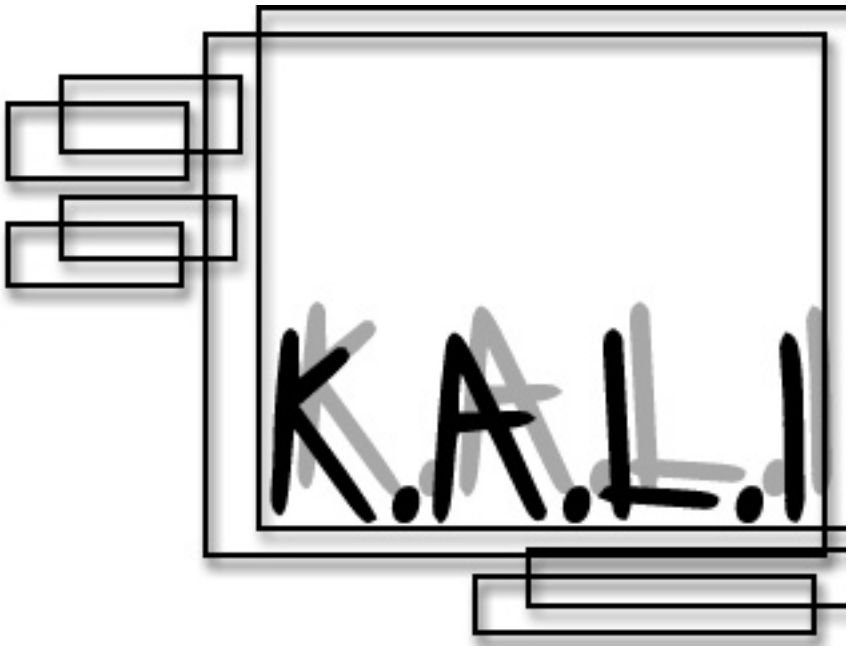
Crossroads
The ACM Student Magazine

Electronic Commerce Universal Access Device:

The Knowledge-Acquiring Layered Infrastructure (KALI) Project

by ***Theodore Chiasson*** and ***Carrie Gates***

Introduction



The goal of the Knowledge-Acquiring Layered Infrastructure (KALI) project is to create an architecture that supports a universal access e-commerce infrastructure. This architecture must support users who have low literacy levels, and allow them to participate in the new knowledge-based economy. Much of contemporary research and development focuses on making access easier for computer-literate end users. Our research is different, in that it assumes a very low level of literacy, computer related or otherwise. This introduces interesting constraints on the design of the architecture.

Technology is creating an ever-widening gap in society. Those not adept at technological wizardry stand to be left behind. Our research focuses on special education students in their last year of secondary school (whose educational program includes life skills training). It is hoped that solutions for this population will extend naturally to other domains, and we shall endeavor to keep extensibility in mind as a primary design goal.

This paper contains a high-level description of the technical requirements of one such enabling infrastructure which meets the above design goals. The KALI project is still in the nascent stages, so this paper concentrates on defining the problem at hand and identifying areas which require further research.

From the Desktop to the Palmtop

Current trends in computing indicate a shift away from general purpose desktop computers towards mobile, hand-held devices. Major industry initiatives in this area include Jini [8] from Sun Microsystems and pervasive computing initiatives from IBM [7] and HP [6]. Examples of the growth in mobile, hand-held computing include the proliferation of cell phones and PDAs (Personal Digital Assistants), such as Palm Organizers [10]. While becoming smaller and more mobile, these devices are concurrently getting easier to use than traditional desktop computers. For example, a hand-held device user would never need to understand desktop computer concepts like operating system version, software installation, or hardware upgrading.

Recognizing the disparity of complexity between desktop and palmtop computing media, it is clear that our goals can be met with a wireless, hand-held, electronic commerce device. This device must be easily accessed by the authorized owner, but entirely inaccessible to anyone else. In addition, this device should be designed to aid in the planning and execution of daily living activities for persons with low literacy and/or cognitive abilities.

Usability Considerations

One design challenge concerns user interface mechanisms. Good user interface design uses symbols which are familiar to the user with a clear and natural mapping from the functionality of a control to its appearance [3]. This mapping must be natural from the end user's viewpoint. Consequently, an understanding of the target population is required before good user interface design can be accomplished. Due to the limitations of our target population, interface mechanisms to be addressed include those for authentication, input processing, and output generation.

- **Authentication** -- Techniques for proving ones identity can generally be classed into four categories:
    - Tokens -- what you have (e.g., smart card)
    - Challenge -- what you know (e.g., username and password)

    - Biometrics -- what you are (i.e., fingerprint, retinal scan)
    - Location -- where you are (e.g. within a building)

  The end users of our research cannot be expected to remember usernames and passwords. The location constraint might be applicable in some circumstances, as discussed later in the section on security. The user's device is itself a form of token, but restricting its use will have to rely on biometric measures. Authentication is particularly important to our end users.
- **Input processing** -- Clear input might be achieved through the use of customizable pictures in conjunction with a touch screen. Examples of globally recognizable symbols include a red stop sign for abort, and a green circle for proceed. Further research is required in this area to determine which particular symbols can be used for interfacing with these individuals.
- **Output mechanism** -- The vast majority of user interfaces display information in textual form. A simpler interface will be through simulated speech delivery. Speech patterns must be easy to comprehend so it is understandable to the end user.

Initial user preferences will be customizable, and based on interactions with special education teachers, parents, and students. An electronic commerce device tailored to the needs of the individual student can be integrated into the life skills training program, and may help the student to succeed in functioning independently after the transition from school to the community.

Design Considerations

The Evolution of Peer-to-peer

During the 1980s and 1990s, advances in technology enabled a paradigm shift from centralized computing to the client-server model. The driving force behind this shift involved the increased computing capacity of client machines and the increasingly distributed nature of networks as they evolved from local area networks to the global Internet. Centralized systems typically housed large applications written by expert programmers for a specific system and architecture. In contrast, distributed client-server systems, partition the world into complex servers and relatively simple clients. Less expertise is needed to develop client applications than was needed for the large centralized applications.

As technology continues to evolve, another paradigm shift is likely to occur -- this time

from the client-server model to a peer-to-peer model [1]. In a peer-to-peer model, each participant in an interaction is equal. Each process or component is independent, and able to dynamically assume the role of a client or server based on the context of the interactions. Numerous specialized multiapplications can be written by applications programmers or even by the end user. The architecture is dynamically reconfigurable by the end user and applications are portable across languages, systems, and architectures.

While the evolution from dumb terminals to personal computers enabled the client-server model to proliferate, the advent of permanently connected home computers, broadband to the home, wireless technologies, and device-oriented computing will drive the next paradigm shift towards peer-to-peer computing.

The vanguard of this peer-to-peer model is already emerging on the Internet, especially in the business to business domain [4]. In the business to consumer domain, the consumer is typically viewed as a client, which restricts the models of interaction that are available. In the absence of a peer-to-peer model, content can be delivered to a client on a periodic basis by having the client poll the server for updates. This model has been adopted in products such as PointCast [11] and Castanet [5]. Further, some interesting new business models have arisen which communicate back to the client via e-mail. Examples include services such as Priceline [12], where consumers can name the price they want to pay for a product or service. Since the user is interacting in a client-server architecture, the response from the server must take the form of e-mail. In a peer-to-peer environment, the user's device would act as a server that priceline.com could contact and interact with directly. Another example is the offering at Mercata [9], where buyers are aggregated to lower the purchase price of goods. In this case, a user can agree to the current price of a product and be guaranteed that the price will either stay the same or go down until the deadline for the sale. This forces the user to commit to the current price in order to participate. In a peer-to-peer environment, the user could potentially request notification when a product of interest dropped below a certain threshold, and hold off on the commitment of funds until the desired price was reached.

Layered, Distributed Architecture

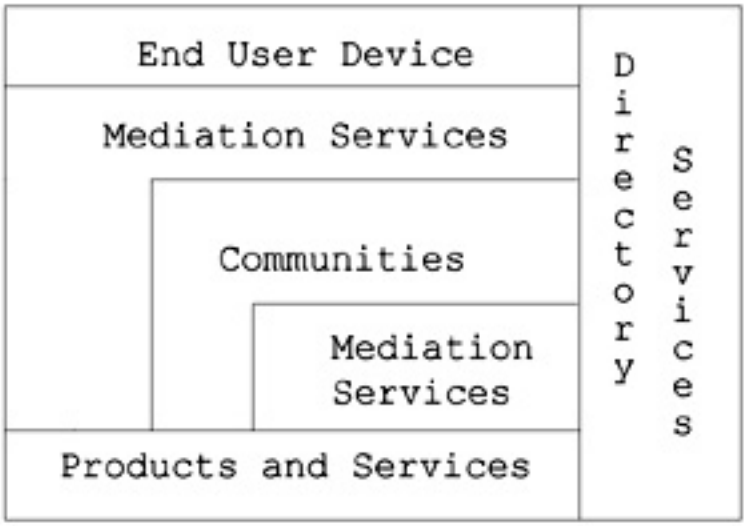


Figure 1. Layers in the KALI environment

Our research develops a layered infrastructure that supports the peer-to-peer paradigm. The sample distributed application we will implement as a proof of this concept is an intelligent mediation environment for electronic commerce that uses profiling information to establish appropriate constraints on transactions, such as preferred vendors for particular goods, location and timing constraints for goods to be picked up or delivered, and budgetary constraints applied over the long term. User profile information is stored in the system, and the profile dynamically learns a user's preferences over time. It is planned that the previously discussed hand-held device, customized for the target users, will act as the interface.

A layered, distributed architecture is used to support the intelligent mediation environment. The distributed nature of the architecture presumes the involvement of different vendors and users across the Internet. Components of the architecture can be located anywhere in the world, and distributed directory services are used to register services and to locate registered services. The user interface device is at the highest layer of the architecture. This device communicates with a mediation layer, which uses user profiling information and vendor offerings to intelligently apply constraints to user requests and come up with a set of goal-oriented transactions. This mediation layer may reside on the user's device, on a dedicated server, or on a shared Internet server. In fact, this layer and all lower layers can be distributed across the Internet on many devices and servers. An intermediate layer is used to accumulate the buying power of many individuals into a community. The mediation process requests information directly from vendor sites as well as through community intermediaries, thus guaranteeing that the best possible price will always be achieved for the end user.

Mediation services can also be employed by communities, which introduces another mediation layer between communities and vendors. Communities only form in instances where bulk purchasing yields sufficient savings to support the operations of the intermediary, or where consolidation of shipping yields additional benefits. Coordination among vendors and communities is used to consolidate deliveries to individual users. Directory services are used by all layers to register their own availability and to look up services offered by other layers. Each layer can access services from peers within its own layer. This allows for direct communication and collaboration between end user devices, and for a recursive mediation structure where high-level mediation services call on lower level services within the same layer. Mediation is discussed in detail a little later.

Distributed Database Transactions

In traditional database processing, transactions are short-lived. For example, when using an automated teller machine to withdraw funds, the user interacts with menus in order to request money. The transaction to actually withdraw the funds does not begin until after the user has committed to the withdrawal. At that point, the transaction request is dispatched to a central database for processing. Upon arrival, the transaction request is processed very quickly, and the response is sent back instructing that the funds be issued or that the transaction be denied. The user might check the balance in the account before withdrawing funds, but this is processed as a separate transaction. In fact, the balance might change between the user checking the amount and their subsequent withdrawal. The user is involved in initiating transactions, but locks on data items are not held in the database between subsequent transactions.

In our model, we enact distributed transactions across multiple vendors and communities. At the lowest level vendor databases are accessed to obtain pricing information and to enact purchasing transactions. These vendor databases are typically legacy database systems, which do not natively support distributed transaction processing. The mediation layer is responsible for managing the distributed transaction processing. Unlike traditional database processing, the end user is involved during the commitment process. Rather than unilaterally chosing a particular purchasing plan on the user's behalf, the mediation layer will ensure that a particular transaction is possible and then getting user verification before accepting the transaction. This model could result in longer transactions than in traditional database processing. Consequently, a new distributed transaction processing model is needed. The

development of such a model is a major focus of our research.

Security

From a security perspective, it is necessary that the end user be able to use their own device securely, with ease (i.e., no password/username/pin). This requires some form of identification unique to the individual, such as fingerprint, retinal scan, voice print, or other biometric technologies. Ideally, fingerprints and voice prints would be used more commonly than the more invasive biometrics, such as retinal scans and iris recognition. However, these less-invasive techniques are also more prone to error. For example, some fingerprints can not be recorded due to cuts or scars that obscure the ridges, while others have ridges that are too fine to be captured well by a photograph. As a result, work has been done on combining biometrics, which has been shown to increase security by reducing the number of false rejects (valid users who are rejected) and erroneous validations (invalid users who are allowed access) [**2**].

Building on the use of multiple biometrics, the level of access can be varied depending on the combination of biometric authentications presented to the device. Thus, purchasing groceries might require only a thumb print, while buying a new car might combine several "more secure" biometric authentications. Access to functionality could be restricted by type of authentication in combination with locality (using GPS), or in some cases with additional constraints such as "in the presence of a registered physician" for access to medical records. A person's individual security profile could be customizable, such that the end user determines which combinations of authentication techniques provide which levels of access.

Such use of biometrics will allow the identification of a unique individual, anywhere in the world. Currently, governments assign IDs to their citizens at birth (e.g., Social Insurance Number in Canada, Social Security Number in the U.S.) If the identification resided instead with an individual's biological makeup through use of biometrics, it would allow unique identification in a truly global sense. Further, it could be implemented in such a manner so as to return control over one's identity to the individual. Rather than a government or corporation storing and combining information based on an assigned ID number, the individual can allow access to only relevant information based on need. By using different biometric keys, cross-correlation of information from multiple sources can be discouraged or made infeasible, hence securing privacy.

With biometric authentication, access to assets is always possible. In a compromising situation, a criminal knows you have full access to funds. Geographic location could potentially be used to prevent global access to accounts. For example, one might configure a security profile to limit the amount of funds available for transfer unless you are actually located at your banking institution. Another approach is to include voice-print as a biometric device, and use the changes in voice-print due to stress to automatically prevent transactions from occurring when the device detects that you may be requesting transfers while under duress.

Data mining techniques might also be used for determining if a transaction is fraudulent. Users typically have usage patterns. Consequently, any transaction outside of this pattern can be declared suspect. Companies, such as Visa, already use neural networks to recognize potentially fraudulent transactions. [**13**]

Mediation

Interaction with the device must be intuitive to the target population. Negotiation of transactions can be accomplished through intelligent mediation, hiding the complexities of the transaction from the user while still affording the user control over the negotiation decisions. Information stored over time in the user's profile can be used to facilitate mediating decisions. Collection, access, and storage of profile information must be performed in a secure fashion. Further, the process of mediation must itself be protected from compromise.

The intelligence of the infrastructure mainly resides in the mediation of activities between the user and the remote servers from which goods and services are be purchased. Factors that could come into play may vary, depending on the domain space in question. For example, in the domain of grocery shopping, a list of preferred foods is requested. A purchasing decision is required that takes into consideration all of the following criteria, and potentially many others:

- Budgetary constraints (both short-term and projected for the long term)
- Dietary constraints (from medical profile consultation)
- Nutritional constraints (based on publicly available sources, i.e., food guide)
- Location constraints (shipping charges/convenience of pickup locations)
- Timing constraints (known long term needs for taking advantage of sale items)

Over time, an evolving personal profile helps facilitate mediation. The more information available to the mediation process, the more effective the device can be.

The process of mediating transactions can be performed at various levels in the architecture, including on the device itself, on a dedicated server on the Internet, or on a shared Internet server. To ensure that privacy is not compromised, profile information is never shared with the vendor sites without authorization from the end user. Instances may arise where it is in the user's best interest to share their profile with vendors -- one example is in the purchase of prescription medication from various different pharmacies. While individual pharmacy chains track your prescriptions to ensure there are no known conflicts in the drugs prescribed, the user has to volunteer information if prescriptions are filled at different chains.

A catalog or directory structure is maintained by the device for use in contacting the appropriate mediation services for a given task. The mediation services themselves also make use of directory services for use in collecting information relevant to assigned tasks. During the mediation process, the user profile information is matched with the device request and the available sources of products and services on the Internet. Negotiation occurs on the user's behalf to enact transactions. These negotiations may cover areas such as price, quality, quantity, timing of deliveries, and payment mechanisms.

Conclusion

A paradigm shift from the client-server model to a peer-to-peer infrastructure is occurring. This evolution is driven in part by the growing need for complex interactions between end users and service offerings on the Internet. By building an intelligent layered infrastructure that acquires knowledge via user profiling and service registrations, much of the complexity of distributed applications can be handled transparently. By moving the transaction complexities into the architecture, the KALI project lifts much of the onus previously placed on the end user, lowering the learning curve and reducing the barriers to entry for those less technologically inclined.

Acknowledgements

This research is supported in part by grants from the IBM Canada Center for Advanced Studies, the Izaak Walton Killiam Fund for Advanced Studies at Dalhousie University, and the National Sciences and Engineering Research Council of Canada.

References

1

Bauer, M.A., Coburn, N., Erickson, D.L., Finnigan, P.J., Hong, J.W., Larson, P.-A, Pachl, J., Slonim, J., Taylor, D.J., and Teorey, T.J. A distributed system architecture for a distributed application environment. *IBM Systems Journal*, Vol. 33, No. 3, 1994, pp 399-425.

2

Frischholz, R.W., and Dieckmann, U. BioID: A multimodal biometric identification system. *Computer.* 33, 2 (Feb. 2000), 64-68.

3

Norman, D. *The Design of Everyday Things.* Doubleday, New York, 1990.

4

Papazoglou, Mike P., Jeusfeld, Manfred A., Weigand, Hans, and Jarke, Matthias. Distributed, Interoperable Workflow Support for Electronic Commerce. *Lecture Notes in Computer Science*, May 21, 1999, Vol. 1402, 192-204.

5

Marimba' Castanet. **http://www.marimba.com/products/castanet-intro.htm**

6

Hewlett-Packard Company. **http://www.hp.com/pressrel/nov99/04nov99a.htm**

7

IBM Pervasive Computing. **http://www-3.ibm.com/pvc/**

8

Jini Connection Technology. **http://www.sun.com/jini/**

9

Mercata: Group Buying Power. **http://www.mercata.com/**

10

Palm, Inc - Handheld Computing Solutions. **http://www.palm.com/prodsoft.html**

11

Pointcast. **http://www.pointcast.com/**

12

priceline.com. **http://www.priceline.com/**

13

Visa - Press Release. **http://www.visa.com/av/news/press_release.ghtml?pr_form_edit=271**

Biography

Theodore Chiasson is currently enrolled in the PhD in Computer Science program at Dalhousie University in Halifax, Canada. Research interests include distributed transaction management, distributed concurrency control, intelligent mediation, and performance.

Carrie Gates is currently enrolled in the PhD in Computer Science program at Dalhousie University in Halifax, Canada. Her research interests include security, electronic commerce, and neural networks.