Analysis of N Category Privacy Models

Marn-Ling Shing *shing@tmue.edu.tw*
Early Child Education Department and Institute of Child Development
Taipei Municipal University of Education
Taipei, Taiwan, R.O.C y

Chen-Chi Shing *cshing@radford.edu*
Information Technology Department
Radford University
Radford, VA 24142, U.S.A.

Lee-Pin Shing *shingle@vt.edu*
Biology Department
Virginia Tech
Blacksburg, VA 24061, U.S.A.

Lee-Hur Shing *leehurshing@yahoo.com*
Engineering Department
Virginia Tech
Blacksburg, VA 24061, U.S.A.

Abstract

File sharing becomes popular in social networking and the disclosure of private information without user’s consent can be found easily. Password management becomes increasingly necessary for maintaining privacy policy. Monitoring of violations of a privacy policy is needed to support the confidentiality of information security. This paper extends the analysis of two category confidentiality model to N categories, and illustrates how to use it to monitor the security state transitions in the information security privacy modeling.

Keywords: Privacy Model, Confidentiality Model, Information Security Model, and Markov Chain Model.

1. INTRODUCTION

Information assurance includes “measures that protect information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities” [1]. In business the job of keeping the company's infrastructure and network safe is growing increasingly complex as the perimeter expands, threats become more sophisticated, and systems become more complex and embedded. Companies are becoming increasingly more dependent on technology for the liability of security and privacy as required by the legislations in state and federal laws such as HIPAA, Sarbanes-Oxley, and California's Security Breach Information Act 1386 [2]. Information security is more than just using a good Intrusion Detection System or firewall; it involves keeping users educated, creating and maintaining good policies, getting the right budget, and sometimes monitoring user activities. In academia maintaining a strict privacy and security of student and employee records are required. There are state and federal laws that protect records containing information directly identifying, or revealing private information for students and employees. For example, they are the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), and the Gramm-Leach-Bliley Act (GLBA),. There are also a variety of security technologies and procedures used to help protect students’ and employees’ information from unauthorized access, use, or disclosure. When highly private information (such as a credit card number or password) are transmitted over the Internet, usually they are protected through the use of encryption, such as the Secure Socket Layer (SSL) protocol. Password management on different servers to maintain privacy policies are necessary. Constant monitoring is needed to prevent the damage as a result of any violation of privacy policy.

Since security becomes an important component in the various services, new standards are emerging for these services. For example, the new auditing standards No. 99 provides a general guideline for the responsibilities and anti-fraud activities of a manager [3]. ISO 17799:2005 provides a general organization security structure [4]. These security standards may be influenced by existing security models. For example, ISO 17799:2005 provides a general organization security structure but many basic security principles may have been discussed and defined in various security models. While supply chain information is similar to any other information systems, it has unique features on confidential and integrity. In order to monitor the security in a supply chain network, it is necessary to model the security state transition in the Bell-LaPadula model [5]. A two-category model has been proposed [6]. This paper intends to generalize from the two-category model to N-category and provides details on analyzing the model and illustrates how to use it to monitor the security state transitions in privacy model.

2. LITERATURE REVIEW

2.1 Information Security Models

There are various models which provide policies from different aspects of security. The Bell-LaPadula model is one of the security models for information confidentiality and has been adopted by the military for a long time. For example, the Bibba model provides security policy in data integrity [7, 8]. On the other hand, Bell-LaPadula model provides security policy to guard against unauthorized disclosure [9]. Bell LaPadula model has been used in the military and is primarily designed for modeling confidentiality [10-11]. It classifies the access levels for the subject into a set of security clearances, such as: top security (TS), security (S), confidential (C), and unclassified (UC). In the mean time the objects have also been classified as corresponding security levels. It does not allow a subject to read the objects at security levels higher than the subject's current level. Every subject must belong to one and only one of the security clearance levels. In addition, every object must also belong to one and only one of the classification levels. For example, a colonel, who is in the TS security clearance, can read the Personnel files. Whereas, a soldier, who is in the UC security clearance, can read the telephone lists. The colonel can also read the telephone lists; however, the soldier cannot read the personnel files.

2.2 The Bell-LaPadula Model for Supply Chain Networks

In a supply chain network, prices offered by suppliers are often confidential due to competition and also are not public information in the buyer's company. The confidentiality of the supplier information is essential in nowadays competitive business world. Chen et al. [12, 13] proposed to use the Bell-LaPadula model for the supply chain network. In order to investigate the security in the supply chain model, it is necessary to be able to model the security state transition in the Bell-LaPadula model. Shing et al. proposed using Markov chain model [6, 14, 15] in a two-category. According to the Bell-LaPadula model, we can classify the employees (or subjects) in the purchasing company into several security clearance levels and different information (or objects) into different security classification levels. For simplicity, assuming that there are two security clearance levels for all employees in a purchasing company (see Figure 1). They are the top officer and other employees. The top officer can access or read two documents: both supplier evaluations and purchasing decision. On the other hand, other employees can only access (read) two documents: the public bidding notices and the public purchasing price list. The top officer can also access the documents which a general employee can access. Other employees cannot access documents for both supplier evaluations and purchasing decision. Table 1 shows security classifications and clearance levels for a purchasing company and its suppliers.

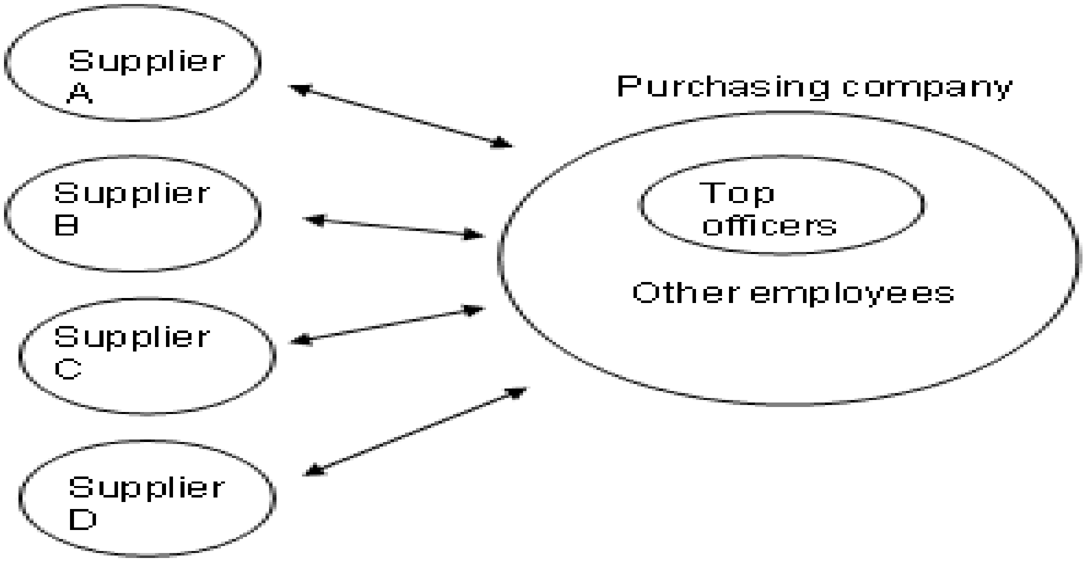

FIGURE 1: Purchasing Company and Their Suppliers.

Security Classification	Purchasing Co. and Suppliers	Documents/ Information
Top Secret (TS)	Managers	Supplier evaluations
Secret (S)	Other employees	Public bidding notices

TABLE 1: Security Classifications in a Supply Chain Network.

The abstract model of the table 1 can be represented as

Subject Security Clearance	Object Classification Level
S_1	O_{11}, O_{12}
S_2	O_{21}, O_{22}

TABLE 2: Security Abstract Classifications in a Supply Chain Network.

3. SEMI-MARKOV CHAIN MODEL

A Markov process is a stochastic process which states that the probability of a system at a state depends only on the previous state, not on the previous history of getting to the previous state [16]. If the states and their transitions at discrete points in time are discrete, it is called a Markov Chain [17-19]. Suppose p(0) represents the vector of the probability that the system is in one of those n states at time 0, p(0)= $\begin{bmatrix} p_1(0) \\ p_2(0) \\ \cdots \\ p_n(0) \end{bmatrix}$, $\sum_{i=1}^{n} p_i(0)$ =1, where $p_i(0)$ represents the probability of the system is in state i at time 0. Then the probability that the system is in one of those n states at time 1 is represented by p(1),

p(1)= $\begin{bmatrix} p_1(1) \\ p_2(1) \\ \cdots \\ p_n(1) \end{bmatrix}$, $\sum_{i=1}^{n} p_i(1)$ =1, where $p_i(1)$ represents the probability of the system is in state i at time 1.
And P(1)=T p(0), where T is the transition probability matrix,

T= $\begin{bmatrix} p_{11} & p_{21} & \cdots & p_{n1} \\ p_{12} & p_{22} & \cdots & p_{n2} \\ \cdots & \cdots & \cdots & \cdots \\ p_{1n} & p_{2n} & \cdots & p_{nn} \end{bmatrix}$, $\sum_{j=1}^{n} p_{ij}$ =1, for i=1,2,…,n (Eq 3.1)

and p_{ij} is the probability of the system in the state j, given it was in the state i. Suppose the probability that the system is in one of those n states at time s is represented by p(s),

p(s)= $\begin{bmatrix} p_1(s) \\ p_2(s) \\ \cdots \\ p_n(s) \end{bmatrix}$

where $p_i(s)$ represents the probability of the system is in state i at time s. Then P(s)=T(T(…(Tp(0))))=T^s p(0),where T is the transition probability matrix. A Markov Chain is a special case of a random walk process [20, 21] , which is defined as “a random variable X_n that has values in set of integers Z”, with
$P(X_n = X_{n-1}+1)=p$ and $P(X_n = X_{n-1}-1)=1-p$, where $p \in (0,1)$.

In general, a random walk process is a semi-Markov Chain. Every entry of the transition probability matrix in a semi-Markov Chain can be arbitrary [19], as in the Definition 3.1 below:

Definition 3.1
A semi-Markov process is a stochastic process that has an arbitrary distribution between state changes and any new state is possible given it is in the current state.

The Markov Chain model will be extended to the semi-Markov Chain using two category confidential model in Section 4.

4. ANALYSIS OF ABSTRACT SEMI-MARKOV CHAIN MODEL

The results in this section were for two category model and proved in [22]. They are listed here for completeness.

Definition. 4.1 A state is recurrent if a state will return back to itself with probability one after state transitions. If the state is not recurrent, then it is a transient. If a recurrent state is called recurrent nonnull if the mean time to return to itself is finite. A recurrent state is a recurrent null if the mean time return to itself is infinite. A recurrent state is aperiodic if for some number k, there is a way to return back in k, k+1, k+2, … transitions. A recurrent state is called periodic if it is not aperiodic.

Definition 4.2 A semi-Markov chain is irreducible if all states are reachable from all other states. It is recurrent nonnull if all its states are recurrent nonnull. It is aperiodic if all its states are aperiodic.

Definition 4.3 If a semi-Markov chain is irreducible, recurrent nonnull and aperiodic, it is called ergodic.

The eight states in the semi-Markov chain model is presented in Table 3 for abstract model in Table 2.

State	Object Classification
1	(S_1, O_{11}), (S_2, O_{21})
2	(S_1, O_{12}), (S_2, O_{21})
3	(S_1, O_{21}), (S_2, O_{21})
4	(S_1, O_{22}), (S_2, O_{21})
5	(S_1, O_{11}), (S_2, O_{22})
6	(S_1, O_{12}), (S_2, O_{22})
7	(S_1, O_{21}), (S_2, O_{22})
8	(S_1, O_{22}), (S_2, O_{22})

TABLE 3: Semi-Markov Chain States for Table 2.

Properties 4.1
P(System is at the state (S_1, O_{ij}) at time t | System is at the state (S_2, O_{2m}) at time t-1)=P(System is at the state (S_1, O_{ij}) at time t) , where *i ,j=1, 2, 3, 4, m*=1,2.

Properties 4.2
P(System is at the state (S_1, O_{ij}) (S_2, O_{2m}) at time t)=P(System is at the state (S_1, O_{ij}) at time t) * P(System is at the state (S_2, O_{2m}) at time t), where *i ,j ,m*=1,2.

Properties 4.3
P(System is at the state (S_2, O_{2j}) at time t | System is at the state (S_1, O_{im}) at time t-1)=P(System is at the state (S_2, O_{2j}) at time t) , where *i ,j=1, 2, m=1, 2, 3, 4*.

Using the following notation:
P(System is at the state (S_1, O_{11}) at time 0) $=a_{11}$
P (System is at the state (S_1, O_{12}) at time 0)$=a_{12}$
P (System is at the state (S_1, O_{21}) at time 0) $=a_{13}$
P (System is at the state (S_1, O_{22}) at time 0) $=a_{14}$
P (System is at the state (S_2, O_{21}) at time 0) $=b_{11}$
P (System is at the state (S_2, O_{22}) at time 0)$=b_{12}$, where $\sum_{j=1}^{4} a_{ij} = 1$ and $\sum_{j=1}^{2} b_{ij} =1$, the initial state of the system is given by

Property 4.4
P(System is at the state *m* at time 0) = $a_{1i}\, b_{1j},$
where *i=1, 2, 3, 4 ,j=1, 2,* and *m=i+4(j-1).*

In calculating the state transition probability, the following trivial properties are needed:
Property 4.5
P(System is at state (S_1, O_{1j}) (S_2, O_{2m}) at time t | System was at state (S_1, O_{1n}) (S_2, O_{2m}) at time t-1) = P(System is at state (S_1, O_{1j}) at time t | System was at state (S_1, O_{1n}) at time t-1) * P(System is at state (S_2, O_{2m}) at time t | System was at state (S_2, O_{12m}) at time t-1),
where *j, n =1, 2, 3, 4,* and *m=1, 2*.

Property 4.6
P(System is at state (S_1, O_{ij}) (S_2, O_{2m}) at time t | System was at state (S_1, O_{ij}) (S_2, O_{2n}) at time t-1) = P(System is at state (S_1, O_{ij}) at time t | System was at state (S_1, O_{ij}) at time t-1) * P(System is at state (S_2, O_{2m}) at time t | System was at state (S_2, O_{2n}) at time t-1),
where *i=1, 2, j =1, 2, 3, 4,* and *m, n=1, 2*.

Property 4.7
The transition probability
$p_{ij} = q_{ij} * r_{11}$
$p_{i\,(j+4)} = q_{ij} * r_{12}$
$p_{(i+4)\,j} = q_{ij} * r_{21}$
$p_{(i+4)\,(j+4)} = q_{ij} * r_{22}$
where *i=1, 2, j =1, 2, 3, 4*.

Property 4.8
If a semi-Markov chain is ergodic, then there exists a unique steady-state or equilibrium probability state.

Depending on the structure of the transition probability matrix, it may not have any steady state exists. For example, a symmetric random walk process which has p=0.5, is periodic. [9].

Property 4.9
For any semi-Markov chain if all the entries of its transition probability matrix are non-zero, then it is recurrent nonnull and aperiodic.

Corollary 4.9
For any semi-Markov chain, if every entry of its transition probability matrix has non-zero in all the entries, then it has an equilibrium state.

Corollary 4.10
If T keeps no change in Corollary 4.9, then the equilibrium state described in Corollary 4.9 is the eigenvector of T', the transpose of the transition probability matrix, of eigenvalues 1.

The next section will generalize the model to n categories and describe some of the properties

5. GENERAL MODEL

The most general abstract model of the Table 1 can be represented as in Table 4 below.

Subject Security Clearance	Object Classification Level
S_1	$O_{11}, O_{12}, \ldots, O_1 v_1$
S_2	$O_{21}, O_{22}, \ldots, O_2 v_2$
…	…
S_n	$O_{n1}, O_{n2}, \ldots, O_n v_n$

TABLE 4: Security General Abstract Classifications.

Definition 5.1.
The abstract model given in Table 4 is called an n category confidential model.

Since the subject S_i can access the objects O_{ij} where $j \geq i$, the states in semi-Markov Chain n category confidential model for Table 4 are listed in Table 5 below.

State	Object Classification
1	(S_1, O_{11}), (S_2, O_{21}), (S_n, O_{n1})
2	(S_1, O_{12}), (S_2, O_{21}), (S_n, O_{n1})
…	…
$\sum_{i=1}^{n} v_i$	$(S_1, O_n\ v_n)$, (S_2, O_{21}), (S_n, O_{n1})
…	…
$\prod_{i=1}^{n} \sum_{j=i}^{n} v_j$	$(S_1, O_n v_n)$, $(S_2, O_n v_n)$, $(S_n, O_n v_n)$

TABLE 5: Semi-Markov Chain States for Table 4.

The total number of states in semi-Markov Chain grows exponentially fast as the total number of subjects n as in the following property:

Property 5.1.
Assume that the total number of subjects is n. The total number of states in the semi-Markov Chain model is $O(n!v^n)$, where $v=max\ (v_1, \ldots, v_n)$.
Proof:

The total number of states in semi-Markov Chain model is $\prod_{i=1}^{n} \sum_{j=i}^{n} v_j$, where $\sum_{j=i}^{n} v_j$ = n. Hence,

$$\prod_{i=1}^{n} \sum_{j=i}^{n} v_j \leq nv(n-1)v \ldots v = n!\, v^n.$$

For example, if there are three categories and at most two objects in each category (i.e., n=3 and v=2), by Property 5.1, the total number of states in the model is no more than 6x8=48 states. Similar properties as Properties 4.1-4.7 are still valid for three category model.

In order to calculate the transition probability matrix for the n category confidential model, we need to use some notations and define a binary operator $\rhd$ on matrices.

Definition 5.2.

Let the matrix $Q_k = (q_{(k),\, i\, j})$ of size $\sum_{i=k}^{n} v_i$ x $\sum_{i=k}^{n} v_i$, where k=1,..,n and $q_{(k),\, i\, j}$ is the probability from state *i* at time 0 to state *j* at time 1 for subject S_k. And let n_k = number f rows/columns of Q_k.
Define

$$Q_r \triangleright Q_s = \begin{bmatrix} q_{(s),11}Qr & q_{(s),12}Qr & \cdot\;\cdot\;\cdot\;\cdot\;\cdot & q_{(s),1,\sum_{i=s}^{n} v_i}Qr \\ q_{(s),21}Qr & q_{(s),22}Qr & \cdot\;\cdot\;\cdot\;\cdot\;\cdot & q_{(s),2,\sum_{i=s}^{n} v_i}Qr \\ \cdot & \cdot & \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot & \cdot \\ \cdot & \cdot & \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot & \cdot \\ \cdot & \cdot & \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot & \cdot \\ \cdot & \cdot & \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot & \cdot \\ \cdot & \cdot & \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot & \cdot \\ q_{(s),\sum_{i=s}^{n} v_i,1}Qr & q_{(s),\sum_{i=s}^{n} v_i,2}Qr & \cdot\;\cdot\;\cdot\;\cdot\;\cdot & q_{(s),\sum_{i=s}^{n} v_i,\sum_{i=s}^{n} v_i}Qr \end{bmatrix}$$

where every entry of the matrix
$q_{(s),ij}Qr$ is obtained by multiplying the entry of the matrix Q_r by $q_{(s),ij}$.
Note that the sum of each row of the matrix Q_i, where i=1,…, n is equal to one. The transition probability matrix T can be calculated using the operator in the following:

Property 5.2.
The transition probability matrix of the n category confidential model is given by
$T = (\ldots(Q_1 \triangleright Q_2) \triangleright Q_3)\ldots \triangleright Q_n)$.

Proof: The proof is similar to the one given by Property 4.7.

Property 5.3.
Every sum of each row in the transition probability matrix T is equal to 1.

Proof: The proof is similar to the one given by Property 4.8.

A result similar to Property 4.4 for n category confidential model can be obtained in Property 5.4.

Property 5.4.
The initial state in the n category confidential model can be calculated by multiplying all initial probability entries of every category in the following:

$$P(0) = (p^{(0)}_i) \prod_{m=1}^{n} n_{mx1},$$

where

$$p^{(0)}_i = \prod_{k=1}^{n} q_k^{(0)},$$

$q_k^{(0)}$ is the probability matrix at state (S_k, O_{k1}), (S_k, O_{k2}),…, $(S_k, O_{k v_k})$, …, (S_k, O_{n1}), (S_k, O_{n2}),…, $(S_k, O_{k v_n})$ at time 0.

Proof: Similar to that of Property 4.4.

For a two category confidential model described in Section 4, n=2, $v_1=2$, and $v_2=2$. Total number of states = $(v_1+v_2)v_2=8$.

$$Q_1 = \begin{bmatrix} q_{11} & q_{12} & q_{13} & q_{14} \\ q_{21} & q_{22} & q_{23} & q_{24} \\ q_{31} & q_{32} & q_{33} & q_{34} \\ q_{41} & q_{42} & q_{43} & q_{44} \end{bmatrix}, \quad \sum_{j=1}^{4} q_{ij} = 1, \text{ for } i=1,2,3,4$$

$$Q_2 = \begin{bmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{bmatrix}$$

$$T = \begin{bmatrix} q_{11}*r_{11} & q_{12}*r_{11} & q_{13}*r_{11} & q_{14}*r_{11} & q_{11}*r_{12} & q_{12}*r_{12} & q_{13}*r_{12} & q_{14}*r_{12} \\ q_{21}*r_{11} & q_{22}*r_{11} & q_{23}*r_{11} & q_{24}*r_{11} & q_{21}*r_{12} & q_{22}*r_{12} & q_{23}*r_{12} & q_{24}*r_{12} \\ q_{31}*r_{11} & q_{32}*r_{11} & q_{33}*r_{11} & q_{34}*r_{11} & q_{31}*r_{12} & q_{32}*r_{12} & q_{33}*r_{12} & q_{34}*r_{12} \\ q_{41}*r_{11} & q_{42}*r_{11} & q_{43}*r_{11} & q_{44}*r_{11} & q_{41}*r_{12} & q_{42}*r_{12} & q_{43}*r_{12} & q_{44}*r_{12} \\ q_{11}*r_{21} & q_{12}*r_{21} & q_{13}*r_{21} & q_{14}*r_{21} & q_{11}*r_{22} & q_{12}*r_{22} & q_{13}*r_{22} & q_{14}*r_{22} \\ q_{21}*r_{21} & q_{22}*r_{21} & q_{23}*r_{21} & q_{24}*r_{21} & q_{21}*r_{22} & q_{22}*r_{22} & q_{23}*r_{22} & q_{24}*r_{22} \\ q_{31}*r_{21} & q_{32}*r_{21} & q_{33}*r_{21} & q_{34}*r_{21} & q_{31}*r_{22} & q_{32}*r_{22} & q_{33}*r_{22} & q_{34}*r_{22} \\ q_{41}*r_{21} & q_{42}*r_{21} & q_{43}*r_{21} & q_{44}*r_{21} & q_{41}*r_{22} & q_{42}*r_{22} & q_{43}*r_{22} & q_{44}*r_{22} \end{bmatrix}$$

This is confirmed by Property 4.7 and 4.8. The example of calculating transition probability for states in Table 1 can be found in [6].
The transition probability matrix can be obtained from Property 5.2 in the following:

Corollary 5.1.
For a three category confidential model of two states each, n=3, v_1=2, v_2=2 and v_3=2. In addition, n_1=6, n_2=4 and n_3=2. Total number of states = $(v_1+v_2+v_3)(v_2+v_3)v_3$=48. Assume $Q_1 = (q_{ij})_{6x6}$,$Q_2 = (r_{ij})_{4x4}$ and $Q_3 = (w_{ij})_{2x2}$. Then $T=(p_{ij})_{48x48}$, where m=1,2, t=1,2, k=1,2,3,4, s=1,2,3,4, i=1,..,6, j=1,…,6 and
$p_{i+6s+24t,j+6k+24m} = q_{ij} * r_{s,k} * w_{t,m}$

Proof: A block of 6 rows/columns for changing indices of $r_{s,k}$ and a block of 24 rows/columns for changing indices of $w_{t,m}$.

A similar result to express the entry of the transition probability matrix explicitly for n category confidential model is in the following:

Corollary 5.2.
For the n category confidential model, assume $Q_k = (q_{(k),ij})$, where i, j = 1, .., n_k, k=1,…, n.
Then $T=(p_{ij})$, with

$$p_{i+\sum_{s=1}^{n-1} i_{s+1} \prod_{m=1}^{s} n_m,\ j+\sum_{s=1}^{n-1} j_{s+1} \prod_{m=1}^{s} n_m} = \prod_{k=1}^{n} q^{(k)}$$

where i, j = 1, …, n_1,
$q^{(k)} = q_{(k),\, i_k,\, j_k}$
and
i_k, j_k = 1, …, n_k
k = 1, 2, …, n.

Proof:
The proof is similar to the one in Corollary 5.1.

For example, if n=3, v_1=7, v_2=3 and v_3=2. In addition, n_1=12, n_2=5 and n_3=2. Total number of states = $(v_1+v_2+v_3)(v_2+v_3)v_3$=120. Assume $Q_1 = (q_{(1),ij})_{12x12}$,$Q_2 = (q_{(2),ij})_{5x5}$ and $Q_3 = (q_{(3),ij})_{2x2}$. Then $T=(p_{ij})_{120x120}$, where i, j=1, 2, …, 12
$p_{i+n_1*i_2+n_1*n_2*i_3,\ j+n_1*j_2+n_1*n_2*j_3} = q^{(1)} * q^{(2)} * q^{(3)}$, with

$q^{(1)} = q_{(1),ij}$
$q^{(2)} = q_{(2), i_2,\ j_2}$
$q^{(3))} = q_{(3), i_3,\ j_3}$
and
$i_2,\ j_2$ = 1, …, 4, 5.and $i_3,\ j_3$ = 1, …, 4, 5.

Although, by Property 5.1, the number of states grows extremely fast, in some cases it can be reduced significantly and the transition probability matrix can become a block matrix. For example, if for a two category confidential model n = 2 and v_1 =2, and v_2 =2 if

$Q_1 = \begin{bmatrix} A & 0 \\ 0 & 0 \end{bmatrix}$, where A is a 2x2 matrix and

$Q_2 = \begin{bmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{bmatrix}$. Then

$$T = \begin{bmatrix} Ar_{11} & 0 & Ar_{12} & 0 \\ 0 & 0 & 0 & 0 \\ Ar_{21} & 0 & Ar_{22} & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

And there are only four rows and four columns are non-zero rows or columns. Therefore there are only four states that are non-zero states, instead of eight states.
Likewise, for a three category confidential model of two states each, n=3, v_1 =2, v_2 =2 and v_3 =2.,, instead of using 48 states, there are some possible cases which can reduce the number of states significantly, as shown in the following assuming parent company can access all states in the child company.:
Case 1: If a parent company (Q_1) invests its own Supplier1 company(Q_2) and has Supplier2 company(Q_3) for competition. There are only 4x2x2=16 states.
Case 2: If a company (Q_1) has Supplier1 company(Parent Q_2) and also has Supplier2 company(Child Q_3) for competition. There are only 2x4x2=16 states.
Case 3: If a company (Q_1) has 2 unrelated Supplier1 company(Q_2) and Supplier2 company(Q_3) for competition. There are only 2x2x2=8 states.

In the next section a two category (e.g. manager and employee categories) and a three category confidential models will be simulated under a variety of distributions.

6. SIMULATION OF STATE TRANSITIONS

6.1 Simulation of Two Category Model (when v_1, v_2 =2)

The simulation methodology can be found in [23] and the results can be found in [22].

6.2 Simulation of Three Category Model (when v_1, v_2, v_3 =2)

A similar simulation results as a two category model for a three category one are shown in Figure 2 and 3 below. The initial state for all different distributions used in the simulation is p(0)=(p1(0), p2(0), …,p48(0))
=(
0.012280573930,0.033676035784,0.041838055971,0.114729155008,0.002450696980,0.006720350341,0.000716168443,0.001963891447,0.041838055971,0.114729155008,0.142535921970,0.390864859910,0.008349153550,0.022895216079,0.002439877449,0.006690680806,0.002450696980,0.006720350341,0.008349153550,0.022895216079,0.000489058225,0.001341105259,0.000142917737,0.000391911882,0.000436835332,0.001197898595,0.001488231833,0.0040810

59139,0.000087174348,0.000239051244,0.000025475005,0.000069858068,0.000237081035,0.000650128364,0.000807699191,0.002214888899,0.000047311614,0.000129738856,0.000013825897,0.000037913653,0.000042252076,0.000115864488,0.000143946425,0.000394732769,0.000008431775,0.000023121782,0.000002464022,0.000006756890) and =1.

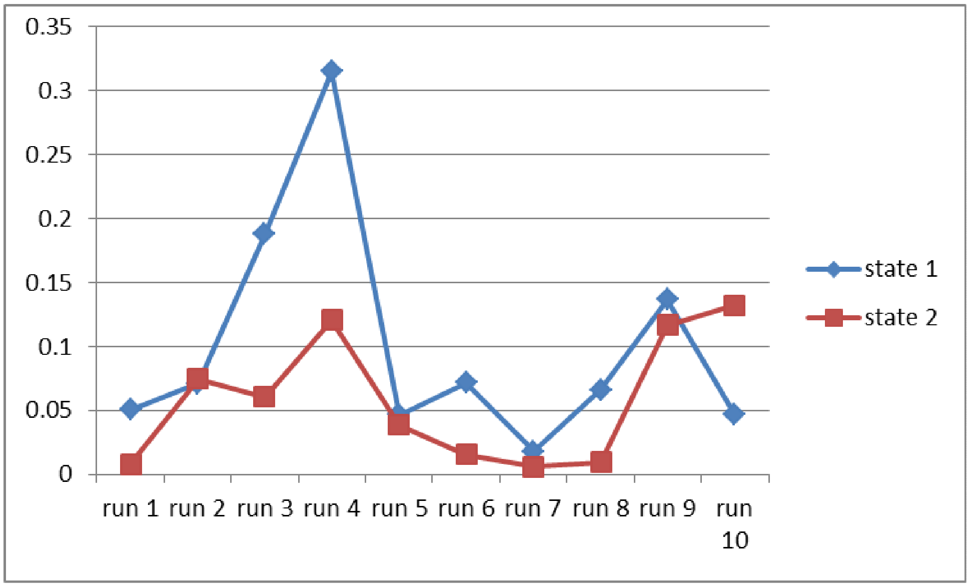

FIGURE 2: The steady states of the ten simulation runs when both category 1, 2 and 3 distributions are uniform (0,1) distribution.

The average steady states of all ten simulation runs for different distributions are shown in Figure 3.

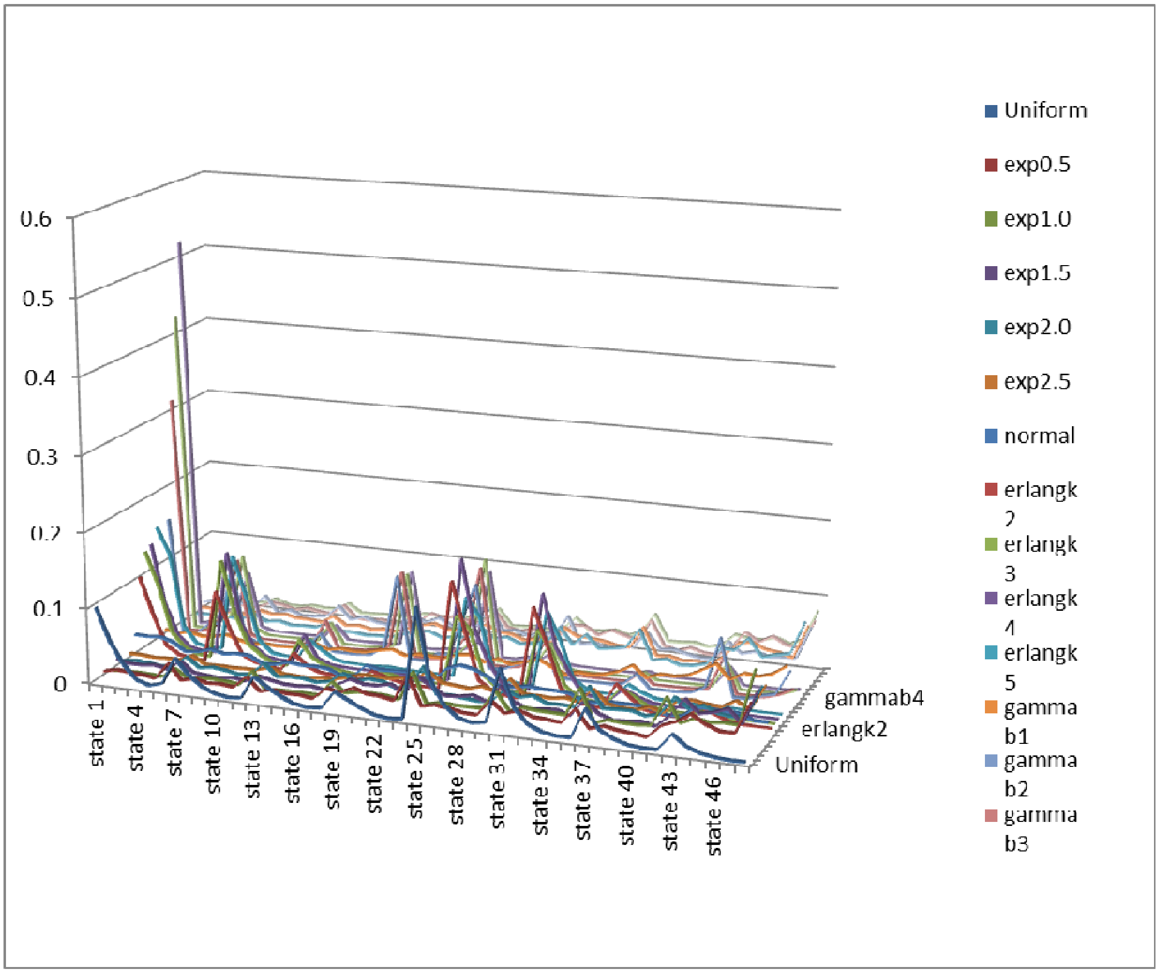

FIGURE 3: Comparison of Steady States for Different Distributions.

In Section 6 it describes how to validate an n category confidential model. An example of a two category model used in previous section is used to show how to use those properties.

7. VALIDATION FOR SEMI-MARKOV CHAIN MODEL

According to Rencher [24], the following two properties show how to test the hypothesis for the mean based on the average of the observations

Property 7.1.

In the n category confidential model if each steady state of an m observations y_i ~ $N_p(\mu_0 , \Sigma)$, i=1,2,…,m are independently identically distributed normal random variables of p parameters each and if Σ is unknown, then the average $\overline{y} = \sum_{i=1}^{m} y_i /m$ ~. $N_p(\mu_0 , \Sigma/m)$. To test the hypothesis H_0: $\mu= \mu_0$ vs H_1: $\mu\neq \mu_0$. We reject H_0 at α level if $n(\overline{y} - \mu_0)' S^{-1} (\overline{y} - \mu_0) > T^2_{\alpha,p,m-1}$, where S is the sample variance-covariance pxp matrix $\sum_{i=1}^{m} (y_i - \overline{y})(y_i - \overline{y})' \Big/ (m-1)$ and p = $\prod_{i=1}^{n} n_i$ is the total number of states and T^2 is the Hotelling's T^2 test.

Property 7.2.

In the n category confidential model if each steady state of an m observations $y_i \sim N_p(\mu_0\ , \Sigma)$, i=1,2,…,m are independently identically distributed normal random variables of p parameters each and if Σ is known, then the average $\overline{y} = \sum_{i=1}^{m} y_i/m$ ~. $N_p(\mu_0\ , \Sigma/m)$. To test the hypothesis H_0: $\mu = \mu_0$ vs H_1: $\mu \neq \mu_0$. We reject H_0 at α level if $m(\overline{y} - \mu_0)' \Sigma^{-1} (\overline{y} - \mu_0) > \chi^2_{\alpha,p}$, where Σ is the variance-covariance matrix, $p = \prod_{i=1}^{n} n_i$ is the total number of states and, χ^2 is the Chi-Square distribution.

Therefore for the two category confidential model described in Section 4 where p=8 and m=10 we can test the hypothesis H_0: $\mu = \mu_0$ vs H_1: $\mu \neq \mu_0$. We reject H_0 $_{\text{at 0.05 level}}$ if $10(\overline{y} - \mu_0)' \Sigma^{-1} (\overline{y} - \mu_0) > \chi^2_{0.05,8} = 15.51$ if Σ is known (Σ can be known from analyzing data from a long history or have a substantial evidence to support it). If Σ is unknown, we reject H_0 if $10(\overline{y} - \mu_0)' S^{-1} (\overline{y} - \mu_0) > T^2_{\alpha,8,9}$, where $\overline{y} = \sum_{i=1}^{10} y_i/10$ is the average of 10 final states of all runs. For the two category model described in Section 5, the mean μ_0 of final states of all ten runs of a randomly generated standard normal distributions N(0, 1) for both manager and employee transition matrices are recorded and the sample variance-covariance matrix Σ is created for each case (See Figure 4).

	state 1	state 2	state 3	state 4	state 5	state 6	state 7	state 8
run 1	0.16311	0.14008	0.15553	0.10319	0.12716	0.10920	0.12124	0.08045
run 2	0.03894	0.17662	0.08872	0.06968	0.06518	0.29565	0.14852	0.11665
run 3	0.27862	0.07009	0.07362	0.12027	0.23486	0.05908	0.06206	0.10138
run 4	0.23942	0.17365	0.20483	0.26506	0.03173	0.02301	0.02714	0.03513
run 5	0.19214	0.13896	0.17713	0.18278	0.08591	0.06213	0.07919	0.08172
run 6	0.02380	0.00512	0.00151	0.00139	0.72377	0.15591	0.04615	0.04231
run 7	0.25390	0.10694	0.07547	0.29020	0.09556	0.04025	0.02840	0.10923
run 8	0.24306	0.46896	0.05676	0.10998	0.03352	0.06469	0.00783	0.01517
run 9	0.25840	0.07277	0.04623	0.07815	0.30881	0.08697	0.05525	0.09339
run 10	0.12906	0.25043	0.14481	0.07030	0.08798	0.17073	0.09872	0.04793
Avg	0.18205	0.16036	0.10246	0.12910	0.17945	0.10676	0.06745	0.07233

Covariance	0.00969	0.00471	0.00625	0.00756	0	0	0	0.00115
	0.00471	0.01349	0.00397	0.00260	0	0	0	0
	0.00625	0.0039775	0.0068362	0.0058177	0	0	0.0028518	0
	0.0075628	0.002606	0.0058177	0.0095794	0	0	0	0.002102
	0	0	0	0	0.0221986	0.0052413	0	0
	0	0	0	0	0.0052413	0.0086107	0.0055392	0.0027665
	0	0	0.0028518	0	0	0.0055392	0.0047032	0.0029542

0.0011575	0	0	0.002102	0	0.0027665	0.0029542	0.0036708

FIGURE 4: Average μ_0 and the sample variance-covariance matrix of Σ of 10 runs of randomly generated standard normal distributions for both manager and employees.

For example, assuming both manager and employee distributions are standard normal, there are ten observations (y_i , i=1,2, …,10) of states in the long run obtained by a manager. They are listed below

(state 1	state 2	state 3	state 4	state 5	state 6	state 7	state 8):
(0.671259	0.122945	0.075425	0.075867	0.038695	0.007087	0.004348	0.004373),
(0.347069	0.270521	0.137034	0.060936	0.07849	0.061179	0.03099	0.013781),
(0.524644	0.067031	0.039512	0.057259	0.237426	0.030335	0.017881	0.025912)
(0.179443	0.277235	0.076472	0.076476	0.114907	0.177528	0.048969	0.048972)
(0.27958	0.099922	0.054449	0.072657	0.272286	0.097315	0.053028	0.070762)
(0.54851	0.187313	0.115711	0.028219	0.074972	0.025603	0.015816	0.003857)
(0.364298	0.008646	0.001995	0.041343	0.510827	0.012123	0.002797	0.057972)
(0.35618	0.043088	0.049767	0.043699	0.366685	0.044359	0.051235	0.044988)
(0.11346	0.075408	0.044019	0.040133	0.302115	0.200791	0.117212	0.106863)
(0.256683	0.064596	0.027857	0.107778	0.305092	0.076779	0.03311	0.128104)

To test the hypothesis H_0: $\mu = \mu_0$ vs H_1: $\mu \neq \mu_0$, where μ_0 =

(0.1820501 0.1603668 0.1024654 0.1291058 0.179453 0.1067649 0.0674549 0.072339)

The average of ten observations is $\bar{y}$ =

(0.364113 0.121671 0.062224 0.060437 0.23015 0.07331 0.037539 0.050558)

If Σ is unknown , from Property 7.1, $10(\bar{y} - \mu_0)' S^{-1} (\bar{y} - \mu_0) = 1979 > T^2_{0.05,8,9} = 697.356$. The null hypothesis is rejected. Therefore the security may have been breached.

The next section shows how the model helps manager to manage the dynamics of the security states.

8. MANAGERIAL IMPLICATIONS

The proposed model is general enough in practice. For example, in a supply chain network there are three groups involved: the purchasing group and two supplier groups. The model uses three security classifications which contains top secret (the purchasing group), secret (the first supplier group) and confidential (the other supplier group). If the first supplier group is not allowed to access the information in the second supplier group, we only need to set the appropriate part of the transition probability matrix to zero. The characteristics of the model are completely determined by the transition matrix. Based on the transition matrix we can determine whether the process will reach to the equilibrium state after a long period of time. Suppose we have a **scenario A** that a manager group first randomly evaluates suppliers before sending out a bid notice and request the bidding price. Then it repeats the whole process. In the mean time, an employee group randomly performs either providing bidding price or reading bidding notices. The transition matrix was given and the semi-Markov chain is periodic with period 4. Therefore, it is recurrent non-null. Since all states can be reachable from all other states, it is irreducible [25]. If at time 0 it has 42% chance that manager evaluates supplier, 40% chance that manager makes buying decision, 2% chance that manager reads biding notice and 16% chance that manager reads retail price and if it has 35% chance that employee reads biding notice and 65% chance that employee reads retail price, then at time 1000000 it has 14% that manager evaluates supplier evaluation and employee reads bidding notice [15]. However, if we follow the **scenario B** that the purchasing group randomly performs those four actions and the supplier group performs those two actions randomly, then each state is a recurrent non-null and aperiodic. That is, the semi-Markov chain is ergodic [25] and the system has a steady state p(s) when time s is large. The simulation result is in the Figure 5 below:

state	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Purchasing initial state	0.284308	0.216797	0.442041	0.056855				
Supplier initial state	0.964208	0.035792						
Time=0 state	0.274132	0.209038	0.426219	0.054820	0.010176	0.007760	0.015821	0.002035
State Transition probability matrix T	0.040019	0.028175	0.646285	0.514467	0.003465	0.002440	0.055963	0.044549
	0.335822	0.428346	0.019121	0.117963	0.029080	0.037091	0.001656	0.010215
	0.007283	0.041699	0.032780	0.014115	0.000631	0.003611	0.002839	0.001222
	0.334275	0.219179	0.019213	0.070854	0.028946	0.018979	0.001664	0.006135
	0.015764	0.011099	0.254588	0.202661	0.052318	0.036834	0.844909	0.672579
	0.132289	0.168736	0.007532	0.046468	0.439031	0.559990	0.024997	0.154216
	0.002869	0.016426	0.012913	0.005560	0.009521	0.054515	0.042855	0.018454
	0.131679	0.086340	0.007568	0.027911	0.437009	0.286540	0.025117	0.092630
Time=999997 state	0.047418	0.076108	0.006181	0.050500	0.215712	0.346228	0.028120	0.229734
Time=999998 state	0.047418	0.076108	0.006181	0.050500	0.215712	0.346228	0.028120	0.229734
Time=999999 state	0.047418	0.076108	0.006181	0.050500	0.215712	0.346228	0.028120	0.229734
Time=1000000 state	0.047418	0.076108	0.006181	0.050500	0.215712	0.346228	0.028120	0.229734

FIGURE 5: A semi-Markov chain Simulation Run using the scenario B.

Figure 5 shows the simulation run using protocol B after one million state transitions. We can see that the system has a steady state p(s)=(0.047418, 0.076108, 0.006181, 0.050500, 0.215712, 0.346228, 0.028120, 0.229734), where s=1000000. And it satisfies Tp(s)=p(s).

Any state which does not belong to one of the possible eight states is violates the security requirement. If an employee evaluates supplier, the system will warn the security manager to take actions. A large manufacturer may have more than hundreds of suppliers for various parts acquisition in different time periods. The semi-Markov chain model can help the managers to understand the confidential status of each supplier and then implement necessary security strategy for the organizations.

9. RESEARCH RESULTS AND CONCLUSION

By combining the subjects and objects possible security levels, all possible states can be listed in the semi-Markov chain model. In conclusion, since the confidentiality policy for the supply chain networks can be modeled by Bell-LaPadula model, semi-Markov chain model can be used successfully to simulate the state transitions dynamically for the Supply Chain networks. As we mentioned early, security standards today are emerging but many basic security principles in the standards can be traced back to existing security models. These standards and models are further impacting on the business strategy for the managers in an enterprise [21, 26]. ISO/IEC 17799:2005 provides "guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management." [4]. The semi-Markov chain model discussed in this paper shows the process of the secured state during the time period in the supply chain network. Any state which does not belong to one of the possible state is considered as impeaching the security. For example, in the previous section only those eight states are allowed. If a general employee is conducting supplier evaluation, which is not in one of those eight states, the system will not allow the process to proceed to the next possible state and managers will be warned on security impeachment. In reality, a supply chain network is fairly complex. A large manufacturer may have more than 500 suppliers for various parts acquisition in different time periods. The semi-Markov chain model can help the managers to understand the status of each supplier and then implement necessary security strategy for the organizations. Although the model is useful for managers, however, because of Property 5.1, the number of states grows exponentially fast when the number of categories grows. It is suggested to be used when both the number of categories and the number of objects are small. This model can be also applied to password management in order to prevent threats from using the same password on other web sites.

10. ACKNOWLEDGEMENTS

This paper is in memory of my mother Sharn-Yun Chen for her life time encouragement, support and insatiable hunger for knowledge. Without her this paper would have never been completed.

11. REFERENCES

[1] CNSS (The Committee on National Security Systems) 4009, 2003.

[2] S. Lipner, Non-discretionary control for commercial applications, Proceedings of the 1982 Symposium on Privacy and Security, 2-10, 1982.

[3] K. Hsu and Z. Zhu, “SAS 99 – Consideration of fraud in a financial statement audit: a new auditing standard”, International Journal of Services and Standards, Vol. 1, No.4, 2005, pp. 414 – 425.

[4] M. Lee and T. Chang, “Applying ISO 17799:2005 in information security management”, International Journal of Services and Standards, Vol. 3, No.3, 2007, pp. 352 – 373.

[5] M. Bishop, Computer Security, Addison-Wesley, 2003.

[6] M. Shing, C. Shing, K. Chen and H. Lee. (2006). “Security Modeling on the Supply Chain Networks”, Journal of Systemics, Cybernetics and Informatics, 2008 , Vol. 5, No. 5, pp. 53-58.

[7] K. Biba, “Integrity considerations for secure computer systems”, Technical Report MTR-3153, 1, Bedford, MA: MITRE Corporation, 1977.

[8] D. Brewer and M. Nash, “ The Chinese wall security policy”, Proceedings of the 1989 IEEE Symposium on Security and Privacy, 1989, pp.206-214.

[9] D. Clark and D. Wilson, “A comparison of commercial and military security policies”, Proceedings of the 1987 IEEE Symposium on Security and Privacy, 1987, pp. 184-194.

[10] D. Bell and L. LaPadula,, “Secure computer systems: Mathematical foundations”, Technical Report MTR-2574, I, Bedford, MA: MITRE Corporation, 1973.

[11] D. Bell and L. LaPadula, “Secure computer system: Unified exposition and multics Interpretation”, Technical Report MTR-2997, Rev. 1, Bedford, MA: MITRE Corporation, 1975.

[12] K Chen, H. Lee and J. Yang, ‘Security Considerations on the Design of Supply Chain Networks’, the Proceedings of Southwest Decision Sciences Institute, Vol. 14, No. 1/2/3, 2006.

[13] K. Chen, M. Shing, C. Shing and H. Lee, "Modeling in Confidentiality and Integrity for a Supply Chain Network," Communications of the IIMA, 2007.

[14] M. Shing, C. Shing, K. Chen and H. Lee. (2006). "Security Modeling on the Supply Chain Networks", Proceedings of EIST 2006, Orlando, FL.

[15] M. Shing, C. Shing, K. Chen and H. Lee. "A Simulation Study of Confidentiality Modeling in a Secured Supply Chain Network", Proceedings of International Symposium on Intelligent. Information Technology Application conference, Dec. 22-23,2008, Shanghai, China.

[16] P. Bremaud, Markov Chains. New York: Springer, 1999.

[17] M. Aburdene, Computer Simulation of Dynamic Systems, Wm. C. Brown Publishing, 1988.

[18] Bhat, N. (1972). Elements of Applied Stochastic Processes, John Wiley & Sons.

[19] M. Molloy, Fundamentals of Performance Modeling. New York: Macmillan Publishing., 1989.

[20] G. McDaniel, IBM Dictionary of Computing. New York, NY: McGraw-Hill, Inc., 1994.

[21] A. Smith, "Strategic aspects of electronic document encryption", International Journal of Services and Standards, Vol. 3, No.2, 2007, pp. 203 – 221.

[22] M. Shing, C. Shing, L. Shing. (2012). "Analysis of a Two Category Confidentiality Model In Information Security", Journal of Communication and Computer, USA, 3(1), 2012.

[23] J. Banks, J. Carson, B. Nelson, Discrete Event System Simulation, New Jersey, Prentice Hall, 1996.

[24] A. Rencher, Methods of Multivariate Analysis. New York: John Wiley & Sons, 1995.

[25] E. Parzen, Stochastic Processes. San Francisco: Holden-Day., 1967.

[26] A. Smith, "Supply chain management using electronic reverse auctions: a multi-firm case study", International Journal of Services and Standards, Vol. 2, No.2, 2006, pp. 176 – 189.