9

A Cost-based Model for Risk Management in RFID-Enabled Supply Chain Applications

Manmeet Mahinderjit-Singh[1], Xue Li[1] and Zhanhuai Li[2]
[1]*The University of Queensland,*
[2]*Northwest Polytechnical University of China*
[1]*Australia*
[2]*China*

1. Introduction

Radio Frequency IDentification (RFID) is a dedicated short range communication (DSRC) technology that enables a physically linked world where every object is identified, catalogued, and tracked through the use of a RFID tag, comprised of an IC (Integrated Circuit) chip and antenna that sends information to the RFID reader in response to a wireless probe. In contrast to barcodes, RFID does not require line of sight or contact between readers (also known as interrogators) and tagged objects. The main advantages of RFID systems are price efficiency and accuracy of stock management. In addition to emerging applications in retail and distribution, RFID has gradually been adopted and deployed in other service industries, including aircraft maintenance; baggage handling; laboratory procedures; security; and healthcare. Although RFID technology has obvious advantages, including increased visibility and fast identification, there are still some problems, including limitation of RFID tag's hardware storage and memory; threat of counterfeiting; and other security and privacy issues (Juels, 2006).

This study focuses on the counterfeiting problem of RFID technology in supply chain management (SCM). This problem appears as RFID tag cloning and fraud attacks (Gao *et.al*, 2004) that lead to financial losses and loss of trust and confidence. The RFID tag cloning and fraud attacks can hinder the adoption and acceptance of RFID technology (Choi *et.al*, 2008; Lehtonen, 2007). Therefore trust management plays an important role as an instrument of decision making whether a system is worthwhile to be used with a minimal risk (Kutvonen, 2005). The tradeoff of trust is considered against risk handling, security and privacy management. The significance of trust in the new emerging ubiquitous technology in a context of RFID is critical. Supply chain involves open network connectivities, physical products transportation, and transaction management, where trust counts in the selection of partners; the selection of software and hardware infrastructure; as well as the adoption of communication systems (Derakshan *et.al*, 2007).

Public acceptance of RFID implications systems is still an open question due to its current limitations and vulnerabilities, (Lehtonen, 2007). In our previous work (Mahinderjit-Singh & Li, 2009; Mahinderjit-Singh & Li 2010), we proposed a novel seven layers trust framework for RFID-enabled supply chain management (SCM). Our seven-layer trust framework provides an approach to establish trustworthiness of large scale tracking systems and

usefulness of RFID systems. This framework suggests a few prevention and detection mechanisms for a variety of security attacks. Also Mirowski & Harnett (2007) believe that RFID cloning and fraud attacks necessitate countermeasures beyond static preventive mechanisms. As most existing research studies focused on static preventive models without much success, we agree with Mirowski & Harnett (2007) that the detection of cloning and fraud attacks is the first line of defense in eliminating these security attacks.

Our study includes minimization of RFID technology error rates, as well as the minimization of predictions of incorrect class labels and the improvement of detection accuracy. We argue that a cost-sensitive approach is essential to reduce the risk of counterfeiting in SCM. For example, in medical diagnosis of cancer disease, where presence of cancer is regarded as either positive (cancer) or negative (no cancer). In this scenario, a false–negative (FN) error is much more serious (and costly) than a false-positive (FP) error. The patient could risk his/her life because of this FN error and missing out of the early detection and treatment. Similarly, in RFID clone and fraud detection, false-negative or failure of detecting fraud tags is very expensive (e.g. counterfeiting associated loss of billions–dollar businesses). This study focuses on closing a current gap in RFID tag cloning detection systems, that has not been dealt with in previous studies, namely the analyses of system costs in FN and FP errors.

The objective of a cost-sensitive model in an intrusion detection system (IDS) is to formulate the total expected cost for the detection of an intrusion. A cost model should consider the trade-offs among all relevant cost factors and provides a basis for making appropriate cost-sensitive prediction decisions. A cost model should comply with the well-known Pareto principle or the commonly regarded 80-20 rule. Pareto rule or 80-20 rule specifies an unequal relationship between inputs and outputs (Shulmeyer & Thomas, 1999). More generally, the Pareto Principle is the observation (not law) that most things in life are not distributed evenly. For instance, the efforts of 20% for using cost model for counterfeit wines detection system could drive 80% of the firm's profits through elimination of counterfeit wines bottles in a supply chain. By applying the Pareto distribution rule, we may eliminate 80% percent of counterfeiting by dealing with the causal factors of the top 20% of the reported RFID cloned and fraud tags. In our hypothesis, we denote that solving FN cost is more important than solving false positive (FP) cost, and that 20% of effort put into detecting the FN cost will lead to an overall system cost reduction of 80%. Our cost model does not involve the cost for products reduction due to an attack; for instance losses in wine prices due to counterfeit attack. We believe that the usage of a cost model in a cloned detector system is able to reduce the chances of counterfeiting as early as in the supply chain plant itself. By doing so, there will be zero counterfeit products after any POS (Point of Sale) at the retailer site.

Risk Management (Lin & Varadharajan, 2006) is a process used to identify possible risks and setting procedure to avoid the risk, or minimise its impact or setting up a strategy to control the risks. Risk management often involves a multi-criteria decision making process in which factors such as economic, health, legal and others are appropriately weighted on a course of action. Because the decision making process can be complex, there is no one decision criterion that must be or is always used. In order to build cost-sensitive IDS models, we discuss the relevant cost factors and the metrics used to define them. Cost-sensitive modeling for intrusion detection must be performed periodically because cost metrics need to deal with changes in information assets and security policies (Lee *et.al*, 2002). It is

therefore important to develop tools that can automatically produce cost-sensitive computations for given cost metrics. The three main costs: damage, response, and operational cost, must be evaluated and quantified based on factors such as cloning attack types and the RFID system environment. Damage cost is a measured loss to the supply chain business which has lost the financial benefits due to cloning and fraud attacks. Response cost is the cost to countermeasures the cloning and fraud attack in a supply chain business. Operational cost is distinguished by the cost of running the detection engine providing function in detecting and responding to both cloning and fraud attacks in a RFID enabled supply chain environment. Hence, the main aim of this chapter is to construct and quantify a cost sensitive model for RFID enabled SCM. The RFID tag cloning and fraud attacks are used in simulating the security attacks and in defining the cost factors in the RFID-enabled supply chain.

We use the Multi Criteria Decision Making (MCDM) (Satty, 1990) model to calculate the costs and decisions. We have use Analytic Hierarchy Process (AHP) technique, which is a MCDM tool in distinguishing the best approach and algorithm for preventing and testing for RFID tag cloning attacks in SCM. The second aim is to extend the MCDM tool through the use of criteria used by supply chain owners when selecting RFID tag cloning and fraud prevention techniques. These criteria include acceptance; cost; security; and complexity. This cost model is the first of its kind with the aim to counter security attacks such as counterfeiting in RFID enabled SCM. The main challenges in the development of the cost model are to represent and identify the different types of costs involved in the detection of the attacks and to maintain responsiveness to changes in these cost factors. Finally, we distinguish the cost properties in a SCM RFID environment. Even though our work is focused on RFID tag cloning and fraud, our trust framework and the cost model will be transferable for countering other types RFID security attacks.

The rest of this chapter is constructed as follows. Section 2 gives a literature review and describes the related cost models. It also introduces some background on countering RFID cloning and fraud attacks. Section 3 explains the design of our cost model for RFID tag cloning and fraud detection system. In section 4 we present on how can use MCDM tool to quantify the related costs and maintain responsiveness to RFID tag cloning and fraud attacks. Section 5 introduces RFID tag cloning and fraud prevention techniques using AHP and MCDM tools. Sections 6 discuss the applicability of the proposed models. Section 7 provides the conclusion and views on future work.

2. Backgrounds and related work

In this section we provide an overview of cost sensitive learning and define cloning, fraud and counterfeiting problems. We define both RFID tag detection classification and cost matrices. Finally, we explain how we could integrate RFID detection and our cost model in our proposed seven-layer trust framework.

Cost-Sensitive Learning is a type of learning in data mining that takes misclassification and other types of cost into consideration (Turney, 2002). The goal of this type of learning is to minimise total cost. The key difference between cost-sensitive learning and cost-insensitive learning is that cost-sensitive learning treats different misclassifications differently (Turney, 2002). Cost insensitive learning does not take misclassification costs into consideration. The goal of this type of learning is to pursue high accuracy when classifying examples into a set of known classes.

Credit card fraud detection, cellular phone fraud detection and medical diagnoses are examples of intrusion detection because intrusion detections deal with detecting abnormal behaviour and are typically motivated by cost-saving, and thus typically use cost-sensitive modeling techniques. Previous work in the domains of credit card fraud (Lee, W., et.al, 1999) and cellular phone fraud (Fawcett & Provost, 1997) have applied cost metrics in evaluating systems and alternative models, and in formalizing the problems to which one may wish to apply data mining technologies. The cost model approach proposed by Lee et.al (2000) formulate the total expected cost of an IDS, and present cost-sensitive machine learning techniques that can produce detection models that are optimized for user-defined cost metrics. The detection technique used by Fan et.al (2000) and Lee et.al (2002) uses an inductive rule learner, Repeated Incremental Pruning to Produce Error Reduction (RIPPER). Their cost model is based on a combination of several factors: The cost of detecting the intrusion; the amount of damage caused by the attack; and the operational cost of the reaction to the intrusion. Lee et al (2002) claimed that the IDS should have minimal costs. However, their work did not consider any related administrative testing costs. Their work has been extended by Chen et.al (2008), who claimed that their approach could potentially lower the consequential cost in current IDSs. Although the generation of fingerprints as a means of authentication increases operational costs associated with the use of IDSs, experimental results show that these incremental costs are limited and that overall cost is much lower than with the Lee et.al (2002) approach.
We adopted the two proposed models above. Since our cloned detector will become a component integrated in the existing Global Electronic Product Code (EPCglobal) Standard, we should be able to use the cost model designed for IDS. Differences include the technique used to quantify the cost model and the detection technique and authentication method used in our cloned detector. We analyse various authentication methods used for supply chain partners and RFID tags by using the MCDM approach. Next, we define cloning, fraud and counterfeiting attacks in a RFID system.

2.1 Problem definition

2.1.1 Cloning, fraud and counterfeiting definition

RFID tags clone occurs in the form of cloned tags on fake products or clone tags on genuine product. Both types are similar in term of the cloned tags.

- An RFID tag is a cloned when the tag identification number (TID) and the form factors is copied to an empty tags (Lehtonen et.al, 2009). Hence there will be a same tags data structure on two different products.
- In contrast, fraud is an act of using the cloned tags and adding the serial numbers of future EPC codes. These future EPC codes are the codes in the systems, which are yet to be tagged to the products.
- Counterfeiting on the other hand is a more generalised term which includes both the act of cloning and fraud of RFID tags and tagging onto fake products in the market for personal benefit.

There are four different attacks that contribute to cloning attack in a RFID system (Mahinderjit-Singh & Li, 2009; Mahinderjit-Singh & Li 2010). Skimming attack occur when RFID tag are read directly without anyone knowledge. Eavesdropping attack happens when an attacker sniffs the transmission between the tag and reader to capture tags data. On the other hand, man in the middle attack occurs when a fake reader is used to trick the genuine tags and readers during data transmission. RFID tag data could also be altered using this

technique and as a result, fraud tags could be generated too. Physical attack which requires expertise and expensive equipment takes places in laboratory on expensive RFID tags and security embedded tags.

We will give a definition of clone, fraud and counterfeiting in RFID tag. Let assume set Ti contain the RFID genuine tags and Tx contain cloned tags derived from Ti. A genuine tag is known as TG and a cloned tag is known as TC. *I* denote an intruder. A list of attacks (*S*) includes Skimming (*S1*), Sniffing (*S2*), Active Attack (*S3*), Reverse Engineering (*S4*) and Cryptanalysis (*S5*)

Thus;

Ti= {TG1, TG2, TG3}

Tx= {TC1, TC2}

S = {S1, S2, S3, S4, S5}.

Attack Types	Attack Pattern	Attack Levels	Model features
Skim (Juel.A,2005) (Dimitriou,2005)	Copy → Cloned	Low (Tag, Reader)	Content Timestamp/TTL R/W on Tag & Reader
Eavesdrop (Bolotnyy et.al, 2007) (Duc & Park, 2006)	Copy → Cloned	Low (Tag, Reader, DB)	Content Timestamp/TTL R/W on Tag & Reader Location
Man-In-The middle (Juels, 2006) (Gao et.al, 2007)	Copy → Cloned Alter → Fraud	High (Tag, Reader, DB)	Content Timestamp/TTL R/W on Tag & Reader Location
Physical (Bono.S, 2005) (Nohl.K, 2008)	Copy → Cloned Alter → Fraud	High (Tag, Reader, DB)	Content Timestamp R/W on Tag & Reader Location

Table 1. RFID Cloning and Fraud attacks

Hence TC1 is a clone of TG1; if and only if both tags have identical TIDs (tag identifier) and share the same form of characteristics. Once the TIDs are the same, all the data and structure of the tag's EPC code such as header, manufacturer id, object class and serial number are identical, i.e., |TG| = |TC|. A TC exists when *I* performs *S* either a single *S* or a combinations of *S* against TG. *S* will produce cloning attack. RFID Cloning is a process of injecting imitated EPC tags in a normal genuine EPC tags batch $TG \subseteq BG$ and $TC \subseteq BC$. Table 1 shows RFID attacks patterns and its model.

By analysing the model features of the different attacks types, we can distinguish different types of RFID security attacks, different levels of attack (high, low) and the different associated compromised RFID components. This model is important for the precise understanding of cloning vs. fraud attacks. A cloning attack is generalised as an act of copying tag data and structure, whereas a fraud attack involves both copying and altering tag data and structure. Based on Table 1, RFID tags compromised by 'Eavesdropping', 'Man in the middle' and 'Physical' attacks will demonstrate deviants in RFID tag data and structure namely tag content tag time (e.g. timestamp and time to live (TTL) (Li *et.al*, 2009)

and tag locality. Next, we define RFID tag cloning and fraud detection classification and a cost sensitive model that can be used for RFID tagging.

2.1.2 RFID tag cloning and fraud detection classification and cost sensitive modeling

Before applying a cost sensitive model to RFID tagging, a RFID dataset is pre-processed to feed into a cloned detector that is based on a classification concept. Suppose that we have a collection, I, of RFID Tags, each labelled as either good or bad, depending on whether or not it is associated with legitimate or fake products. The set of all possible classes can thus be defined as C = {good, bad}. Bad tags could be either cloned or fraudulent/fake tags. We approximate the unknown target function, $F: I \times C = \{1, 0\}$. The value of $f(i, c)$ is equal to one if the RFID tag, i, belongs to the class c and equal to zero if not. It is now possible to define a classifier as an approximation function, $M: I \times C = \{1, 0\}$. The objective of the learning task is to generate a classifier that produces results as close to that of F as possible. Compute a model or classifier, C, by some learning algorithm L that is predicted from the features:

$$<fn,\ldots\ldots fn\text{-}1>$$

The target class label is *fc*, 'cloned' .

Hence, $C = L(T)$, where L is a learning algorithm . Each $t \in T$ is a vector of features, where we denote *f1* as the 'transaction amount' (tranamt), and *fn* as the target class label, where the denoted clone $(t) = 0$ (legitimate transaction) or 1 (cloned or fraudulent transaction). Given a 'new unseen' transaction, x, with an unknown class label, we compute $fn(x) = C(x)$. C serves as a clone detector. Within the context of financial transactions, cost is naturally measured in dollars (e.g. US dollar is used in his chapter). However, any unit of measure of utility applies here. Hence, the cost model for this domain is based on the sum and average of loss caused by cloned and fraudulent tags. We define a set of transactions S, a fixed overhead amount, and a cloned detector C (or classifier, C). The overhead amount is the cost of running the IDS operation. The total potential loss is the transaction amount (tranamt) losses for both cloning and fraudulent transactions. The cost matrix outcomes such as FN, FP, hit and true negative (TN) is as shown in Table 2 and is used for distinguishing whether the cost is a 'tranamt' (t) or an overhead.

$$\text{Total Potential Loss (S)} = \sum_{t\epsilon\ SCLONED(t)\ \&\ t\epsilon\ SFRAUD(t)=true} tranmt\ (t) \qquad (1)$$

Outcomes	Cost (t, Overhead)	
Miss (False Negative, FN)	tranamt (t)	
False Alarm (False Positive, FP)	Overhead 0	If tranamt (t) > overhead If tranamt (t) ≪ overhead
Hit (True Positive , TP)	Overhead 0	If tranamt (t) > overhead If tranamt (t) ≪ overhead
Normal (True Negative, TN)	0	

Table 2. Prediction of Cost model using tranmt (t) and overhead

2.2 Trust framework and IDS

The deviation of RFID technology based trust takes places when simple soft trust (including experience and reputation) is taken up to a higher level known as hybrid trust. Hybrid trust in a RFID system is more than just a hard or security trust based on authentication of soft

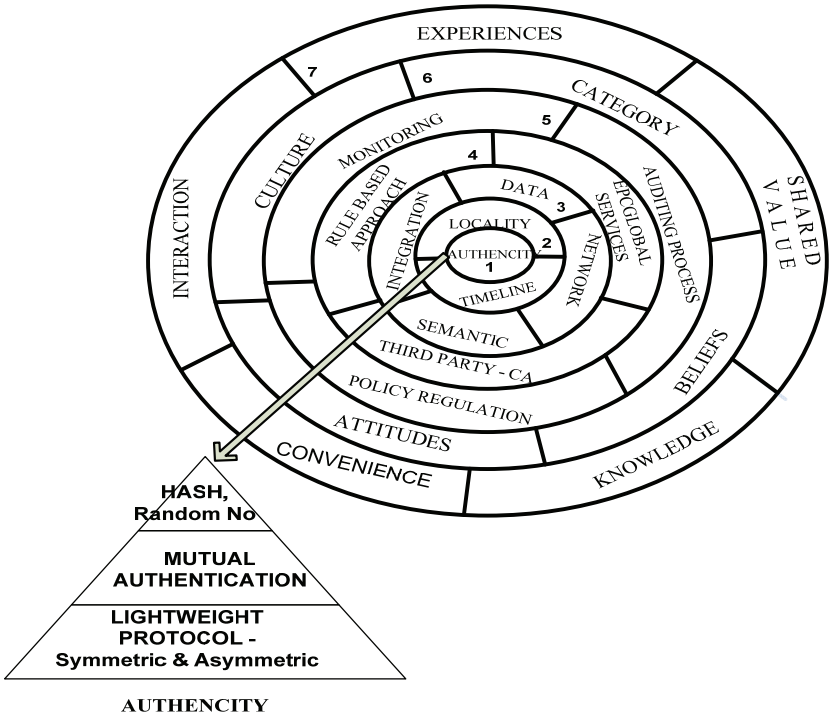


Fig. 1. Seven Layer Trust Framework [8]

trust as argued by Lin and Varadharajan (2007). In our definition, trust in a RFID technology system is defined as a comprehensive decision making instrument that joins security elements in detecting security threats with preventing attacks through the use of basic and extended security techniques such as cryptography and human interaction with reputation models. Since a trust model that disperses privacy is a weak and non-usable model, our trust framework ensures privacy and does not compromise security measurements. In addition, we argue that a trust model for a technological system should always include human interaction through the use of a feedback and ranking model. Our trust framework provides a theoretical solution for the trust gaps discussed in Section 1. In addition, our proposed trust framework (Figure 1) functions as :

- a solution to optimising trustworthiness by employing core functions at three main levels:
  a. The RFID system physical level (i.e. tags and readers) security and privacy level core functions;
  b. The RFID service core functions at the middleware level through utilisation of multiple data integration platforms such as the EPC trust services (http://www.epcglobalinc.org) and third party software systems such as intrusion detection systems (IDS) which can also be used; and
  c. The core functions at application level through use of reputation systems based on user interaction experiences and beliefs and

- to provide guidelines for designing trust in solving open system security threats.

2.3 EPCglobal network

EPCglobal (http://www.epcglobalinc.org), a subsidiary of GS1, has used EPC naming conventions to identify and trace products movement using RFID technology . This application is named the EPCglobal Network. The EPCglobal Network introduces a few dedicated components, such as the Object Naming Service (ONS) and the EPC Information Services (EPCIS) that may or may not be needed for future applications (Ranasinghe et.al, 2007). The ONS functions as an EPC resolution service that provides a look up a service to resources that provide further information about an item identified by a particular EPC. The ONS uses the standard Domain Name Service (DNS) for resolving EPCs. EPCIS permit applications to share and use EPC data across different enterprises. In each application, each local company will have its own local database and local EPC-IS. In addition, a Discovery Service (DS) (still under development) is a registry which registers incoming and outgoing products (Ranasinghe. and Cole, 2007) and functions as a item-level tagging server.

2.4 Architecture of our cost based cloned detector

In this section we design a cost based RFID tag cloning detector into our proposed trust framework and into the EPCglobal service. Figure 2 gives an outline on how our proposed detection system will work in a supply chain environment and in an EPCglobal network.
The following is a list of assumptions used in our system:

1. By utilising our proposed seven-layer trust framework, detection functions take place in layer-4.
2. Our trust framework is placed in EPCglobal services.
3. Local EPC-IS only share information that can be assessed by all assigned supply chain partners. Distributed network architecture is employed. Distributed network architecture eliminates the problem of information overload and makes it easier to exchange information. Manufacturer s and trading partners create and store their own serialised information about each and every product in their own local EPC-IS. The manufacturer manages and hosts a database that stores information about the generation of their products. Trading partners manages their local EPC-IS and store information about products movement through the supply chain. This local EPC-IS is accessible by all supply chain partners. Each involved partner makes this information available to authorised parties using the internet.
4. The Discovery service (DS) record incoming and outgoing product sand track products by using item-level tagging. DS functions as a key management server in which it generates public keys for System Administrator (SA) testing purposes. EPCglobal DS is equipped with a key management mechanism using a specific cryptography algorithm for public key encryption (RSA). It stores access control policies that comply with the role based access system. A role-based access control (RBAC) system has two phases in assigning privileges to an employee: first the employee is assigned one or more roles, and hen the role(s) are checked against the requested operation.
5. Supply Chain (SC) partner authentication is done through a certificate authority (CA) service using our trust framework. The partners that need to access the clone detector to provide their local certificate to the CA server installed in our trust framework.

6. The Object Naming Service (ONS) could be used to point to an address in the EPCglobal network where information about the product being questioned is stored. This service is important if a product need to be traced and tracked.
7. Item-level tagging is employed in our scenarios.
8. Attackers could be either from the organisation or outsiders.They are mainly 8 different points used by attacker to inject cloned and fraud in the SCM.

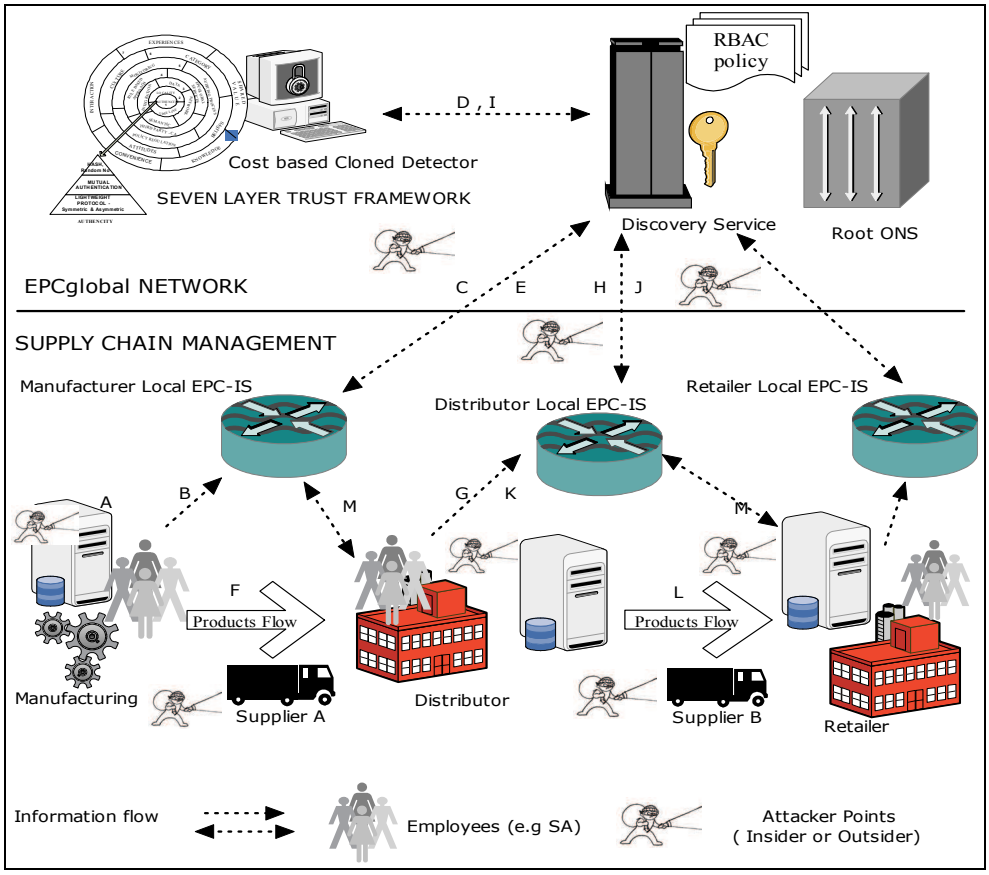


Fig. 2. Cost based Cloned Detector in a Supply Chain Management and EPCglobal Network environment.

a. An EPC lifecycle begins when a manufacturer tags a product. At the manufacturer's place, EPC tags are fixed to products. These EPC tags are furnished with codes and KILL/ACCESS passwords, upfront.
b. A manufacturer records products information into the local EPC-IS.
c. The EPC-IS registers EPC knowledge with EPC Discovery Services (DS).
d. Before the product leaves the manufacturer's site, the product is fed into the cloning detector.

e. The result is sent to the manufacturer's local EPC-IS. If a cloned tag is detected, a trigger is sent to the manufacturer's SA.
f. If not, the supplier is requested to move the product to the distributor's front door.
g. At the front door, the distributor records the product into their local EPC-IS.
h. The EPC-IS records with the EPC DS where tags are next fed into the cloning detector.
i. If a clone is detected, the distributor's SA is triggered. The alarm log is kept in the DS.
j. The alarm log is sent to distributor's local EPC-IS.
k. Before the products leaves the Distributor's site (at the back door), the RFID tags are fee into the cloning detector again to check for if there have been any cloning or fraudulent processes at the distributor site.
l. Once confirmed as genuine tags, distributor sends the tagged products to the retailer site. The same process takes place at the retailer site.
m. Any supply chain partner can access any other partner's EPC-IS for tracking and tracing purposes.

2.5 Testing process by system administrators

In this section we discuss how RFID tag cloning and fraud detection as well as cost modelling are supported by our proposed trust framework (Mahinderjit-Singh & Li, 2009; Mahinderjit-Singh & Li 2010). In supply-chain-wide RFID systems, increasingly large data volumes are being exchanged, which in turn increases the risk for competitors to intercept this information (Gao et.al, 2004). Trust relationships between supply chain suppliers and distributors curb cheap RFID tag cloning. RFID tag cloning and fraud detection can be detected in a supply chain at an initial stage if there is proper transfer of ownership with secure and authorised information exchange. We extend our proposed trust framework to establish a cloning and fraud detection system that has an integrated cost sensitive model.

Our RFID detection system has three main components: collection; detection; and response. Collection is the component that collects a RFID event set E that is supplied by different supply chain partners. RFID event sets are then sent to the detection component where the information sources are analysed. Several detection functions are performed in this component, such as pattern matching; traffic or protocol analysis; finite state transition; etc. The response component notifies the system administrator where and when an intrusion takes place. Two types of roles, an attacker and a system administrator (SA), are considered in current IDSs and are defined below.

Attackers attempt to gain unauthorised access to computer systems, tend to be malicious and possess a wide range of tools such as unauthorised RFID readers for performing the unethical acts of reading and manipulating genuine RFID tags to produce fake tags. Their behaviour is potentially harmful to the supply chain system. Almost 80% of attackers are the employees within a supply chain (P.Marcellin , 2009)

System administrators (SAs) take charge of protecting the system and are minimising the costs of network management; system maintenance; and excessive use of resources. They are appointed and authorised to examine enterprise networks from attackers' perspectives, and use vulnerability testing tools that are the same as or similar to those used by hackers. Their objectives are to help an enterprise evaluate its security level, and identify the vulnerable elements that need to be repaired.

Employment of layer 5 of our trust framework, the auditing module, supports the testing functions performed by SAs. Authentication and identification processes, applied through

any authentication method or strong security protocol for identification purposes, begin prior to the SA accessing the system. After accessing the system, the SAs perform security tests and use testing techniques to identify malicious RFID tags. The security protocol concurrently calculates the key within the Discovery Service (DS) and matches it with any malicious RFID tag keys (a pre-shared secret managed by the SA). The tags are then sent to a cost based cloning detector for security testing.
When the cloning detector finds a cloned tag, the alert system is triggered: First, the system tests for the existence of a secret key in the tag. If present, it treats it as a security-testing tag and executes the second step. If not, the tag is considered as cloned and the response component starts to inform the SA. In the second step, with the tag treated as a security testing tag, the validating algorithm is used to verify whether the shared and secret keys are identical. If they are identical, the response component does not generate an alarm to alert the SA, but logs the occurrence. If they are not identical, the security-testing tag is considered as a malicious attempt to forge the secret key. An alarm is generated to alert the SA to the attack of the protected system and suitable actions are taken to avoid system loss. Section 3 presents our proposed cost model.

3. Proposed cost model for RFID cloning detector

In this section, we discuss our proposed cost sensitive cost model and how we derived its algorithm. We use Bayes rule to forms the foundation of pattern recognition and embodies the definition of conditional probability. Bayes theorem is essentially an expression of conditional probabilities. More or less, conditional probabilities represent the probability of an event occurring given evidence. To better understand, Bayes Theorem can be derived from the joint probability of *ci* and *x* (i.e. *P(ci,x))* as follows:

$$P(ci, x) = P(ci \mid x)P(x) \; ; \; P(x,ci) = P(x \mid ci)\, P(ci) \tag{1}$$

where $\boldsymbol{P(ci \mid x)}$ is referred to as the *posterior*; $\boldsymbol{P(x \mid ci)}$ is known as the likelihood, P(ci) is the prior and $P(x)$ is generally the evidence and is used as a scaling factor. Therefore, it is handy to remember Bayes Rule as:

$$P(ci, x) = \frac{P(ci)\, P(ci|x)}{P(x)} \tag{2}$$

In practice, the same type of misclassification error may have different cost impacts depending on the object to be classified, contrary to the fixed misclassification cost approach, where costs remain constant regardless of the data to be classified. As a caveat, we have used US dollars (US$) as a measure when discussing the RFID domain, but these costs can be converted to some other meaningful unit of measure of utility that may be more appropriate for the IDS case.

$$R(\alpha i|x) = \sum_{j=1}^{n} Cij(x)P\,(cj|x) \tag{3}$$

$$R(\alpha i|x) = \sum_{j=1}^{n} Mij(x)P\,(cj|x) \tag{4}$$

where the Cij is the misclassification cost function taking into account the properties of the data point x and Mij is the test cost function taking into account the properties of the data point x

We examine the major costs factors associated with a SCM cloned tag detector, which include: misclassification cost due to successful intrusions initiated by attackers; Response Cost due to these intrusions; and the Testing costs associated with SA testing of authentication methods. We identify the following major cost factors associated to intrusion detection: Damage Cost; Response Cost; and Operational Cost.

a. Damage Cost (*Dcost*) characterises the amount of Damage to a target resource caused by an attack when intrusion detection is unavailable or ineffective. There are two different Damage Costs, *DcA*(e) and *DcS*(e). *DcA*(e) is the Damage caused by hackers and may harm the system. *DcS*(e)is the amount of security testing cost associated with the SA's function that may Damage the system.
b. Response Cost (*Rcost*) is the cost of acting upon an alarm or log entry that indicates a potential intrusion. There are two different Response Costs, *RcA*(e) and *RcS*(e). *RcS*(e) is the Response Cost for recovery from the testing performed by the SA.
c. Operational Cost (*OpCost*) is the cost of processing the stream of events that are monitored by an IDS and of analyses of related activities, made available through the application of intrusion detection models.

The detection outcome *e* is one of the following: false negative (*FN*); false positive (*FP*); true positive (*TP*); or true negative (*TN*). The costs associated with these outcomes (outlined in Table 3) are known as consequential costs (*CCost*), as they are incurred as a consequence of prediction. *CCost* is the cost summation of Damage and Response Costs. The terms used in our cost model are as following:

Detection Outcomes	CCost	Condition
FN′	$\sum_{e \in E'A} DcA\ (e) + \sum_{e \in E'S} E3\ DcS\ (e)$ $0 \leq E3 \leq 1$	
FP′	$\sum_{e \in E'A} RcA + \sum_{e \in E'NORM} P(e)$ 0	If *DcA* (e) ≥ *RcA* (e), e ∈ E′A If *DcA* (e) < *RcA* (e), e ∈ E′A
TP′	$\sum_{e \in E'A} RcA + \sum_{e \in E'S} E4\ DcS(e)$ $0 \leq E4 \leq 1$ $\sum_{e \in E'A} DcA\ (e)$ $\sum_{e \in E'SA} E3\ DcS(e) + \sum_{e \in E'NORM} P(e)$ $0 \leq E3 \leq 1$	If *DcA* (e) ≥ *RcA* (e), e ∈ E′A If *DcA* (e) < *RcA* (e), e ∈ E′A ∀ ∈ E′ SA
TN′	0	

Table 3. Cost Model associated with FN, FP, TP , and TN outcome as Consequential Cost (CC)

$E'A$ = *Event by Attackers*
$E'S$ = *Event by System administrator*
DcA : Damage cost of attacker
DcS : Damage cost of system administrator
RcA : Response cost of attacker
OcA : Operation cost of attacker
OcS : Operation cost of SA
P : Penalty cost rate of positive false detection
$q1$: Negative false detection rate
$q2$: Positive false detection rate
Our proposed decision tree algorithm objective is in reducing misclassification cost for the cloned and fraud detection problem. Once the algorithm have achieved this objective, the cost model which calculates the total cost for cloning and fraud tags will be employed.A decision tree algorithm could be made cost sensitive by selecting those attributes that have highest gain at each stage of the tree building process (Ling et, al, 2006). The gain is defined as:

$$\text{Gain} = \text{priorCost} - \text{cCost} - \text{attribCost} \times N \tag{5}$$

priorCost = cost of misclassification before the split
cCost = cost of misclassification after the split
attribCost = cost of evaluating the attribute over which the split is taking place.
N = number of instances.

$$\text{currentCost} = \sum_{i=0}^{n} \sum_{j=0}^{n} (N * distj) * Cjk \tag{6}$$

where: n is the number of values that the attribute can take ,
N is the number of instances or RFID tags ,
D is the number of attributes,
distj is the probability of class value j
Cjk is the cost of misclassifying an instance of class j as that of class
k, where k is the dominating class of the split.
T is training dataset
Given a distribution for c classes, the dominating class I for that node is calculated as follows:

$$\arg\min \text{cost} = \sum_{j=0}^{c} \text{distj} * Cji \tag{7}$$

We would not explain further on our proposed algorithm and its evaluation in this chapter and focus more on the cost model instead.
We can now define the cost model for the cloning detection system .When evaluating a system over some labelled test set *E*, where each event, $e \in E$, has a label of normal or one of the cloned , we define consequential cost (CCost) and cumulative cost of the IDS as follows:

$$\text{Consequential Cost (CC)} = \sum_{e \in E} (DcA + RcA) \tag{8}$$

$$\text{Total Cost (E)} = \sum_{e \in E} (CCost(e) + OpCost(e)) \tag{9}$$

$$\text{TotalCost (e)} = current\ cost * \sum_{i=1}^{N}(\sum_{j=1}^{T} DcA\ (e) + \text{RcA(e)} + \text{OcA(e)}) \quad (10)$$

$$\text{TotalCost (e)} = currentcost * \sum_{i=1}^{N}(\sum_{j=1}^{T} DcS\ (e) + \text{OcS(e)}) \quad (11)$$

$$DcA\ (\text{e}) \geq RcA\ (\text{e}),\ \text{e} \in \text{E'A} \quad (12)$$

It may not always be possible to fold Damage and Response Costs into the same measurement unit**. I**nstead, each should be analysed using its own relative scale. We must, however, compare and then combine these costs so that we can compute *CCost(e)* for use in the calculation of Cumulative Cost as shown in (2) and (3). Cost total is categorised in two parts:

- the total costs associated with attacks; and
- the total cost associated with SA testing.

Based on equations (7) and (8), N is the number of training datasets and T is the number of tags attacked. The overall total cost is calculated as a sum of all costs associated with all compromised RFID tags. In Table 4 and Table 5 extends the cost matrix outcome to predict the total cost of detection vs. non-detection of an attack vs. no attack. Table 4 shows the misclassification cost matrix for attackers and Table 5 displays the test cost matrix associated with the SA role. The explanations are discussed below.

Misclassification cost (Cij)

	Attack	***No Attack***
Detection	*RcA + OcA*	*RcA + OcA + Pe*
No detection	*DcA + OcA*	*OcA*

Table 4. 2x2 cost matrix for attacks detection

SA testing cost (Mij)

	Attack	***No Attack***
Detection	*DcS + Pe + OcS*	*0*
No detection	*DcS*	*OcS*

Table 5. 2x2 cost matrix for SA testing detection

Detection algorithms of all kinds often create false positives. For example, an RFID IDS may detect a 'cloned' where there are only some RFID tags that look like a 'cloned' to the algorithm is being used. When developing detection algorithm, the trade-off between false positives and false negatives threshold values can be varied to make the algorithm more restrictive or more sensitive. Restrictive algorithms risk rejecting true positives while more sensitive algorithm risk accepting false positives.

Detection algorithms of all kind often create misses as well. For example, if in a medical diagnosis, if a doctor fails to detect cancer in a patient that is a false negative. When developing detection algorithms or tests, a balance must be chosen between the risks of false negative and false positives. Usually there is a threshold of how close a match to a given sample must be achieved before the algorithm reports a match. The higher this threshold is,

the more false negatives and fewer false positives exist. The description on each value of true positive (TP), false negative (FN), false positive (FP) and true negative (TN) costs are listed below:

TP Cost

If an attack occurs and the IDS detects it successfully, the associated cost is $((1-q1))$ *RcA* + *OcA*. *TP Cost* is incurred in the event of a correctly classified cloned tag, and involves the cost of detecting the clone and possibly responding to it. To determine whether a response will be needed, *RCost* and *DCost* must be considered. If the Damage done by the attack to resource *r* is less than *RCost*, then ignoring the attack reduces the overall cost. Therefore, if *RCost(e)* > *DCost(e)*, the intrusion is not responded to other than logging its occurrence, and the loss is *DCost(e)*. If *RCost(e)* ≪ *DCost(e)*, the intrusion is acted upon and the loss is limited to *RCost(e)*. Because this state is the opposite state to a false negative detection, the detection rate can be derived as $(1 - q1)$. *OcA* is the default cost if the IDS is settled and the *RcA* is generated because the IDS detects malicious tags.

FN Cost

FN Cost is the cost of not detecting a cloned attack. When the system falsely decides that a RFID tag is not cloned and does not respond to it, the attack will succeed, and the target resource will be Damaged. The *FN Cost* is therefore defined as the Damage Cost associated with the attacker (*DcA*) or the Damage Cost associated with the system administrator *DcS,* related to event *e.* The expected cost in this scenario is $q1$ (*DcA* + *OcA*). *OcA* is the default cost if the IDS is settled and *DcA* occurs because the IDS fails to detect malicious packets. $q1$ is a negative false detection rate.

FP Cost

FP Cost is incurred when an event is incorrectly classified as an attack, i.e., when *e* = (*normal*, *p*, *r*) is misidentified as *e′* = *(a′, p′, r′)* for some attack *a*. If *RCost*(*e′*_) ≪ *DCost*(*e′*), a response will ensue and the Response Cost, *RCost*(*e′*), must be accounted for. In this instance, since normal activities may be disrupted due to an unnecessary response, a false alarm should be penalized. For our discussion, we use *PCost*(*e*) to represent the penalty cost of treating a legitimate event *e* as an intrusion. For example, if *e* is aborted, *PCost*(*e*) can be the Damage Cost of a *DOS* attack on resource *r*, because a legitimate user may be denied access to *r*. The expected cost in this state is $q2$(*RcA* + *OcA* + *Pe*). Because 'false positive detection' is a false detection the same as in case 2, the generated cost is expected to be *Rcj* + *OcA*. However, this scenario causes an additional penalty cost *Pe* due to a false response. $q2$ is a false negative detection rate.

TN cost

TN Cost is always 0, as it is incurred when a system correctly decides that an event is normal. This decision is therefore associated with no Damage Cost, as only Operating Cost for maintaining the IDS is required. Section 4 discusses how MCDM is used to quantify costs in our cost model.

The detection algorithm that is embedded within the cost sensitive model is based on the description of our proposed cost matrix outcome as described earlier. Figures 3 and 4 demonstrate our proposed cost model within an improvised decision tree

Input: Training data: T= {t1,… tm} where each example Ti has attributes {pi,….pn) and a class ci
: Classifier C with learning algorithm L
: Misclassification cost, Cij

Output: W: the predicted test class, alarm log, response
For $\forall$ *T* $\in${*ti, … tm*}
C ⟵ *L(T)*
Create a Root node for the tree
Initialize all the weights in T, Wi=1/N, where N is the total number of the examples.
Calculate the prior probabilities P(Cj) for each class Cj in T. P (Cj) = $\sum_{Ci} Wi / \sum_{i=1}^{n} Wi$
Calculate the conditional probabilities P (Aij | Cj) for each attribute values in T. P (Aij | Cj) = P (A) / $\sum_{Ci} Wi$
Calculate the posterior probabilities for each example in D.P(ei | Cj) = P(Cj) Π P(Aij | Cj)
Update the weights of examples in D with Maximum Likelihood (ML) of posterior probability P(Cj|ei); Wi= PML (Cj|ei)

If (all the examples in T are in the same class ci)
{
Return (the single node tree Root with label ci)
}
Else
{
Let a be the Best attribute (T)
For (each possible value v of a) do
{
Add a new tree branch below Root, which correspond to the test a = v
If (Dv is empty)
{
Below this branch add a new leaf node with label equal to the common class Value in D.
}
Else
{
Below this branch add the subtree (Dv,A-a)
}
}
}
Return Root
End learning phase

C = {Ti , Tx}
For $\forall$ *Tx* $\in${*Cloned*, Fraud}
Calculate the expected misclassification cost R(αi*/x) by equation (10)*
W= arg minj R(αi*/x)*
If DCost > RCost, response is triggered
Else store in alarm log

Fig. 3. Pseudo code for misclassification cost by attackers using Decision Tree

Input : Training data : T= {t1,……., tm} where each example Ti has attributes {pi,….pn) and a class ci
: Classifier C with learning algorithm L
: Test cost, Mij
: SA test : Ts = {t1,……., tm} where each example Ti has attributes {pi,….pn) and a class ci

Output: W : the predicted class
For T ∈{ti, … tm}
C ⟵ L(T)
Create a Root node for the tree
Initialize all the weights in T, Wi=1/N, where N is the total number of the examples.
Calculate the prior probabilities P(Cj) for each class Cj in T. P (Cj) = $\sum_{Ci} Wi / \sum_{i=1}^{n} Wi$
Calculate the conditional probabilities P (Aij | Cj) for each attribute values in T. P (Aij | Cj) = P (A) / $\sum_{Ci} Wi$
Calculate the posterior probabilities for each example in D.P(ei | Cj) = P(Cj) Π P(Aij | Cj)
Update the weights of examples in D with Maximum Likelihood (ML) of posterior probability P(Cj | ei); Wi= PML (Cj | ei)

For ∀ T ∈{Ts}
Calculate the expected test cost R(αi /x) by equation (11)

Fig. 4. Pseudo code for test cost by attackers using Decision Tree

4. Quantifying cloning and fraud cost using MCDM tool

In this section we use the MCDM approach in quantifying costs. For our purposes, we define decision making as the process of choosing among optional alternatives based on multiple criteria. For each of these decisions, we consider several factors or criteria and we also consider several optional alternatives. In group decision making these criteria and alternatives are more complex and must be determined prior to the development of related judgment scores or evaluation values. We adopted the simplest method for MCDM, using cross tabulation and weighting methods. The following equation describes how cross tabulation and weighting is represented:

$$\text{Normalized score , } Zk(Oi) = \frac{1}{2}\left(1 - \frac{sum}{totalsum}\right) \tag{13}$$

$$U(Oi) = \sum_{k=1}^{M} Zk(Oi) \times w(Ck) \tag{14}$$

where *Zk(Oi)* is the normalised score of option *Oi* under criterion *Ck* and *w(Ck)* is the normalised weighting for criterion *Ck*. The summation of the damage, response and operational costs will always be for the representation of ten tags for any conditions such as cloned, fraud or for the purpose of testing by SA. Section 4.1 discusses how MCDM is used to quantify cost for a RFID tag cloning attack. Section 4.2 describes the evaluation of the cost of a fraud attack.

4.1 MCDM for RFID tags cloning attack

This section introduces how costs associated with cloning attacks by attackers are quantified in a RFID system. Attacker Damage Cost (*DcA*) and attacker Response Cost (*RcA*) are the

two costs discussed here. *DcA* is the amount of cost related to the Damage to target resources if intrusion detection is unavailable. Two main factors, criticality and lethality (Lindqvist & Jonsson, 2007); (Northcutt, 1999) are used to measure and define these costs. Criticality measures the importance of the targeted resource of an attack and evaluates it in terms of cost to replace, including unavailability and disclosure costs. For instance, the cost of replacing cloned RFID tags is much less than the cost of replacing the complete organisation database. *DcA* is a result of combining criticality with the attack category. Based on cost measurements factors and based on our problem definition, we use the simplest method of applying MCDM, using a cross table with target resources in RFID systems (tags, readers, database and RFID network) as criteria; and types of security cloning attacks as alternatives. Table 1 displays the *ADCost* for RFID cloning attack.

Attacks | Target Resources	**Skimming**	**Eavesdropping**	**MIM**	**Physical**	**SUM**
Tags	30	15	25	30	100
Readers	20	30	40	10	100
Database(local)	20	30	35	15	100
Network	10	40	40	10	100
Sum	**80**	**115**	**140**	**65**	**400**
Normalized Score	**20.0%**	**28.8%**	**35.0%**	**16.3%**	**100%**

Table 6. Criticality of RFID components in term of replacing, unavailability and disclosure for Damage cost

	Tags	**Reader**	**Database**	**Network**	**Sum**
Importance Level	20	15	30	35	100
Importance Weight	20.0%	15.0%	30.0%	35.0%	100.0%

Table 7. Weight Importance of RFID components

Attacks| Costs	**Weights**	**Skimming**	**Eavesdropping**	**MIM**	**Physical attack**	
Tags	20.0%	6.00	3.00	5.00	6.00	
Readers	15.0%	3.19	4.79	6.38	1.60	
Database(local)	30.0%	1.58	2.36	2.76	1.18	
Network	35.0%	0.99	3.96	3.96	0.99	
Sum	**100.0%**	**11.8**	**14.1**	**18.1**	**9.8**	**53.7**
Normalized Score		**21.9%**	**26.3%**	**33.7%**	**18.2%**	**1**

Table 8. Damage Cost (*DcA*) Evaluation based on scores of attacks and target resources factors

Based on Table 8, we could distinguish the damage cost for each attack using different RFID components.For instance, the damage cost for skimming attack on ten RFID tags is USD

6.00.'Man in the middle' attack has the highest associated Damage Cost, followed by that associated with 'eavesdropping' attack. 'Man in the middle' attack high Damage Cost is related to its related probability that all RFID components, especially tags and the network, have been compromised. The related impact on the organisation is greater than simply replacing the components with new ones. The disclosure of information from the tags and database could lead to further losses due to unavailability costs and to future related serious security attacks, such as fraud, that could jeopardize the complete RFID system. RFID tags are generally exploited more than RFID readers, as they are more vulnerable to attack. This fact is supported by RFID tags typically having little or no security measures. In the supply chain management environment, RFID tags take up less storage space and are of low cost compared to RFID readers.

RcA is the Response Cost associated with acting upon an alarm. A Response Cost can be either manual or automatic and is determined based associated IDS capabilities and organisation policies; attack types; and target resources. Measurement of a Response Cost is similar to that of a Damage Cost, and includes the factors of criticality and attack category. Table 9 displays a Response Cost for a RFID cloning attack.

Attacks | Target Resources	**Skimming**	**Eavesdropping**	**MIM**	**Physical**	**Range**
Tags	15	15	30	40	100
Readers	15	35	40	10	100
Database(local)	20	25	35	20	100
Network	20	30	35	15	100
Sum	**70**	**105**	**140**	**85**	**400**
Normalized Score	**17.5%**	**26.3%**	**35.0%**	**21.3%**	**100%**

Table 9. Criticality of RFID components in term of replacing, unavailability and disclosure for Response cost

Attacks | Costs	**Weights**	**Skimming**	**Eavesdropping**	**MIM**	**Physical attack**	
Tags	20.0%	3.00	3.00	6.00	8.00	
Readers	15.0%	2.39	5.59	6.38	1.60	
Database(local)	30.0%	1.58	1.97	2.76	1.58	
Network	35.0%	1.98	2.97	3.46	1.48	
Sum	**100.0%**	**8.9**	**13.5**	**18.6**	**12.7**	**53.7**
Normalized Score		**16.7%**	**25.2%**	**34.6%**	**23.6%**	**1**

Table 10. Response Cost (*RcA*) Evaluation based on scores of attacks and target resources factors

Based on Table 10, we can conclude that a simpler attack such as a 'skimming' attack has a much lower Response Cost compared to a complex attack (such as a 'physical' attack). This is because a 'physical' attack requires more complex mechanisms for an effective response.

In addition, we have totaled up the relative cost for the Damage and Response Cost to calculate the *CCost* based on formula (2). From Table 11, we could conclude that 'man in the middle' attack has the highest normalized score.

Costs | Attacks	Skimming	Eavesdropping	MIM	Physical	Sum
Damage	11.8	14.1	18.1	9.8	53.7
Response	8.9	13.5	18.6	12.7	53.7
Sum	20.7	27.6	36.7	22.4	107.5
Normalized Score	**19.3%**	**25.7%**	**34.2%**	**20.9%**	**100%**

Table 11. Consequential Cost (CC) Evaluation for summation between Damage and Response Cost

4.2 Operational cost

Operational Cost (*OcA)* includes the default cost of running an IDS. This could include the amount of time and amount of computing resources needed to extract and test features from the raw data stream that is being monitored. In practice, *OcA* is associated with time. For instance, time should be minimised in the detection of a security problem and related generation of an alarm, as the longer the time taken, the higher the associated cost. There are two cost factors which need careful examining: 1) the computing resource cost per each of the four attack types); and 2) the time taken per attack type. To compute the computing resource related cost, the different events and transactions that occur in a supply chain need to be taken into account. Table 12 depicts the time taken to handle each attack type and Table 13 the test features, based on their computing resource related cost. It takes more time to handle a 'physical' attack than other attack types. This is because a 'physical' attack requires understanding of cryptanalysis techniques and is associated with a greater amount of laboratory work. We have analysed *OcA* related to the four different cloning attack types based on a typical RFID system in an integrated RFID EPCglobal service (Ranasinghe & Cole, 2007, Verisign Inc, 2007).

	Skimming	Eavesdropping	MIM	Physical	Sum
Importance Level	15	35	45	60	155
Importance Weight	9.7%	22.6%	29.0%	38.7%	100.0%

Table 12. Operational cost relative to time taken in handling 4 cloned attacks.

The main cost inherent in the operation of an IDS is the amount of time and the computing resources needed to extract and test features from the raw data stream that is being monitored. We classify features into four relative levels, based on their computational costs:

- Level 1 features can be computed at the beginning of the service (e.g. tagging)
- Level 2 features can be computed at any point during the transaction of RFID tags in a single plant or site; e.g. Movement of tags in a distributor plant (shipping , receiving)
- Level 3 features can be computed at the end of a single supply chain tag transaction at the end of the plant movement; e.g. Movement and transactions of tags from manufacturer to retailer plant

Levels	L1: Computed from the beginning of service (e.g tagging)	L2: Computed at any events of RFID movement between two plants. (e.g shipping, receiving).	L3 : Computed at all the events in a single SCM from manufacturer to retailer(e.g tagging, pack, shipping, receiving)	L4:Computed at the overall of operation of interconnected EPCglobal network (EPCIS, DNS) such as tracing and tracking. (Involves L1,L2 and L3)	**Sum**
Importance Level	**1**	**5**	**10**	**100**	**116**
Importance Weight	**0.9%**	**4.3%**	**8.6%**	**86.2%**	**100.0%**

Table 13. Four relative levels of test features based on their computing resources cost for Operating Cost (*OcA)*.

- Level 4 features can be computed at the end of multiple supply chain plants in a interconnected network connection, but potentially require access to data of many prior connections. These are temporal and statistical features and are the most costly to compute. The computation of these features may require values of the lower level (i.e., levels 1, 2, and 3) features. Table 10 depicts the four relative test features for different attacks.

Features | Attacks	**Weights**	**Skimming**	**Eavesdropping**	**MIM**	**Physical attack**	
L1	0.9%	10.00	15.00	15.00	10.00	
L2	4.3%	11.01	11.01	13.21	8.81	
L3	8.6%	21.46	17.17	25.76	17.17	
L4	86.2%	21.41	21.41	26.77	21.41	
Sum	**100.0%**	**63.9**	**64.6**	**80.7**	**57.4**	**266.6**
Normalized Score		**20.7%**	**20.9%**	**26.1%**	**32.4%**	**1**

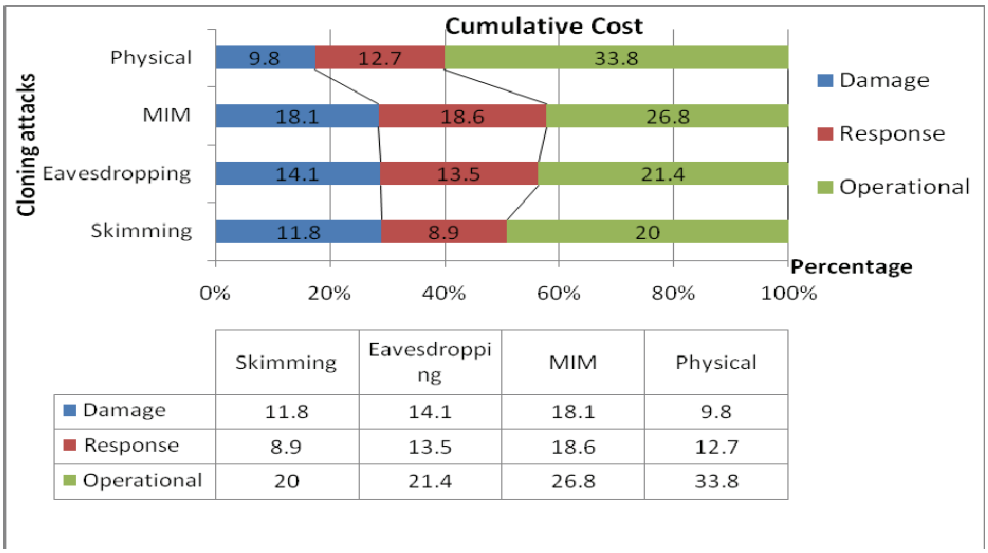
Table 14. Operational Cost (*OcA*) Evaluation based on scores of test features and cloning attacks types

Test features look into the computing resources used in a counter measuring attack. 'Physical' attacks require more testing of raw features and are harder to counter than other attack types. In order to calculate Cumulative Cost or overall cost by using formula (3), the end result is based on two scenarios: The first scenario is the summation of *CCost* (Damage and Response Cost) with Operational Cost, relative to the cost of the time taken in handling the attacks. This is shown in Figure 15.

Based on Figure 7, Cumulative Cost for a 'man in the middle' attack is the highest, followed by that for a 'physical' attack. 'Skimming' attacks have low overall costs because the attack requires less expertise and a lower Response Cost.

Features | Attacks	Weights	Skimming	Eavesdropping	MIM	Physical attack	
Features	70.0%	19.2	19.4	24.2	30.3	
Time	30.0%	0.9	2.0	2.6	3.5	
Sum	**100.0%**	**20.0**	**21.4**	**26.8**	**33.8**	**102.0**
Normalized Score		**19.6%**	**21.0%**	**26.3%**	**33.1%**	**100.0%**

Table 15. Operational Cost (*OcA*) Evaluation based on weight for test features and time



	Skimming	Eavesdropping	MIM	Physical
Damage	11.8	14.1	18.1	9.8
Response	8.9	13.5	18.6	12.7
Operational	20	21.4	26.8	33.8

Fig. 7. Overall Cost Evaluation for summation between Consequential Cost and Operational Cost

4.3 Quantifying RFID tag fraud attack and system administrator testing

This section looks at *DcA* and *RcA* the respective Damage and Response Costs in detecting a fraudulent act. Fraud involves injection of products with future EPC codes or past batch EPC codes. It involves first cloning and then modifying existing EPC codes. The cost types for fraudulent events are similar to that of cloning attacks. The difference is the need to monitor the progress of the attack when calculating Damage Cost and Response Cost, as a fraud attack has a greater impact on the performance of the system than a cloning attack. The contributing factors for its greater impact include:

a. An inconsistent number of tags and readers
b. A higher bandwidth
c. Unauthorized locations /sites visited by tags (as obtained from tracking and tracing processes)
d. The transaction time – greater or smaller than a given transaction time range.

We consider fraud attacks and SA testing damage (*DcS)* together since they have similar cost impact factors. In a real-time situation, a fraud attack is potentially in progress by the

time it is detected, meaning that its measured Damage Cost at a point in time is potentially only a part of its total Damage Cost. This is represented by the formula '**Progress X Damage Cost'**, where attack progress is represented by the percentage of the attack's progress. We use the simpler 'skimming' attack cost ($11.80) obtained from Table 8 when calculating fraud attack Damage and Response Costs. Table 16 displays relative costs for fraud attacks and associated SA testing.

Progress of attacks | Attacks	Progress attack	Damage Cost (Fraud)	Progress attack for SA	Damage Cost (SA)	Sum
Tags Count	1	11.8	1	11.8	
Location	0.8	9.44	0.5	5.9	
Time	0.8	9.44	0.5	5.9	
Bandwidth	0.5	5.9	0.5	5.9	
Sum		**36.6**		**29.5**	**66.0**
Normalized Score		**55%**		**45%**	**100%**

Table 16. Cost relative to Damage Cost for fraud attack and SA test and Progress attack value

There is no reason to calculate Response Cost for SA testing, since SA testing is done using an upfront authentication mechanism and requires secure identification of a system administrator, thus preventing their injection of cloned or fraudulent tags in the system. Response Cost is thus associated only with fraud attacks, and not with SA tests. Table 17 shows the Response Cost for fraud attack and response cost used is similar to response to handle skimming attack. The amount of Response Cost is related to the number of affected tags.

Progress of attacks | Attacks	Progress attack	Response Cost (Fraud)	Sum
Tags Count	1	8.9	
Location	0.8	7.12	
Time	0.8	7.12	
Bandwidth	0.3	2.67	
Sum		**25.8**	**25.8**
Normalized Score		**100%**	**100%**

Table 17. Cost relative to Response Cost (Attacks vs. Target resources) and Progress attack value

We analyse *CCost* in terms of its difference between cloning and fraud attacks. The cloning Damage and Response Costs are captured from section 4.1. Based on these results, we are able to conclude that cloning attacks have higher Damage as well as Response Costs than fraud attacks. This occurs because a fraud attack is only part of a cloning attack. A cloning attack needs to occur before a fraud attack can occur.

Costs | Attacks	Cloning	Fraud	Range
Damage	53.7	36.6	1-100
Response	53.7	25.8	1-100
Sum	107.4	62.4	170.02
Normalized Score	**63.2%**	**36.8%**	**100%**

Table 18. Consequential Cost (CC) Evaluation for summation between Damage and Response Cost

Operating cost for fraud attack will follows the similar formulation in section 4.2. Table 19 and Table 20, compares both time taken in handling fraud and cloning and test features for fraud and cloning. Detection of fraud is much simpler than any cloning attack. This is because in practical and based on our theory, fraud tags will have identifiers which are not in the system. Thus simple similarity test is good enough to distinguish the EPC tags stored in the database. By using similar weight in cloning attack operational example in Table 12, we have allocated an average of 30 minutes to detect a fraud attack and features test used for skimming attack.

Features | Attacks	Weights	Skimming	Eavesdropping	MIM	Physical attack	Fraud attack	
L1	0.9%	10.00	15.00	15.00	30.00	63.90	
L2	4.3%	11.01	11.01	13.21	17.62	28.14	
L3	8.6%	21.46	17.17	25.76	25.76	27.43	
L4	86.2%	21.41	21.41	26.77	26.77	17.10	
Sum	**100.0%**	**63.9**	**64.6**	**80.7**	**100.1**	**136.6**	**445.9**
Normalized Score		**14.3%**	**14.5%**	**18.1%**	**22.5%**	**30.6%**	**1**

Table 19. Operational Cost (*OcA*) Evaluation based on scores of test features for cloning and fraud attacks

Features | Attacks	Weights	Skimming	Eavesdropping	MIM	Physical attack	Fraud attack	
Features	70.0%	19.2	19.4	24.2	30.3	19.2	
Time	30.0%	0.9	2.0	2.6	3.5	1.7	
Sum	**100.0%**	**20.0**	**21.4**	**26.8**	**33.8**	**20.9**	**122.9**
Normalized Score		**16.3%**	**17.4%**	**21.8%**	**27.5%**	**17.0%**	**100.0%**

Table 20. Operational Cost Evaluation based on scores of test features and cloning attacks types

Cumulative Cost calculations for fraud attack are different based on two scenarios. In this scenario *CCost* is added to the relative cost of different test features for computing resource related cost and time taken in handling attack (as shown in Figure 20). We have compared Cumulative Cost for both cloning and fraud attacks, and though the difference is not great, cloning attacks take up more operating time due to related countermeasures, which causes it to have a slightly greater cost. The operational cost for SA testing purposes will be a constant figure of 20.0, similar to operational cost to handle skimming attack.

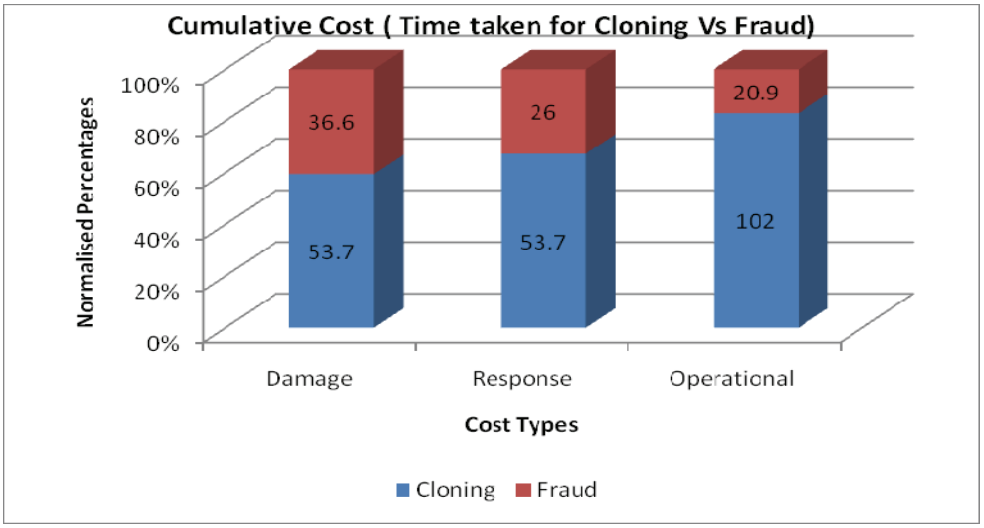


Fig. 8. Overall Cost Evaluation for summation between Consequential Cost and Operational Cost (Time taken to handled fraud and cloning attacks)

4.4 Cost model calculation

This section contains an analysis of cost sensitive and cost insensitive models, and introduces a cost model input cost matrix for a detection system.Assuming that we have a cloned detection system that functions upfront, we could feed the cost matrix result in our cost model. Since our cost system is quantified using the MCDM tool and is based on the cost model calculation in Table 3 and Table 4 which are calculated using MCDM in section 4.1 and 4.3, we could list estimated Damage, Response and Operational Costs according to this cost model. The difference between a cost sensitive and cost insensitive model is that a cost sensitive method initiates a response if $DCost \geq RCost$ and corresponds to the cost model, whereas a cost insensitive method responds to every predicted intrusion and is representative of current brute-force approaches to intrusion detection. Table 21 displays the overall cost model calculation for a cloning attack and Table 22 displays the overall cost model calculation for a fraud attack.

Table 23 shows the difference between cost sensitive and cost insensitive models for both cloning and fraud attacks. For instance, in a supply chain environment where both fraud and cloning are the act of counterfeiting, the total potential loss is estimated based on formula (1) in our model and is calculated to be US$1692.90. If this cost sensitive model is

calculated for cloning attack for 'skimming attack ' for ten RFID tags, we will obtained a cost reduction of $US77.8 compare to cost insensitive model which gives us $US193.20. On average, the risk for our cost sensitive model on 'skimming attack' on each RFID tag over skimming attack will be estimated at $US7.80. Table 24 displays the cost of $US139 that should be bear by an organsation for every ten RFID tags tested. This testing cost is much lesser than 10% of the overall cost of counterfeiting and worth to be considered as well in any intrusion detection system.

Cost types | Cost matrice	**FN**	**FP (DCost ≥ Rcost)**	**TP (DCost ≥ Rcost)**	**TP (DCost < Rcost)**	**TP (∀ ∈ E′ SA)**	**TN**	**Sum**
ADCost(Cloning)	53.7			53.7	53.7	0	
Operational Cost	102	102	102	102	102	102	
ARCost(Cloning)		53.7	53.7			0	
Penalty		**20**			20	**0**	
Sum	155.7	175.7	155.7	155.7	175.7	102	920.5
Normalized Score	**16.9%**	**19.1%**	**16.9%**	**16.9%**	**19.1%**	**11%**	100.0%

Table 21. Overall cost calculation for ten cloned attack

Cost types | Cost matrice	**FN**	**FP (DCost ≥ Rcost)**	**TP (DCost ≥ Rcost)**	**TP (DCost < Rcost)**	**TP (∀ ∈ E′ SA)**	**TN**	**Sum**
ADCost (fraud)	36.6			36.6	36.6	0	
Operational Cost	20.9	20.9	20.9	20.9	20.9	20.9	
ARCost(fraud)		26	26			0	
Penalty		**20**			**20**	**0**	
Sum	57.5	66.9	46.9	57.5	77.5	20.9	327.2
Normalized Score	**17.6%**	**20.4%**	**14.3%**	**17.6%**	**23.7%**	**6.4%**	**100%**

Table 22. Overall cost calculation for fraud attack

Attacks | Cost model	**Cost Insensitive**	**Cost Sensitive**	**Sum**
Cloning	920.5	331.4	
Fraud	327.2	113.8	
Counterfeiting (Sum)	1247.7	445.2	1692.9
Normalized Score	**73.7%**	**26.3%**	**100%**

Table 23. Cost Model for cloning, fraud and counterfeiting

Cost types | Cost matrice	FN	FP (DCost ≥ Rcost)	TP (∀ ∈ E′ SA)	TN	
SDCost	29.5		29.5	0	
Operational	20		20	20	
Penalty			20	**0**	
Sum	49.5		69.5	20	139
Normalized Score	**35.6%**	**0.0%**	**50.0%**	**14.4%**	**100.0%**

Table 24. Cost Model calculated for SA testing (using matrix in table 5)

5. RFID tag prevention techniques using MCDM

In this section we apply Analytical Hierarchy Process (AHP) and MCDM approaches (for different units of range) to select optimal supply chain authentication techniques and RFID tag authenticity verification methods.

AHP is a structured technique for dealing with complex decision making. AHP is a decision making tool that can describe a general decision making process by decomposing a complex problem into a multi- level hierarchical structure of objectives, criteria, sub criteria and alternatives, and is a well-known decision theory model developed by Saaty (1990). Its primary attribute is quantifying relative priorities for a given set of alternatives on a ratio scale, based on the judgment of the decision-maker. It provides an easy way to incorporate multiple experts' opinions and control of consistency in judgments. In addition, the AHP method ensures high repeatability and scalability controls. Applications of AHP have been reported in numerous fields such as conflict resolution, project selection, budget allocation, transportation, health care, and manufacturing (Harker, 1989).

AHP determines the criteria weightings indirectly based on scores of relative importance for each in pair-wise comparisons. The comparison ratings are on a scale of 1 to 9, resulting in a ratio of importance for each pair with the maximum difference that one criterion is 9 times more important than another. A matrix of pair-wise comparisons is determined in this way (where *Ci / Cj* is just shorthand for the relative importance of *Ci* to *Cj*). In AHP, the final weightings for the criteria are the normalised values of the eigenvector that is associated with the maximum eigenvalue for this matrix. Saaty (1980) suggests that this procedure is the best way to minimise the impact of inconsistencies in the ratios. Consistency Ratio is a comparison between Consistency Index and Random Consistency Index, or, in formula:

$$CR = \frac{CI}{RI} \tag{15}$$

We utilise the AHP tool in distinguishing the best approach and algorithm for preventing RFID tag cloning attacks in supply chains, and which is also suitable for use in testing processes used by SAs. In addition, we extend the MCDM tool based on criteria that best suit supply chain owners' needs when selecting RFID tag cloning and fraud prevention techniques. Among the defined criteria are acceptance, cost, security and complexity.

5.1 AHP tool for SA prevention techniques

In this section, we observe two different approaches. The first approach show the different methods used by SAs to handle authentications and select of algorithms. The second

approach uses trust analysis based on tag cloning and fraud prevention techniques. The MCDM model can also be used in selecting the best tag cloning and fraud prevention approaches and the best approach for authentication that can be used by the System Administrator (SA) in testing the system.

Authentication is an essential element of a typical security model. It is the process of confirming the identification of a user (or in some cases, a machine) that is trying to log on or access resources. While authentication verifies the user's identity, authorisation verifies that the user in question has the correct permissions and rights to access the requested resource. The two work together: Authentication occurs first, then authorisation. In a RFID enabled supply chain management tracking and tracing system website, authentication and authorisation are essential. Based on organisational role, role based access control can be employed in which the administrator at each site are responsible for their own site. For instance, an administrator is only able to view other supply chain partner reports and not able to edit or delete them. In an IDS system, one of the SA tasks are to monitor and maintain the availability and execution of the detection system.

In addition, SAs are also responsible to test the system to ensure the IDS system is still relevant and able to detect cloned and fraud tags precisely. Thus, appropriate and secure modes of authentication approaches are required to ensure that the SA account is always protected. SAs can be authenticated by entering a password, inserting a smart card and entering the associated PIN, providing a fingerprint; voice pattern sample; retinal scan;, or using some other means to prove to the system that they are who they claim to be. Biometrics such as fingerprints, voice patterns or retinal scans are just a few of human traits known to be uniquely used in authentication. Biometric authentication is normally the most secure and the hardest to be compromised or cracked.

Single Sign-On (SSO) is a feature that allows a user to use one password (or smart card) to authenticate to multiple servers on a network without re-entering credentials. IP Security (IPSec) provides a means for users to encrypt and/or sign messages that are sent across the network to guarantee confidentiality, integrity, and authenticity. IPSec transmissions can use a variety of authentication methods, including the Kerberos protocol or using public key certificates issued by a trusted certificate authority (CA). By using AHP approach, we have analysed the authentication alternatives against criteria such as processing time, cost, security and complexity. These criteria are the required validation factors for any authentication method .Table 25 shows an example on how to calculate overall weight for alternatives using AHP. The AHP model results as shown in Table 25 indicates that the biometrics method provides the most appropriate authentication mode in terms of security and minimal time in processing the public key fingerprint.

Pair-wise comparison generally refers to any process of comparing entities in pairs to judge which entity is either preferred; or is found to have a greater amount of some quantitative property. The normalized principal Eigen vector is also called the **priority vector.** Since it is normalized, the sum of all the elements in priority vector is 1. The priority vector indicates the elements' relative weights.

A comparison of the different authentication methods used by supply chain partners indicates the following authentication results: Sign on (38.08%); biometrics (41.74%) and IPSec (15.86%). Biometrics is most popular authentication method, followed by the sign on method. The Consistency Ratio of these figures is less than 10%, which is acceptable due to the subjective nature of the measurement factors. The subjective judgment needs to be revised if the Consistency Ratio is greater than 10%.

Criterias	Processing Time	Cost	Security	Complexity
Processing Time	1	1	5	1
Cost	5	1	7	1
Security	0.2	0.14285714	1	3
Complexity	1	0.11	0.14	1
Sum	7.2	2.25	13.14	6

Criterias					Sum	Priority Vector
Processing	0.14	0.44	0.38	0.17	1.13	28.25%
Cost	0.69	0.44	0.53	0.17	1.84	45.94%
Security	0.03	0.06	0.08	0.50	0.67	16.68%
Complexity	0.14	0.05	0.01	0.17	0.37	9.13%
Sum	1.00	1.00	1.00	1.00	4.00	100.00%

Techniques	Sign on	Biometrics	IPSEC
Sign on	1.00	1.00	7.00
Biometrics	1.00	1.00	3.00
IPSEC	0.14	0.33	1.00
Sum	2.14	2.33	11.00

Normalised Matrix for Only Processing Time Criterion				Sum	Priority vector
	0.467	0.429	0.636	1.532	51.05%
	0.467	0.429	0.273	1.168	38.93%
	0.067	0.143	0.091	0.300	10.01%
Sum	1.000	1.000	1.000	3.000	100.0%
		lambda max	**3.104**		
		consistency index (CI)	**5.20%**	**n =**	**3**
		consistency ratio (CR)	**8.97%**		

	Processing Time	Cost	Security	Complexity	Overall Weight
Weight	**36.69%**	**36.69%**	**7.47%**	**2.17%**	
Sign on	51.05%	25.78%	30.01%	61.44%	**38.08%**
Biometrics	38.93%	44.40%	42.82%	22.50%	**41.74%**
IPSEC	10.01%	21.40%	23.35%	32.87%	**15.86%**
Overall Consistency of Hierarchy			**5.64%**		

Table 25. SA Criteria's and Techniques for Testing Cost Using AHP tool

	MD5	SHA	PKI	Overall Weight
Weight	**22.30%**	**22.30%**	**55.40%**	
MD5	40.98%	40.98%	40.98%	**40.98%**
SHA	47.36%	47.36%	47.36%	**47.36%**
PKI	11.66%	11.66%	11.66%	**11.66%**

Overall Consistency of Hierarchy: 7.06%

Table 26. SA Criteria's and Algorithms for Testing Cost Using AHP tool

We have evaluated three different public key algorithms (PKI, MD5 and SHA) that can be used in different algorithm approaches by applying AHP approach as shown in Table 24. Certificate services are part of a network's Public Key Infrastructure (PKI); have been applied in EPC global service; and are applicable to RFID systems (EPCGlobal Certificate Profile, 2008). Standards for the most commonly used digital certificates are based on X.509 specifications. In a public key cryptography, a 'fingerprint' is created by applying the keyboard hash function to a public key. SHA and MD5 are examples of 'fingerprint' algorithms.

Theoretically, MD5 and SHA1 are algorithms for computing a 'condensed representation' of a message or a data file. This uniqueness enables the message digest to act as a 'fingerprint' of the message. Among the algorithms used for SA authentication, SHA is the best algorithm to use (as shown in table 26). This is because SHA provides more strength of security compare to MD5 algorithm. However the disadvantage of the SHA algorithm is that it requires more storage space for its key management functionality.

5.2 MCDM for tag's authenticy

The second part is an evaluation of different tag authentication methods through the use of various supply chain criteria, applying the MCDM approach (usage of ranking with different range). The supply chain criteria are selected based on the assumption that a supply chain company that is willing to spend minimal whilst still maintaining the appropriate security features standard for their low cost tags; and curbing both cloning and fraud attacks on their tags. Table 27 displays the most appropriate tag authentication for a supply chain based on our analysis (M.Mahinderjit Singh & L.Xue., 2009).

Criterias | Techniques	EPC Design	Tags Design	Lightweight Protocol	Lightweight ECC	Steganography	
Acceptance	3	4	1	2	5	
Cost	3	5	1	2	4	
Security	1	2	5	3	4	
Complexity	2	1	3	4	5	
Sum	**9**	**12**	**10**	**11**	**18**	**60**
Normalized Score	**21.25%**	**20.00%**	**20.83%**	**20.42%**	**17.50%**	**100%**

1 = Best ; 2 = Good ; 3 = Fair ; 4 = Weak ; 5 = Bad

Table 27. Evaluation based on rank scores of Tag's authencity Techniques for Various Supply Chain Criterias

The value of each row is either 1,2,3, 4 or 5 and represent the rank (shown in Table 27). Since smaller rank value is more preferable than higher rank value. Table 28 indicates that each criterion has a different range. For instance, the range for cost is in indicated in dollars in contrast to that for acceptance which is indicated in rank. It is not viable to the sum of the values of the different multiple criteria does not deliver a valid result. We need to transform the score of each factor according to its range value so that all factors have comparative ranges.

Criterias | Techniques	EPC Design	Tags Design	Lightweight Protocol	Lightweight ECC	Steganography	Range
Acceptance	3	4	1	2	5	1-5
Cost	1.5	5	0.5	1	2	$0.5 - $5.00
Security	1	0.8	0.3	0.6	0.5	0.3-1
Complexity	2	1	3	4	5	1-5
Sum	**7.5**	**10.8**	**4.8**	**7.6**	**12.5**	**43.2**
Normalized Score	**20.66%**	**18.75%**	**22.22%**	**20.60%**	**17.77%**	**100%**

Table 28. Evaluation based on range scores of Tag's authencity Techniques for Various Supply Chain Criterias

We transform the score value of each factor to have the same range value of 0 to 1. A formula based on the simple geometry of a line segment is used to linearly convert the score of each factor from table 28 to table 30 to a single shared range.

$$new\ score = \frac{nub - nlb}{oub - olb}(original\ score - olb) + nlb \tag{16}$$

Each factor has different importance weightings based on its organisation's priorities. Since the weighting is a subjective value, the result changes with changes to the factors' weightings. Table 29 displays an example of organisation 'A 'are weighting priorities in selecting their most appropriate tag authentication methodology.

	Acceptance	Cost	Security	Complexity	Sum
Importance Level	20	40	30	10	100
Importance Weight	20.0%	40.0%	30.0%	10.0%	100.0%

Table 29. Supply Chain Criteria's Weight of Importance

Table 30 shows the end result of normalizing the weighting of each factor, demonstrating the opportunity for an organization to compare different based factors based on a normalised range where individual factors are weighed according to the organization's personal requirements and needs. We are able to demonstrate that, for a organisation 'A' that emphasizes cost factors over security factors, a lightweight ECC would be the most appropriate technique for securing their low cost tags. This result contraindicates the prediction that lightweight ECC might be the preferred way in the future for securing low

cost tags. This prediction is based on the fact that lightweight ECC uses only 64K of RFID tag storage and provides strong authenticity comparable to that of any other lightweight public key infrastructure.

Criterias | Techniques	Weights	EPC Design	Tags Design	Light-weight Protocol	Lightweight ECC	Stegano-graphy	
Acceptance	20.0%	-0.100	-0.100	-0.200	-0.150	0.200	
Cost	40.0%	0.011	-0.067	0.033	0.022	-0.033	
Security	30.0%	-0.071	-0.043	0.029	-0.014	-0.029	
Complexity	10.0%	0.150	0.200	0.100	0.050	-0.200	
Sum	**100.0%**	**-0.010**	**-0.010**	**-0.038**	**-0.092**	**-0.062**	**-0.212**
Normalized Score		**4.9%**	**4.5%**	**18.0%**	**43.4%**	**0.292134831**	**100.0%**

Table 30. Supply Chain Criteria's and Techniques Weighted scores

6. Applicability discussions

In this section, we analyze how well MCDM quantified costs associated with cloning and fraud attacks. In the first part we discuss on the MCDM quantified cost result for cloning attack. The second part discusses the cost results obtained for fraud attacks, and for SA tests and authentication exercises. Finally, we analyze the validity of using cost sensitive and cost insensitive models for costing purposes.

6.1 RFID Tag cloning attack

Based on the result obtained from the MCDM approach, a 'man in the middle' attack has the highest Damage Cost of all attacks. This shows that a high Damage Cost is not associated with highly complex attacks (e.g. 'physical' attacks) or with easy attacks (e.g. 'skimming' attacks), but with specific techniques used in and means of the attack taking place. Although unavailability and disclosure Damage associated with 'man in the middle' attacks has an high risk impact on the occurrence of future cloning and fraud attacks, simpler attacks have a much lower Response Cost.

A comparison of consequential costs (the summation of Damage and Response Costs) indicate that both 'eavesdropping' and MIM attacks have a higher consequential cost than other attacks. Time factors are used in the ranking system, correspondent to the level of complexity in detecting and responding to the attack, to calculate Operational Costs associated with an IDS handling a cloning or fraud attack. MCDM criteria include extracted test features from raw RFID streams. There are four different levels of extracting test features. Our results indicate that highest rank extracted test features are from an interconnected supply chain partner's organisation within an EPCglobal service, due to the difficulty in obtaining shared computing resources between different partners and establishing various EDI services among them.

Cumulative Cost calculations indicate the association of the highest cumulative Operational Costs with 'man in the middle' attacks and of the lowest costs with 'skimming' attacks. Based on this information, we conclude that 'man in the middle' cloning attacks cause the

greatest overall losses in terms of money, time and computing resources. This result implies that measures to prevent 'man in the middle 'cloning attacks in a supply chain management is likely to minimise the impact of counterfeiting on an organisation.
The prevention measures that could be taken in eliminating MIM attacks include: 1) refresh the tag secret key immediately after a reader has been authenticated; 2) maintain tag output changes, as this minimises opportunities for replay attacks and the related risk of a faked tag; 3) keep the number of communication rounds and operation stages minimal to avoid redundant operations; maintain scalability and eliminate the risk of 'man in the middle; and 4) design the coordinating global item tracking server to include a timely tracking system that maintains freshness necessary due to the randomness of keys used in inter-organisational item-tracking activities.

6.2 RFID tag fraud, SA testing and authentication techniques

The main differences between fraud and cloning attacks in regards to the similar Damage; response; and Operational Cost types, are based on the criteria factors used in applying a MCDM tool to calculate these costs. Fraud attack costs are associated with the progress of the attack rather than with the type of attack that contributed to it. This is due to the fact that a fraud attack occurs only after a tag has successfully been cloned after one or more previous attacks. The progress of a fraud attack is closely associated with inconsistency of tag count, related to the travel of tags to unauthorised locations:; the need for a higher bandwidth for fraud detection in unauthorised locations; and inconsistencies between travel timeframes associated with illegal tags. Similar criteria factors are used to calculate costs associated with SA testing.
In a comparison of *CCost* for cloning and fraud attacks, the latter attack type has significantly lower associated *CCost*. This is due to the fact that fraud attacks are a part of cloning attack SA test costs are calculated using only Damage Cost, as SAs do not have malicious intentions towards the system and are able to use the system only after their system authentication, which is transparent during system audit procedures, classified as usage by a legal and authorised user.
Biometric authentication methods are the most secure and suitable method for use by supply chain partners in supply chain management, as indicated by the AHP tool. The SHA algorithm can be used to create a 'fingerprint' for the public key of this biometric application. Tag authentication methods that minimise storage needs and use minimal key bits are preferred, such as lightweight public cryptography (e.g. ECC and lightweight protocol).

6.3 Cost sensitive vs. Cost insensitive

We have extended the MCDM tool for evaluating *CCost* (Damage and Response Costs) calculations in our cost model. The aim for calculating both Damage and Response Costs is the evaluation the cost impact of a cost sensitive vs. that of a cost insensitive cost model. The difference between the cost impact of a cost sensitive and cost insensitive model is that a cost sensitive model initiates an SA alert only if $DCost \geq RCost$ and if it corresponds to the cost model. Cost insensitive methods, in contrast, respond to every predicted intrusion and are demonstrated by current brute-force approaches to intrusion detection.
Estimation of losses indicates that it could be reduced by up to 73% if a cost sensitive model is used in a system.

This impressive result is obtained using quantified cost for counterfeiting; and indicate that to optimally curb both cloning and fraud attacks, it is necessary to aim to minimise false negative in a system rather than to optimise accuracy of detection and elimination of false positives. The underlying principle for every business model should remain to minimise financial losses without compromising system security or product quality.
In addition our RFID cost model also included testing cost operated on the detector system by supply chain employee; the system administrator. The result display that testing cost only takes up less than 10% for every misclassifications cost reported. As the role of testing indicates the relevance of IDS and boost the accuracy of the dataset rules, the component of testing should never be compromised on the ground of losses in dollar.
The result also indicates the significance of calculating both misclassification and testing cost in any cost model.

7. Conclusions and future research

In this chapter, we have proposed cost-based approach using MCDM tool to quantify cost when curbing counterfeiting in RFID-enabled SCM. We have extended this tool to analyze the different authentication approaches, including for tag authentication, which can be used by system administrators. We have shown that the MCDM approach could be used for implementing a practical cost-sensitive model, as validated by our analytical results. We contend that the definitions of damage; response; and operational costs are complex, especially when applying theoretical attack criticality and progress attack in determining cloning and fraud costs. Our future work will focus on the implementation of our cost model and on development of robust RFID tag detectors for cloning and fraud attacks. We will use the cost model to estimate costs to predict total financial losses related to RFID tag cloning and fraud.

8. Acknowledgements

This work is partially sponsored by University Sains Malaysia (USM) and the NSFC JST Major International (Regional) Joint Research Project of China under Grant No. 60720106001.

9. References

S. Bono *et al.*: Security Analaysis of a Cryptographically-Enabled RFID Device. In P. McDaniel, ed., *USENIX Security '05*, pp. 1-16. 2005.

E.Y. Choi, D.H. Lee and J.I. Lim: Anti-cloning protocol suitable to EPCglobal Class-1 Generation-2 RFID systems, *Computer Standards and Interfaces* 31 (6) (2009), pp. 1124–1130.

L. Bolotnyy, G. Robins: Physically Unclonable Function-Based Security and Privacy in RFID Systems, percom, pp.211-220, *Fifth IEEE International Conference on Pervasive Computing and Communications (PerCom'07), 2007*

D.N. Duc, Park, J., Lee, H., Kim, K.: Enhancing Security of EPCglobal GEN-2 RFID Tag against Traceability and Cloning. In: *Symposium on Cryptography and Information Security, Hiroshima, Japan (January 17-20, 2006)*

T. Dimitriou., "A Lightweight RFID Protocol to protect against Traceability and Cloning attacks" in *Security and Privacy for Emerging Areas in Communications Networks, 2005.*

SecureComm 2005. First International Conference on (05-09 September 2005), pp. 59-66.

R. Derakhshan, M. E. Orlowska, and X. Li. (2007). RFID data management: Challenges and opportunities. In: D. W. Engels, *IEEE International Conference on RFID 2007. IEEE International Conference on RFID 2007, Grapevine, Texas, USA, (pp 175-182). 26-28 March, 2008*

W .Fan, Lee, W., Stolfo, S., Miller, M.: A multiple model cost sensitive approach for intrusion detection. In*: Proc. Eleventh European Conference of Machine Learning, Barcelona Spain, pp. 148–156 (2000)*

X.Gao Gao, Hao Wang, Jun Shen, Jian Huang, Song, "An Approach to Security and Privacy of RFID System FOR Supply Chain," Proceedings of the *IEEE International Conference on E-Commerce Technology for Dynamic E-Business (CEC-East'04), pp 164-168, 2004*.

P.T.Hacker: The art and science of decision making: The analytic hierarchy process. In: Golden, B.L., Wasil, E.A., Harker, P.T. (Eds.), *The Analytic Hierarchy Process: Applications and Studies. Springer, Berlin, pp. 3–36.*

A. Juels:RFID security and privacy: a research survey, *IEEE Journal on Selected Areas In Communications, VOL. 24, NO. 2, FEBRUARY 2006, vol. 24, pp. 381-394, 2006.*

A. Juels: Strengthening EPC Tags Against Cloning, (M. Jakobsson and R. Poovendran, eds.), *ACM Workshop on Wireless Security (WiSe), pp.67-76. 2005.*

S. Kutvonen: Trust management survey, Proccedings of iTrust 2005, number 3477 in *LNCS, pp 77--92 , Springer-Verlag.*

W.Lee , Fan, W., Miller, Matt, Stolfo, Sal, Zadok, E.: Toward cost sensitive modeling for intrusion detection and response*. J. Comput. Security 10, pp 5-22 (2002)*

W.Lee, Sal Stolfo and Kui Mok, A Data Mining Framework for Building Intrusion Detection Models. Proceedings of the *IEEE Symposium on Security and Privacy, Oakland, CA, pp. 120-132. 1999.*

M.Lehtonen, et.al: Trust and Security in RFID-Based Product Authentication System , *Systems Journal, IEEE, vol. 1, pp. 129-144, 2007.*

M.Lehtonen., Michahelles, F., Fleisch, E.: How to Detect Cloned Tags in a Reliable Way from Incomplete RFID Traces. *In 2009 IEEE International Conference on RFID, Orlando, Florida, April 27-28, 2009, pp. 257 - 264.*

X. Li, J. Liu, Q. Z. Sheng, S. Zeadally, and W. Zhong: TMS-RFID: Temporal Management of Large-Scale RFID Applications*, International Journal of Information Systems Frontiers, Springer, July 2009,*

C. Lin, V.Varadharajan .: A Hybrid Trust Model for Enhancing Security in Distributed Systems. *In: Proceedings of International conference on availability, reliability and security (ARES 2007), Vienna, pp. 35–42 (2007) ISBN 0-7695-2775-2*

C.Lin and V. Varadharajan: Trust Based Risk Management for Distributed System Security - A New Approach, in *Proceedings of the First International Conference on Availability, Reliability and Security*: IEEE Computer Society, pp 6-13 2006.

C.X Ling, V.S Sheng, Q. Yang, "Test Strategies for Cost-Sensitive Decision Trees," *IEEE Transactions on Knowledge and Data Engineering, pp. 1055-1067, August, 2006*

U. Lindqvist and E. Jonsson: How to systematically classify computer security intrusions, in *Proceedings of the IEEE Symposium on Research in Security and Privacy*, Oakland CA, May 1997.

M. Mahinderjit- Singh and X. Li , "Trust Framework for RFID Tracking in Supply Chain Management," Proc of *The 3rd International Workshop on RFID Technology – Concepts, Applications, Challenges (IWRT 2009), Milan, Italy, pp 17-26 , 6-7 May 2009.*

M. Mahinderjit- Singh and X. Li (2010): Trust in RFID-Enabled Supply-Chain Management, in International *Journal of Security and Networks (IJSN), 5, 2/3 (Mar. 2010), 96-105. DOI= http://dx.doi.org/10.1504/IJSN.2010.032208.*

M.2008, EPCglobal Certificate Profile [online]," Available http://www.epcglobalinc.org/standards/cert/cert_1_0_1-standard-20080514.pdf

L. Mirowski, & Hartnett, J.: Deckard: A system to detect change of RFID tag ownership. *International Journal of Computer Science and Network Security, 7(7), 89–98.*

P. Marcellin: Attacks from within can be worse than those from without [online], Available on: http://www.themanager.org/resources/Attacks_from_within.htm

K. Nohl, D. Evans, Starbug, and H. Pl¨otz: Reverse-engineering a cryptographic RFID tag, in *USENIX Security Symposium*, July 2008, pp. 185–194.

S. Northcutt. *Intrusion Detection: An Analyst's Handbook*, New Riders, 1999.

C. Pei-Te and L. Chi-Sung: IDSIC: an intrusion detection system with identification capability, *Int. J. Inf. Secur.*, vol. 7, pp. 185-197, 2008.

D.C. Ranasinghe, and M.G. Harrison, and Cole, P.H.: *EPC network architecture* In: Cole, P.H. and Ranasinghe, D.C., (eds.) *Networked RFID Systems and Lightweight Cryptography: Raising Barriers to Product Counterfeiting. Springer; 1 edition. pp. 59-78 ISBN 9783540716402*

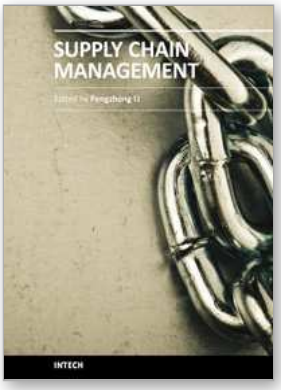
T. Saaty: An exposition of the AHP in reply to the paper remarks on the analytic hierarchy process. Management Science 36 (3), 259–268.

G. G. Shulmeyer and J. M. Thomas: The Pareto principle applied to software quality assurance, in *Handbook of software quality assurance (3rd ed.)*: Prentice Hall PTR, 1999, pp. 291-328.

F. Tom and P. Foster: Adaptive Fraud Detection, *Data Min. Knowl. Discov.*, vol. 1, pp. 291-316, 1997.

P.Turney: Types of cost in inductive concept learning. In *Workshop on Cost-Sensitive Learning at ICML*. Stanford University, California; 2000:15-21.

VeriSign Inc: EPC Network Architecture , http://interval.hu- berlin.de/downloads/rfid/IT_Infrastruktur/013343.pdf (2004).



Supply Chain Management
Edited by Dr. pengzhong Li

ISBN 978-953-307-184-8
Hard cover, 590 pages
Publisher InTech
Published online 26, April, 2011
Published in print edition April, 2011

The purpose of supply chain management is to make production system manage production process, improve customer satisfaction and reduce total work cost. With indubitable significance, supply chain management attracts extensive attention from businesses and academic scholars. Many important research findings and results had been achieved. Research work of supply chain management involves all activities and processes including planning, coordination, operation, control and optimization of the whole supply chain system. This book presents a collection of recent contributions of new methods and innovative ideas from the worldwide researchers. It is aimed at providing a helpful reference of new ideas, original results and practical experiences regarding this highly up-to-date field for researchers, scientists, engineers and students interested in supply chain management.

How to reference
In order to correctly reference this scholarly work, feel free to copy and paste the following:

Manmeet Mahinderjit-Singh, Xue Li and Zhanhuai Li (2011). A Cost-based Model for Risk Management in RFID-Enabled Supply Chain Applications, Supply Chain Management, Dr. pengzhong Li (Ed.), ISBN: 978-953-307-184-8, InTech, Available from: http://www.intechopen.com/books/supply-chain-management/a-cost-based-model-for-risk-management-in-rfid-enabled-supply-chain-applications

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

© 2011 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike-3.0 License, which permits use, distribution and reproduction for non-commercial purposes, provided the original is properly cited and derivative works building on this content are distributed under the same license.