Proceedings of the 1998 Winter Simulation Conference
D.J. Medeiros, E.F. Watson, J.S. Carson and M.S. Manivannan, eds.

EVALUATION OF ELECTRONIC CASH THREAT SCENARIOS USING MICRO DYNAMIC SIMULATION

Kazuo Ezawa
Gregory Napiorkowski
Mariusz Kossarski

Mondex International Limited
Atlantic Technology Center
Suite 109, 100 Campus Drive, P.O. Box 972
Florham Park, New Jersey , 07932-0972, U.S.A.

ABSTRACT

This paper discusses the evaluation of the electronic cash counterfeit threat scenarios using micro dynamic simulation. This modeling technique provides information needed for the quantification of economic risk exposure in conjunction with other analytical tools. It also allows the evaluation of the effectiveness of various on-chip risk management capabilities. And by generating test data, it allows the assessment of the effectiveness of the host system based counterfeit transaction detection models.

1 INTRODUCTION

The quantification and evaluation of a hypothetical threat caused by an introduction of a counterfeit value is critical to the management of a smart card based electronic cash scheme. A critical role is played by a micro dynamic simulation model of an electronic cash economy. To substitute for the non-existing actual data on the latter, the model generates the electronic transaction details in the laboratory-like setting. In other words, this type of model allows us to conduct experiments by injecting streams of counterfeit value into the scheme and observing how efficient different risk management techniques are in dealing with the problem.

The simulation results can be used to assess the effectiveness of various on-chip as well as off-chip (i.e. host system based) risk management capabilities. In general, a threat scenario is viewed as a "business case" from both the counterfeiters' and electronic cash issuer's perspectives. Varius threat scenarios are assessed as an illustration.

The paper is organized as follows. This section consludes by defining the terms and concepts used in the paper. Section 2 reviews the basic features of micro dynamic simulation models as applied to an electronic cash scheme in general. Section 3 introduces a specific micro dynamic simulation model designed for the Mondex Scheme. Section 4 discusses the on-chip risk management techniques applicable to electronic cash. Sections 5 and 6 deal with the evaluation and subsequent selection of the on-chip logic. Section 7 concludes the paper with an outline of the future work topics.

The remainder of this section is used to define the terms and concepts we use in the paper.

Electronic Cash Issuer (ECI): a firm that creates smart card based electronic cash and manages the respective electronic cash scheme. Mondex International is an example of the ECI.

Electronic Purse: an electronic cash application on a smart card

Threat Scenario: Sequence of steps undertaken and places of engagement by counterfeiters to create and exploit the counterfeit electronic cash. The examples of counterfeiters are: organized crime, "researchers" challenged by the cryptography, and hostile governments.

ECI Response: Countermeasures undertaken by an ECI to prevent, detect, contain and recover from a counterfeit attack. A response can be *on-chip* and/or *off-chip* based.

Quantification of a Threat Scenario: A comparison of "gains" to "costs" related to a threat scenario, i.e. a business plan. Note that each such quantification results in two business plans, respectively from the counterfeiter's and ECI's perspectives. For the latter, a gain is tantamount to a loss reduction that can be attributed to the adopted response.

2 MICRO DYNAMIC SIMULATION

To quantify a threat scenario one needs to observe, in reality or by means of models (formal and/or mental), the following phases: Creation of counterfeit value, Interaction

of electronic purses (transactions), Diffusion of both legitimate and counterfeit value throughout the economy, and Incident Responses of ECI (countermeasures)

At the moment, no actual data on the above phases exist in the new ECI economy. Moreover, it is extremely unlikely that any actual observations regarding counterfeit value will be available in the foreseeable future. Therefore a quantification of a given threat scenario has to be based on the observations generated in a laboratory-like environment. Simulation modeling offers such an environment. It allows, through setting distributions of various parameters, to control and observe the behavior of all phases of a threat scenario. One can propose, depending on their properties and underlying techniques, different classifications of simulation models. One can classify the simulation models based on the level of aggregation of modeled phenomena and the role played by the "time" variable. According to the first criterion, the simulation models are assigned into *macro* or *micro* categories. The second criterion differentiates the *dynamic* models from the *static* ones. A more comprehensive discussion of these model classes can be found in (Harding, 1996), where a number of static and dynamic micro simulation models to evaluate tax, social and general economic polices are introduced.

The task to quantify a threat scenario requires, among other information, data on individual purses' transactions as well as on the effectiveness of the on-chip based response. Therefore our laboratory environment consists of the *micro dynamic simulation model*. In general, it is a computer model that imitates the dynamics of the electronic cash scheme. It has the following important features:

- Mimics the expected longer term evolution of the electronic cash scheme
- Reflects, through respective model parameters, short term behavioral patterns, e.g. seasonal fluctuations
- Follows the transaction behavior of individual purses, e.g. a number and frequency of transactions
- Keeps a complete record of all individual transactions

The above features allow an analyst to perform various experiments as if conducted in a real market place. The essence of every experiment is to:

- Design a threat scenario and inject the related counterfeit value into the system
- Build in and invoke during the simulation the on-chip and off-chip based responses

The simulated diffusion of the counterfeit value and an effectiveness with which it can be detected and contained provide the critical information that allows to quantify a threat scenario in question.

3 MONDEX MICRO DYNAMIC SIMULATOR (MMDS)

MMDS is a particular application of the micro dynamic simulation concept to the Mondex electronic cash scheme. The model's design is flexible enough to reflect not just today's but also other possible future scheme structures. MMDS was used to assess the effectiveness of the selected responses vis a vis various threat scenarios (see the following sections of the paper). To provide the context for our analysis, in the following we discuss the Mondex structure.

Mondex Structure: The are four distinct levels of participants in the Mondex scheme: *Originator, Members, Merchants* and *Consumers.* To interpret their respective role in the scheme one can think of an originator as a central bank. Members' functionality is similar to that of commercial banks. Merchants' and consumers' functionality is self explanatory. At each level, the participants are given specific types of purses which are known as *purse classes.* Different classes have their pre-specified *purse limits.* The purse class structure determines what purse classes can communicate (transact) with each other.

Figure 1 depicts graphically the basic elements of the Mondex structure. The arrows indicate the directions of potential transactions. Solid lines indicate transactions currently allowed, and dotted lines indicate the transactions severely restricted (or disallowed) at this stage of product evolution.

Figures 2, 3, and 4 show examples of input and output screens of the MMDS. To increase model's flexibility and the level of detail, as far as the transaction patterns are concerned, each level of scheme participants can be further segmented. Segments within the same level of participants differ from each other by their respective transaction patterns, as defined, for instance, by number and type of daily transactions.

Specifically, Figure 2 shows the top level of the MMDS model. It displays the name of the originator as a circle. It allows to define the characteristics of the Mondex economy (e.g. US) using Microsoft Windows™ graphical user interface.

Figure 3 shows a window that defines a member segment given the originator, in this case, US. It allows the user to specify various characteristics of the member segment, ranging from, for example, member type (merchant bank, consumer bank, or both) to birth/death rates for members, merchants and consumers (i.e. population growth and decline.) One can also designate a

member segment as counterfeit one by clicking the corresponding "counterfeit" check box. Note that, at the purse level, MMDS keeps tracks of individual purse setting such as purse limit, value balance and on-chip logic (e.g. checks whether credit turnover limit reached the set threshold -more details in Section 5), etc.

Figure 4 shows the impact that counterfeit activities have on the number of locked up purses. This is the direct effect of the on-chip logic. The most of the locked up purses are the legitimate purses that intentionally contacted counterfeited purses, i.e., in order to buy the counterfeited value at discount. When a preset condition is met, the on-chip logic turns on autonomously the mechanism to lock them up.

An ability to produce and analyze multiple runs of the MMDS model under different scenarios allows to add one more important benefit of the micro dynamic simulation: an experience in the management of the electronic cash economy before the scheme is actually rolled out.

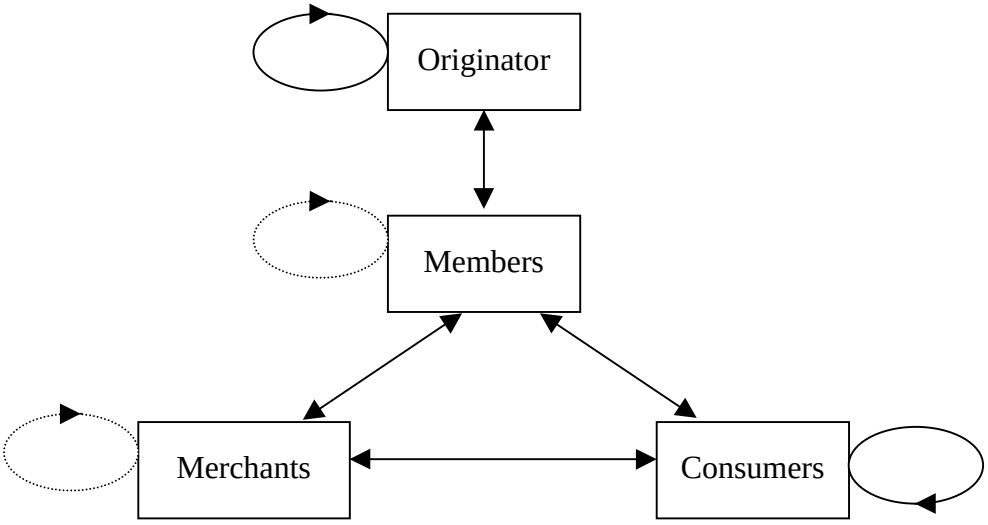

Figure 1: Transactions Among Different Class of Purses

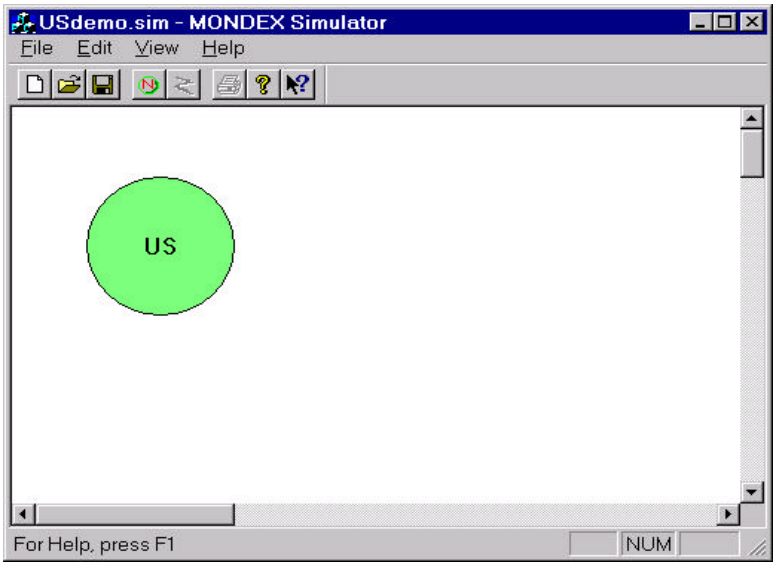

Figure 2: Example - Top Level Mondex Micro Dynamic Simulator

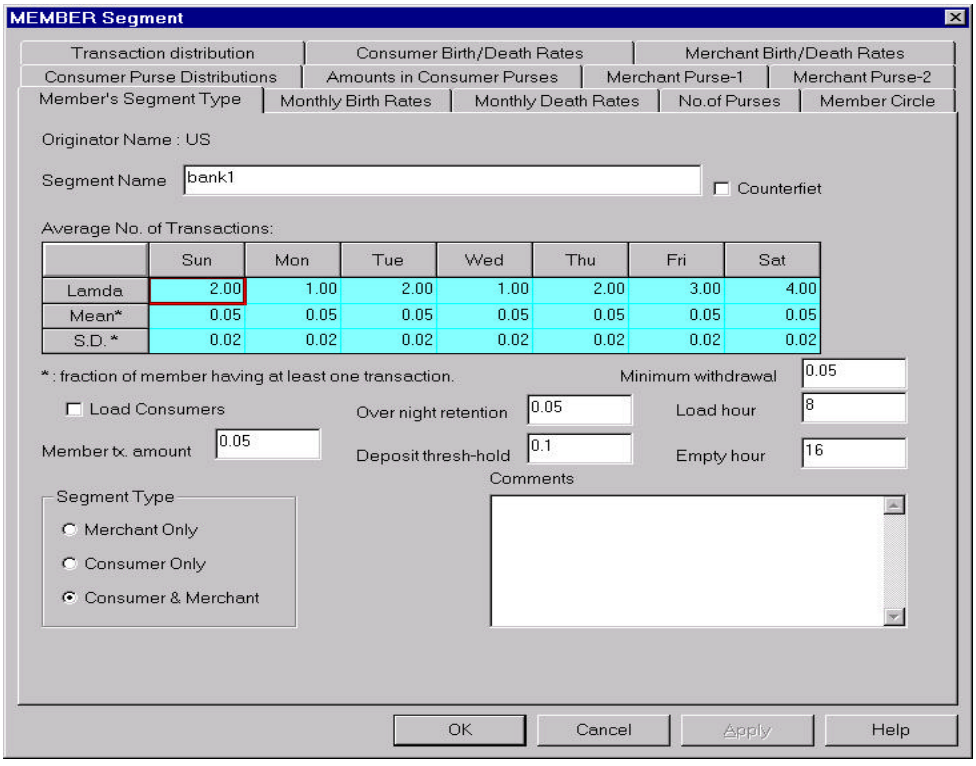

Figure 3: Example Input Screen - Member Segment Specification

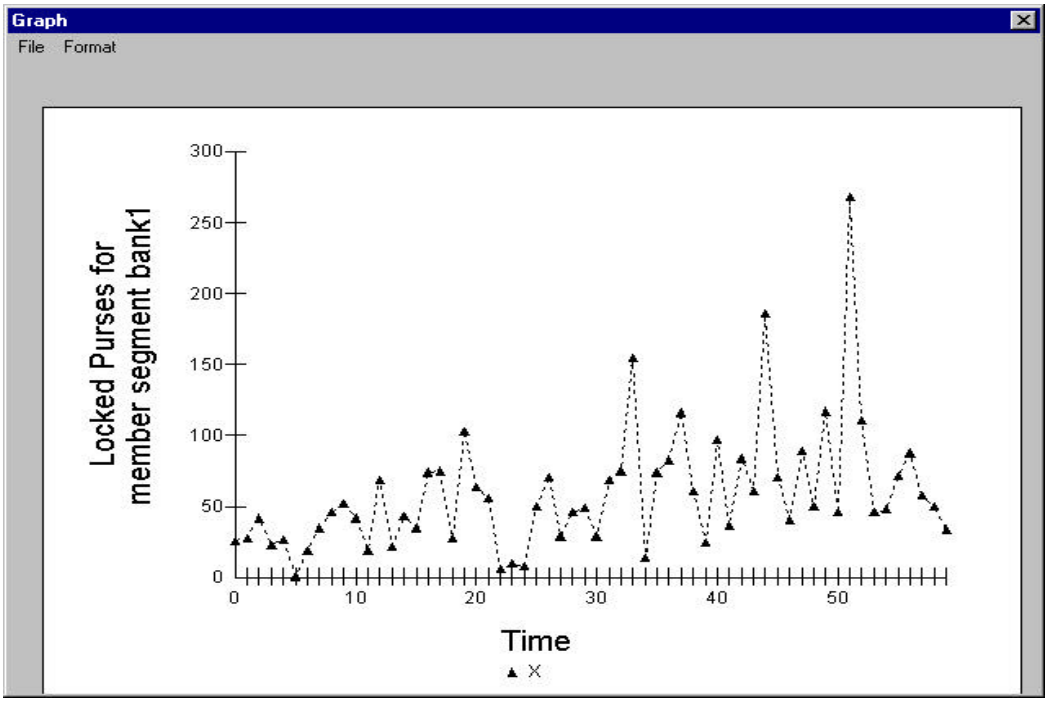

Figure 4: Example Output - Impact of Counterfeit Activity

The risk management capabilities, such as that of Mondex, need to be continuously upgraded to match new potential threats in the rapidly evolving electronic commerce. Again, the MMDS plays a critical role in the evaluation of both on-chip and off-chip new risk management methods to anticipate and prepare for the future challenges.

In addition to being a tool to evaluate the effectiveness of on-chip logic, the MMDS model generates transactions that are used to train off-chip detection model(s). The MMDS model is to be calibrated for every respective currency originator (i.e. country) to reflect the particular behavior of its purse users and their transaction patterns.

4 ON-CHIP RISK MANAGEMENT

The gain to counterfeiters (and corresponding loss to ECI) depends, to a large extent, on the effectiveness of the on-chip risk management. This section is entirely devoted to this important issue.

On-chip functionality for the "security" application has been around for many years, but for the risk management application it is a new and relatively unexplored field. In the past, an old generation of simple chips with a limited computing capability forced the scheme operators to rely heavily on the host systems to gather intelligence for transactions and monitoring (e.g. on-line transactions and authorization.) A new generation of chips, which the smart card based electronic cash product uses, offers more computing power and memory and allows us to take advantage of a "distributed" intelligence (i.e. on-chip "intelligent agent") as opposed to a "central" intelligence on the host systems.

This distributed intelligence is superior in terms of effectiveness and timeliness of risk management functionality to that of the central intelligence. It allows for real-time information gathering, monitoring and counterfeit detection. Also, an on-chip incidence response can be triggered at the time a purse transaction takes place.

The on-chip risk management capability is protected by the chip (tamper resistance) itself. To disable its capability, one has to pass the layers of the chip security.

One of the critical elements and advantages of the on-chip risk management capability is that it continuously functions, even under complete physical security breakdown. The fact remains that although the risk management functionality of the compromised chip will be disabled by the counterfeiters, in order to benefit from their activities, they need to interact with legitimate purses. The latter will still have active and functioning on-chip risk management capability (see Figure 4) It is unlikely to pass all the screens without triggering some actions by the on-chip risk management functionality.

Detection methods: In general, there are two primary methods to detect fraud and/or counterfeit. The first one measures the "velocity" of transactions, and the other compares transactions against "statistical signature" of the purse. It is true for both on-chip and off-chip (i.e., host system based) detection. The "velocity" method, which monitors amount and volume of transactions, is widely used in the telecommunication and financial industries to monitor potential fraudulent transactions. The "statistical signature" method, which monitors transactions against the past behavioral patterns is more computationally intensive and requires more infrastructure support. This technique is also commonly utilized by various industries to monitor net bad debt as well as fraudulent transactions and accounts (Ezawa, 1995; Ezawa, 1996).

For example, Mondex risk management uses both "velocity" and "statistical signature" methods in on-chip as well as off-chip risk management. The "credit turnover limit" is a good example of "velocity" based method implemented as the on-chip risk management monitoring and detection capability.

Incidence response: As we discussed, the on-chip risk management has on-chip incident response capability in an autonomous mode. On the other hand, one of the most effective ways to respond to the counterfeit contingency is at the chip level by a central command to activate on-chip incidence response on a contaminated segment of purses. It will function autonomously without outside intervention. It is the fastest way to respond to the potential incident.

5 EVALUATION OF ON-CHIP RISK MANAGEMENT CAPABILITY USING MMDS

In the performed evaluation, the threat scenarios assume that there are "**golden goose**" counterfeit purses in the economy, and the population in the consumer counterfeit segment uses legitimate Mondex purses to receive Mondex value from the "golden goose" purses and spend it.

Three counterfeit scenarios have been considered. They differ in what counterfeit purse classes capable of creating counterfeit value (a golden goose) are in operation: 1) member purses, 2) consumer purses or 3) merchant purses.

On-chip Logic: Two types of on-chip risk management logic are evaluated: cumulative debit and cumulative credit turnover limits. They are defined as follows:

- cumulative **debit** turnover limit (CDTL) -- a maximum amount a purse can **spend**
- cumulative **credit** turnover limit (CCTL) -- a maximum amount a purse can **receive** from sources other than a member

CDTL monitors the amount of spending regardless of the source or the destination of the Mondex value. It

measures the overall spending, the flow of Mondex value through a purse. It presumes that the counterfeiters (or money launders) and their collaborators will have very high flows of Mondex values through their purses. On the other hand, **CCTL** monitors more selectively. It monitors the flow of incoming Mondex value just from consumers and merchants (e.g., refund.) It is based on the assumption that the counterfeiters (or money launders) and their collaborators will avoid contacting the members, and the most of transactions will take place between consumers or be merchant refunds. CCTL presumes that monitoring the sources of Mondex value helps to detect the potential counterfeiting/money laundering activities.

When a purse is locked up due to the on-chip logic, both credit and debit operations will be suspended until the purse contacts a member to get unlocked. Note that this locking mechanism can be different from the actual implementation on the product.

Criteria of effectiveness: There are two key factors to consider: time to detect from the start of counterfeit activities; and containment of counterfeit activities at the point of transaction

Time to detect: It is a measure of ability to provide the earliest possible warning of counterfeit activities at their initial stage, even if the volumes transacted are low. If detected early, the counterfeit activities are easier and less costly to contain.

Containment: By constraining the functionality of fraudulent cards, it contains/restrains the flow of counterfeit values to the market. Fraudulent cards are the legitimate cards that are held by the fraudulent population that knowingly and willingly buys counterfeit value at discount from counterfeiters and their collaborators. When counterfeiters and their collaborators try to use/load the purses to distribute counterfeit values, most of these fraudulent cards are quickly disabled.

The most effective on-chip logic should generate, in a short time, a large number of locked up fraudulent purses and thereby force them to contact members to get unlocked (and be "exposed"). If these purses refuse to contact a member, their activities will be practically blocked.

MMDS simulation based results: It turns out that, overall, the CCTL logic works better. However, no alternative logic stochastically dominates the other, i.e. no logic consistently out-performs in all counterfeit scenarios. The CCTL works very well in scenario 2) and 3), and the CDTL works slightly better in scenario 1).

The CCTL logic has the following advantages:

- effective in case of high value consumer to consumer transaction scenarios, such as involving counterfeit and money laundering transactions
- reacts quickly to counterfeit activities
- locks purses before counterfeit values are spent
- a larger number of fraudulent purses gets locked
- sensitive to the setting of credit turnover limit (i.e. it is a fine instrument.)
- The debit turnover limit has the following advantages:
- effective in case of high value spending transaction scenarios
- relatively robust in setting of debit turnover limit (i.e. it is a rough instrument.)

Note: Since credit/debit turnover limit/ratio will affect the flows of Mondex value from other than member purses, it may have a desirable impact of restraining **money laundering** activities. It makes it difficult for a money laundering purse to transfer large sums to other money laundering purse without triggering the on-chip logic locking up mechanism. In particular, the latter should be efficient in case of consumer purses involved in the money laundering activities.

6 ON-CHIP RISK MANAGEMENT LOGIC SELECTION

We stated in the previous section that the CCTL is preferred to the CDTL. However, the quantification of a given threat scenario requires that the cost/benefit analysis be performed. In this section we discuss a simple decision theoretic economic risk model (based on Computer Aided Decision Evaluation Tool (CADET) model (Ezawa, 1992) which was created to quantify the benefit of having on-chip logic and to measure a tradeoff between the two alternative on-chip logic mechanisms.

Note that this model should be considered just an illustration of how one can use decision theoretic approach to the problem of economic risk analysis with respect to the electronic commerce in general, and the cost/benefit analysis of on-chip logic in particular.

Figure 5 shows an influence diagram created for the analysis. An influence diagram is a graphical representation of a decision problem under uncertainty, explicitly revealing probabilistic dependence and the flow of information. It provides an intuitive framework to describe problems as they are perceived by decision makers, and to incorporate the knowledge of experts.

Variables: There are three uncertain variables (oval shape): "Counterfeit Scenarios," "Potential Loss," and "Percentage Prevented." The decision variable (rectangular shape) is "On-chip Feature" (Logic). The objective/goal variable (rounded square) is "Prevented Loss." For example, it allows assignment of probability of

alternative scenarios represented by the variable "Counterfeit Scenarios." And in case of the variable "Potential Loss," potential loss distribution and probabilities are assigned given the outcome of "Counterfeit Scenarios."

Results: The model produces the cumulative probability curve (value lottery) as shown in the Figure 6. The model can compute the expected loss due to counterfeiting activities 1) without any on-chip logic protection, 2) with CCTL, 3) with CDTL and 4) both CCTL and CDTL. The model showed that, overall, the CCTL is the most effective. The effects of 4) are marginally higher than those of 2) and 3) in terms of the expected prevented loss. It indicates that there is a little gain of having both logic on the purse, considering the cost of both implementations.

7 SUMMARY

This paper discussed the evaluation of the counterfeit threat scenarios using micro dynamic simulation models. This modeling technique provides information needed for the quantification of economic risk exposure in conjunction with other analytical tools. We discussed various issues related to the smart card based electronic cash risk management. In this respect, the simulation allows the evaluation of the effectiveness of various on-chip risk management capabilities for the smart card based electronic cash. And by generating test data sets, it allows the assessment of the effectiveness of the host system based counterfeit transaction detection models, since the actual data of counterfeiting is not and will not be available in the foreseeable future.

REFERENCES

Ezawa, K. J., and Scherer, J. B., 1992, Technology Planning for Advanced Telecommunications Services: A Computer-Aided Approach, *Telematics and Informatics*, 9(2), pp. 101-112.

Ezawa, K.J., and Napiorkowski, G., 1998, "Assessment of Threats for Smart Card based Electronic Cash" *Proceedings of the 2nd International conference in Financial Cryptography*.

Ezawa, K.J. and Schuermann, T., 1995, "Fraud/Uncollectible Debt Detection Using a Bayesian Network Based Learning System: A Rare Binary Outcome with Mixed Data Structures," *Proceedings of the 11th Conference Uncertainty in Artificial Intelligence*, Morgan Kaufmann, pp. 157-166.

Ezawa, K.J., Singh, M., and Norton, S.W., 1996, "Learning Goal Oriented Bayesian Networks for Telecommunications Risk Management", *Proceedings of the 13th International Conference on Machine Learning*, Morgan Kaufmann.

Ezawa, K.J., and Norton S., 1996, "Constructing Bayesian Networks to Predict Uncollectible Telecommunications Accounts," *IEEE EXPERT*, Vol. 11, No. 5, pp. 45-51.

Harding, A.(editor), 1996, "Microsimulation and Public Policy", North-Holland

Napiorkowski, G. and Borghard, W., 1996, "Modeling of Customer Response to Marketing of Local Telephone Services" in Dynamic Competitive Analysis in Marketing, Springer Verlag

AUTHOR BIOGRAPHIES

KAZUO EZAWA is a senior vice president of Mondex International. His expertise includes risk management, decision analysis, influence diagrams, Bayesian network learning, and normative expert systems. He received an MS in operations research from the University of Michigan, Ann Arbor , and a Ph.D. in engineering economic systems from Stanford University.

GREGORY NAPIORKOWSKI is a vice president of Mondex International. His expertise includes econometric and statistical model building, system design, and simulation. He received an MA and Ph.D. in Economics from Warsaw Economic School in Poland, and also received an MBA from Fordham University in New York.

MARIUSZ KOSSARSKI is a vice president of Mondex International. His experience includes management, development, and implementation of software solutions for major Fortune 100 companies. He received an MS in Computer Science from Warsaw University in Poland.

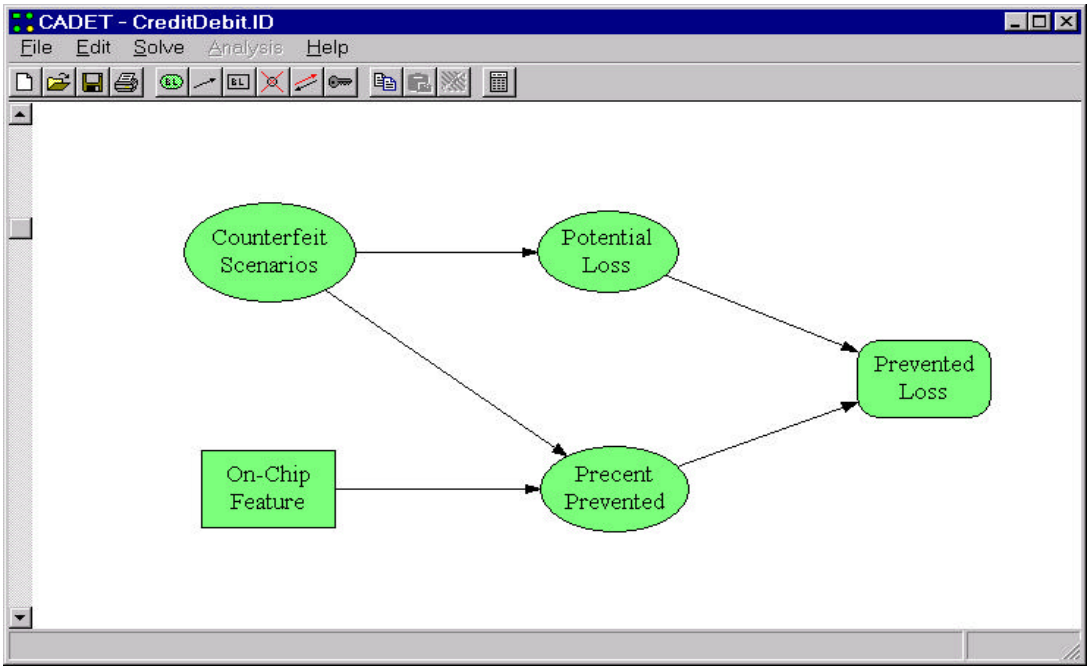

Figure 5: Influence Diagram Mode1

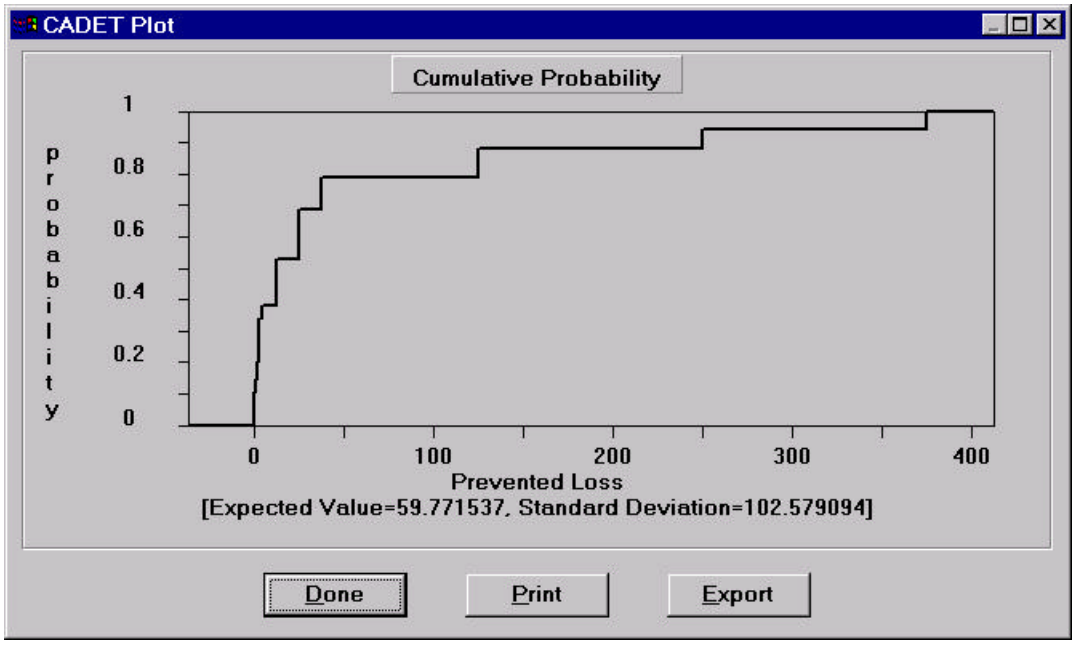

Figure 6: Cumulative Probability Graph