirements (lower number of recognitions) and of communication effort. Similar benefits could be obtained by using pre-recognizers trained to recognized user height or sex, and thus pre-segmenting the template database before actual matching.

4 EVALUATION DESIGN

The evaluation requires conducting empirical tests of the system in conditions as close to regular as it is possible. Evaluation scenario assumes that after prototype system is designed and implemented, it is deployed in real PoS that in future could be a cooperator of the metropolitan service framework, and its usage data are collected and analyzed. During the analysis the data are confronted with formulated research hypotheses related to system usability.

4.1 Research Hypotheses

For usability evaluation the following four research hypotheses have been formulated:

H_1: Automatic transactions provide users with higher convenience level and similar duration as compared to traditional transactions.

Contactless card payment (estimated approx. 5 second long) has been assumed as a reference traditional transaction. In the presented approach the customer service process is changed, from a traditional sequence: order (Z1) followed by a payment (P1), into a sequence: passive identification (I2), order (Z2), payment authorization (P2) (cf. Figure 1). Assuming stages Z1 and Z2 as comparable in terms of execution time, the goal is to get the total duration of I2 and P2 equal or less than the duration of P1.

H_2: Automatic payments reduce number of user actions undertaken for transaction authorization down to zero.

H_3: In the real-world environment using the prototype system will result in more than 80% successful

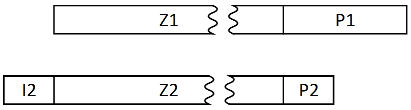


Figure 1: Stages of customer service sequence.

face identification attempts. In the group of successful face identification attempts, more than 80% is not preceded by earlier misidentification.

H_4: Applying context-based authorization method selection based on trust, risk and convenience criteria results in gradually decreasing transaction duration.

4.2 Experiment Setup

In the experiment an existing PoS (local bar "The End Cafe") with a group of its regular customers who usually conduct a typical (routine) transactions has set a research environment. It has allowed for collecting results reflecting requirements of intelligent PoS while maintaining reasonable experiment time and number of participants.

The system has been used by 22 users (14 women, 8 men), for the period of 16 days (7th to 22nd December). The participants were selected from existing clients of the bar that visited it at least 2-3 times per week, are familiar with internet banking and utilize contactless payment cards at least once a week. The age of participants was in the range of 20 to 30. The bar staff has been informed about the system setup and trained to use it for customer service properly. The prototype system has been parametrized to classify a payment as a routine after two or three similar payments. In order to allow participants to make a number of payments, each has been provided with 150 PLN worth electronic wallet. During the experiment participants have spent totally 2837 PLN and have performed 251 payments, which is more than 10 payments per person.

The participants have made transactions according to their will and have not been steered nor pushed in any way neither by staff nor by researchers. At the same time, logging subcomponents of the system's components have been used to log every significant system event. The events have been defined to build complete and detailed descriptions of every possible customer service path. During the experiment neither technical nor organizational difficulties that could have impact on the results have been reported.

4.2.1 User Registration

After the participants recruitment, each participant has been equipped with RFID marker in the form of card, sticker or fob, and the application instances have been installed on participants' smartphones. In the PO-side component responsible for user identification there have been stored sets of face image patterns, which have been registered with a seller-side component responsible for tracking, acquiring, segmenting, filtering, and streaming user face images at the PoS, according to the strict procedure. Ten different (mimics, angles, distances) images of each face have been collected. It has introduced desired diversity of the training set, also because of different face lighting on the images of different kind, with different face rotation or distance. It has to be noted that sensor has not been installed in this same horizontal axis as typical location of user face, but slightly above and rotated. This also has had impact on requirements regarding diversified orientation of the faces in the training set (both "ahead" and "slightly upwards, towards camera"). During initial tests it has been confirmed that three-quarter views decrease recognition accuracy and therefore they have been excluded from training process. Detected faces have been visually outlined, which facilitates choosing optimal acquisition moments, so that operator has a control over the training set quality (framing, distance, sharpness, angle, lost tracking). Face registration has been performed at the PoS, which has two main advantages. First, it facilitates registration by not requiring any additional client's visits in the operator's location. Second, the registration environment conditions are similar to recognition environment conditions which improves recognition accuracy.

Name, ID photo, face and RFID identifiers, as well as user identifiers in the seller and operator systems have been stored in the dedicated component at the PO side. In another PO-side component, device vendor, model and OS version, as well as device token (for PUSH communication within Google Cloud Messaging) and list of supported authorization methods have been stored. In the authorization component, patterns for authorization method, PIN and optionally fingerprint hash, have been stored.

Before the user registration procedure each participant underwent an individual in-depth interview and was briefly informed about the system operation. Additionally, a web page explaining the idea of automatic payments and system operation was published and presented to all participants.

4.2.2 Data Collection

During the experiments a number of event classes has been registered in components' logs. In the process of user identification the following event classes are registered: face detection event, recognition event, confirmation event, "reject and change the method" event, “reject and try again” event, and transaction abort event. In the process of transaction authorization the following event classes are registered: transaction start, acceptance, transaction decline, and sending authorization request to client/seller.

For those events, apart from exact timestamp, the following identifiers are registered: identification method identifier, client identifier, transaction identifier, identifiers of available authorization methods, identifiers of used authorization methods, transaction status (e.g. button code, reason for the rejection), as well as many parameters related to face identification, such as: number of detected faces, correct recognitions number, advantage of correct recognitions over misrecognitions, correct recognitions quality, average and median of recognitions and misrecognitions quality, and identifiers of the decision rules that are fulfilled.

Apart from data collected by the system itself, all participants were invited for a second round of in-depth interviews where they could express their opinion about the system operation.

5 EVALUATION RESULTS

The evaluation results presented in this section have been obtained as an effect of data mining and statistical analysis of three distinct log sets, generated by four components of the system. The results from the first subsection are related to user identification phase, and the results from the second subsection are related to subsequent phase, i.e. transaction authorization phase. The third subsection contains an overview of users opinions gathered during and after the experiment.

5.1 User Identification

Totally, there were 282 successful user identifications performed by the system. This value does not indicate the number of performed transactions, since there are cases where for a single identification a sequence of transactions is conducted, and there are cases where successful identification does not precede successful transaction authorization.

Identification Methods. From among successful identifications, even 72% have been conducted with face biometrics, and only 28% with RFID card, despite the fact, that every user has been equipped with such card and could freely use it. A number of successful identifications in the respective experiment weeks for different identification methods is presented in Figure 2.

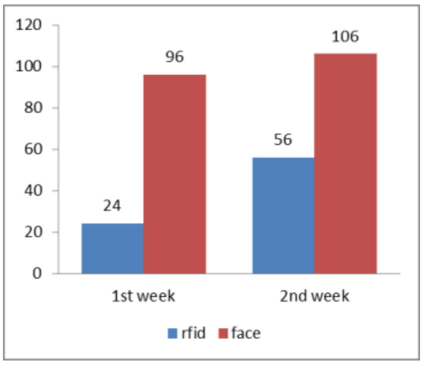
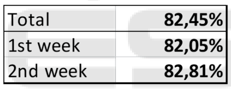


Figure 2: Number of successful identifications for different identification methods in respective weeks.

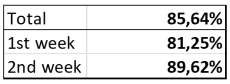
Accuracy of Identification with Face Biometrics. Among from all attempts to identification with face, i.e. cases where new client has appeared at PoS willing to identify himself or herself with a face, 202 have been successful and 43 have failed. These values expressed by percentages for distinct weeks are presented in Figure 3.



Total	**82,45%**
1st week	**82,05%**
2nd week	**82,81%**

Figure 3: Percentage of successful identifications for respective weeks.

In the group of successful face-based identification attempts, 173 have not been preceded by any earlier unsuccessful attempts (named as “seamless identifications”), and 29 have been preceded by unsuccessful attempts (named as “difficult identification”) within time period of 30 seconds. Seamless identifications percentage for respective weeks is presented in Figure 4.



Total	**85,64%**
1st week	**81,25%**
2nd week	**89,62%**

Figure 4: Percentage of seamless successful identifications in relation to all successful identifications.

High percentage of successful identifications has persisted in the consecutive days of the experiment and it has never dropped below 72%, which is presented in Figure 5. The labels on horizontal axis denote days of December, two weeks from December 7th to December 18th. Weekends and pre-Christmas days (December 21st and 22nd) are excluded because of very low number of clients at the campus bar in those days producing non-representative results.

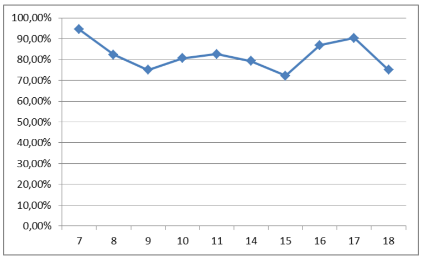


Figure 5: Percentage of successful face identifications in the consecutive days.

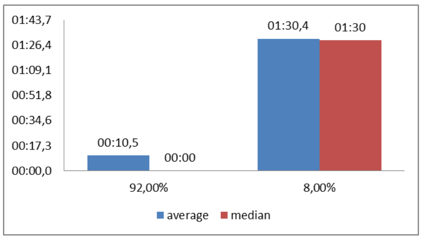


Figure 6: Average and median authorization durations in case of single and repeated authorization.

Duration of the Identification with Face Image. Duration of the face identification has been measured from the moment of the first face recognition of the user (even if the recognition does not fulfills the heuristic criteria of the final identification, even if the face image appears once, and even if it belongs to the “misrecognitions” set), to the moment of receiving the identification message at the seller’s device. The median of identification duration is 34 seconds.

Independently, the durations of the seller confirmations have been measured, i.e. time between the moment of receiving the identification message at the seller’s device and the moment of seller’s manual approval with the button. Median of confirmation time is 3 seconds.

5.2 Transaction Authorization

During the evaluation, 225 transactions have been successfully conducted, 92% of them required single authorization attempt, and 8% required repeated authorization.

Authorization Duration. Average duration of the transaction authorization for transactions that require single attempt is 10,5 second and median of this duration is below 1 second (because of the relatively high number of automatic authorizations). In the rare cases when repeated authorization has been required (e.g. a user inputs wrong PIN), the duration has been much longer (Figure 6). Authorization duration is measured from the moment when the order is already put together, through transaction authorization process, to the payment settlement done.

In Figure 7 median duration of authorizations (blue bars) for respective days are depicted. Evident decrease of the transaction duration is observed, which is a consequence of familiarizing users with the system as well as of constantly increasing fraction of automatic authorizations during the evaluation (because of building a history of transactions that increases trust). Downward trend (trend line) is strengthened by the fact that in the last three days (16-18) in which the durations have been short, the highest number of transactions have been conducted (red bars).

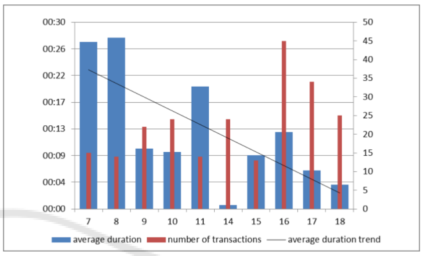


Figure 7: Average authorization durations for respective days.

User Faults During Transaction Authorization. Percentage of transactions requiring repeated authorization in the respective days is presented in Figure 8. Clear downward trend can be observed. As in case of transaction duration, it is a consequence of familiarizing users with the system as well as of constantly increasing fraction of automatic authorization method which eliminates user faults.

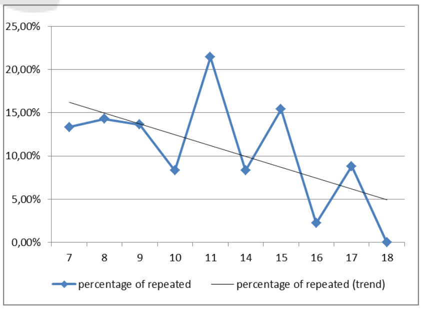


Figure 8: Percentage of transactions requiring repeated authorization in the respective days.

Context-based Authorization Method Choice. In Figure 9 a number of successful authorizations in the respective days for different authorization methods is visualized. Increasing usage of automatic method is visible. It is a consequence of users' building a history of transaction that increases level of trust, which is a one of the conditions for choosing this method by the system. It confirms that system works according to expectations.

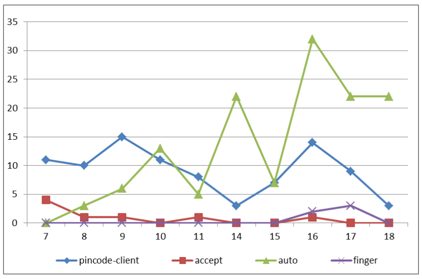


Figure 9: Number of successful authorizations in the respective days for different authorization methods.

Above-mentioned tendency is visible better if data are expressed relatively, which is presented in Figure 10.

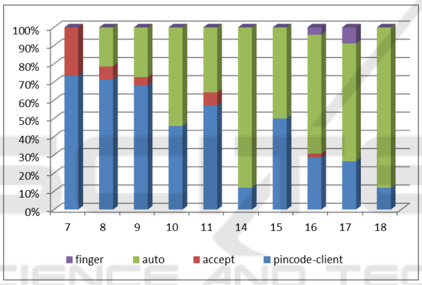


Figure 10: Distribution of different authorization methods in the respective days.

In Figure 11 medians of transaction durations for different authorization methods for respective weeks are presented. It can be observed that durations of manual accept authorization (with a smartphone) in the second week are lower than in the first week. The main reason for this advantageous trend is getting experience by users' with the new notification and confirmation interface. The PIN-based authorization duration is constant since this method is already known for users and since PIN always requires few seconds to be typed, regardless of user experience. Authorizations with fingerprint have been performed only few times (since only few users have used devices with a fingerprint scanner) and only in the second week, thus their durations cannot be considered as representative.

5.3 Users Opinions

During the experiment randomly selected transactions were followed by a request to fill in a short questionnaire regarding the subjective quality of user experience. The questionnaires were provided via regular payment mobile application immediately after the transaction. In 83 responses collected from these questionnaires the majority of respondents indicated that in their opinion the automatic payment procedure is more convenient (61.4%) and more secure (52%) than a traditional contactless payment. They also responded that the whole process was faster (50%) than a traditional contactless payment.

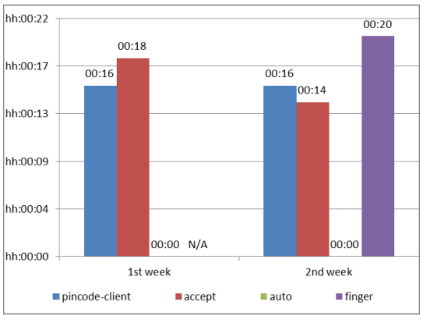


Figure 11: Medians of authorization durations for different authorization methods in respective weeks.

During the second round of in-depth interviews all participants were encouraged to present their own opinions about the system. The opinions include both positive and negative statements. Positive statements can be summarized by the following keywords: convenience, speed, innovation. Negative statements were focused mostly on inconveniently long identification time. It is also worth to notice that some participants felt uncomfortable when their personal data (photo and name) intended for the sales clerk could be visible to other clients in the queue, which pinpoints that the seller-side of the system should protect privacy of clients data.

6 CONCLUSIONS

Results of the evaluation confirm that proposed modus operandi for the automatic authorization as well as its goals and benefits are achievable under the constraints of a real-world PoS. Prototype system build based on proposed architecture and algorithms indeed has allowed evaluation participants for routine payment authorization in the passive mode. The seller just confirms the single identity recognized by the system with one tap, and does not need to choose between possible matchings losing his time and focus like it is required by systems reported in the related works. The main advantage of the proposed approach comes from its context-awareness and dynamic authorization method selection, which allows for gradually achieving the trust level required for passiveness.

The right balance between convenience and security, which are always at odds, is constantly provided. Obtained results allow to verify particular research hypotheses defined in the Section 4.1.

The hypothesis H_1 has not been confirmed during the evaluation. Although median of authorization durations is far below 5 second limit, the second component of the total duration, i.e. identification, takes much longer time (c.f. Section 5.1). It results in conclusion that applied approach to face recognition needs further optimization. The long recognition time is not caused by computation complexity nor performance issues, but by too frequent inaccurate (conflicting) recognitions in the image sequence which delay obtaining consistent result for a given user. This difficulty can be overcome by employing additional filters that can detect and eliminate error-prone frames from the video stream and by optimizing parameters of heuristic for the final identification.

The hypothesis H_2 has been confirmed. In cases when passive identification and authorization have been conducted, all the users had to do was to verbalize the order and pick up the products. One aspect of the identification process has been shifted to the seller (manual confirmation of a single identification result), but practically it had not significant influence on the duration of the whole process (c.f. Section 5.1).

Collected data confirm the hypothesis H_3. The percentage of the successful identifications based on face biometrics is 82.45%, and the percentage of the "seamless" face identifications within the group of successful identification is 85.64%.

Also the hypothesis H_4 has been confirmed. Data presented in Section 5.2 show that transaction authorization duration is gradually decreasing as users build a history of transaction that increases level of trust, which is a one of the conditions for choosing more convenient and fast authorization methods.

To sum up, analysis of the collected quantitative data allows to confirm three of four research hypotheses. In case of rejected hypothesis, the element that needs further optimization can be easily identified. Generally, the evaluation has confirmed that the approach proposed for passive transaction authorization is achievable despite the difficulties introduces by variable real-world condition at PoS. As a future work it is planned to analyze additional factors extracted from the video signal and depth data (e.g. user height, mimics, pose, age, sex) and non-video features (behavioral patterns for time, place, amount, type of good) that can be used to improve the recognition quality, speed, and security of the system.

ACKNOWLEDGEMENTS

The research was supported by Santander Universidades. We thank our colleagues from Bank Zachodni WBK and Symetria who provided insight and expertise that greatly assisted the research. We also thank Rafał Wojciechowski from our Department for support with implementation and prototype deployment.

REFERENCES

Al-Ghawi, S. S., Hussain, S. A., Rahbi, M. A. A., and Hussain, S. Z. (2016). Automatic toll e-ticketing system for transportation systems. In *2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC)*, pages 1–5.

Alliance, S. C. (2012). Emv and nfc: Complementary technologies that deliver secure payments and value-added functionality. http://www.smartcardalliance.org/resources/pdf/EMV_and_NFC_WP_102212.pdf.

Anh Tran, Q. et al. (2016). Finnish grocery retailing market assessment for the deployment of payment innovation: Case: Uniqul face recognition payment application.

Apple (2014). Apple pay. http://www.apple.com/apple-pay/.

Biyo (2014). Biyo wallet. http://biyowallet.com/.

Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K., and Senior, A. W. (2013). *Guide to biometrics*. Springer Science & Business Media.

Bowyer, K. W. (2015). Selfies to emerge as both payment, anti-fraud solution. *Biometric Research, Virtual Special Issue*.

Chinrungrueng, J., Sunantachaikul, U., and Triamlumlerd, S. (2007). Smart parking: An application of optical wireless sensor network. In *2007 International Symposium on Applications and the Internet Workshops*, pages 66–66.

Fujitsu (2011). Palmsecure pay. http://www.fujitsu.com/us/solutions/business-technology/security/palmsecure/.

Google (2015a). Android pay. https://www.android.com/pay/.

Google (2015b). Google hands free. https://get.google.com/handsfree/.

Hassett, J. (1994). Automatic debiting parking meter system. https://www.google.com/patents/US5351187. US Patent 5,351,187.

He, W., Li, Q., and hua Sun, W. (2015). Discussion on multi-sensor detector fusion of internet of things in vehicle management.

Lee, J. (2015). Jcb piloting fujitsu palm vein authentication technology for payments. http://www.biometricupdate.com/201510/jcb-piloting-fujitsu-palm-vein-authentication-technology-for-payments.

LiquidPay (2015). Liquid pay. http://www.liquidpay.com/.

Lucnova (2015). Freshx. https://www.freshxapp.com/.

Mainetti, L., Patrono, L., Stefanizzi, M. L., and Vergallo, R. (2015). A smart parking system based on iot protocols and emerging enabling technologies. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, pages 764–769.

Nakagawa, A. (2015a). Method of automatically adjusting toll collection information based on a number of occupants in a vehicle. https://www.google.com/patents/US20150379782. US Patent App. 14/316,488.

Nakagawa, A. (2015b). Method of automatically adjusting toll collection information based on a number of occupants in a vehicle. https://www.google.com/patents/US20150379782. US Patent App. 14/316,488.

Narzt, W., Mayerhofer, S., Weichselbaum, O., Haselbck, S., and Hfler, N. (2015). Be-in/be-out with bluetooth low energy: Implicit ticketing for public transportation systems. In *2015 IEEE 18th International Conference on Intelligent Transportation Systems*, pages 1551–1556.

Narzt, W., Mayerhofer, S., Weichselbaum, O., Haselbck, S., and Hfler, N. (2016). Bluetooth low energy as enabling technology for be-in/be-out systems. In *2016 13th IEEE Annual Consumer Communications Networking Conference (CCNC)*, pages 423–428.

Samsung (2015). Samsung pay. http://www.samsung.com/us/samsung-pay/.

Smowton, C., Lorch, J. R., Molnar, D., Saroiu, S., and Wolman, A. (2014). Zero-effort payments: Design, deployment, and lessons. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp '14, pages 763–774, New York, NY, USA. ACM.

Ta, T. D., Le, D. A., Le, M. T., Tran, T. V., Do, T. T., Nguyen, V. D., Trinh, C. V., and Jeon, B. (2015). Automatic number plate recognition on electronic toll collection systems for vietnamese conditions. In *Proceedings of the 9th International Conference on Ubiquitous Information Management and Communication*, IMCOM '15, pages 29:1–29:5, New York, NY, USA. ACM.

Wójtowicz, A. and Chmielewski, J. (2017). Technical feasibility of context-aware passive payment authorization for physical points of sale. *Personal and Ubiquitous Computing*, 21(6):1113–1125.