International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-1 Issue-1, April 2012

Secure Multimodal Mobile Authentication Using One Time Password

R. Mohan, N. Partheeban

Abstract: ***Security concerns are on the rise in all areas such as banks, governmental applications, healthcare industry, military organization, educational institutions. Government organizations are setting standards, passing laws and forcing organizations and agencies to comply with these standards with non-compliance being met with wide-ranging consequences. There are several issues when it comes to security concerns in these numerous and varying industries with one common weak link being passwords. Most systems today rely on static passwords to verify the user's identity. However, such passwords come with major management security concerns. Users tend to use easy-to-guess passwords, use the same password in multiple accounts, write the passwords or store them on their machines. Further more, hackers have the option of using many techniques to steal passwords such as shoulder surfing, snooping, sniffing, guessing. Several 'proper' strategies for using passwords have been proposed. Some of which are very difficult to use and others might not meet the company's security concerns. Two factor authentication using devices such as tokens and ATM cards has been proposed to solve the password problem and have shown to be difficult to hack. Two-factor authentication (T-FA) or (2FA) is a system wherein two different factors are used in conjunction to authenticate. The proposed method guarantees that authenticating to services, such as online Shopping, is done in a very secure manner. The system involves using a OTP (One Time Password) Algorithm generation of Dynamic password for second way of authentication. One time password uses information sent as an SMS to the user as part of the login process.***

Index Terms: Mobile Authentication, Secure Multimodal, Two Factor Authentication, One Time Password.

I. INTRODUCTION

A secure and accessible multimodal authentication method that uses a one-time-password client installed on a mobile phone allows usage by people whose functional impairments adversely affect their ability to use existing solutions. Usability is the extent to which specified users can Use a product to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use. Accessibility is a precondition for usability. The title of the project is Secure Processing System in Online Transaction. If a customer to use personal password to confirm his identity and protect his/her credit card when the card is used on the Atm, providing greater reassurance and security. To make Atm password even simpler and safer, a secure processing system is being introduced Common authentication method. Include passwords, PINs, tokens, biometry, smart cards, and one-time codes from tokens or code generators. The aging of the population is another factor. As they age, people often experience multiple mild to- moderate impairments.1 about 20 percent of the population aged 50+ Suffer from severe vision, hearing, and/or dexterity. The prevalence of such disabilities increases with age. To further analyze the situation, we did a rough analysis of different authentication and identification methods with regard to various user groups. Table 1 gives an overview. It indicates the challenges of various authentication methods for different user groups. The table is only an indication; the real. Accessibility and usability of each authentication method relies, of course, on the implementation. Failure to provide accessible and usable authentication services could preclude use for many people and, in some cases, cut them off completely from vital online services.

A.Proposed Block Diagram

The proposed system allows user or customer to use a personal password to confirm his identity and protect his/her card when the card is used on the Internet, providing greater reassurance and security. The proposed system is a security system that tells on-line retailers that the user is a genuine cardholder when he shops on-line.In this proposed system specifically the example of online book shop is taken to represent the online transaction. After the selection of the book the user can select the credit card payment mode.

Revised Manuscript Received on 30 April 2013.
* Correspondence Author
R.Mohan*, B.E (M.E), Dept. of PG Studies & Engineering, S.A.Engineering College, Chennai-77, Tamil Nadu, India, E:mail: mohanpaavai@gmail.com
Mr. N.Partheeban, M.Tech., PhD, Associate Professor, Dept. of IT, S.A. Engineering College, Chennai (Tamil Nadu), India, E mail: knparthi78@gmail.com

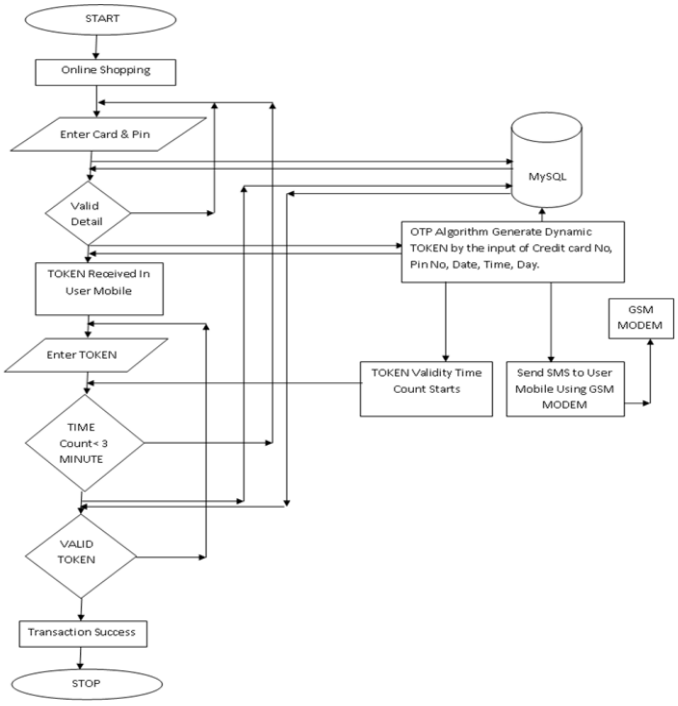


Fig .1 Proposed Diagrams

Enter the secured processing system (SPS) for secured transaction. It improves the security of Internet payments by providing an additional password to the user. Using the password the user can successfully make his payment. Online card transactions over Internet need enhanced security. Secure processing system facilitates additional security by way of a cardholder-chosen password, which is known only to the cardholder.SPS is a new way to add safety when the users buy online. Adding a personal password to the existing Credit Card ensures that only the authorized card holder can use Card online. It's easy to activate the SPS service on your existing Card.User enter details and the password will appear in the authorized mobile phone, enter the password in the appropriate box and submit, and payment is over.SPS receives credit card details from the card issuing bank which is invisible to the customer. SPS provides verification details to the customer. It verifies the password and other details. Cardholders enter their PIN on the key pad to generate a one-time code for secure authentication by SPS.Dynamic passcode authentication is one solution that uses the added security of credit cards to offer better protection against online fraud. The primary benefit of this system is the reduction in disputed transactions and the resultant exception handling expense and losses. Thus the proposed system is adding an extra layer of security at the point where you enter credit card information online. The service helps to prevent unauthorized online use before it happens by confirming your identity with an additional password.

Given the demographic shift in many countries toward elderly populations and the subsequent increase of chronic health conditions and disability, this could affect millions of people around the world. It indicates the challenges of various authentication methods for different user groups. The table is only an indication; the real accessibility and usability of each authentication method relies, of course, on the implementation. Failure to provide accessible and usable authentication services could preclude use for many people and, in some cases, cut them off completely from vital online services. Given the demographic shift in many countries toward elderly populations and the subsequent increase of chronic health conditions and disability, this could affect millions of people around the world. In addition, security software might directly conflict with the software and hardware that disabled users normally depend on, such as assistive technology. If third-party software such as screen readers can access authentication mechanisms, malicious. Programs could mask themselves as assistive technology, compromise authentication information. A potential blocker for the success of mobile cloud com-putting is the encumbered I/O functionality of mobile devices.

To further analyze the situation, we did a rough analysis of different authentication and identification methods with regard to various user groups. Age-related physical and cognitive declines and their associated difficulties are among the reasons for the lower-level use of ICT by elderly people.Failure1 to address issues related to attitude, culture, and lack of digital literacy and skills is another reason The prototype (that is, the modified client application) took the OTP as an argument and sent it to the driver for audio in a similar manner as the original application took the OTP and sent it to the screen driver. A repeat option is available at the bottom left of the menu In this paper, we propose and develop a complete two factor authentication system using mobile phones instead of tokens or cards. The system consists of a server connected to a GSM modem and a mobile phone client running a J2MEapplication. Two modes of operation are available for the users based on their preference and constraints. The first is a stand-alone approach that is easy to use, secure, and cheap. The second approach is an SMS-based approach that is also easy to use and secure, but more expensive. The system has been implemented and tested.

II. PROBLEM STATEMENT

A. Challenges of Common Authentication Methods

A common authentication method is to use a security token in combination with a website, but this might present accessibility challenges for many users, such as those with reading disabilities. Obviously, blind people can’t read a code card, and many elderly and partially sighted people also have problems with such cards, which typically present many codes compactly and in relatively small text. People with dyslexia might have trouble with such a presentation too, especially when the number of digits or characters increases.

Blind people solves this by letting someone they trust read them the code, which they then store as audio, as Braille on paper, or on their computer; however, this introduces additional security and privacy issues. To increase security, many Internet bank are replacing code cards with hardware token.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

To make this solution accessible, the hardware token must provide audio and large digits. Based on an opinion from the Norwegian Equality and Antidiscrimination Ombud, a Norwegian bank had to make this alternative available to customers at the same price as the text only alternatives. Some banks have introduced the mobile phone as the security token. The use of mobile phones presents new opportunities for inclusive design without the need to produce and distribute new varieties of hardware tokens. However, using third-party text to- speech software installed on a mobile phone might not be an alternative because if the phone's text-to speech software can access the code, malware could also access it.

Even if we apply current accessibility standards and guidelines, several problems related to the security mechanisms accessibility and usability might not be addressed. First, the solutions might not be usable even when they adhere to accessibility standards and guidelines; second, current accessibility standards might be inadequate to solve the accessibility issues of various security mechanisms.

The use of additional modalities is an important strategy for making ICT more accessible. Because authentication is a major obstacle for visually impaired users, we chose to explore whether the use of audio as an adjunct to text and numbers would improve a mobile authentication service's accessibility. Many people wear earplugs with their mobile devices, which is convenient if the audio information is confidential or private. We also hypothesized that the use of audio in this application would benefit reading- and writing impaired users.

B. A Mobile Authentication Prototype with an Audio One-Time Password

In collaboration with Encap (www.encap.no), wedeveloped a mobile phone authentication prototype. The prototype is based on Encap's existing solution, which is approved by the Norwegian Banks Standardization Office (BSK) as a mobile two-factor authentication solution for BankID. Applications for this solution include secure log-in to Internet banking, mobile banking, and two-factor authentication of Internet shopping card transactions. However, blind and severely visually impaired people couldn't use the existing solution. Although introducing another modality, such as audio, is a necessity for blind or severely visually impaired people, we also wanted to investigate.

Encap adapted its bank-approved authentication client for mobile phones—the Encap Mobile One Time Password Client—to include a vocal reading of the one-time-password (OTP) used to log in to the Store brand Bank Internet banking solution. The client runs on any mobile device supporting J2ME/ MIDP 2.0. The voice was prerecorded; we used a low-cost solution to add this audio to the application. A project member simply digitally recorded a greeting, some basic instructions, and the numbers zero to nine. The OTP is a six-digit number.

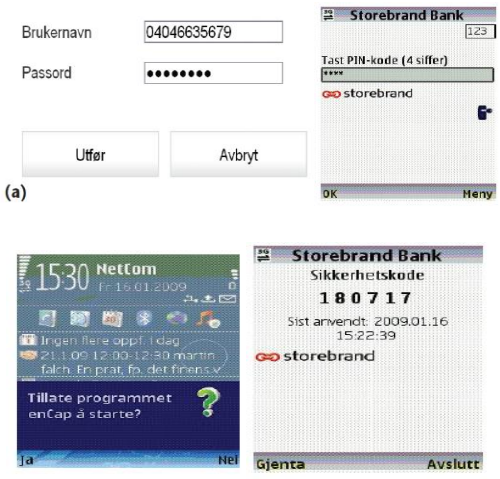


Fig. 2. The mobile authentication prototype log-in procedure. (a) The user logs in with the audio pass code. (b) A security warning appears at application start up: "Allow the Encap application to start?" (c) The mobile application provides a one-time password.

The prototype (that is, the modified client application) took the OTP as an argument and sent it to the driver for audio in a similar manner as the original application took the OTP and sent it to the screen driver. A repeat option is Available at the bottom left of the menu. At the same time it automatically sends an alert to the user's mobile phone, and the authentication client starts up. An auditory prompt on the phone then asks for the user's PIN to access the authentication client. The user punches in the PIN on the phone.

III. ENSURE MOBILE AUTHENTICATION SECURITY

A. Security in the Prototype

The prototype uses two output channels for the OTP—the phone's audio driver and the phone's screen driver. We haven't investigated whether an audio driver is more prone to security attacks than a screen driver, but the prototype uses two drivers compared to one in the original solution. Another issue is the new repeat function. The auditory OTP automatically repeats twice, and the user can press a repeat button to have the OTP read out loud again—as many times as desired, as long as the OTP is displayed on the screen. We didn't estimate this new function's potential security risk. The use context is another factor.

The prototype is meant for use with a mobile phone with earphones, making it difficult for other people in the area to hear the code—or at least as hard as it is to peek over a person's shoulder and see the code. However, if the user accesses the application without earphones, the code will be played through the phone's loudspeaker, making it easier for people to eavesdrop. This might be an argument for not offering the audio version of the application to deaf people.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

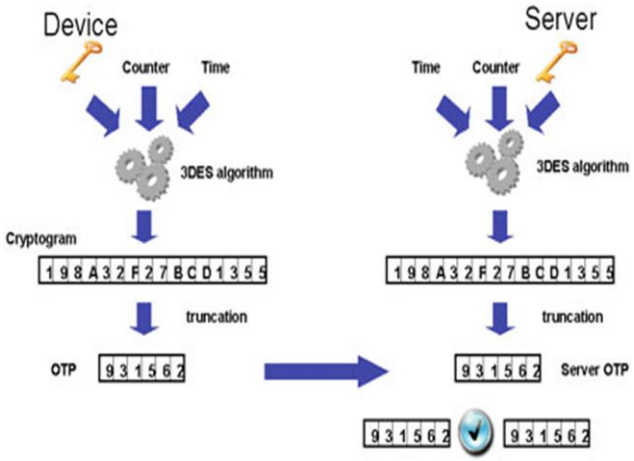
On the other hand, a blind person would probably control the phone's audio better than its display. However, because we ran the test on the users' private phones, our tests effectively demonstrated the issue's complexity.

B. Tests with Dyslectic and Visually Impaired Users

We conducted the tests chiefly in the users' homes or workplaces using their own PCs and mobile phones. Only one of the participants with dyslexia used assistive technology, whereas four participants with vision impairment used screen readers and magnification software on both their mobiles and computers. Participants had a range of cell phone carriers. The tests were part of a more comprehensive investigation, but in this article, we focus on the tasks related to logging in to the Internet banking service. We followed a comprehensive interview guide for each session and encouraged participants to "think aloud" during the session. (See "The 'Thinking Aloud' Method" sidebar for details.) We collected written consent and audio recorded the sessions. A researcher sat next to the user and took notes based on observations of user actions and obstacles as well as verbal input. If users got stuck and couldn't continue on their own, the researcher gave tips on how to continue, which they also noted. Researchers used their notes and recordings when writing detailed descriptions from each test session. The results are based on a thematic analysis of the detailed test notes. Some of the mobile phones displayed security warnings when the authentication application attempted to start up (see Fig. 2.1b). These warnings were related to allowing an application to start up on the mobile, allowing the mobile phone to send and receive data over the mobile network, and so on. This challenge is unchanged from the original solution. With some models, these messages appeared even though researchers switched them off when installing the Encap application. Because these messages gave no auditory notification, vision-impaired users missed them altogether, and had to be told by the researchers. This is an operating system security setting issue, and care must be taken to ensure that the settings are adjusted so the Encap software isn't blocked on start-up.

C.Generating OTP Algorithm:

The current epoch-time in a 10 second granularity and 4-digit PIN that a user enters. A 16-hex-digit secret that has been created when the device was initialized. When entering a PIN, the MID let displays the first 6 digits of the MD5-hash. This is the one time password. The password can be verified by the server, as the server also knows the current time, Init-Secret and PIN of the user. To compensate time differences, the server will accept passwords from 3 minutes in the past to 3 minutes in the future. In addition, different time offsets can be specified for each user on the token and/or the server. Each password will be accepted only once. After 8 successive failed authentication attempts a user gets locked out. Authentication is based on two factors: a PIN known by the user and the Init-Secret stored on the mobile device.OTP algorithms normally are based on a static key (per device) and to make the numbers (OTPs) change use variables called 'moving factors, often time, event or both. Some tokens use a time based algorithm.



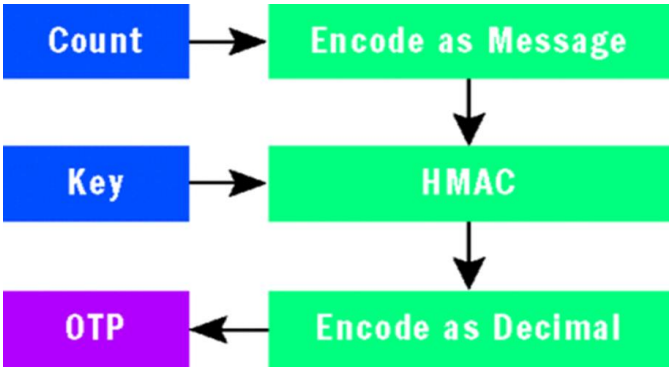


Fig.3. One Time Password

This means that if you can get to the key of a token and then you know the algorithm (secret sauce) and the current time, voila' you can generate the changing number. Some other tokens use a counter or event (the number of times a user presses the button to display the OTP) as the moving factor. This means that every token has a differing variable and hence for an attacker it is really difficult to predict what that number is for a particular token. A keyed hash message authentication code (HMAC) is a key-based cryptographic hash. Or to put it another way, an HMAC takes an arbitrary message and a key and maps the message to a fixed-size digest value ensuring that only someone with the same key can produce the same digest value from the same message. The first computational step for HMAC-OTP is to take the count value and encode it as the input message for an HMAC computation. In this implementation, the message is an 8-byte buffer set to the counter value. Figure 2 depicts this and the following two steps. The next computational step is to compute the HMAC of the above message with the user's key. Note that I addressed byte ordering in this implementation in order ensure that it is compliant with the RFCs.he issue with time as a moving factor is obviously that it is a common variable across all devices and everyone in the world knows what the current time is.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

This means that if you can get to the key of a token and then you know the algorithm (secret sauce) and the current time, voila' you can generate the changing number. The password can be verified by the server, as the server also knows the current time, Init-Secret and PIN of the user. To compensate time differences, the server will accept passwords from 3 minutes in the past to 3 minutes in the future. In addition, different time offsets can be specified for each user on the token and/or the server. Each password will be accepted only once.

The application was up and running, an audio notification asked the user to type a PIN on the phone (see Figure 1a). This is a security measure to restrict access to the application if the mobile goes missing. Most conventional one-time-password generators use the same principle. Researchers gave the PIN to participants verbally. One participant who used a PIN to restrict access to her mobile phone's SIM card mistook the requested PIN for this code. Four participants commented that the procedure was unclear or that the instructions could have been clearer.

The statements included, "I'm not sure where to key the PIN, on the mobile or at the PC," and, "The instructions should have been better. "This was the first time participants had used this application, and this will likely be less of a problem once they're familiar with the procedure. Next, the mobile application displayed and read out the one-time pass code to be typed into the Internet banking website (see Figure 1c). There was some confusion as to where this pass code was to be written— that is, on users' mobile phones or computers. Five participants commented that the procedure was unclear or that the instructions could have been clearer

Yet again, this will likely be less of an issue when users become more familiar with the sequence. However, the user interface clearly could be improved. Two participants experienced time-outs because they took too much time to type in the pass code. To remedy this issue, participants suggested giving more time, notifying users of the time allowed, or asking whether the user needs more time.Overall, we interpret the application's layout, including the font and number size, as acceptable; three participants commented on it positively and the rest didn't comment on it at all. Some concerns were raised in terms of the use of magnification software on the mobile because important functions of the authentication software's user interface.

IV. DESIGN IMPLEMENTATION

A. User Interaction Design

Developing the Graphical User Interface of View Layer in Java Server Pages for customers to login and select the items to purchase in web with Java Script Technology. Today, few developers of secure applications take accessibility into account, or they consider it only at the end of the software engineering process, rather than deploying accessibility at all stages of development. Little literature in the area of accessible and usable security exists, and it's rarely applied in practical implementation. Designers of accessible security solutions face additional challenges compared to universal design in areas where security is not paramount. Security aspects can prevent ordinary use of assistive technology to access information, and security functions can be difficult to use.

B. Server Validation and Process

Implementing the Model Layer of getting the inputs form the View Layer and processing of the Validation of Data logically in servlet Technology and forwarding the Response to Tomcat server in turn Display the corresponding view Page. The study doesn't give quantitative answers, such as how large a proportion of the population would prefer this kind of solution or how efficient it is compared to the original solution. However it does give a deeper understanding of the accessibility of security solutions, especially the issues to consider when including audio in a mobile security application. When the solution is fine-tuned, a quantitative and experimental set-up comparing the performance of the new solution with the old one would be appropriate, to determine whether performance would be lost for nondisabled users. However, it does give a deeper understanding of the accessibility of security solutions, especially the issues to consider when including audio in a mobile security application. When the solution is fine-tuned, a quantitative and experimental set-up comparing the performance of the new solution with the old one would be appropriated.

C. Database Interaction

Connecting the Database Driver used with Control Layer to validate the Request received from the Tomcat server and Responding the further process and is implemented Globalized such that the Database can be changed easily in code. First,
when developing security solutions make usability and accessibility priorities from the word go. Although we got useful feedback from one iteration, we strongly recommend several iterations of user testing.

D. Generating OTP Algorithm

The card no and pin no from the view layer and Current Day ,Date and time are taken from the packages and implemented as parameter for the OTP Algorithm . As a result it will generate the dynamic password. The simplest and oldest method of entity authentication is the password-based authentication, where the password is something that the claimant knows. This is to ensure interoperability with assistive technology such as screen readers, Braille display.

E. GSM Modem Implementation

GSM modem is a specialized type of modem which accepts a SIM card, and operates over a subscription to a mobile operator, just like a mobile phone. From the mobile operator perspective, a GSM modem looks just like a mobile phone. Importing the common Driver and connecting the Modem to the PC with serial port. A GSM modem is a wireless modem that works with a GSM wireless network. A wireless modem behaves like a dial-up modem. The main difference between them is that dial-up modem send sand receives data through a fixed telephone line while a wireless modem sends and receives data through radio waves.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

V. CONCLUSION

Finally, use multimodality—that is, auditory, visual, and tactile I/O channels—in the security applications or solutions for increased accessibility. Multimodality lets users compensate for a functional impairment by using another sense or function to interact with a device or application. For example, a visually impaired person can gain access to text and numbers through auditory or tactile output, or a deaf person can "hear" auditory output through text or sign language alternatives. This application is only a model to show how security in mobile banking can be improved and more work is needed after running and launching attacks on the system in a real time environment. This application is a working model that can be developed to become an important tool for banking customers.

REFERENCES

1. S. Milne et al., "Are Guidelines Enough? An Introduction to Designing Web Sites Accessible to Older People," IBM Systems J., vol. 44, no. 3, 2005, pp. 557–571.
2. ISO 9241-11:1998, Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs)—Part 11: Guidance on Usability, Int'l Organization for Standards, 1998.
3. Z. Obrenovic, J. Abascal, and D. Starcevic, "Universal Accessibility as a Multimodal Design Issue," Comm. ACM, vol. 50, no. 5, 2007, pp. 83–88.
4. T. Rønning, "Hverdagsteknologi for Alle—eller Nesten Alle" ("Everyday Technology for All—or Nearly All), Norges Blinde (The Blind in Norway), no. 6, 2004.
5. I. Klironomos et al., "White Paper: Promoting Design for All and e-Accessibility in Europe," Universal Access in the Information Society, vol. 5, no. 1, 2006, pp. 105–119.
6. K.S. Fuglerud al., Universal Design of IT-Based Solutions for Registration and Authentication, tech. report DART/02/09. Norwegian Computing Center, 2009.
7. L. von Ahn, M. Blum, and J. Langford, "Telling Humans and Computers Apart automatically," Comm. ACM, vol. 47, no. 2, 2004, pp. 56–60.
8. H. Jameel et al., "Human Identification through ImageEvaluation Using Secret Predicates," Topics in CryptologyCT-RSA 2007, LNCS 4377, Springer, 2006, pp.67–84.
9. M. May, Inaccessibility of CAPTCHA: Alternatives toVisual Turing Tests on the Web, vol. 2008, W3C WorkingGroup Note, 23 Nov. 2005; www.w3.org/TR/turingtest.
10. M.E. Zurko and K. Johar, "Standards, Usable Security, and Accessibility: Can We Constrain the Problem Any Further?" Proc. 4th Symp. UsablemPrivacyandSecurity(SOUPS08),2008;http://cups.cs.cmu.edu/soups/2008/SOAPS/zurko.pdf.
11. P. Wintlev-Jensen, "Ambient Assisted Living Joint Programme Objectives and Participation Rules," presentation at ICT 2008, 2008; http://www.alpsbiocluster.eu/call-for-projects/aal/AAL_Nakita_Vodjdani.pdf.
12. P.T. Jaeger, "Beyond Section 508: The Spectrum of Legal Requirements for Accessible e-Government Web Sites in the United States," J. Government Information, vol. 30, no. 4, 2004, pp. 518–533.
13. H. Hochheiser, J. Feng, and J. Lazar, "Challenges in Universally Usable Privacy and Security," *Proc. Symp. Usable Privacy and Security* (SOUPS 08), 2008; cups. cs.cmu.edu/soups/2008/SOAPS/hochheiser.pdf.
14. A. Jameson, "Usability Issues and Methods for Mobile Multimodal Systems," *Proc. ISCA Tutorial and Research Workshop on Multi-Modal Dialogue in Mobile Environments*, 2002; http://citeseerx.ist.psu.edu/viewdoc/ summary? doi=10.1.1.10.6704

AUTHOR PROFILE

R.Mohan received the bachelor's degree in 2009 in computer science & engineering from Anna University in Meenakshi College of Engineering. He is currently doing Master's degree in computer science & engineering from Anna University in S.A Engineering College. His research interests include Data mining & Data Warehousing, Mobile Computing wireless networks, network security. Topics include coverage problems in mobile Authentication, Secure Multimodal Authentication. He is a member of the IEEE.

N.Partheeban received the bachelor's degree in 1998 in Computer Science & Engineering from Madras University. Master's degree in 2005 in Software Engineering from Bharath University. He is currently doing Ph.D. in Information &Communication Engineering from Anna University of Technology and also Associate professor, Head of the Department in Information Technology in S.A Engineering College. His research interests include Data mining & Data Warehousing, web services & E-Learning, Network Security. He is a membership of the ISTE, IAENG.

.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)