RC24099 (W0611-024) November 6, 2006
Computer Science

IBM Research Report

What's Next Charles Schwab? Personal SPACE for Personal Financial Investing in Future Markets

Dawn N. Jutla
Sobey School of Business
Saint Mary's University
NS, Canada

Dimitri Kanevsky
IBM Research Division
Thomas J. Watson Research Center
P.O. Box 218
Yorktown Heights, NY 10598

Research Division
Almaden - Austin - Beijing - Haifa - India - T. J. Watson - Tokyo - Zurich

What's Next Charles Schwab? Personal SPACE for Personal Financial Investing in Future Markets

Dawn N. Jutla
Sobey School of Business
Saint Mary's University, NS, Canada
Dawn.jutla@smu.ca

Dimitri Kanevsky
Human Language Technologies
T.J. Watson Research Centre
IBM New York

Abstract

Companies whose missions are to empower individuals to take control of some aspect of their lives will face technological challenges to provide *S*ecure, *P*rivacy-aware, *a*nd *C*ont*E*xtual (SPACEd) solutions which scale to tens of millions of potential mobile customers in emerging markets. The authors present some promising human-centered solutions to these future technological challenges for online financial service providers in the scope of personal investment services.

Introduction

With over 6 million active client accounts and close to two hundred thousand in daily average client trades, the current market leader in online financial services provision, Charles Schwab and co differentiates with *personal customer service, competitive pricing, and best-of-breed financial service applications* for attracting and retaining its customer base. These three core anchors of Schwab's competitive strategy are tied to the company's ability to leverage new technologies to create and take advantage of emerging market opportunities. New technologies enable new or improved personalized financial service offerings, faster client response time, cost reductions in service offerings, and the opening of new markets.

Recognizing a new channel for customer service and expansion, many financial service companies, including Schwab and eTrade, moved to provide wireless access to its customers in early 2000. Schwab launched a wireless service, first named PocketBroker, and later re-branded as Schwab Wireless, to allow mobile Web customers to look at their account information, move money between accounts, get quotes and alerts, read market news and sector trends in real-time, and make online trades with their Web-enabled phones, Blackberries, BlackBerry Pearls, or PalmPilot PDA devices. Alliances with wireless service providers such as T-Mobile, Cingular, Sprint Nextel, and Verizon put Schwab wireless access directly onto the user's device interface, via an icon on the phone or PDA wireless menus.

Not all of Schwab's active clients transact through the Web or wireless channels. Thus, at most the technologies supporting these channels' users currently need to scale only to the low millions of users. Because of the high intensity of broadband connectivity and easy access to PCs in the USA, wireless-based services are not necessarily under executive focus in the North American market. A Touch Tone Trader service was rolled out in Europe to satisfy its citizens' high adoption and use of the telephony channel. However**,** companies with missions of empowering individuals to take control of some aspect of their lives (e.g. Charles Schwab's mission is to allow users to take control of their financial lives), are assessing the future market opportunity in emerging superpower countries, such as China, where the predominant access device is the mobile handheld. For companies such as these, the technological challenges in such markets will be in issues of (1) scalability to tens of millions of users at superior service performance, (2) multimedia-based client personalization, and (3) security and privacy provision and risk management.

Mobile Client Portfolio

Grid services and on-demand computing are technologies which address scalability issues. For example, in 2004, with an eye on improving transaction response time for its new services and retain its service performance as a competitive advantage, Schwab and co. deployed a Linux-based grid connecting its high-end servers. At the same time, it rolled-out grid technology over thousands of low cost servers to increase its applications performance. However, grid technologies are not sufficient in a future solution, involving further millions of potential clients, as network bottlenecks and congestion will continue to be an issue. Despite backbone and last mile bandwidth upgrades, the network congestion problem remains as the number of Internet users and the ratio of video content in applications' data are growing simultaneously.

Companies, such as Akamai (www.akamai.com), demonstrate useful models for addressing the network scalability problem in several application domains. Akamai's Edge servers, located at servers at local telecoms, distribute content and application programs to users, and thus can bypass most network bottlenecking issues by avoiding data center network paths. Computer science literature also has numerous examples of distributed models addressing scalability and performance issues. Thus a distributed architecture approach to scale to millions of users is necessary.

For personal investment services, we propose the use of a virtual client briefcase which allows a mobile user to travel with his/her virtual portfolio "following" or "shadowing" him/her everywhere and accessible via any local server computer near the user [7]. In particular, users with a PDA can be connected to any computer at any participating building (e.g. a

local bank or telecom) and immediately get at a financial services computer interface and data in their virtual briefcase or client portfolio related to them.

The virtual client portfolio can contains items as personal user data (e.g. user biometrics, client's financial portfolio data), general data that is often used by the client (e.g. dictionaries), software packages for office-type applications (e.g. database, spreadsheet, personal time management) and for multimedia and security (e.g. supporting speech, handwriting and user verification recognition systems), and specialized financial services applications e.g. those subscribed to from online discount brokers. Maintenance of the briefcase contents will occur on certain events, such as, the service provider pushing an update to clients' financial service applications. Figure 1 provides an example of how the virtual portfolio scheme works through a path of possible movement of a person from her home to the airport.

There are various ways to distribute a virtual client portfolio between a server and a client. Usually, the client devices would perform functions needed for front-end processing. For example, a front end of a speech recognition system can include a microphone and signal processor. Front ends are needed in the mobile world to support user verification and identification systems as well as natural language processing systems. Backends of various applications are usually stored on the server-side. Automatic speech recognition can include decoder output processing at the backend. Other examples of backends at the servers may be for user identification, natural language understanding, or even word processing.

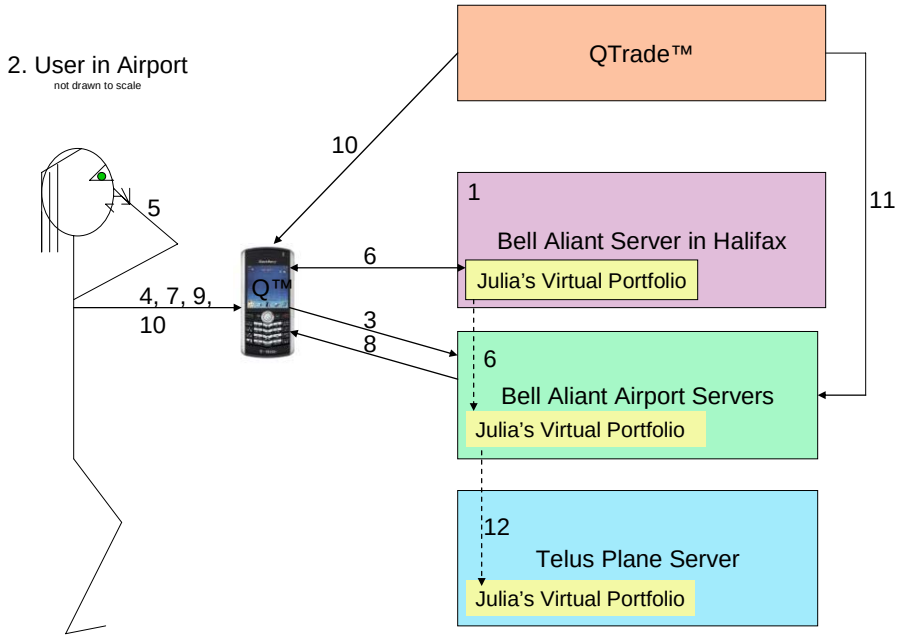

Figure 1. Example Scenario of the Mobile Virtual Portfolio Approach: (1) Julia's home is in Cape Breton, Nova Scotia and her virtual portfolio is stored mostly on Bell Aliant's servers. (2) Young Julia has won $5000.00 cash prize and a trip to NYC in an MBA student case competition. Today she is going to NYC and travels to the airport. (3) While waiting for a delayed flight to Newark International, Julia connects to Bell Aliant wireless services at the airport and browses through her BlackBerry Pearl™'s icons. She remembers her classmates in her Finance class recommending Microsoft with its buy rating. (4) She wants to invest $2000.00 of her cash winnings and taps the Qtrade™ icon. (5) Before Julia's virtual portfolio can be downloaded from Bell Aliant's central server to the Bell Aliant's servers at the airport, Bell Aliant must verify that the user is Julia. She is requested to use her gesture pin to identify herself. (6) Her gesture pin is verified on Aliant's servers and her virtual portfolio is sent to the airport's servers. (7) Julia now enters her trade information and invokes her risk management services. Based on her investment and trade category selections, portfolio-based financial applications perform risk management services on her financial information. (8) Bell Aliant's airport server sends the results to Julia on her PDA. (9) She decides to trade and inputs the requisite information on Qtrade™'s trading screen on her BlackBerry Pearl™'s wireless application interface. (10) Qtrade™ uses voice biometrics to verify Julia's identity and confirms the transaction. (11) The transaction confirmation updates her virtual portfolio. (12) Julia boards the plane. Her virtual portfolio moves to the plane's servers and is deleted off the airport's servers as per her privacy preferences around length that her data can be kept.

The client virtual portfolio consisting of applications and data may be stored in a server package and could be dynamically transferred from server to server as a client moves along a mobile network path. There are several design options for the

movement of the virtual client portfolio. In a static option, a local server can host the application programs and services and/or client data all the time, and the client can connect to these services when needed. A slight variation can be a scenario where the client device holds the data while the server holds the financial application services. In another design option, an encrypted virtual portfolio can move to another trusted server as the client moves into the range of this server, and the client can access the financial services on the new server, while the virtual portfolio can be deleted on the previous server. Alternatively, if a client path is known, trusted servers along the path can maintain copies of the virtual portfolio. Consistency strategies for these options are standard.

The advantage in all these options is that application services execute locally and the client may access an up-to-date portfolio nearest to her. The virtual portfolio scheme distributes network load to the server nodes immediately before the last mile connections. The usual alternative to the virtual portfolio proposal is congesting networks paths to the companies' centralized server farms within various countries.

Various devices allow detection of a person/client near some server location, including, and not limited to, a radio frequency tag, pressure sensor, ultrasonic detector, motion detector, and active signal from the client device. As clients are located near servers in the virtual portfolio traveling scheme, communication between them may occur using short range radio waves with large channel capacity. Several methods exist for detecting which shadow server is closer to a person depending on the client detection schemes. One popular method is to measure the strengths of the signals the servers receive from the client, and based on the result, cooperating servers decide which server will be associated with the client.

The virtual portfolio's distributed management provides a scalable solution to avoid network congestion on backbones and drop-off routes. The server load, which normally would be at Qtrade's data centers, offloads to a large number of local sites. In the example, processing is done at Bell Aliant's central and airport servers.

Improving Personalization via Conversational Data Mining (CDM)

Future business information systems, including emerging financial market platforms, will incorporate *multi-user input* to complement other external feeds from reliable electronically networked sources for enhancing business intelligence and competitive advantage. Organizations will focus on how future intelligent information systems can provide security, privacy, and context at the *user-level*

Examining context provisioning for mobile user applications, we find that apparatuses, such as, conversational data mining (CDM) [5] allow for attributes associated with a human voice to be determined and stored. The attributes can be used to improve the quality of the organization's metadata repositories for more effective and efficient customer and content management. These attributes may be further utilized for modification of the business logic of an underlying information system, which would then ultimately impact the business logic of the dialog management with the user. Many mobile-based financial transactions may be customized, in future, based on user context attributes such as location (remote or local), urgency, gender, age, literacy level, or social situation etc.

Key steps in conversational data mining are:

(1) Conducting a conversation with a voice system user either through human operator or automatic voice-enabled interface

(2) Capturing and digitizing the user utterances into a digitized speech waveform, extracting at least one acoustic feature, and storing the acoustic feature in a user model.

(3) At least one acoustic feature extracted from the digitized speech waveform is correlated with at least one gender attribute, such as gender, age, accent, native language, dialect, socioeconomic classification, educational level, and emotional state of the user. These attributes are used to adapt the user model.

(4) The user model is implemented in a storage structure and device that allows for data mining thereon.

(5) The attributes in the user model can be used to modify the logic of the voice system and to trigger adaptation of the logic of the underlying information systems in real-time.

The Dialog Management unit, shown in Figure 2, conducts a conversation with the user. The dialog management unit is implemented as a cooperating set of question-answering (Q/A) agents. The dialog management unit, and hence Q/A agents, can include the following capabilities: natural language understanding, natural language generation, finite state grammar, and/or text-to-speech synthesis for machine-prompting the user in lieu of, or in addition to, a human operator.

An audio capture module is coupled to the dialog management unit and captures a speech waveform associated with utterances spoken by a user during a conversation. An acoustic front end is coupled to the audio capture module and is configured to digitize the speech waveform and extract at least one acoustic feature. Examples of acoustic features of interest are MEL cepstra computation, and emotional state features, such as, running average pitch, running pitch variance, pitch jitter, running energy variance, speech rate, shimmer, fundamental frequency, and variation in fundamental frequency. Video capture and processing can augment audio input and processing. Video information can help identify or further classify user attributes, and train the various models used in the classifiers. For example, a smile means a jovial mood, red-faced may mean angry or embarrassed etc.

A processing module analyzes the acoustic and video features to determine any correlation to a relevant user attribute, e.g. an attribute listed in (3) above. The gender of a user can be determined by classifying the pitch of the user's voice, or by simply clustering features. In the latter method, voice prints associated with a large set of speakers of a given gender are built and a speaker classification is done on the two sets of models. The age of a user can be determined via classification into groups, similar to gender. Broad classes of ages, such as children, teenagers, adults, and senior citizens can be separated in this fashion.

Emotional categories which can be recognized are hot anger, cold anger, panic, fear, anxiety, sadness, elation, despair, happiness, interest, boredom, shame, contempt, confusion, disgust, and pride [5]. Furthermore, attributes can be captured for multiple users, and correlated. For instance, a couple shopping together online may display both similarity and differences in reactions to e-commerce interactions with vendors. Thus the processing module supports an emotional state classifier, a speaker clusterer and classifier, accent identifier, and associated knowledge stores as shown in Figure 2.

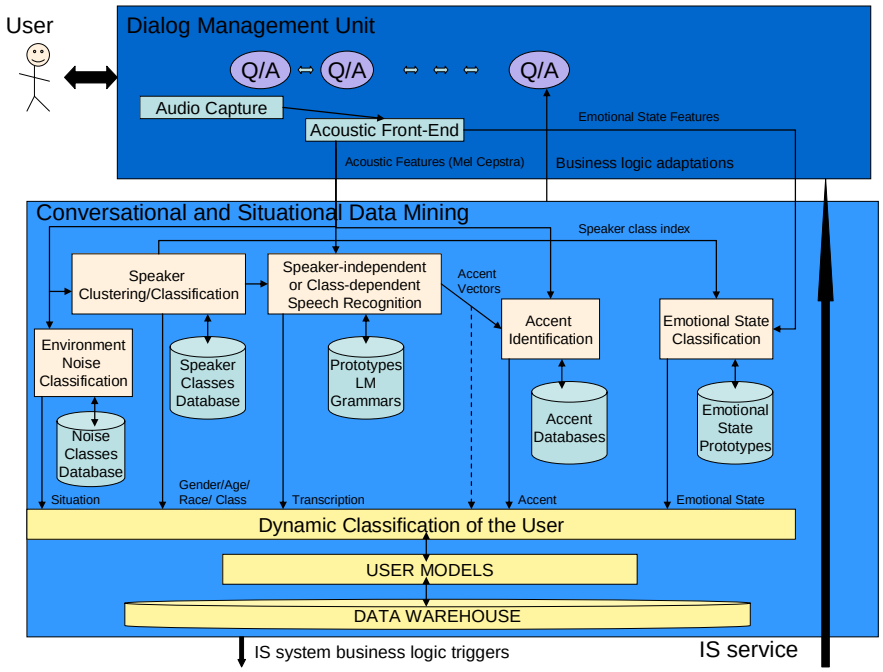

Figure 2. Conversational Data Mining

In addition to providing important emotional, demographic, and cognitive context data to user models, other contexts, such as situational and social contexts, can be captured by processing environmental noise at the same time that the speaker data is processed. It is possible to classify noises emanating from cars, trucks, mopeds, aircrafts, trains, people, traffic, subways, supermarket, office, conference room, etc. to augment situational awareness context. The CDM architecture is augmented to support situational contexts, as in [10], through the environmental noise classifier shown in Figure 2

Industry analysts (e.g. from Gartner Group) are predicting that organizations will have to be competent at classifying demanding users expecting various levels of excellence in customer service. The CDM scheme described here will provide technological assistance to support the customer-focused organization in industries with fierce competition.

OK-AD Classification of Biometric Security

Currently, financial service companies with an online channel indemnify their customers from loss through Internet security exploits. In 2005, eTrade cites multi-factor authentication as a strategic advantage. In early 2006, Charles Schwab and co. announced that the company will absorb the loss due to any online security issue a client experienced. This company action to reduce its customers' security concerns around the Internet channel may be profitable with three million online clients but risk figures may be less acceptable at 20 million clients, despite the spread potential. Moreover, the lack of accountability mechanisms for security exploits in the wireless channel is far greater than on the Web channel.

The landscape for security solutions for the wireless and wired Web is classified in "OKAD" mechanisms which verify what the client **O**wns, **K**nows, **A**re, or **D**oes, and are based on the notion of Total Biometrics [4]. The OK mechanisms, those which verify what the client owns (e.g. a userid) and knows (e.g. a PIN number), are commonplace in online banking and access to workplaces' networks. The shortcomings of the OK mechanisms are well known, including, stories similar to the unwitting employee writing the passwords to AIDS patients' databases on a 3M sticky and pasting it to the host database server machine. The stronger AD mechanisms are user biometric-based – that is, they verify access identities based on personal biological characteristics.

Type A (what the users are) security biometrics are generally stronger than the OK, and D counterparts as they are not easily transferable to other users. Examples features of type A biometrics include facial bone structure, signature, face temperature infrared pattern, hand geometry, writing instrument velocity, writing instrument pressure, fingerprint, and retinal print. OKAD mechanisms are used together to provide layers of defence or multi-factor authentication mechanisms. Type A user biometrics can be synthesized consisting of user voice

print, static or dynamic textual information, and other semantic user information. Semantic information can also be those gleaned from conversational data mining (such as age and gender). In an implementation, such a biometric can also contain video information.

The multimedia security architecture in [6] is type A and utilizes knowledge known by the user and knowledge acquired by the speech recognition engine (e.g. speech rate, accent, preferred vocabulary, and/or preferred requests). The system is capable of building new questions, either by learning about the user or, after identifying the user, asking new questions, and storing and using these answers in future verifications. New user knowledge is then potentially acquired at each user interaction and the system can embody logic to adapt and maintain the user model at various stages of the user's lifetime. The system can auto-correct user models if a calculated security score is poor, and the user can be verified/authenticated by other valid means.

Such a user biometric-based security system protects against common security exploits such as playback as the latter cannot handle the random dynamic questioning and real-time dialog. Even if all the answers are known (say, by a relative or former friend), this voice security method protects as speech rates etc. in the voice prints will be different. The system also scales better than many existing voice-based verification schemes [6]. Details of the user models, text-independent speaker recognition, automatic speech recognition techniques, and score estimator process can be found in [2, 5]. There is also an opportunity to use private data management questions as part of the set of security questions so that the user time to access a privacy-aware service is faster. For privacy-awareness, with respect to data and application access in the mobile world, semantic analyzers, and ASR techniques should include knowledge of the privacy domain.

In step 10 of the scenario provided in Figure 1, where Qtrade™ uses type A voice biometrics, as in [6], to verify Julia's identity at the airport, it is also possible to strengthen the security system with multi-factor authentication based also on question-answering. The type K security solution in [8] works particularly well for a noisy situation such as found in an airport or stock market floor, where voice may fail. The apparatus in [8] allows the user to answer questions without voice. The user can respond to a query, such as "show a face that you are familiar with", by pointing a finger via a touch-tone pad to multiple choice answers that are represented as pictures. The picture set may contain, for example, a set of pictures of strangers and a face of a person's son.

Less well known are the type D security methods which capture what a person uniquely *does*. A *gesture PIN* [4] is a *behavioral* password which includes a series of intentionally performed user gestures which are extracted, processed, and compared to corresponding pre-stored data. For example, a gesture pin may consist of the following three gestures: touch one's nose, step forward, and step directly to the left. Habitual or reflexive unintentional gestures or movements and sounds occurring during the performance of a gesture pin may be incorporated in the behavioral password. As an example, perhaps a particular user habitually bends his head down each time he touches his nose. User performance characteristics, such as, the speed of transitioning from one gesture to the other, may also be incorporated in the behavioral password. Speech features including accent, stress, and the spacing between utterances may be incorporated in the behavioral password. Behavioral passwords can be overlaid on conventional passwords such as the content of an oral answer to a prompted question. Thus one embodiment of a gesture pin may have all four OKAD properties.

Gesture pins have an advantage in a noisy environment where voice identification and answering questions by voice can fail. In an implementation, a "natural" gesture pin consisting of natural gestures that a person may do anyway, such as scratching a nose, or combing hair, may be useful since some gestures are not private and can be seen by other people. A natural gesture pin could prevent both disclosure of the pin to a watching public, and any perception that the user is a crazy person.

To show how the gesture pin would work at a technical level, consider that a personal investor is prompted for her gesture pin and produces a sequence of gestures, sounds, and text which her PDA camera, microphone, and keypad capture. A gesture recognition module maps the recorded gestures into a behavioral pattern - decoded gesture pin. A module matches the decoded gesture pin to a behavioral pin (user pin) stored in a user pins/productions database and determines whether user access is denied or granted.

Digitization of video signal involves spatial sampling and quantization for reduction in computational complexity. Each digitized image is timestamped and can be represented as a single vector or point in an n-dimensional vector space, where n is defined as the number of pixels in an image, the number of different colors represented, and the number of different intensities with which the colors can be represented. Several points may correspond to a relatively fixed position (e.g. a finger on a nose). These points will be located near to each other in the n-dimensional space and thus be clustered together and replaced by a representative cluster point. A clustering module clusters the vectors using general clustering methods further reducing data variability and computational complexity. Time labeling of frames is preserved so that characteristics associated with the performance of gestures (e.g. the speed of performing a gesture or sequence of gestures) may be later extracted. Accordingly, in the case of a cluster vector, its time variable is updated to reflect the time variable of all the vectors within the associated cluster.

After clustering, the clustered vectors/frames are then input to a gesture segmentation module which consists of a frame comparator, and stroke detector and collector. The frame comparator compares consecutive frames to measure the speed of the positional changes of the user's body. Second, frames are compared with a library of basic positions required to interpret user gestures. These positions include, for example, pictures of a finger touching an object (e.g. nose, forehead, ear, wall, table) or pictures of essential elements of body parts movements (e.g. a straight versus folded arm, a closed versus open eye). A symbol is formed from a concatenation of strokes where a stroke is defined as a series of images which represent the user performing a particular gesture. Examples of strokes are "stand", "move hand up", "touch nose", "move hand

down", "touch forehead", etc. Whereas, an example of a symbol, is "nodding" which concatenates "move head up" and "move head down" strokes. The collection of symbols forms a vocabulary. Each symbol corresponds to a Hidden Markov Model (HMM). A sequence or string of gesture symbols may be interpreted as a semantic unit again reducing computational complexity and adding "human" reasoning to the gesture pin system.

Implementation of such behavioral biometric systems will assure uniqueness of user pins on user enrollments, and other pin management activities. What is pertinent to organizations is that a scheme such as a gesture pin can support any or all human-centered OKAD properties for mobile security in support of commerce.

SPACED User Portfolio and OKCAD

A SPACEd object is **S**ecure, **P**rivate, **a**nd **C**ont**e**xtual. A Personal Investor's virtual portfolio may be SPACEd with the conversational data mining solution [5] for context support, and with multi-factor biometric authentication as in [4, 6]. What remains for us to show is how to add privacy-awareness.

Privacy legislation in the Financial Services sector provides a highly motivating hand-of-the-law factor for executives to pay close attention to user privacy. GLB Regulation P (1999) in the USA, Canada's 1983 Privacy Act and the Private Information Protection and Electronic Documents Act (PIPEDA, 2001), and the EU's 1995 Data Directive are in force with respect to privacy compliance for nationals and multinationals, conducting any financial transactions within and across borders. Regulations limit financial institutions' use of data across lines of business e.g. travel and medical insurance information held by one business unit cannot be automatically shared with decision makers in the loans unit. Such regulations mean that organizations capture similar user data at multiple points, and may build and maintain user models per business unit in order to personalize the customer's service experience. Central user models are possible as long as usage of the data therein is controlled, that is, owned and used by separate units.

The personal investor's client portfolio and its contents, including applications and data, can be made user-preference-aware in several aspects, such as privacy, social, ethical, and economic user concerns. A preference can be a fact or user rule. An example of a personal investor's privacy preference may be for the company not to disclose her personal data to its third party telemarketing partners. An ethical preference may be not to purchase stock of a company which employs child labor. An economic preference may be a regulation such as country law which stipulates that no more than 30% of an investment portfolio can be in a foreign country. A social preference may be user unwillingness to buy stock of a company that deals with selling guns. We extend the classification of total biometrics given in [4] to include such general user preferences, including privacy preferences.

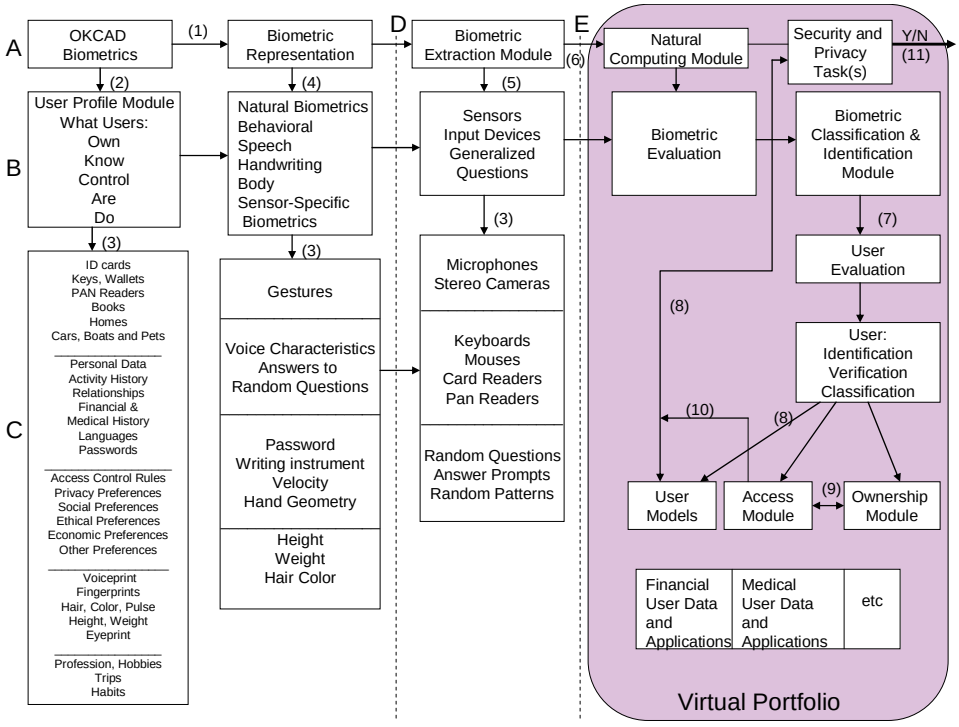

Figure. 3 OKCAD Biometrics for the Mobile User's Virtual Portfolio. (1) OKCAD biometrics can have different biometric representations which the biometric extraction module detects and extracts and passes on to the natural computing module for processing to fulfill a security task(s). (2 The User Profile module maintains the split of OKCAD into what users own, know, control, are, and do. (3) Block C places the OKCAD, biometrics, and biometric extraction methods into categories. (4) Biometric representation is broken

down to natural and sensor biometrics. (5) Biometric extraction can occur either through sensors, input devices, or generalized questions, and may be either at the client-side (D), server-side (E), or both. (6) The natural computing module classifies user biometrics as unintentional/intentional and their combinations of sources. (7) User evaluation includes identification, verification, and clustering. (8) User models are retrieved and/or updated. (9) Ownership module establishes proof of possession. (10) Access module decides whether the user gets access. (11) The security and privacy task(s) module provides the results to the user and updates the User models.

Figure 3 shows a classification of OKCAD security and privacy (and user preference) mechanisms, and illustrates what categories of biometrics and related user data or models may be stored in the user's virtual, mobile portfolio. The **C,** introduced to OKAD, refers to what the user **c**ontrols such as access to personal data.

User privacy preferences specify which data and for what purpose(s) the data can be accessed, whether it can be shared with others, how long the data can be retained, and so on. Thus key steps for privacy management at the multimedia user interface involve statements and questions around user consent, user access to personal information organization's collection, storage, retention, and use of user data. Privacy management in classification systems, such as the conversational data mining module, can be first ascertained in a system. Specifically, companies may store and must comply with stated users' privacy preferences. Details for a privacy management process for adding privacy-awareness to conversational data mining (CDM) may be found in [3].

Recall that a user's virtual portfolio may contain user biometric data and biometric processing applications, as well as financial data and its applications. Since external and internal applications may access the virtual portfolio data, access control for private data is necessary. Privacy preferences or rules may differ on an application-basis, or at a finer level, on a transaction-basis.

User privacy management has binary consequences similar to access control in the security component. For instance, can the organization "collect" (substitute "collect" with "store" or "share" or "use for a particular purpose") particular user data – yes or no? The user data can be video of the user, audio, text, etc. which can characterized by various attributes such as actions (e.g. text updates, user gestures), states (e.g. red-face), relationships among multiple users (e,g, familial, co-worker), and so on.

Aspects of user models for privacy management can be found in [2]] and an XML privacy vocabulary in the P3P specification [9]. Some user model attributes for privacy, from the organization's perspective, include individual data release rules, client trust (in the organization) attribute, user role, and user tenure with the organization. In addition, organizations must support governance models for privacy management with respect to various sectors, and countries.

What's Making the Trade?

In 2006, Schwab and co. announced a price reduction for its online trade fee in what some call the simmering stage of a potential price war. A recent Canadian survey [1], with 1641 participants rating 10 online brokers in Canada, finds that the number one reason a client stays with a particular online financial service company is its service pricing - specifically the trade fee in personal online investing. There were five other factors of importance to users, identified in [1], relating to the availability of (1) tools for researching stocks and mutual funds and for financial planning and portfolio building, (2) trading tools for mutual funds and bonds, (3) wide variety of investment selection including bonds, guaranteed investment certificates, and guided portfolios, (4) information to show how personal investments are doing, and (5) website utility.

The online channel is the cheapest service delivery channel due to its customer self-serve model. In the long term, this channel, along with mobile interfacing, is expected to cause most industry disruption. The human-centred technologies we present and refer to are relevant and useful in addressing the technical challenges around financial services scalability, security, and privacy for mobile personal investment.

New business models and opportunities for financial service providers arise when relevant technologies become available. For example, the mobile personal investment channel is suited to impulse shoppers. Many clients buy stocks, mutual funds, options, and so on, based on recommendation (word of mouth, newspaper, analyst on TV). The decision to make the trade may happen on the train, taxi, or plane, on the sidewalk on seeing a visual trigger, or at home.

Human-centred technologies for increasing customer service quality and satisfaction, security, privacy, and personalization may become significant enablers of wealth creation. Such technologies could allow financial services companies to readily serve any sophisticated or naive client, within the range of a mobile network, in current and future markets. Well then, Charles Schwab, could SPACE be your next frontier?

References

[1] Carrick R., Smart Money's 2006-07 On-Line Broker Rankings, The Globe and Mail , Toronto, Sept 16, 2006.

[2] Jutla D.N., Bodorik P., Zhang Y., PeCAN: An Architecture for Privacy-aware User Contexts for Electronic Commerce on the Semantic Web, *Information Systems*, Elsevier, 31:4, pp. 295-320, June 2006, appeared online April 2005.

[3] Jutla D.N. and Kanevsky D., Adding User-Level SPACe: Security, Privacy, and Context to Intelligent Multimedia Information Architectures, IEEE/ACM/WIC Web Intelligence/Intelligent Agents Technology First International Workshop on Web Privacy Intelligence, Hong Kong, December 18, 2006.

[4] Kanevsky, D., Maes, S.H, US Patent No., 6,421,453 B1, Apparatus and Methods for User Recognition Employing Behavioral Passwords, 2002

[5] Kanevsky, D., Maes, S.H., Sorenson, J.S., US Patent No. 6,665,644 B1, *Conversational Data Mining*, 2003

[6] Kanevsky, D. and Maes, S.H., US Patent No. 6,529,871 B1, Apparatus and Method for Speaker Verification/Identification/Classification employing Non-acoustic and/Acoustic Models and Databases, 2003

[7] Kanevsky D. and Zadrozny, W.W., US Patent No 6,912,580 B1, Virtual Shadow Briefcase in Servers Supporting Moving Embedded Clients, 2005.

[8] Kanevsky D. Maes, S.H., and Zadrozny, W.W., US Patent Application, US20010044906A1: Random Visual Patterns used to obtain Secured Access: http://appft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=2&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=57&f=G&l=50&co1=AND&d=PG01&s1=dimitri.IN.&s2=kanevsky.IN.&OS=IN/dimitri+AND+IN/kanevsky&RS=IN/dimitri+AND+IN/kanevsky

[9] P3P standard at www.w3c.org/p3p

[10] Smith, D., Ma, L., Ryan, N., Acoustic Environment as an indicator of social and physical context, Personal Ubiquitous Computing, 2006, 10:251-254.

Dr. Dawn Jutla is a Professor of Information Systems and Computer Science in the Department of Finance, Information Systems, and Management Science at Saint Mary's University in Halifax, Nova Scotia, Canada. She has authored over 70 papers in e-commerce and e-government. She is co-author of the 2001 book entitled *e-Business Readiness: A Customer-Focused Framework* in the Addison Wesley Information Technology Professional Series

Dr. Dimitri Kanevsky is an IBM T. J Watson researcher, master inventor, and project manager. His areas of expertise span human language technologies, mathematics, communication technologies for accessibility, and speech recognition for embedded devices and transcription. He holds 89 US issued patents and more than 100 worldwide. Between 2002 and 2006 at least 9 of his patents were classified in the top 10% for major impact on IBM's business.