

Usable security using social authentication for online transactions by low literate users

Interaction design project I

By-

Prashant Sachan

IDC, IIT Bombay

126330004

Guided by-

Saurabh Srivastava

Nitendra Rajput

IBM Research Laboratory

New Delhi, India

July 2013

Industrial Design Centre,
Indian Institute of Technology
Bombay, India



This Interaction Design degree project, titled **Usable security using social authentication for online transactions by low literate users** is done in partial fulfillment of the requirement for the degree of Master of Design in Interaction Design at Industrial Design Centre, IIT Bombay.

It was done with IBM Research Lab, New Delhi.

Duration: May to June, 2013

Declaration

I declare that this written submission represents my ideas in my own words and where others' ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all the principles of academic honesty and Integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission.

I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources that have thus not been properly cited or from whom proper permission has not been taken when needed.

Prashant Sachan
Interaction Design, IDC, IIT Bombay
Roll no. 126330004

Mumbai, India

July 2013

Table of contents

Abstract.....	09
Introduction.....	11
Background & Related Work.....	12
User Study.....	15
Motivations & Implications.....	18
System Design.....	19
Field Trials.....	20
Results.....	23
Discussions & Conclusion.....	27
References.....	47

Abstract

Authentication techniques for mobile applications in developing regions have largely been adopted from those used in developed countries. While there has been significant research done to determine how human behavior affects authentication techniques in the developed world, much less attention has been paid to devising novel authentication techniques for users in developing regions.

In this project, we consider authentication mechanisms that rely on shared information possessed by members of a social network. We describe a proof of concept field study to investigate how ties within the close-knit social structures in developing regions can be leveraged to provide an authentication mechanism for mobile phones users. This involved a two-stage field study involving 174 subjects conducted over a period of 5 months. The basis for using social authentication, in which users are queried about events and other private info by friends and family members they nominated, was derived through studies involving 54 participants. This was followed by a field study of a mid-fidelity prototype involving 120 participants. Our results indicated that users find social authentication simple and usable, and that more familiarity with this technology will significantly improve its efficacy.

1. Introduction

Non-cash transactions have been increasing at a steady rate of about 8% every year, worldwide [1]. This growth is even higher in emerging markets in Africa and Asia (20%). More of this growth has been in the electronic and mobile payment space (58.5%). All electronic payment transactions face challenges with respect to user authentication. Prior research studies in this field have confirmed that users forgetting passwords is a very common problem in electronic payments [2]. This is expected to be an even bigger problem in developing regions. While low literacy and unfamiliarity with technology can be reasons, a more fundamental one is cultural preference for oral interactions.

Biometric authentication (face [3], fingerprint [4], voice [5]) provides a more usable form of authentication and avoids some of the pitfalls of using passwords, but it also requires a more sophisticated end-user device, which must have cameras, fingerprint scanners, microphones, etc. An end-user in a developing region is likely to perform payments using a basic mobile phone that does not possess such sensors. What will serve users in developing regions, especially low-literate users, are authentication techniques that do not rely on expensive feature phones or easily forgettable passwords. One such category of authentications involves leveraging users' trusted social networks to generate challenges and responses; legitimate users are unlikely to make mistakes and unauthorized users unlikely to guess the right responses. Though these mechanisms are culturally suitable to the target demographic, little research has been done to assess their suitability for authentication purposes and the user experience.

While the recent growth in social networks has demonstrated the willingness of users to share relevant content with those close to them, such content has not been used for security purposes. In this paper, we

investigate how a user's social network can be used to authenticate him/her. In a canonical scenario, selected friends in a user's social network provide a question-answer pair that only that user can answer. Such a question-answer pair can be related to an event that these two people have experienced, or any other shared secret. In a real-world application, the user is successfully authenticated only if he/she provides the correct response to the posed question. To decrease the likelihood of unauthorized users guessing the right answer, authentication may also require the user to answer multiple questions posed by different members of the social network.

We believe that our target users would be more likely to correctly answer questions like: "What is the song we performed on our wedding night?" instead of remembering a password. Complex passwords are unlikely to be remembered, and both simple and complex passwords are typically shared by these users with others for safekeeping, thereby often defeating the purpose of having a password. This allows users to authenticate themselves through low-end phones without extra hardware, and will be a more engaging mechanism for authentication, especially for low-literate users in developing countries. To such users, sophisticated, and highly secure authentication mechanisms may prove barriers to entry in the world of mobile transactions, or may prompt them to opt out of authentication altogether, leaving them vulnerable. Our goal in this paper is to outline and evaluate a set of authentication mechanisms that significantly increase usability without unduly sacrificing security.

We describe how we validated our proposed social authentication system by conducting an initial field study with 54 users to understand user's views on three issues: banking; information exchange and exposure to any authentication techniques; and usage of mobile phones. This study provided insights from: i) users who did not have a bank account, ii) those who had an account, and iii) bank employees who perform physical authentication. We show how design guidelines were derived from this

study and a mid-fidelity prototype of the social authentication mechanism developed. The prototype was tested with 36 low-literate users using a voice interface and another 84 users using a text-based web interface. We then analyze the information provided by these users and present insights into the type of question-answer pairs that users post into the system. We also analyze the question-answer pairs from a security perspective. We show how user feedback reveals that users prefer social authentication for its simplicity.

To summarize, the main contributions of this project are:

- Determination of problems with existing authentication systems through a field study.
- Outlining a novel way to authenticate users using social network content, thereby achieving a balance between usability and security.
- Analyzing question-answer content posted by people for authenticating their friends; determining that the content is secure and can be matched using simple text-mining solutions, and is also useful for authentication.

While the study is conducted in India, we believe that the underpinning concepts are not specific to Indian culture, and that such authentication mechanisms can be applied in most developing countries where low-literate users reside.

2. Background and Related work

The work presented in this paper relies on prior research and engineering done in the area of mobile banking for low-literate users. Our goal is to increase adoption of mobile banking transactions by providing security as well as enhancing usability. In this section, we first discuss the security and usability aspects of such transactions, and describe why we focus on user authentication. Then we do an overview of the related work in authentication and mobile banking, and show how our contribution differs from, and enhances the state-of-the-art.

2.1 Mobile Banking: Security and Usability

Any mobile banking solution, especially one that targets the low-literate demographic, must consider not just its security properties but also its usability. As we will discuss further below, these two requirements often conflict, and require a balance to be struck. But first we list the different security properties any mobile banking solution must satisfy, and discuss in detail the property we focus on in this project. Typical scenarios involve transactions conducted between mobile devices and servers, or between mobile devices (payment protocols), where users of the mobile devices possess accounts with the participating banks. Security in this context is the requirement that only authorized users be allowed to access and draw funds from accounts, and that transactions are carried out with complete integrity.

1. Confidentiality and integrity: All communication from one mobile device to another, or from a user's mobile device to a remote server, must be secured against eavesdropping and data tampering. This is a necessary condition for any commercial protocol. In practice, this can be ensured using cryptography. Telecom network communication is invariably cryptographically protected, and protocols like SSL and TLS are

eavesdropping- and tamper-proof for all practical purposes.

2. Authentication of the end device: A mobile device should not be able to masquerade as another. Often, users register their mobile devices with their financial service providers; only legitimate devices are permitted to conduct transactions on users' behalf, thereby adding another layer of protection. Telecom service operators typically ensure this in practice, using the SIM technology, for example.

3. Authentication of the user: Only authorized users must be allowed to perform sensitive mobile banking transactions. This must be ensured through a separate mechanism even if the end device is authenticated, because devices may get lost or stolen. In practice, this is ensured through a challenge-response mechanism that required the user to provide some piece of information that is known only to him/her and is extremely unlikely to be known to others. Most commonly, this is a password or a PIN number, though a custom question-answer pair may also be set by users through secure out-of-band mechanisms.

While mobile banking must be secure, it must be usable as well. By usable, we mean that a transaction must involve minimal physical effort and incur minimal cognitive burden on the part of the user. If the task is too complex (e.g. user is required to set a long password and a PIN as well as additional security questions), a typical user will avoid performing it or frequently make mistakes. Hence, an overly complex protocol will deter users, resulting in the loss of commercial opportunity for financial companies and users alike. On the other hand, an overly simple protocol (e.g., a very short PIN number) is highly insecure; what is simple for the user is likely to be simple for an attacker as well. Also, a number of users, especially those living in remote rural areas, prefer to share their passwords and PIN numbers with others (typically people they trust) for safety and reliability [9]; this reduces the security value of such secret information. Therefore, the goal of usability is often at cross-purposes with

the goal of security [6].

Examining the list of security properties above, it is apparent that properties #1 and #2 do not pose a challenge to the usability of a mobile banking solution. Cryptographic operations in the underlying network protocols and SIM card authentications are transparent to the user and do not require manual intervention. On the other hand, the mechanism user to authenticate users (#3) directly impacts usability, and that is the security aspect we focus our attention on for the remainder of this paper.

Intuitive Authentication Mechanisms — though widely used authentication mechanisms like passwords, PIN numbers, and user-defined questions are fairly secure, their usability decreases with stringency. Also, these techniques were designed in the PC era, and are less suited to mobile phones, on which typing is cumbersome and error-prone. The error rate, and general difficulty of use, is much higher, for low-literate users, many of whom will find it impossible to carry out such tasks or be reliant on others for assistance [7, 8]. Clearly, solving the usability problem involves the design of more intuitive user input mechanisms. The two modes of input other than writing that are available to us are verbal and visual. Research on HCI using these two modes has been going on since before the mobile era, but has now taken on a new urgency because of users' reliance on their mobile devices to perform a variety of private and secure tasks. Speech and voice recognition techniques are constantly being improved, the latest effort being Apple's Siri [9]. Voice recognition-based authentication has been attempted [10], though is still some way to go before such mechanisms are foolproof. Authentication mechanisms that rely on cookies being stored in a browser require no interaction on the part of the user [11], but security breaks down if the device falls into the wrong hands. Captchas and images are also frequently used (e.g., in Facebook) for authentication; these are easy to use and fairly foolproof.

Lastly, biometric-based authentication techniques are very promising as

they provide both ease of use and foolproof security. The most popular technique relies in fingerprint matching [12]; though this has been available for a number of years on PDAs and laptops, it is likely to be more widely relied on with the release of the iPhone 5S. The problems with using fingerprints are: (i) this technique is only available on smart phones, and not on basic ones which the vast majority of low-income and low-literate people use, and (ii) fingerprint authentication may not be foolproof for people who perform a lot of manual labor. In this paper, we describe our efforts to sidestep these problems and limitations by leveraging yet another aspect of a user's experience, his/her social network.

2.2 Mobile Banking for Low-literate Users

Mobile money transactions have been studied from an interface perspective [13] and it has been observed that iconic interfaces perform better than the standard menu-based interfaces for low-literate users. Challenges with respect to authenticating users is presented in [14] where the authors propose a low-cost authentication mechanism using printed codebooks, which provide improved security while not requiring any additional sensors at the user device. Not using sensors is a design constraint that our work also adopts. The issues with respect to passwords and its sharing are presented in [15]. This work raises important issues such as the need for people with disabilities to share passwords with their cares, and for other people to share with their family to establish social trust. Such challenges with passwords are somewhat alleviated in the social authentication solution that we propose in this paper. Challenges with respect to adoption of mobile banking with low-literate users in developing countries are presented in [16] where the authors mention that lack of trust in the system is a major barrier to adoption. We believe that the involvement of social groups will make users more likely to trust our proposed social authentication system.

We start from the hypothesis (justified, in our view) that social network members share information that is both private and confidential, and therefore can be used as the basis for authentication. To this we add the intuitive interaction mode of voice calls, whereby users are called on their mobile phones, and a verbal query/response protocol ensues. Through our research, we attempt to gauge both the feasibility and the efficacy of social network-based authentication techniques as an alternative to the techniques already in use. We do not claim that our method is superior to these others in terms of security, but that it is different and is much more usable for our target demographic. Later in this paper, we will discuss the results obtained from our user study and comment on the security implications.

3. User study

To understand existing banking processes and to determine the gap between what exists and what is needed, we conducted semi structured interviews and qualitative user study with 54 users. The study was conducted in New Delhi, India as well as the semi-urban areas of Nithari and Morna Ambedkar Gram, Noida, (about 45 miles from New Delhi.). Twelve of the participants were literate and technology-savvy users in New Delhi. The others were selected from the semi-urban areas. Like many Indian villages, these areas have an agriculture-based livelihood, ranging from very small- to medium-sized farms. Many farmers from distant villages visit this area to sell their agricultural products. The residents who are not farmers are employed as property dealers, local shop owners, vendors, etc. To understand issues with respect to authenticating a particular transaction, we also visited two banks in the vicinity - Indian Overseas bank and Ghaziabad Zila Shahkari bank, Nithari, Noida.

We aimed to broadly understand the banking related problems which users face in their daily life related. We also aimed to understand the following basic questions:

- How do users manage money?
- What mode of transaction did they prefer?
- How and where do they keep the details of their money?
- What were the instances when they faced problems in banking activities and what did they do to resolve them?

To find answers to these questions, we met 36 low-literate and 18 Literate participant users. 22 out of the 36 low-literate users did not have knowledge of banking services and had no bank accounts. The remaining 14 users had knowledge of banking services and possessed bank accounts. Of the 18 literate participants, 12 were bank users and 6 were

bank officials who managed the bank in rural areas. These were managers, clerks of rural banks and postal services who dealt with low-literate bank account holders on a daily basis. The 12 literate users had bank accounts and had used Internet banking facilities. We interviewed the participants one-on-one, with open-ended conversations that lasted for at least an hour. These interviews gathered demographic information, identified problems they faced in monetary transactions, and elicited information about the use of mobile phones in their day-to-day lives. We also captured opinions about how they expect mobile payment technology to influence their lives to make positive changes. We collected past experiences and stories that participants shared about their experience in banking.



Figure 1. Researcher conducting the field study

We now discuss our findings from this study.

3.1 Trust and banking

We found that low-literate users who had a bank account preferred to go to a bank along with a trusted person, even if the accompanying person was low literate himself. We found that banking was a group activity for a lot of users; i.e. they would be accompanied by son or wife or somebody known from the village. We observed that a lot of them found it very difficult to fill the administrative forms and seek help of the bank employees. One of participants who lived in a village nearby and came along with his (illiterate) wife told us—“I usually bring her whenever I come to bank. She manages the documents while I stand in the queue. Usually Babus (clerks) help women more than us.” Participants who were accompanied with a non-family member in the bank were open to share their own banking details. When asked, many affirmed that their friends knew their account details, and that they trusted their friends completely.

Banks considers a customer illiterate if he is not able to write his name. Most of these users used thumbprints to sign their transactions. One of the officials told us- “We generally recognize all the account holders in our bank. We extend all our help to make them aware of banking processes.” They also knew most of the account holders socially and authenticated them by facial recognition. Because of these social connections, the officials often permitted transactions by account holders’ immediate family members if the holder himself was not present.

Most of the participating users who did not own a bank account were afraid of visiting the bank. Many complained about the complicated banking processes and having to fill multiple forms. They prefer to lend and borrow money directly amongst friends and family. We observed that they remembered all transaction details and very rarely recorded them in writing. All the monetary transactions depended heavily on trust, i.e. on reputation and verbal commitments.

On the other hand, most of the literate participants reported that their preferred mode of doing transaction was Internet banking. One reason was the frequent signature mismatches that occurred with cheques.

Banking and payments on behalf of others was common. These included mobile bills, electricity bills, credit card bills, and train tickets bookings. A user said—“My friends call me late at night to recharge their Internet connection. It is a helpless situation because one cannot go in night physically to do the recharge.” We observed that people did not hesitate to share their credit card information with their social group members.

3.2 Information Exchange and Security Issues

Low-literate users exhibited a cultural preference to share information verbally. Their financial details were usually known to someone amongst their close friends and family members. One of the participants told us—“I feel more secured if I share my bank details with my brother. He is most educated among all of us in family”. We observed similar behavior in participants having no bank accounts; records of transaction were kept orally within the social circles, but seldom written. Monetary disputes were settled in Gram Panchayats (village councils) or social meetings. We also found that the main pieces of banking-related information that people both needed and preferred to share with the members of their social circle were: account information, monetary transactions, government benefits and schemes, and farming payments.

For literate users, we found that details of bank accounts (e.g., outstanding balance, name of banks, bank passbooks, cheque books) were shared among family members (wife, parents, relatives) and close friends. Users typically did not share PIN numbers and passwords for Internet banking because they thought it would be of no use to others, but they were open to handing their ATM cards and PINs to others to withdraw money from ATM machines.

Having multiple bank accounts to manage money was found to be very common among the literate participants. Most of them had separate

saving accounts for their salaries. Every user had faced challenges in managing their passwords; these also included PINs for bank accounts, one-time passwords, T-Pin for mobile banking, Interactive Voice Response, credit cards, etc. 7 out of 12 participants reported that they had their own ways of managing passwords. A user reported—“I have framed logic to assign a password to different accounts. I follow that to avoid confusion”. 10 out of 12 participants complained of forgetting their transaction password, which prevented them from concluding their transactions. A user complained—“I have made a habit of requesting new password whenever I login to a trading account which I use not so frequently. This is so very easy for me than to remember it”.

3.3 Usage of Mobile Phone

Nearly 90% of low-literate users we surveyed possessed mobile phones, which were used as personal or shared resources. Many had feature-phones while others had low cost multimedia phones. The phone was primarily used to make and receive calls. Though low-literate participants could access their contact lists, they were obviously not able to use the SMS service. They only used those applications on the phone which were simple for them to use, or for which another family member had trained them. All frequently used applications could be invoked with click or two. Many of them used a mobile to seek information from their friends but none of them ever tried calling a banking IVR system.

Every literate participant we surveyed possessed a mobile phone. Out of 18, only 3 participants were using a feature phone while had other smart phones. Only two of the literate participants had used mobile banking over the phone to check their account balance. None of them had done any transaction through their phones. The reason for low incidence of mobile banking was not related to the lack of perceived security. It was because such users had access to the Internet at home and work, and they found it easier to use banking portals on PCs compared to mobile phones.

4. Motivations and Implications

For banking and authentication, trust and dependency on family members and social circles was one of the prominent observations that came out from the user study. Sharing and consumption of information over mobile phones was another. These observations inspired us to investigate social network-based authentication as a way to provide such users with an easier mobile banking experience.

In our technique, members selected from a user's social network can post personal questions that they think only he can answer with the bank authentication system. While making a transaction, the user tries to authenticate himself by identifying the questioner and answering the question correctly. Given the likelihood of strong ties within social networks in both literate and low-literate communities, we believe our technique can work for users with varied educational backgrounds and exposure to technology. It could be used independently or combined with other security and authentication techniques such as biometrics.

Our proposed mechanism has several advantages compared to an authentication mechanism in which user must remember a password or passphrase. Our method has a contextual similarity with the practice of sharing PIN numbers and passwords, and is hence a familiar method for our targeted demographic. The overall user experience of authentication is improved, as he/she listens to a known voice and a question whose answer he can quickly recall (but which a user outside his social circle cannot.) In his culture, this method may also help in strengthening social ties, as it would honor a member of his circle to be designated as a question-poster. This would likely encourage others to use the mobile banking service.

As described in the "Security and Usability" section (Section 2), our system is predicated upon the availability of secure communication and device authentication mechanisms. We rely on commercial telecom networks to ensure an adequate level of confidentiality, integrity, and non-repudiation for all practical purposes. For user authentication, we rely on the user's social network as a private space and a circle of trust. We use a challenge-response mechanism that is a little different from the traditional password-, PIN-, and security questions-based mechanisms. The difference is that the challenger is not just the back-end server but also a combination of that server with a legitimate user's social network member, who we consider a trusted third party. Since the response mechanism can be verbal in addition to text-based input, this process is much more usable than the traditional alternatives. Later in the paper, we will discuss other equally usable non-verbal mechanisms that involve text input. We also rely on the mobile banking system to securely obtain a user's social network member's identity and connect with them for the purpose of obtaining a challenge question; as mentioned earlier, we leverage the security provided by telecom networks and web protocols for this purpose. Alternatively, friends may present themselves in person at the bank to register their questions and answers. At the outset, we do not limit the nature of the challenge question and the expected response, but rather treat them as experimental variables. Later in the results section, we will comment on the security value of such questions and consider their implications for commercial mobile banking systems.

5. System Design

Our authentication system allows the user two modes of input: voice and text. Voice input can be used by all users (even illiterate) whereas text input requires basic literacy. We describe how the authentication process works in each mode, and discuss their relative advantages and drawbacks.

5.1 Voice-Based Authentication System

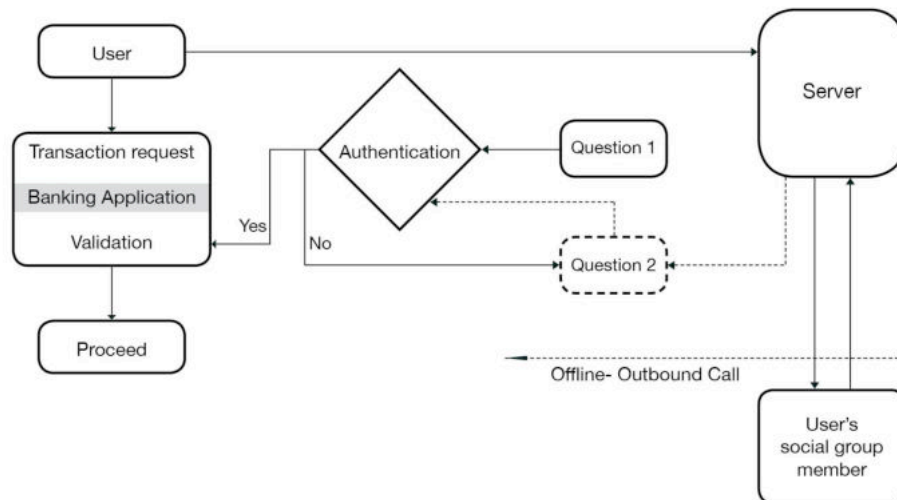


Figure 2. Authentication Protocol

A user initiates a mobile banking transaction and completes the initial steps leading to a sensitive request (e.g., money transfer, bank balance information). The banking system calls the user on his mobile device, selects a pre-recorded question posed by a member of the user's social

network, and plays it back. The answer to this question is a shared secret possessed by the user and the questioner. The question is based on recent conversations, private topics, events, or experiences that the questioner believes only the user is capable of knowing and answering. The user attempts to answer the question, and the banking system compares that answer to a pre-recorded correct answer in its database. This can involve simple speech recognition: a few clearly spoken words. If the answers do not match, the system sequentially selects alternative questions from its database for a pre-configured number of attempts. If the user correctly answers any of these questions, the transaction succeeds; otherwise, it fails.

5.2 Web-Based Authentication System

A user initiates a mobile banking transaction and completes the initial steps leading to a sensitive request (e.g., money transfer, bank balance information). The banking web site selects a pre-recorded question posed by a member of the user's social network, and displays it on the UI. The user attempts to answer the question, and the banking system compares that answer to a pre-recorded correct answer in its database. The matching algorithm may range from a simple string comparison to text mining or context analysis.

If the answers do not match, the system sequentially selects alternative questions from its database for a pre-configured number of attempts. If the user correctly answers any of these questions, the transaction succeeds; otherwise, it fails. In both these systems, a user can nominate a list of social network contacts at configuration time, and dynamically update (add, remove, or reorder in terms of priority) it when he wishes. This can be easily done using IVR (interactive voice response) or an Internet banking account.

We also allow a nominated social contact of the account holder to change a question. This will involve the contact making a call to the authentication system, and changing previously saved questions and answers using IVR. The changes are saved but not committed until the account holder approves the changes. The authentication system periodically attempts to seek a decision (approval or rejection of the changes) from the holder through voice calls, SMS, reminders delivered when the holder logs into his account, or through an out-of-band method.

5.3 Comparison

It is obvious that voice input is more usable and can be used by a wider demographic compared to text. On the other hand, the accuracy of matching a user's answer to the pre-recorded answer stored in the banking system's database is much higher in text mode as the content of the answers themselves are unambiguous. Speech recognition is not close to being a precise art, and therefore a voice-based authentication system will sometimes make mistakes. To improve the odds, the system gives an account holder multiple chances to authenticate himself. Yet this also increases the probability of an unauthorized user getting an answer correct by chance. There is an inherent tradeoff here between usability and security. Yet, many users are satisfied with the accuracy of IVR, and the quality of speech recognition keeps improving (e.g., Apple's Siri.) So we can reasonably expect that security and accuracy will increase without any sacrifice in usability.

6. Field trials

We conducted field trials to understand how users perceive the proposed authentication mechanism, and to find out what kind of content they would like to post. We evaluated the design of voice- and web-based social authentication with different user groups in two separate controlled studies, our research focus being the following:

1. Analyze the nature of content posted by the users.
2. Determine the accuracy of our authentication systems and its acceptance by the users.

The voice-based prototype was tested primarily with low literate users, while the web-based system was tested with literate and tech-savvy users. Our study of literate users and the web-based system also helped us compare social authentication with existing authentication techniques.

6.1 Voice-Based Authentication Study

We deployed a voice based mid-fidelity prototype in which we would call a voice application over a simple phone network. We recruited participants and asked them to nominate two social group members for the experiment. Then we asked one social group member to record a question for the participant. After the confirmation of his question the social group member recorded an answer. When we approached a participant for whom a question had been recorded, the prototype played back that question without revealing the answer. Once he answered, both question and response were saved in the database as audio files. Later we analyzed these files, manually comparing actual responses with the correct answers. In the future, we will use automated speech recognition software for such comparisons and examine how that affects the accuracy.



Fig 3. Researcher conducting voice-based social authentication study.

The experiment was conducted with 36 users from the areas of Nithari Gram, Mubarakpur village, and slums in Noida. We met each participant individually, introduced them to the study, the prototype and provided them instructions to operate the phone (if required.) We emphasized the seriousness of the task and explained the adverse affects of posting poor/unwise questions. All users were low-literate males with less than 10 years of formal education. 21 out of 36 participants had no banking knowledge, while 15 were banking users. Every user was allowed one attempt to post a question and provide an answer.

6.2 Web-Based Authentication Study

First, we created and deployed a web-based authentication form. Then we recruited participants and asked each one to nominate a social group member for the experiment. The web page had detailed description about the authentication mechanism and emphasized the seriousness of this task. We asked the members to input their email address, a question, and an answer for the participant. After the form submission, a link was sent to the participant through email. On clicking the link, a question was displayed for the participant to answer. Questions and responses were automatically saved in the database.

This experiment was conducted with 84 participant users in city of Mumbai, India. All were literate and had prior experience of using mobile phones, the Internet, and banking. We met each participant individually, introduced them to the study, the prototype and provided them instructions to use the web-based questionnaire. We clearly explained that posting poor/unwise questions could have adverse effects like security breaches.

6.3 Classification of Challenge Response Pair

We defined weakness dimensions for the authentication questions and framed categories for the challenge-response pairs. The dimensions were guessability, attackability, automatic attackability, ambiguity, lack of memorability, and hesitation in answering. We classified the questions into the following 3 categories:

- **Public**— Answers may be known to many people, e.g. date of birth, nickname, etc. These measure high on dimensions of guessability, attackability, automatic attackability, and are hence not ideal for authentication.
- **Private**— Answers are known only to two or more people in a limited social group with specific shared experiences, e.g. What movie did we watch yesterday? These measure high on ambiguity and lack of memorability, but low on guessability, attackability, and automatic attackability.
- **Sensitive**— This is personal information, typically shared by not more than two people e.g. information about diseases and relationships. These measure high on hesitation in answering, but relatively lower on other dimensions.

To find more patterns in the nature of content posted by people, we classified the questions as follows:

- **Info-seeking**— Quantitative information (e.g., age, price).
- **Consent-seeking**— Assent or denial questions (yes or no).
- **Event-based**— Questions that demanded a qualitative or a descriptive answer based on a specific event.
- **Entertainment-based**— Questions on movie dialogues or game-playing scenarios.

To evaluate the accuracy of our system, we categorized the quality of the responses as follows:

- **Exact (WTW) match**— Response is an exact match with the pre-recorded answer. We will refer to this as word-to-word in the rest of the paper.
- **Total mismatch**— Response is completely incorrect, syntactically or semantically.
- **Approximate match**— Response contains all the words in the pre-recorded answer, but also a few extra words. It can be matched with the help of a simple text matching or regular expression matching algorithm. We will refer to this as text mining in the rest of the paper.
- **Identical meaning**— Response is semantically correct but has a different sentence structure. It can be matched using a complex Natural Language Understanding (NLU) system. We will call this contextual analysis in the rest of the paper.

7. Results

We first analyze the data (question-answer pairs) posted by users (who represented social contacts of account holders.)

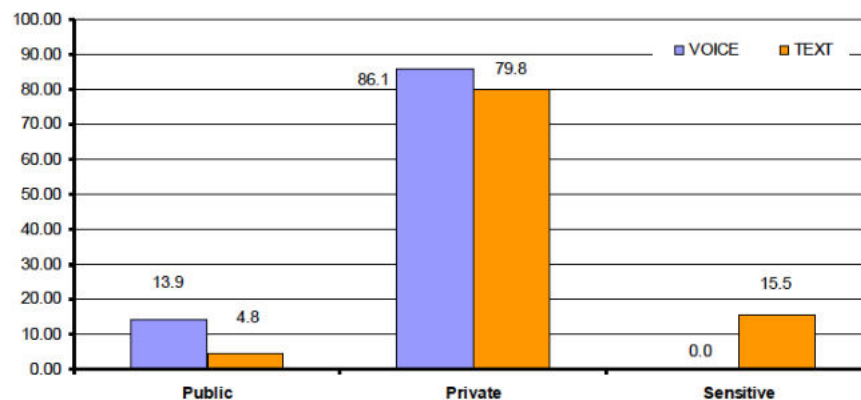


Figure 4. Question Category in two Prototypes.

As seen in Figure 4, there were a very high number of private questions, which were more prone to ambiguity, and lack of memorability, but less to guessability, attackability, and automatic attackability. For the voice prototype, nearly 14 % of the posted questions were public which others could have easily answered. The number was lower (4.8%) for the web based prototype. Interestingly, a high number of questions (15.5%) were sensitive questions such as “When did we make love for first time?” This data inspires confidence in users’ ability to select authentication questions that will be hard for unauthorized users to guess the right answers to.

As shown in Figure 5, the Info-seeking category had the highest number of questions. Though this distribution has no security implications, the preponderance of Info-seeking questions implies that a bank’s authentication system will automatically match the responder’s answer with the actual answer with high accuracy. We will discuss this accuracy

further in reference to Figure 8 later in this section. We can conclude from Figures 4 and 5 that users are very likely to post private questions that have Info-seeking content in them.

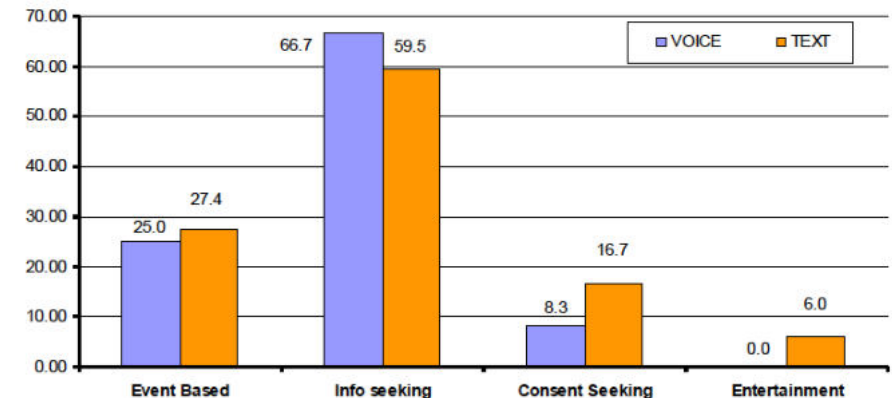


Figure 5. Question content type in two Prototypes.

7.1 Overall Accuracy

Let us now analyze the types of techniques that will be used to match a user’s response with the pre-recorded answer posted by his nominated social group contact.

Figure 6 shows the distribution of answers based on their categories (WTW, CA, etc.) For the voice-based prototype, only 9 responses (25%) were word-to-word matches with the correct answer to the question that was posted by the user’s social contact. 27 responses were not perfect matches, but 6 could be matched by text-mining and 7 by contextual analysis; 14 were incorrect. On the other hand, 84 responses were recorded for the web-based prototype, of which 81 were correct. A majority (52) matched word-towards providing a fairly high assurance of accuracy.

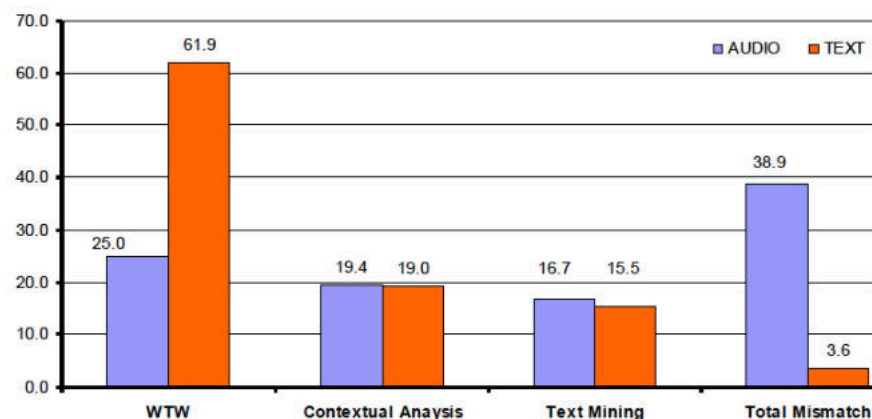


Figure 6. Percentage Correctness of Responses.

Most of the low-literate users seemed to be more interested in listening to their own-recorded voice on the mobile phone than in coming up with a suitable question. We believe that the interaction experience intimidated them. In a real time scenario, we expect this to happen quite often. Therefore it is probably advisable to allow users some practice or test runs with the question selection technology to put them at ease. Alternatively, they could be informed a day or two in advance so that they are mentally prepared to frame a suitably question. When formally framing the question that will be posed in a real authentication scenario. They will be more likely to focus on the content of the question, which will result in a better authentication system. Doing evaluations after allowing the users some adjustment time is on our agenda for the future.

In the web-based prototype, we observed that people put a lot of thought into posting a question and answer (in contrast to the voice-based prototype.) Every user was familiar with the web-based medium and quickly grasped the concepts we explained at the beginning of the experiment. This resulted in a system with high accuracy.

7.2 Ease of Use

To glean qualitative insights, questionnaires were presented to the literate users after using the web-based prototype. The users were asked to rank the system based on their perception of its usability, measured using 5 factors (partly based on the QUIM model [17]): memory load, likeability, self-descriptiveness, operability, and ease of use. Users ranked these parameters on a 1 (very low) to 5 (very high).

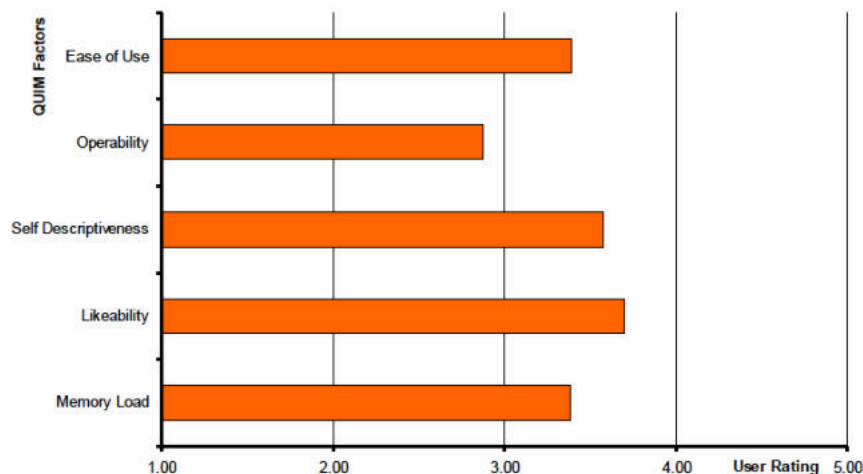


Fig 7. Qualitative Factors vs. User ratings for Web Based Authentication.

As shown in Figure 7, most of the factors were ranked “medium-to-high” except for operability, which was ranked “low-to-medium”. We believe that this was due to the fact that our authentication method relies on the question posted by social circle member and the actual user had little control on the authentication question selection. Since it was hard for low-literate users to understand the above-mentioned terminologies; most of the feedback for the voice-based system was taken in the form of verbal comments. Most of the users stated that the system was effective and easy to use, especially those users who had knowledge of banking

processes. While one of the participants commented—“I will tell my wife to post a question & answer of my choice and then I can answer correctly every time”; this is similar to the way he would have used a conventional pass phrase-based mechanism.

7.3 Dependency of Accuracy

We observed a higher accuracy for Consent-seeking questions in both the prototypes (Figures 8 and 9). In the voice-based system, word-to-word accuracy for such questions was low because participants usually posted full sentences even when the expected response was yes or no. For the web-based system (Figure 9), the highest accuracy for Consent-seeking questions was observed when the answers were matched word-to-word (obviously); note that such questions are not that secure, as an unauthorized user has a 50-50 chance of guessing the right answer. We observed the least accuracy for Info-seeking questions in the voice-based prototype. A closer analysis revealed that participants responded in long sentences to these questions, thereby reducing the accuracy.

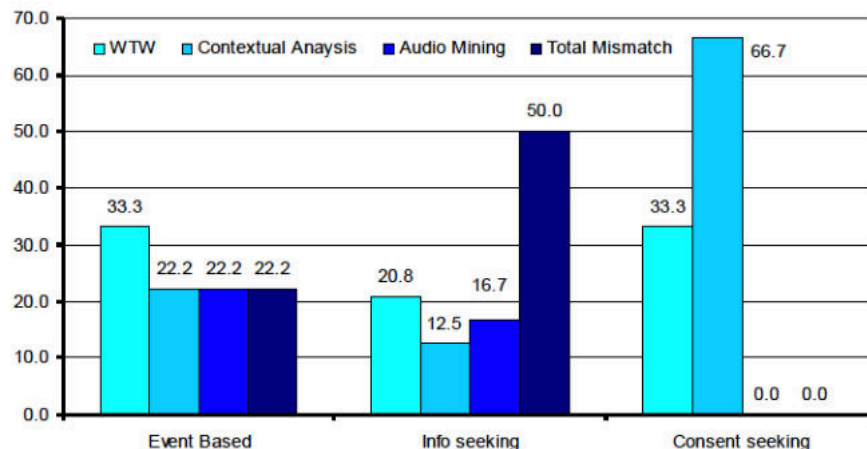


Figure 8. Accuracy Vs Question Type in Voice-based system.

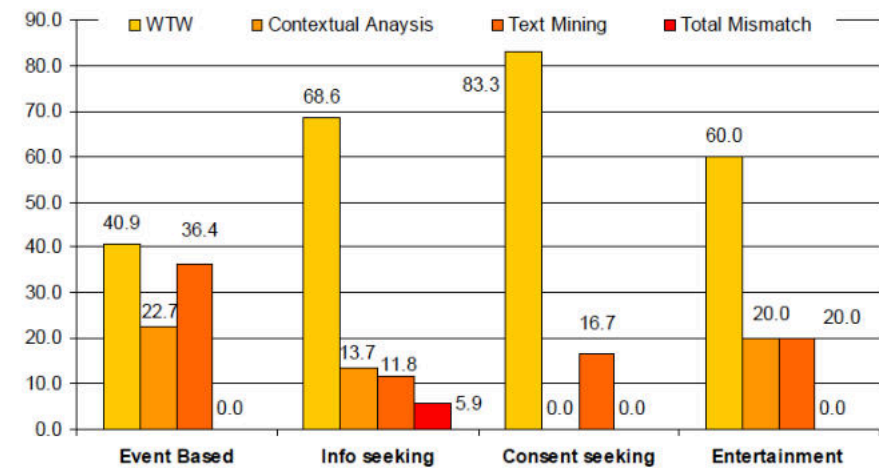


Figure 9. Accuracy Vs Question Type in Web based system.

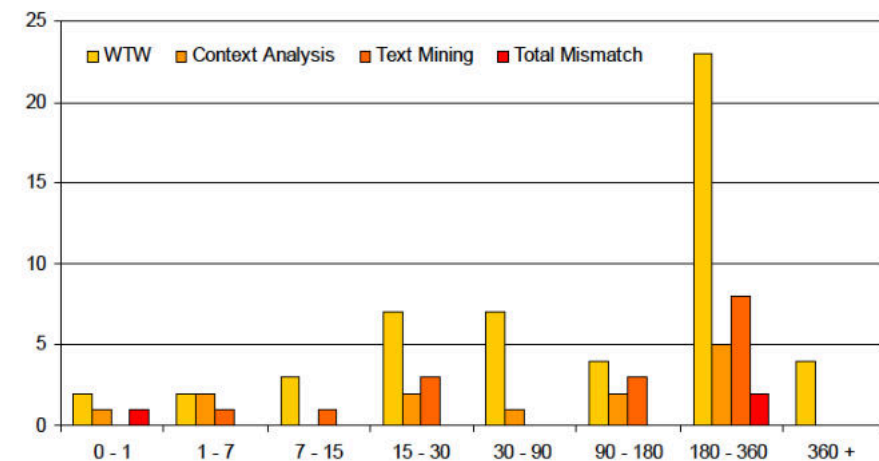


Figure 10. Accuracy Vs time when topic /event of question happened.

Most of the questions were based on events that occurred between 180-360 days before the date of the study (Figure 10).

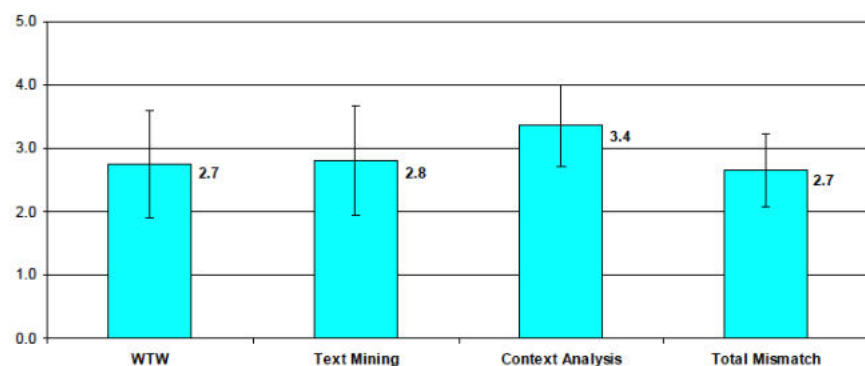


Figure 11. Rating of Stress (on scale of 5) Vs. Accuracy.

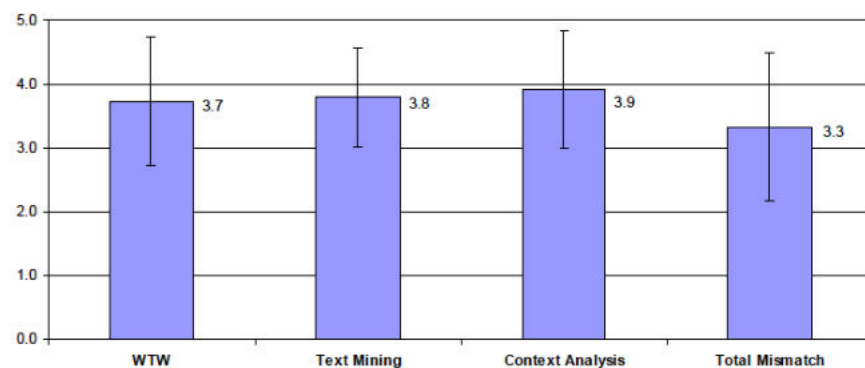


Figure 12. Rating of privacy of a question (on scale of 5) vs. Accuracy.

We also asked the users to rate the system in terms of the amount of stress they felt while posting answers to the questions asked by their social contacts and in terms. Stress ratings were done on a scale of 5 (5=high to 1=low). Answers requiring contextual analysis for successful matches required the most effort for the framer, and so were slightly more stressful (Figure 11). We also asked the users to rate the questions they had just heard based on its perceived privacy on a scale of 5 (highly private =5 to less private = 1). As illustrated in Figure 12, there is no statistical variation in the perceived nature of the privacy with the type of the question.

8. Discussions and Conclusions

We set out to evaluate the efficacy of social network-based authentication in mobile banking systems along two dimensions—usability and security, which are often at cross-purposes. Our results show that such systems are indeed user-friendly and provide feasible alternatives to existing systems, especially for our target demographic. On the other hand, the results also show that the security of a social authentication system depends heavily on how it is used. In this section, we do a deeper security analysis, and suggest avenues for improvement and research.

We observed that greater ease of use was accompanied by a greater (mistakenly) perception of security. This was true of our users, even though they did not grade the system high on operability. Mostly private and Info-seeking questions, which require low cognitive burden to frame but may not provide the most security, were posted. Much can be attributed to the unfamiliarity of this technology to our target demographic. Our system depends heavily on the right content, based on personal interaction between the social members, being posted. Getting low-literate users to pose questions that are private and provide accurate answers will require more intuitive ways of using the tools, more training, and more awareness of the security risks.

The users being authenticated had a hard time delivering a response using the right words even when they knew the answer, especially in the voice-based system. And with a high total mismatch rate (38.9% for voice), our authentication system is not as foolproof as it ought to be. Yet, our classification of answer types suggests that using better speech- and text-recognition technology will result in improved matching whenever the user delivers a correct response (61% for voice and 96% for text); in other words, authorization false positives (i.e., genuine user denied access) could be reduced. An alternative is to allow multiple attempts, as mentioned earlier. There is a security usability tradeoff here: more

attempts will decrease the false positive rate but may also drive up the false negative rate (i.e., an unauthorized user being allowed access).

Another way of addressing the drawbacks in response matching is better user interface design. The system could suggest hint/example questions, expected to be private and requiring precise word-to-word match answers, to question setters. To the user being authenticated, the length of the answer could be hinted at by providing auditory/visual cues.

Now let us consider some inherent security flaws in social authentication. From a conceptual perspective, our reliance on a trust relationship existing between social network members is flawed. The question a member chooses to record is selected subjectively, and its confidentiality can hardly be guaranteed in a scientific manner [18]. An unwise choice of questions will inevitably result in unauthorized entities taking advantage. Also, the social network members themselves may turn adversarial. Such members may deliberately choose to pose questions they know the legitimate user will not be able to answer, thereby breaking our authentication mechanism. Alternatively, the social network members could themselves masquerade as the legitimate user, answering accurately the questions they themselves posed, thereby gaining unauthorized access. Our system must therefore be augmented with revocation mechanisms and randomness; i.e., never rely on a single social network member for authorization.

There are a number of avenues for future research, particularly in security. One necessary step is to augment social networks with dynamic trust models that provide some assurance of a questioner's integrity. We could use information analytics to determine what information is truly private and confidential, and thereby automatically filter out questions that can be easily answered by unauthorized parties. It is also necessary to have multiple questions and questioners (akin to multiple security layers), randomized questions, and periodic updates of the question bank for our authentication framework to meet the bar for commercial purposes. We

could also mine a user's social network data (with the user's permission) to determine his closeness with his network members, thereby aiding in the selection of suitable questioners. One lesson we can take away from our results is that the usability of our technique alone may ensure a higher overall level of security over password- and PIN-based techniques. This is because low literate users are highly likely to share private passwords with third parties who can then take advantage; the insecurity of sharing secret information is likely to be lower than the insecurity of an answer being guessed.

9. References

- 1 Capgemini and RBS, World Payments Report 2013.
<http://www.capgemini.com/wpr13>.
- 2 Sonia Chiasson, P. C. van Oorschot, and Robert Biddle. 2006. A usability study and critique of two password managers. In Proceedings of the 15th conference on USENIX Security Symposium - Volume 15 (USENIX-SS'06), Vol. 15. USENIX Association, Berkeley, CA, USA, (2006).
- 3 K. Jonsson, J. Kittler, Y.P. Li, J. Matas, Support vector machines for face authentication, Image and Vision Computing, Volume 20, Issues 5–6, (2002).
- 4 Jain, A.K.; Hong, L.; Pankanti, S.; Bolle, R., "An identity authentication system using fingerprints," Proceedings of the IEEE, vol.85, no.9, pp.1365,1388, Sep (1997).
- 5 Douglas A. Reynolds, Speaker identification and verification using Gaussian mixture speaker models, Speech Communication, Volume 17, Issues 1–2, August (1995).
- 6 Christina Braz and Jean-Marc Robert. 2006. Security and usability: the case of the user authentication methods. In Proceedings of the 18th International Conference of the Association Francophone d'Interaction Homme-Machine (IHM '06). ACM, New York, NY, USA, 199-203.
- 7 Supriya Singh, Anuja Cabraal, Catherine Demosthenous, Gunela Astbrink, and Michele Furlong. 2007. Password sharing: implications for security design based on social practice. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '07).
- 8 Indrani Medhi, Aishwarya Ratan, and Kentaro Toyama. 2009. Mobile-Banking Adoption and Usage by Low-Literate, Low-Income Users in the Developing World. In Proceedings of the 3rd International Conference on Internationalization, Design and Global Development: Held as Part of HCI International 2009 (IDGD '09), Nuray Aykin (Ed.). Springer-Verlag, Berlin, Heidelberg, 485-494.
- 9 Apple – iOS7 – Siri, <http://www.apple.com/ios/siri/>.
- 10 Shilpa Kaman, K. Swetha, Syed Akram, G. Varaprasad . Remote User Authentication Using a Voice Authentication System. Information Security Journal: A Global Perspective. Vol. 22, Issue 3, 2013.
- 11 Kevin Fu, Emil Sit, Kendra Smith, and Nick Feamster. 2001. Dos and don'ts of client authentication on the web. In Proceedings of the 10th conference on USENIX Security Symposium - Volume 10 (SSYM'01), Vol. 10. USENIX Association, Berkeley, CA, USA, 19-19.
- 12 De-Song Wang; Jian-Ping Li, "A new fingerprint-based remote user authentication scheme using mobile devices," Apperceiving Computing and Intelligence Analysis, 2009. ICACIA 2009. International Conference on , vol., no., pp.65,68, 23-25 Oct. 2009.
- 13 Medhi, I., Nagasena, G. S. N., and Toyama, K. A Comparison of Mobile Money-Transfer UIs for Non-Literate and Semi- Literate Users. Proc. ACM Conference on Computer Human Interaction, Boston, USA, 2009.
- 14 Panjwani S., Cutrell E. Usably Secure, Low-Cost Authentication for Mobile Banking. Proc. of Symposium On Usable Privacy and Security (SOUPS) 2010, Association for Computing Machinery, Inc., (2010).
- 15 SinghS, Cabraal A, Demosthenous C, Astbrink G, Furlong M, Password Sharing: Implications for Security Design Based on Social Practice, CHI '07 Proc. of the SIGCHI Conference on Human Factors in Computing Systems (2007).
- 16 Medhi, I., Ratan, A. and Toyama, K. Mobile-Banking Adoption and Usage by Low-Literate, Low-Income Users in the Developing World. Proc. Human Computer Interaction International, San Diego, USA, (2009).

- 17 Seffah, A.; Kececi, N.; Donyaee, M., "QUIM: a framework for quantifying usability metrics in software quality models," In Proceedings of Second Asia-Pacific Conference on Quality Software (2001).
- 18 Rabkin A. Personal knowledge questions for fallback authentication: Security questions in the era of Facebook. Symposium on Usable Privacy and Security (SOUPS) 2008, July 23–25, Pittsburgh, PA USA (2008)