# 14

# Security Control and Privacy Preservation in RFID enabled Wine Supply Chain

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

Modern identification procedures such as radio frequency identification (RFID) are able to provide transparency in applications including supply chain, logistics and equipment management. The benefits of visibility and fast identification provided by RFID technology especially in supply chain management (SCM) reduce the risk of counterfeiting (Gao et al., 2004). There are two mainly ways in which RFID technology supports a visible and fast identification processes: 1) RFID allows for new, automated and secure ways to efficiently authenticate physical items; and 2) As many companies invest in networked RFID technology for varying supply chain applications, the item-level data can be gathered in any case (Lehtonen et al., 2006).

Despite these benefits, RFID technology is still not widely implemented. The main reasons are, firstly, the difficult are, firstly, the difficult technical aspects of implementation resulting in high setup costs, secondly, growing security and privacy concerns. Our focus in this paper is to discuss the second reason for the low take-up of RFID technology, that is, security and privacy concerns. We argue that without applying maximum security and privacy, trustworthiness between supply chain partners will be minimal. As a result, the effectiveness and collaboration of traditional supply chain environment with RFID technology cannot be achieved. Given that humans cannot read the RFID tags on items and the tags themselves maintain no history of past readings, the challenge of security and privacy in this technology is related to the nature of RFID tags and their functionality (Juels, 2005). A retailer inventory that is labeled with unprotected tags may be monitored and read by unauthorised readers. The inventory data holds significant financial value for commercial organisations and their competitors. Once data has been accessed by unauthorised users, it can be cloned on empty tags, giving rise to the counterfeiting issue. Counterfeiting in the form of cloned or fraudulent RFID tags is the consequence of a lack of security measures and trustworthiness among the supply chain partners when RFID technology is used to automate their business transactions.

Privacy violations stem from the fact that when goods are tagged, the manufacturers, retailers and consumers will be able to track the goods beyond point-of-sale (POS) because they have associated data. Even if the tags only contain product codes rather than unique serial numbers, a consumer's taste in brands "constellation" can betray their identity.

Moreover, even if the responses of the tags are encrypted, the owner can also be identified and tracked by the fixed encrypted code. While consumers fear omnipresent surveillance, organisations are primarily interested in protecting company-internal data from unauthorised access and potential manipulation. These problems are not, however, completely independent of one another, considering the fact that data security represents a prerequisite to guarantee data privacy.

Bottled wine counterfeiting is a multi-billion dollar industry, which has increased drastically since the early 1990s. A report produced by Australian IT (Mar, 2007) shows that counterfeit wines accounted for almost 10 percent of the global market. In terms of wines, most counterfeiters aim to counterfeit expensive wines by tampering the labels or marking of the bottles. Recently, the ability of RFID to identify, authenticate and track items and activities in the supply chain is seen as a possible solution to the counterfeiting damage occurring in the wine industry. RFID has been used in the wine supply chain to provide visibility at each step of the supply chain process and to provide unique identification for tracking not only lots and cases but also at the item-level. An example of RFID usage in the wine industry can be explored in the real-life business scenario of Domenitz.L and Kravitz.J (2008).

Even though RFID is seen as an anti-counterfeiting tool, the use of passive RFID tags is a significant problem for industry including the wine industry. The low-cost passive tags currently used in the wine industry may not be able to provide sufficient security compared to active tags. Passive tags have lesser storage and memory space and provide insufficient security against security threats such as RFID tag cloning and fraud which lead to counterfeiting. For example, the tags used by Domenitz.L and Kravitz.J (2008) for tracking purposes can be easily cloned and all the historical information can be stolen. If this occurs, a fraudulent batch of wines produced with similar historical data can hit the market without anyone noticing the lack of authenticity of the products.

In order to address wine bottle counterfeiting, three different modules need to be incorporated together. These three modules are: 1) prevention; 2) detection; and 3) privacy. Prevention techniques focus on preventing a clone or fraud attack. Meanwhile, detection techniques are used to notify or record an attack in progress. Both modules are equally important and are not interchangeable since we cannot prevent what we cannot detect. The prevention module aims to provide security to all the layers concentrating mostly on the application, communication and the physical layers. Prevention of cloning involves the design and development of tags from the physical layer up to application level. Since intrusion prevention systems (IPS) are able to prevent attacks in real-time and manage the supply chain functionality through traffic flows, each part of the RFID system such as the tags, readers, communication channel, middleware and database are able to be protected. We will propose a simple yet powerful method to prevent counterfeiting in a supply chain plant. The aim here is to shield the whole supply chain plant from security attacks such as skimming, eavesdropping and replay attacks from occurring in the first place.

In contrast to prevention, the detection module focuses only on the application level. An intrusion detection function can tackle a compromised system more precisely since the knowledge of how and what has attacked the system is more clear compared to a prevention system. Prevention techniques are not guaranteed and may let an attack through, but dealing with a compromised system by responding to suspicious behavior and generating an alarm is possible with a detection system. However, the issue we tackle here is beyond the effort to minimise the error rate: the aim is to improve the percentage of the incorrect prediction of class labels and to deliver higher detection accuracy. In real-world

applications, cost is treated unequally and the misclassification cost can be significant. We argue that a cost sensitive approach is essential in reducing the risk of counterfeiting in a supply chain. For example, in medical diagnosis of a cancer disease, if the cancer is regarded as the positive class, and non-cancer (healthy) is regarded as the negative class, then missing a cancer (the patient is actually positive but is classified as negative), is called a "false negative" and is much more serious (thus expensive) than the false-positive error. The patient could lose his or her life because of the delay in the correct diagnosis and treatment. Similarly, in RFID clone and fraud detection, a false negative or failure to detect fraudulent tags could be very expensive with counterfeit items reaching the market and causing millions of dollars of loss. In this chapter we aim to construct cost model detection using supervised learners from available tools such as WEKA ( Hall.M and Frank.E *et.al*, 2009). The objective of our study is to classify RFID tags using supervised learners to categorise RFID tags and detect the genuine (good) and fraudulent (bad) tags. Our RFID tag clone and fraud detector will employ RFID SCM tracking and tracing functions such as tag history attributes, event timestamp and time to live (TTL) (Li *et al*.,2009) as important factors. We believe this simple experiment using a cost sensitive detection method for RFID tags in a supply chain environment is the first of its kind.

Finally, the privacy module is useful to support the handling of security attacks such as cloning and fraud attacks. This is because tracking RFID tags is an essential step in cloning yet may compromise a partner's privacy (Mahinderjit-Singh & Li, 2009). As for certain applications which require tracking, such as supply chains and drug pedigree tracing, privacy is a sensitive issue since the tracing and tracking processes may violate privacy in the first place. Thus, ensuring privacy protection while dealing with cloning attacks is crucial. Our third objective will be to provide a comprehensive guideline in tackling privacy concerns in the counterfeiting issue.

This chapter is directed towards a problem-driven context. Counterfeiting in an RFID based-wine supply chain is considered as a problem. We will tackle the counterfeiting issue in this supply chain example by using three different modules, namely, prevention, detection and privacy. Our first contribution is to propose a prevention method which is simple yet affordable to be implemented in a supply chain environment. The second is to detect counterfeit tags attached to wine bottles by utilising the cost sensitive concept. Finally, we provide a comprehensive privacy guideline handling the counterfeiting issue in a supply chain plant.

The main significance of this paper is to demonstrate how privacy preservation and security protection through prevention and detection can be maintained in an open-loop RFID supply chain such as the wine industry. In addition, a complete methodology on the most optimal and easy to use technique, approach or guideline in dealing with counterfeiting is presented. This research will closely study the relationship between these three modules in an RFID-enabled supply chain. The information on handling the supply chain in the wine industry can be extended to other goods or other RFID applications. The solution will be supported by using our seven-layer trust framework. The rest of this chapter is constructed as follows. Section 2 gives a literature review on RFID security and privacy issues in the supply chain. It also demonstrates the proposed trust framework. Section 3 explains the RFID-based wine supply chain. In Section 4 we outline how all three modules of prevention, detection and privacy can be employed to tackle counterfeiting in the wine industry. Section 5 provides a discussion. Section 6 provides the conclusion and views on future work.

## 2. RFID security and privacy in supply chain system

In this section, we present a taxonomy of the security and privacy issues of RFID-enabled supply chain management. Firstly, we discuss the challenges and problems related to security in an RFID system. The discussions in this section are essential in understanding why the trust mechanism is important in addressing security and privacy issues in RFID.
Lack of standardisation among different manufacturers of tags and readers makes it harder for a sharable security mechanism to operate in an open system environment. The network issues include the insecure communication between tags and readers. The attacker is able to remove the tag from the product and the lack of sufficient pedigree security makes it much easier for an authentic product to be forged. In addition, the lack of communication bandwidth and management introduces the problem of key management in ubiquitous computing (Juels, 2005). The architecture deployment in a supply chain environment, which includes the position of tags and alignment of readers in a centralised server, could cause erroneous readings such as duplicate records in the system and a reduction in accuracy. In addition, the RFID tag scalability issue in the supply chain environment needs attention. The growth of tag and reader size over time according to the needs of the supply chain business shows the importance of designing an architecture that is able to cope with future advancement.
On the other hand, the simple middleware design currently used by the Electronic Product Code (EPC) global network (http://www.epcglobalinc.org) does not take into account the evolving RFID technology and meet the business owner's requirements. There is no dedicated middleware component for ensuring security needs such as authenticating (Lehtonen, Michahellas & Fleisch, 2007). These are among the issues concerning RFID in an open system environment as they affect the security and privacy of the data, which is the information on the tags linked to the enterprise database. This causes data inconsistency and leakage. In light of all these issues, the impact on human trust in the RFID technology is critical and contributes to the lack of data sharing mechanisms in SCM. The next sub-section will examine the RFID security taxonomy directed towards RFID security attacks.

### 2.1 Taxonomy of RFID security attacks in the supply chain

The taxonomy of RFID security attacks in the supply chain is based on three security mechanisms – authentication, authorisation and trust services. This section is structured as a discussion on each of these mechanisms.

**A) Authentication**

In a supply chain environment, there are several methods available to combat product counterfeiting. These methods include the use of electronic pedigree (Koh, 2003), serialisation (Johnston, 2007), product authenticity and RFID tag authentication. The electronic pedigree used for drug authenticity can trace and track items by checking and updating transactions in a sequence. This method will be invalid if any party, for instance, a retailer acting deliberately, does not update the database whenever a product leaves the store at the point-of-sale. Non-cryptography techniques that are simple and cost effective (Koh, 2003; Nochta, 2005; Johnston, 2007) were proposed to combat counterfeiting. But certain techniques such as the trace and track approach proposed by Koh (2003) do not solve cloning problems thoroughly due to the storage of the tag information in plaintext. However, the track and trace approaches which deal with the locality factor could bring additional information on when and where cloning would have taken place place

(Lehtonen, 2007). Other approaches are proxy-based, such as the RFID Authentication Processing Framework (APF) (Ayoade et al., 2005) and Certificate Authority (CA). Both these techniques can reduce the counterfeiting issue caused by an unauthorised reader by authenticating the reader and hindering the ability of a fake reader to access the tags. The CA functions in a similar but more systematic way by storing a list of good readers on the centralised server. Finally, techniques such as watermarking (Potdar & Chang, 2006) do provide some degree of protection against cloning. However, the protocols are not adequate for low-cost EPC tags and require higher numbers of bits to ensure ultimate security.

**B) Authorisation**

In order to realise the business benefits of RFID, trading partners must be able to exchange data. The manufacturer, distributor and retailer all share RFID data. Access control involves the process of determining whether a user can perform a specific operation on resources. Based on the policy introduced by Wang et al. (2008), we argue that RFID system attacks within a supply chain can be eliminated when policies are assigned at product-level and item-level. In addition, a Discovery Service (DS) which is still under development can be utilised as another registry where incoming and outgoing products are registered (Ranasinghe & Cole, 2007) and can function as an item-level tagging server. Another important point is using role-based policy for the RFID access control systems (Seong et al., 2006). Languages such as SAML, XML, XACML and even WS-Security are suitable and widely used in RFID especially in supply chain services. In addition, the concept of e-pedigree (Frey.M , 2008) in the pharmaceutical industry proves that the sharing and tracking of information within an EPC network is able to provide accuracy and eliminate security threats. Another approach to sharing and exchanging information in RFID is using the Electronic Product Code Information Services (EPC-IS) model (Ranasinghe & Cole, 2007) which is a component of the EPC global network. The method for exchanging EPC-IS events uses protected communication channels based on HTTPS and SSL. EPC-IS enhances data sharing and visibility and monitoring day-to-day RFID applications. Each local company will have its own local database and local EPC-IS.

**C) RFID Trust Service**

The importance of the trust role in dealing with the security threats in RFID is a novel approach and is the first of its kind. Trust in the adoption of RFID among business partners is likely to be affected by two main challenges in RFID technology. First, the security and privacy threats in the system reduce the confidence in the system especially when RFID tagging is used for counterfeiting purposes. Second, the lack of any attack detection model in the RFID network makes the security and privacy threats go unnoticed.
Among the other reasons which contribute to the decrease of trust in RFID are:

i. Open system environment – Supply chain management exists in an open system environment with various types of RFID system interface, organisational protocols and communication interface (Derakhshan, Orlowska & Li, 2007). As a result, with multiple data integrations models existing, it is harder to develop a standardised and common data exchange and integration model among them.
ii. Minimal authentication, authorisation and tracking services capabilities – RFID middleware only includes the common models for data exchange transactions. Models such as EPC-IS, ONS, EPC-DS only provide common transactions (http://www.epcglobalinc.org). The lack of capabilities in authentication models and

tracking mechanisms built in to the RFID middleware supports the point that the design of RFID network infrastructure fails to address the security and privacy challenges. So far, e-pedigree, which is used for drug tracking, is the only model for tracking and tracing the whereabouts of products in the drug supply chain environment (http://www.rfidupdate.com/articles/index.php?id=1277).

iii. The existing EPC Trust Service – The current EPC trust model is the only trust model so far in RFID technology providing authentication and authorisation. EPC-Trust functions by using a third party (CA) in authenticating devices and users in a supply chain model (Verisign Inc, 2004). The trust model does not cover any security mechanism for RFID tags and readers and is without any detection model.

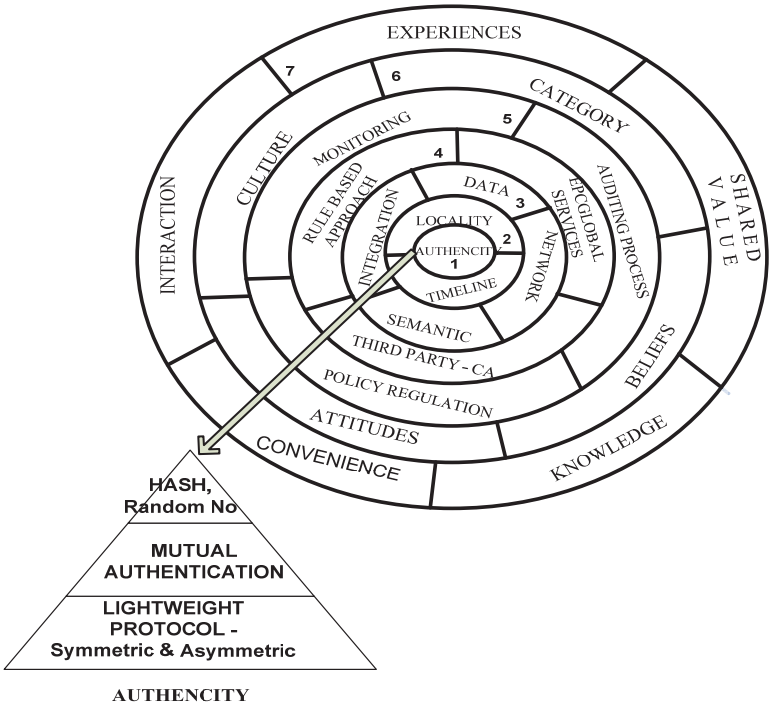



Fig. 1. Seven-layer trust framework (Mahinderjit-Singh and Li ; 2009)

Based on the factors that impact on the confidence rate in RFID adoption and the technology functionality, the base argument for this research is that both prevention and detection models are needed to tackle these issues. A better model of trust is needed especially one with the capability for preventing and detecting security and privacy threats. Further, the trust model must stand in an open system environment by supporting multiple protocols and communication interfaces between various organisations. This trust model could also be assimilated with supply chain service standards such as EDI/XML and SOA. Thus, in this chapter we carefully study the previous literature to determine the gaps in the research before proposing our idea and solutions. This extension of knowledge will be considered as

a map for more secure and efficient business transactions in open system supply chain management.

Based on the seven-layer trust framework (Mahinderjit-Singh & Li, 2009), trust in an 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". In addition, a trust model for a technological system should always include human interaction through the use of a feedback and ranking model. Among the functions of the trust framework (Figure 1) is the provision of guidelines for designing trust to solve open system security threats. The next sub-section focuses on RFID privacy concerns.

### 2.2 RFID privacy taxonomy

An RFID system should consider both privacy and security in its design structure and the focus of the proposal should be on the information system and not the technology. Privacy is the ability of the RFID system to keep the meaning of the information transmitted between the tag and the reader secure from non-intended recipients. The main privacy challenge in RFID is due to the nature of the RFID tag operation. Tags are "promiscuous'': they can be read by entities outside their owner's knowledge. Among the privacy concerns are tracing and tracking, profiling of products and secret tag reading (Ayoade, 2007). Approaches to deal with these concerns include: (i) tag killing (Sarma et al., 1999) in which the tags of sold items are disabled or removed at the point-of-sale; (ii) tag blocking (Juels et al., 2003) in which a blocker tag creates a radio frequency environment that prevents unauthorised scanning of consumer items; (iii) hash encryption (Juels, 2005) in which the information stored in tags is encrypted in a dynamic manner; and (iv) a rewriteable memory and random number approach (Gao et al., 2004) in which only authorised readers are able to access the tags.

In RFID applications such as a supply chain, an RFID tag may change its owner multiple times. To tackle this issue, a secure ownership transfer is essential. Ownership transfer means that once an RFID tag is transferred from two different owners, all information associated with the tag will need to be passed on as well. This should be done without compromising the privacy of either the old or new owner to ensure that tracing and retaining of the tag's information is not possible. Some ownership protocols that tackle ownership transfers are proposed by Osaka et al. (2006), Saito et al. (2005) and Song (2008). The Osaka-Takagi-Yamazaki-Takahashi (OTYT) protocol. (Osaka et al., 2006) uses symmetric encryption and hashing and provides privacy protection for both new and old owners. However, without any consideration of after-sale information recovery, this scheme is also prone to message manipulation attack since similar random numbers could be used to query a tag twice. The Saito protocol (Saito et al., 2005) makes use of properties such as three-way authentication using a TTP server but is prone to eavesdropping and only supports new owner privacy. This is because the fundamental approach of their scheme is to provide support for the backward channel without consideration of forward channel communication. Through security analysis done by Pedro (2010), the proposal by Song (2008) provides three important ownership transfers, which are new owner privacy, old owner privacy and authorisation recovery for transaction after POS. However, the mutual authentication method used is prone to many attacks such as tag and server impersonation, data leakage and denial-of-service attack. As a result, it is difficult to ensure privacy without

compromising security if only symmetric cryptosystem is used without any provisions made in terms of a secure server's communication setup.
Hargraves and Shafer (2004) suggested that identifiability, observe-ability and link-ability of RFID tags with associated data should be minimised and the RFID system should be developed with authorisation, authentication and encryption on a routine basis to ensure trustworthiness of the RFID system. In VeriSign (2008), an innovative way to minimise the sharing of information is by applying distributed network architecture. This type of networked RFID system ensures that partners only store their serialised information about each product in a database and this information is only accessible to authenticated and trusted partners. Another approach will be to apply policies (Garfinkel et al., 2005). Garfinkel et al. (2005) emphasise the need for guidelines which require human and technology intervention and the need to educate humans in accessing RFID technology and facilitate understandings of how privacy threat can be handled.

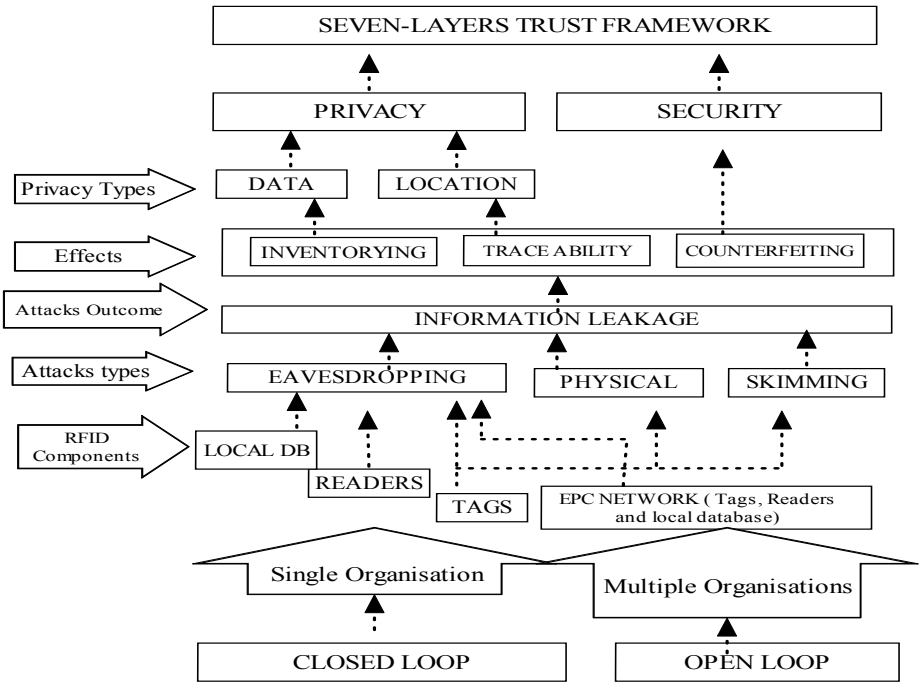



Fig. 2. RFID Privacy Concerns Categorisation

In the seven-layer trust framework (Mahinderjit-Singh & Li, 2009), both security and privacy are integrated in the first 5 layers. The trust framework could be applied to maintain an RFID system which is able to handle security threats without compromising privacy effects. Layer 2 – privacy looks into time and locality factors which are related to the privacy of data and location. Mahinderjit-Singh and Li (2009) argued that the privacy component is necessary to support the handling of cloning attacks because tracking of tags is an essential step towards cloning-detection and this may compromise a partner's privacy. Thus, this layer is to ensure the privacy protection while dealing with cloning attacks. We also believe

trust management is the key for the overall protection of security and privacy in an RFID system. In Figure 2, we categorise privacy attacks in RFID within single and multiple organisation loops and show how both privacy and security are a part of any trust model, which in our case is the seven-layer trust framework.

## 3. An example of RFID SCM in wine industry

In this section, we present an example of the supply chain in the wine industry. This example is important for understanding the degree of the counterfeiting risk in RFID technology. The counterfeiting issue in this example will also be used to design an appropriate solution in terms of preventing counterfeiting, detecting the clone and fraud attacks and preserving the privacy of the users in this supply chain example.
The aim of counterfeiters is to counterfeit expensive wines by tampering with the labels or markings of the bottles. Among the anti-counterfeit techniques are the traditional method of tasting the wines, biochemical methods (http://www.enotes.com/forensic-science/wine-authenticity), and using hologram labels, tamper-proof security seals and smart corks (Sagoff, 2008). However, the easily tampered, unsecured holograms and lack of mechanisms for traceability offered by the above techniques have led to the problem of low visibility, non-authentic and inaccurate transactions for tracing and tracking the movement of wines in a supply chain. Instead of solving the counterfeiting issue, more vulnerability loopholes are presented to the counterfeiter to perform attacks. The challenges of RFID usage in the wine industry are as follows:

i. the identification of liquids
ii. the short lifespan of the passive tag battery currently used for RFID tracking and monitoring
iii. the lack of a preventive mechanism to cope with future counterfeiting once the tamper-proof seal on the wine is tampered with,
iv. the nature and limitation of the passive RFID tags.

The issue of identifying liquid is troublesome for the reason that liquid absorbs and reflects radio waves. The passive RFID tags for identification of the wines at e-Provenance are placed under the bottle and this reduces the read accuracy. According to Yeo (2006), the reading accuracy can be enhanced if the tag is placed on the top of the bottle. In order to be able to track and monitor purchased wine, the tags used for tracking must survive a life span of many years. However, the outcome of the RFID tags used currently is limited and only last for two years. The low-cost passive tags used currently may not be able to provide ultimate security compared to active tags. Passive tags have lesser storage and memory space and have insufficient security against security threats such as RFID tag cloning, fraud attack and counterfeiting. The tags used by e-Provenance (2008) for tracking purposes can easily be cloned and all the historical information can be stolen. A fraudulent batch of wines produced with similar historical data can hit the market without anyone noticing the lack of authenticity of the products.

### 3.1 RFID tagged wine supply chain management

Based on Report of Wine Traceability (2005), the function of each supply chain business partner in a typical wine production environment are as follows:

a. Wine Producer - The wine producer is responsible for receiving the grapes and for the production, manufacture and/or blending of wine products.

b. Transit / Cellar - The transit cellar is responsible for the receipt, storage, dispatch, processing, sampling and analysis of bulk wine, as well as record keeping of appropriate information about what is received and what is dispatched. The transit cellar can be part of the filler/packer company (geographically separate or not) or can be outsourced. What differentiates the bulk distributor from the transit cellar is that the former has a commercial role, whereas the latter has only a role of transit with no commercial and no invoicing goal.
c. Filler - The filler/packer is responsible for the receipt, storage, processing, sampling, analysis, filling, packing and dispatch of finished goods, as well as record keeping of appropriate information about what is received and what is dispatched.
d. Distributor - The finished goods distributor is responsible for the receipt, storage, inventory management and dispatch of finished goods, as well as re-packing and re-labelling.
e. Wholesaler / Retailer - The retailer receives pallets and cartons from the finished goods distributor and picks and dispatches goods to the retails stores. Figure 4 shows the flow of wine beginning from the grape grower up to the retailers.

Figure 3 shows the flow of supply chain business transaction between various partners in a wine environment. In addition, in this figure we are also able to pin-point the vulnerability points in which a counterfeit attack could takes place. Few scenarios of how the attack happens are also listed.

Besides the flow among normal supply chain partners, another process worth mentioning in the wine supply chain is the consolidation or merger of a few players in order to enhance profits and reduce the cost of labor and infrastructure. This process is critical if security measures are not taken upfront. The consolidation process could input counterfeit wines that are later sent to the distributor (licit chain) or the other retailers (illicit chain). The end process of the counterfeit wines here is the sale to the consumer. One more route of the counterfeiting process is the act of the thief in stealing information directly or indirectly. The direct stealing of information involves the help of a third party, someone who is the employer of the licit supply chain. An indirect attack is an attack done by using the internet such as eavesdropping, man in the middle and skimming. The function of the thief is critical. The thief can manipulate the information of the wines or even the wine bottles and input them into consolidation process or even sell the information to the retailer and consumer.

Based on the vulnerability points illustrated above in Figure 3, the following scenarios demonstrate typical cases of RFID tag cloning and RFID tag fraud:

- Bordeaux Corp produces 1000 cases of wines with each case containing 100 bottles. The cases are then sent to the distributor. Bob, an employee of the distributor, steals the EPC information of 100 wine cases and supplies it to Carol, the attacker. Carol then copies the EPC tag numbers into empty tags and tags fake cases of wines. These wines are later shipped to several states within the country to different retailers.
- Reagan Corp, a shipping company, is plotting to steal a bulk load of wines that it has been entrusted with transporting. These wines have tamper-proof bottles with passive RFID tags attached. Rather than trying to defeat the tamper-proofing of the bottles, Reagan creates fake cheaper wine bottles, and clones the associated passive EPC tags. It swaps the bogus bottles while it has custody of the real ones.
- An anonymous reader belonging to Carol (an attacker) was placed at the warehouse belonging to Alice. When the Cabernet Sauvignon wines transported by Suiko Corp reached the warehouse, Carol eavesdrops on the communication channel, actively

performs a relay attack (man in the middle attack) and records a series of messages exchanged between the genuine reader and the trusted local database. Based on the encrypted EPC data obtained, Carol's reader communicates with the database. As there is no reader authenticity needed at the database side, the encrypted key is exchanged by the database. Carol now uses this key information received and performs a brute force attack on other EPC tags tagged on the cases. The guess game was able to reveal the key used for all the EPC tags scanned. Carol now sells this information to Alex, Alice's competitor who injects the data into cloned EPC tags and tags them on to cheaper goods and sends the goods to another retailer.

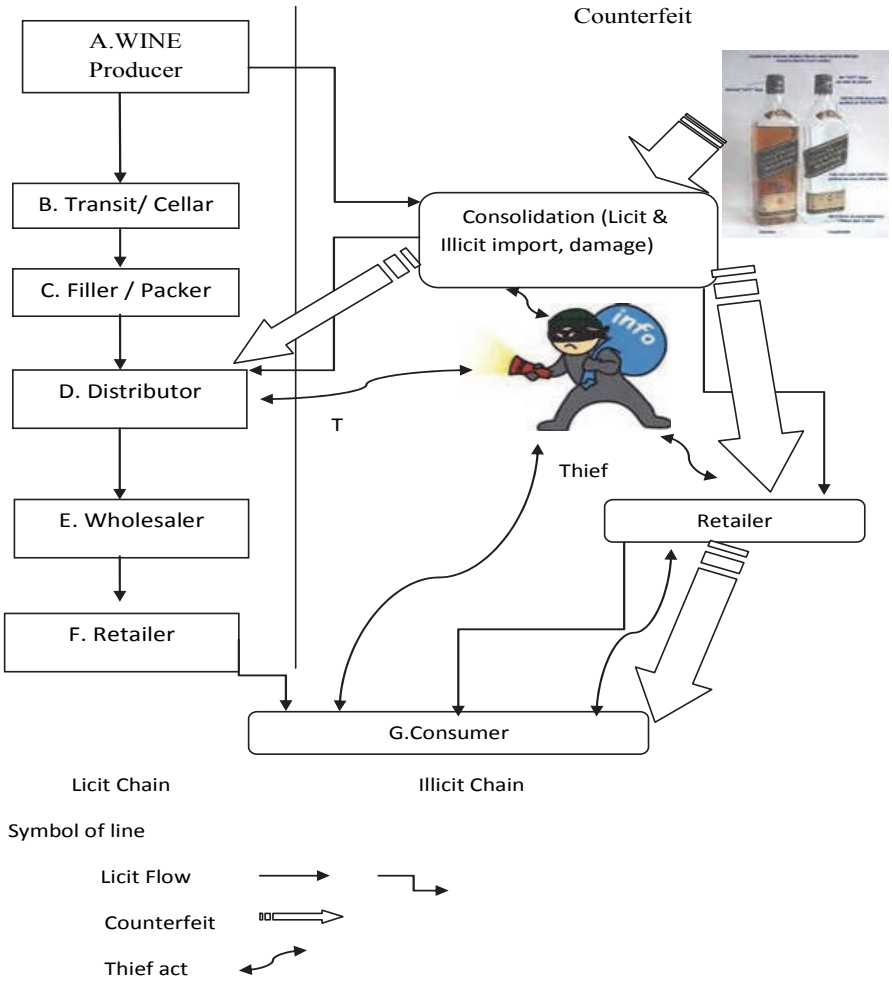



Fig. 3. Wine Vulnerability Points

Counterfeiting in the RFID-based system used in wine industry can be tackled using three categories: security, privacy and detection. The security solution looks into how we can protect the RFID tags on the wine bottles against cloning and fraud attacks. The privacy solution looks into how we can preserve the privacy of the partners and maintain the confidentiality of the information recorded by them and shared between them. Detection plays its role in detecting the cloned and fraud tags in an RFID-based system.

## 4. Clone/fraud handling through prevention, detection and privacy

### 4.1 Security - prevention of cloning in RFID-based wine system

The requirements of the cloning prevention system are data integrity and authenticity. In order to eliminate cloning, there is an essential need for complete authentication between all the RFID components. This includes providing integrity to the information within the tags. In addition, the need to sign the data is essential to show that the data has not been tampered with throughout the communication channel. The cloning prevention system must be able to prevent the skimming, eavesdropping and active attacks which are major security attacks that contribute to cloning in RFID systems. In addition, careful attention needs to be given to the fundamental problem of low-cost tags which provide less space on the tags and reduced memory capability. The security attributes necessary to handle a cloning attack include the following:

- A tag identifier must always be encrypted (e.g., hashed) before transmission between tag-reader-server begins. This reduces skimming and eavesdrop attacks on RFID tags and the system.
- Immediately after a reader has been authenticated, the tag must refresh a secret key. As long as the tag output changes, the chances of a replay attack can be reduced and there are no opportunities to fake a tag. Without knowledge about the secret key, an adversary can never create a set of encryption values.
- Three-way mutual authentication should always take place in any system including encryption and hash on tags, readers, and the data entries in databases.
- Synchronisation between tags and databases should always be consistent to eliminate cloning and eavesdropping.
- The number of communication rounds and operation stages should be minimal without any redundant operations to maintain scalability and eliminate the chances of replay and DOS attacks.
- The server for coordinating the global item tracking should be designed with a timely tracking system to maintain the freshness of randomness of the keys used in inter-organisational item-tracking activities. This helps against DOS attacks and cloning. It ensures that even though a key is compromised, an adversary can only capture a single tag rather than a bulk of tags.
- The most appropriate supply chain prevention mechanism should consider efficiency with a low-cost and practical approach. The techniques employed will need to be performed within the limitation of tags and RFID constraints. Therefore, techniques such as the physical uncloneable function (PUF) (Devadas et al., 2008) and watermarking technology (Potdar & Chang, 2006) are out of the question. The first is too costly and the latter is not efficient and practical when utilised on low-cost RFID tags.

- EPC-PAS and EPC-TAS should be modelled into the current EPC global network (Lehtonen, 2007).
- Item-level tracking should be used to diminish counterfeiting especially for luxury products such as jewellery and wine.
- A novel trust solution with an associated prevention mechanism via authentication for tag readers and supply chain partners is required. The trust model should be designed with some human interaction and feedback capability to enhance trust even more.

We also propose a simple prevention mechanism which is able to prevent cloning and fraudulent tags in a supply chain management. Since RFID tags are the most vulnerable point for any security attack in an RFID system, the tags should not be embedded with any important or confidential information. They should always function as pointers in which essential information such as secret key information or random numbers is stored in the database. In this proposed model, we make use of the message authentication code (MAC) algorithm. The function of the MAC algorithm is similar to the hash function in which it authenticates a message using a key and produce an authenticated code (Menezes et al., 1996). Message authentication codes are useful in many situations. If we need to perform basic message authentication without resorting to encryption for efficiency reasons, MACs are the right tool for the job. In addition, we add the public key cryptosystem to provide an added security capability which is signature capability. The concepts of random numbers and timestamps are used to track the liveness of the tags and to eliminate replay attacks. We make use of the Certificate Authority (Menezes et al., 1996) a third party trusted entity to maintain a higher security level of authenticating the readers. The benefit of this approach is that it eliminates the risk of compromised readers.

At this point it is important to articulate the assumptions for the cloning prevention system. These assumptions are:

- Channel between reader and database is secured.
- Trusted party, CA authenticates readers upfront.
- A Key Distribution Centre (KDC) is required to distribute and manage the secret key used by the tags and database.
- Tags used here are passive and compliant to Class 1 generation 2 (CIG2) tag with security function such as 16 bit pseudorandom generator.
- Timestamp values will be used to prove the authenticity of the tags based on the timeline starting from the movement information. For example, at location 1, the duration between the lifetime will be recorded according to the tags. The database on the trusted server will update the range of timeframe for any particular location and add the duration of the time. Finally, both timestamps will be similar or the difference of the timeline will be derived by a value of + 0.5 seconds or less.
- The random number will be generated from the CIG2 capability to produce the sequences from a 16 bit generator.

Figure 4 below provides a graphical representation of how the IPS framework will function, and shows the framework of how the required algorithms and security requirements will function.

The cloning technique that can be applied in the RFID-enabled supply chain functions through a number of steps. The readers in an RFID system should always be authenticated to ensure authenticity and eliminating the replay attack scenario from arising. First, the readers will read and send a query to the RFID tag. We assume that RFID tags only function as identifiers without any sensitive and important information on the tag. The only

information on the tags will be the ID, random number and the timestamp. Next, the reader will send the information from the tag to the database. Here, the MAC algorithm will be used to distinguish whether the tag ID and the random number between the tags and the one stored in the database is similar. The KDC server will be used to generate the secret key each time a tag is checked for its authenticity. The benefit of the MAC value is that it protects both the data integrity of the message as well as its authenticity, by allowing the verifier (which possesses the secret key and which in our example is the KDC server) to detect any changes to the message content. Based on the calculation of the timestamp to ensure the authenticity of the tag ID, the response will then be sent to the tag by the reader.

| Pseudorandom generator - PNRG | | |
|---|---|---|
| CA | Message Authentication Codes | |
| Reader | Timestamp | |
| | Database | Tags |
| The Notation of the system are : | | |
| CA | Trusted server | |
| ID | Tag ID | |
| R(0,1,…n) | Reader's ID | |
| D | Database | |
| x | Secret key distributed by Key Distribution Center | |
| TS | Timestamp | |
| MAC[m] | A MAC computed by applying secret key x to message m | |
| r | Random number | |
| → | Information movement (Send/Receive) | |

Based on method illustrated in Figure 4, we are able to provide the below system analysis on how the proposed prevention approach is able to reduce the chances of counterfeiting in a supply chain plant:

The use of the CA – the CA will have the list of authorised readers upfront and will only authenticate the trusted reader. This eliminates the possibility of a compromised reader.

The use of MAC with a secret key which is hashed and encrypted will protect the integrity of the message and eliminate the eavesdropping attack and skimming attack from occurring. The security of the communication channel between the database and tags is guaranteed because of this.

The use of KDC – the Key Distribution Centre function provides a secret key to both tags and database. The use of a trusted dedicated server will reduce the chances of the key being compromised by an adversary. In addition, the key in the KDC will be generated randomly. The number of bits used to generate the keys will impact on the security level. Using higher

numbers of bits will guarantee a stronger key. If a particular key is being compromised, the adversary is only able to clone the particular tag and not the entire batch.

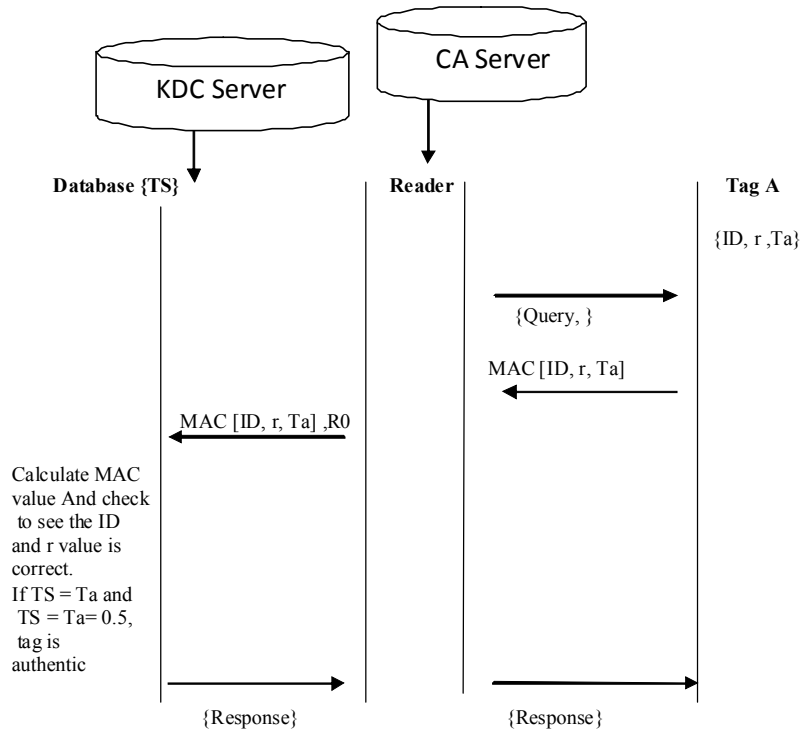



Fig. 4. Cloning Prevention Method

The use of timestamps will reduce the chances of the replay attacks that allow cloning to take place. The duration of time from each location will show the authenticity of a tag. The duration will be added and a rounded-up value for the TTL will be stored in the database.
The use of random numbers will increase the difficulty for an adversary to guess the key value of the tag.
It is worth mentioning that we have shown how three different attacks which are skimming, eavesdropping and active attacks through replay attack are able to be removed by utilising the above algorithm. However, physical attacks will only be addressed by using a higher level of key values. In addition, reverse engineering attacks could only be addressed by using a secure hardware implementation such as PUF (Devadass, 2008). Hence, we do not discuss these two attacks in our chapter. As supply chain management uses passive tags with low capabilities, we are not able to protect the RFID tags by using high-end security properties. However, by employing the trust framework, we are able to use third party solutions such as the CA server and KDC server. All the calculations of the MAC algorithm keys will be done at the database end. RFID tag information will store only minimal ID information. With minimal information, the probability of being skimmed and

eavesdropped upon will reduce. This model could be used for any RFID application such as the wine supply chain in our context.

### 4.2 Detection of cloning and fraud wine bottles in RFID system

This section explains RFID supply chain, RFID data structure and how TTL will be used in our proposed system. There are four different attacks in an RFID system (Mahinderjit-Singh & Li, 2009; Mahinderjit-Singh & Li 2010). Skimming attack occurs 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.

The strength of any RFID application is fully capitalised when the temporal and location information are correctly utilised in eliminating data security issue in RFID. Real time monitoring of events such as fraud and cloning attacks in RFID application are still rare.

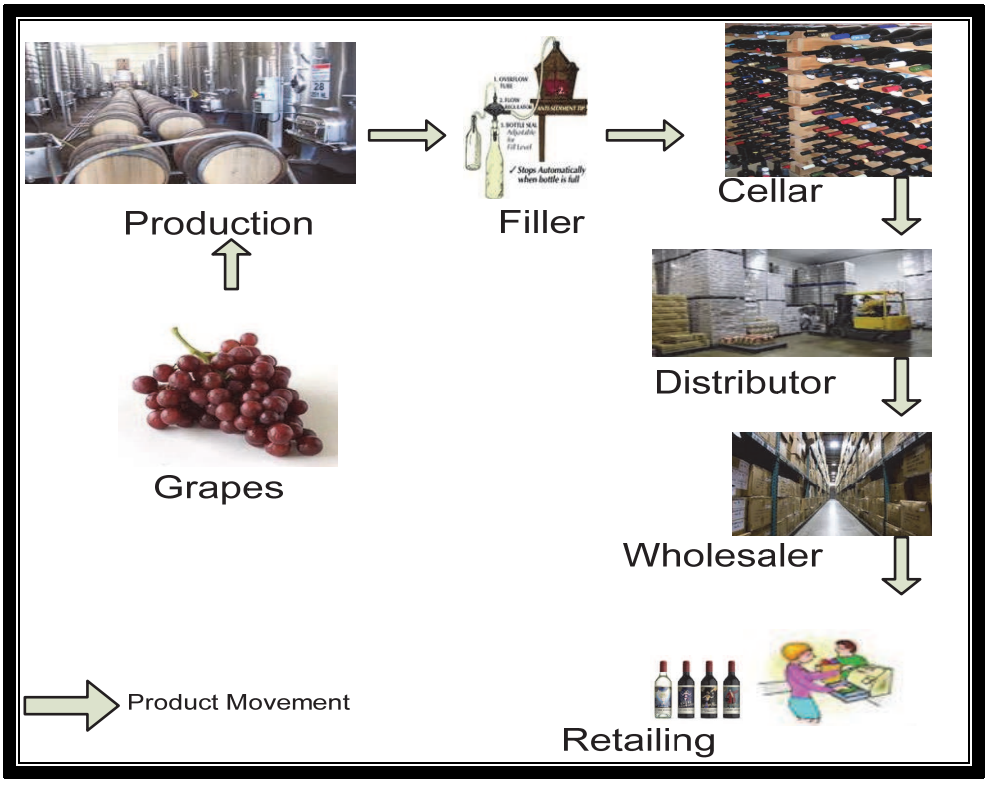



Fig. 5. Wine Supply Chain

Figure 5 shows a wine SCM environment with four different sites (Manufacturer, Distributor ,Wholesaler and Retailer). RFID tags are attached to the products for instance wine bottles. RFID based supply chain system involves the movement and flows of millions of data. The data generated consists of RFID tuples of the form of (EPC, location, time), where *EPC* is the unique identifier read by an RFID reader, *location* is the place where the RFID reader scanned the item, and *time* is the time when the reading took place. Tuples are usually stored according to a time sequence.

Each sites will have their own database system and this distributed manner database system are combined with a centralized EPC global server; EPC- Information Server. (EPC-IS). Our trust framework will resides in centralized server with ONS and EPC-IS (Verisign,2004) . The trust framework, fifth layer, mainly the detection module will consists predefined rules of real time monitoring and tracking system. The tracking and monitoring system can even play role as an intrusion detection system by using events rules and triggers function in database. Among the rules are as below:

- If, for instance, a product was identified at specific read points, e.g., 'shelf' (R3) and then 'exit' (R6),without having first been identified at the read point 'checkout' (R4 or R5), then it could be a matter of cloned or fraud.
- If a pallet P, which is containing the objects O1, O2, and O3 when leaving the production facility (M2 or M3) was identified as having only the objects O1 and O3 at the distributors receiving dock (D1 or D2), then the object O2 could have been replaced with O4 during transportation. These mean counterfeit products are injected.

**i) Data structure time to live(TTL)**

TTL indicates the time restriction that targets events should satisfy. Since most RFID application has a restriction time, we believe if carefully defined, we can use the notion of TTL to detect clones and fraud tags in a typical SCM. Based on TTL taxonomy (Li.X et.al , 2009), there are 4 different notions of TTL given based on the event types, both primitives and complex categorised based on events as Absolute TTL (TTL*a*), Relative TTL (TTL*r*), Periodic TTL (TTL*p*) and Sequential TTL (TTL*sE*). The detection process of cloned and fraud tags are able to manipulate all the above TTL notions. However, based on RFID applications, we determine that three relevant TTL notion for a SCM transactions and monitoring process is mainly *TTLa, TTLr* and *TTLs.* We also argue that the absolute *TTL (TTLa)* notion can be further categorised based on RFID applications. Some applications such as drugs and fast moving products for e.g. diary and foodstuff requires restriction in expiry date as the *TTLa* compare to product such as wine and jewellery. These expensive products emphasize more on manufacturing time. We will introduce the new notion of *TTL* called *Initial TTL (TTL i)*.

*TTLi* specifies the period of time a RFID tag is tagged on the product. By tracking, monitoring and storing the *TTLi* in the system; we are able to classify cloned RFID tags from genuine tags. Below are some examples to show the practicality of the usage of *TTL*.

i. *Example 1 - Initial TTL (TTLi):* Suppose 1000 new RFID tags have been purchased from its manufacturer. Each tag is then scanned by the reader denoting the birth time of the tags. Once the tag is tagged to a product such as wine, the expire time of tag is also stored. The period between this birth time and expire time areconcluded as *Initial TTL*. For products such as wine, *TTLi* is extremely important. Since the *TTLi* is an event happening at the manufacturer site, any fraud injection of fake wine bottles after the manufacturer site can be detected.

ii. *ii) Example 2 – Relative TTL (TTLr)* – In a wine based SCM, when the wines bottles are transported from the manufacturer site to the distributor site, the transportation period need to be carefully tracked. If the time to reach a destination is more than its relative *TTL*, an alarm will be raised as the state of bottles are suspicious. *Relative TTL* also indicates the period time the bottles are scanned by multiple readers at the front door of the distributor up to the time period the bottles leaves the site. Thus the *TTLr* can be categorised as *transfer TTL (TTLt)* and *site TTL (TTLs). TTLt* is the restriction time for all the movement time from one point to the other. Meanwhile *TTLs* is the whole site location e.g. Manufacturer, Distributor and Retailer period from the time it enter a site where it will be processed for unpack or repack up to the time it leaves the site.
iii. *iii) Example 3 – Sequential TTL (TTLsE)* – The products movement from the manufacturer site upto the retailer site is denoted by the *TTLsE. TTLsE* is the sum of all the *TTLr* in a supply chain. If the time from the manufacturer site and till the retailer site exceed or lesser than the *TTLsE*, the event could be suspicious.

*SiteTTL (TTLs) = Time of RFID within a site such as manufacturer, Distributor and Retailer*
*TTLs = tend (Distributor site) – tstart (Distributor site)*
*TransferTTL (TTLt) = Time taken when moving products from site A to site B*
*Sequential TTL (TTLsE) = Overall accumulated time from Manufacturer site up to Retailer site*
*The audit data for a single RFID is given below:*
Audit tag, for a single RFID tag ,

$$T = < Po, Pm, Psd, Pt, Pr > \text{ where:}$$

$$Po = \textit{operation} \text{ match rate,}$$

$$Pm = \text{mean of TTL, where TTL} = \{ \text{TTLs,TTLt, TTLsE} \}$$

$$Psd = \text{standard deviation of TTL, where TTL} = \{ \text{TTLs,TTLt, TTLsE} \}$$

$$Pt = \text{rate of tag responses, and}$$

$$Pr = \text{R/W (mean and standard deviation) rate.}$$

**ii) Cost- Sensitive learning**

Cost-Sensitive Learning is a type of learning in data mining that takes the misclassification costs (and possibly other types of cost) into consideration. The goal of this type of learning is to minimize the total cost (Turney, 2000). Many works for dealing with different misclassification costs have been done, and they can be categorized into two groups. One is to design cost sensitive learning algorithms directly (Turney,1995; Domingos,1999). The other is to design a wrapper that converts existing cost-insensitive base learning algorithms into cost-sensitive ones. The wrapper method is also called cost-sensitive meta-learning **(**Witten and Frank , 2005., Domingos,1999) sampling (Zadrozny,2003), and weighting (Ting,1998). Cost-sensitive meta-learning converts existing cost insensitive base learning algorithms into cost-sensitive ones without modifying them. Cost-sensitive meta-learning techniques can be classified into two main categories, *sampling* and *nonsampling*,in terms of whether the distribution of training data is modified or not according to the misclassification costs. This paper focuses on the nonsampling cost-sensitive meta-learning approaches. The non-sampling approaches can be further classified into three subcategories: relabeling, weighting, and threshold adjusting, described below. The first is *relabeling* the

classes of instances, by applying the minimum expected cost criterion (Witten and Frank , 2005). *Relabeling* can be further divided into two branches: relabeling the training instances (Witten and Frank , 2005) and relabeling the test instances (Domingos, P. 1999) .
In Relabeling approach such as Metacost (Domingos, P. 1999)and Cost Sensitive Classifier (Witten and Frank , 2005), cost C is known at the learning time. The technique to modify the inputs to the learning algorithm to reflect cost C includes :

i. If there are 2 classes and the cost of a false positive is λ times larger than the cost of a false negative, put a weight of
   λ on each negative training example
   λ = C(1,0) / C(0,1)
ii. Then apply the learning algorithm as before
iii. Setting λ by class frequency (less frequent class has higher cost)
   λ ~ 1/nk, nk - number of training examples from class k
iv. Setting λ by cross-validation

WEKA (http://www.cs.waikato.ac.nz/~ml/weka.), an open source Java package which contains machine learning algorithms and Metacost algorithm are used for solving the RFID cloning issue in SCM.

**iii) Cost –based Counterfeiting Detection Architecture and Result**

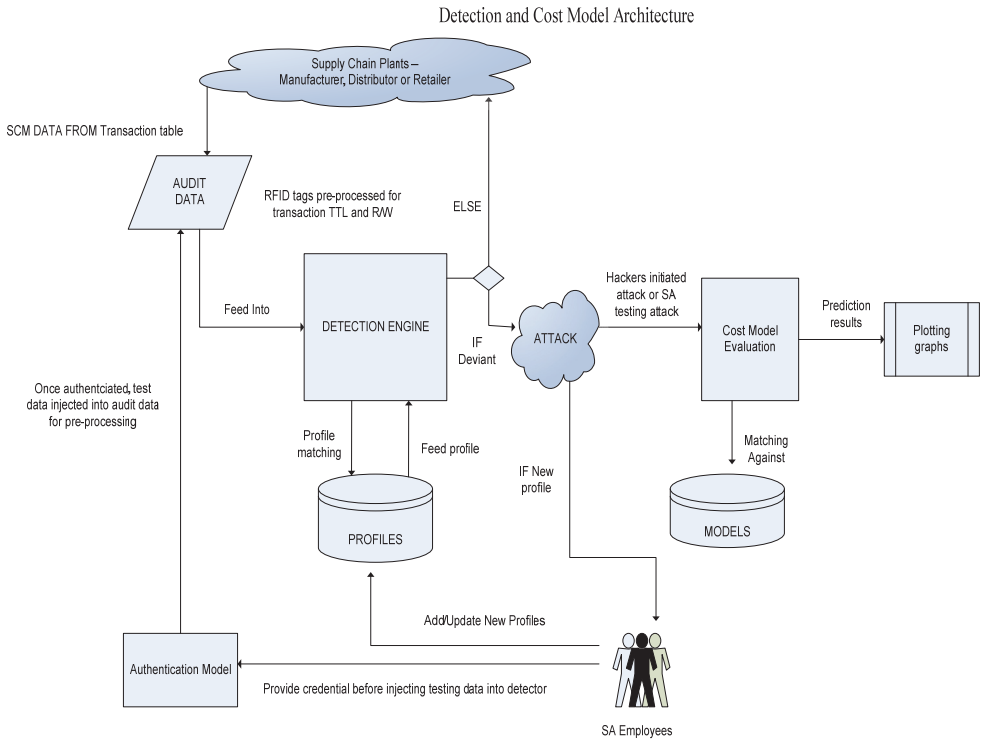



Fig. 6. Detection and Cost Model Architecture

Input: Training data: T= {t1,… tm} where each example Ti has attributes { Po, Pm, Psd, Pt, Pr} 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 $\in \{Cloned, Fraud\}$
A (k x k) misclassification cost matrix L,
L = a classification algorithm
Output: W
Estimate the class probabilities P(yi|xi)
Relabel
W= L (x,y)
Return W

Fig. 7. Pseudo code for Decision Tree (J48 algorithm) with Metacost

In this section we discuss how RFID tag cloning and fraud detection as well as cost modelling are supported seven layer trust framework (Mahinderjit-Singh & Li, 2009; Mahinderjit-Singh & Li 2010). Our RFID detection system has three main components:pre-processing; detection; and response and decision module as shown in Figure 6.Pre-processing 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 and decision component notifies the system administrator where and when an intrusion takes place and calculate the total cost of any attack.

Applying the dataset from the simulated RFID supply chain, 3000 example of RFID traces are generated from manufacturer site up to retailer site. RFID traces is then pre-processed into audit dataset which includes attributes such as Tags ID, location ID, TTLs (mean), TTLt ( mean) , TTLsE( mean and standard deviation ) and Read/write ( mean and standard deviation. The datasets are then feed into Weka engine by applying Metacost algorithm shown in Figure 6. The audit data will then be feed into a filtering system upfront for normalization purposes. CfsSubsetEval with Best First technique are used to determine the evaluation of attributes and search methods.

The base classifiers used were Naive Bayes, Random Forest and Weka's implementation of a Support Vector Machine (SMO), JRIP and C4.5 (J48) decision tree. Default Weka options were used for the Naive Bayes , Random Forest and JRIP but for the SMO "build logistic models" was set to true and for the J48 tree "Pruning" was disabled. Receiver Operating Characteristic (ROC) curve is a plot of the probability of true positive (recall) as a function of the probability of false alarm across all threshold settings. An ROC curve provides an intuitive way to evaluate the classification performance of RFID detection system. Recall represents the probability of detection of cloned tags and precision is the proportion of the correctly predicted genuine tags in each prediction class. In this study, we will utilize ROC for models evaluation.

The engine is trained with a training dataset. Cloning attacks such as skimming, eavesdropping and man-in the middle are simulated. To train the models cross-validation was employed. Cross-validation is a standard statistical technique where the training and validation data set is split into several parts of equal size, for example 10% of the compounds for a 10 fold cross validation. An independent test dataset is simulated as well. However, for the differing classifiers they have used across-the-board costs of 20, 40, 60, 80,100, 200, 500 etc. Weka normalises (reweights) the cost matrix to ensure that the sum of the costs equals the total amount of instances. Next we will illustrate one of the algorithms, J48 used with Metacost in WEKA tool. The pseudo code for Decision Tree (J48 algorithm) with Metacost is shown in figure 7. The ROC curve plotted in figure 8 takes in to account a few classifiers in WEKA. Based on this ROC curve, we could conclude that various classifier provide different performance based on the setting and nature of the classifier itself. For instance, Naïve bayes provide the larger area of ROC curve which indicate, it has the best performance. In addition, the true positive is almost 98% with only less than 2% of false alarm.

In a cloned detection RFID enabled supply chain, misclassifying cloned tag as genuine is undesirable. Result shows that when we increase *cost-ratio* from 20 to 10,000, recall rate increases, although the rate of increase depends on the algorithm. However, although not unexpected, is the decrease of *precision* which implies needless analysis of large number

false positives (shown in fig.9) SMO, JRIP and J48 algorithms consistently reach *Recall* rates close to 1 at high cost ratios, with precision slightly above 0.1.

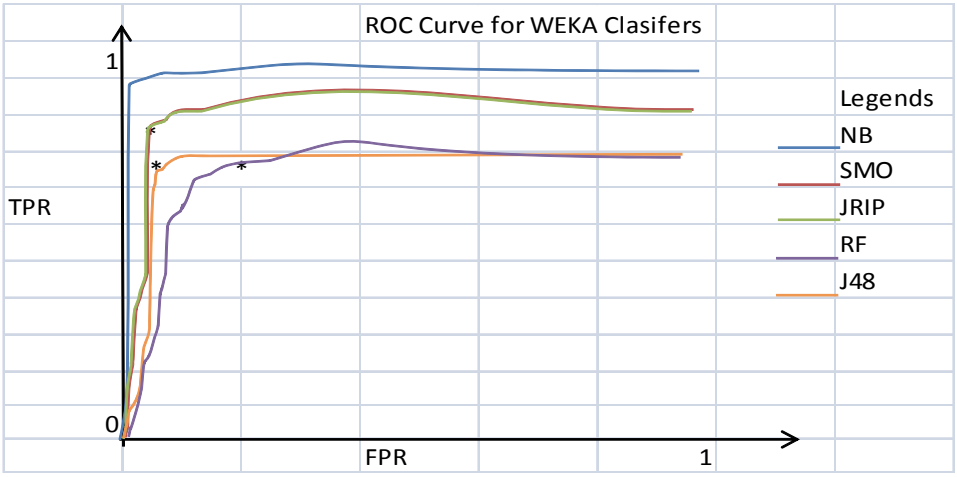



Fig. 8. ROC Curve plot for WEKA Classifiers

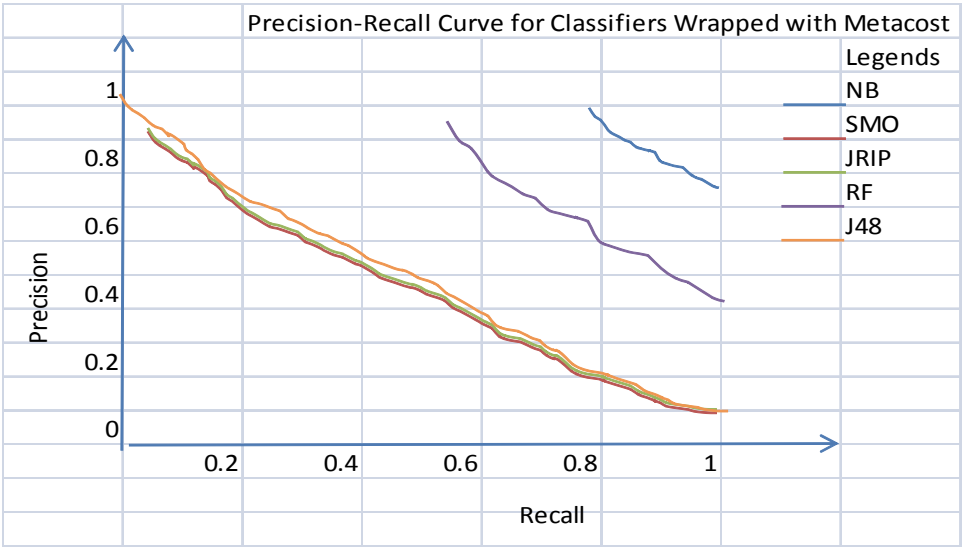



Fig. 9. Precision-Recall Curve for Various Classifiers in WEKA

Figure 10 indicates the accuracy of various classifiers against misclassification costs. We could conclude that as cost ratio increases, the accuracy of classifier decreases as well. An important implication from this study is that we can use cost to choose suitable operational threshold (based on different *cost-ratio*) to control a classifier's performance.

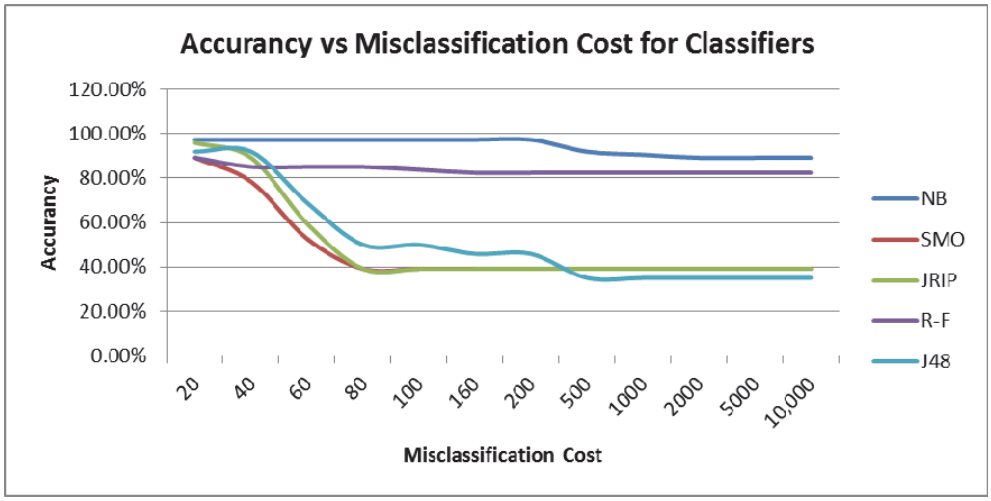



Fig. 10. Accuracy vs. Misclassification Cost for Classifiers

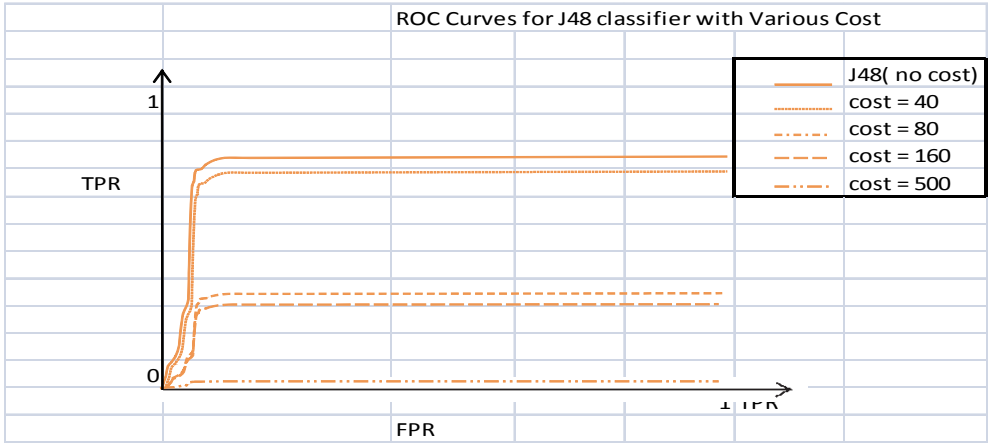



Fig. 11. ROC Curve for J48 classifier with various Costs

In practice, exact costs are rarely known and could change as we learn more about system requirements, its design, operational environment, etc. When considering a wide range of cost ratios the resulting models differ significantly. For instance from Fig 11, J48 classifier is made cost sensitive when the cost ratio was set to be 500 with accuracy of 35.1%. This means that FN needs to be 500 times more expensive than FP for J48 to transform to cost sensitive. Overall, J48 provides the most robust and versatile classifier for imbalanced RFID dataset compared to other classifiers.

With respect to construct validity, cost ratios in our experiments, which vary from 20 to 10,000 might not include all meaningful cost differentials. Different intrusion detection systems may have their own cost ranges of interests. The selection of classifiers is another possible source of bias. We cannot exclude the possibility that a classifier not studied here could show significantly better performance. Nevertheless, based, we believe that the chance of such a classification algorithm being in existence is rather low. The results above could be implicated by the small datasets used in the training models. When small dataset are used, classifier cannot accurately estimate the class membership probabilities and the imbalanced in class distribution of the dataset.

Any RFID cloned detection classifiers used must be correlated with cost since lower cost properties projects to lower or zero cloned tags in the system. This also impact positively in reducing the counterfeit attack which risks billions of dollars losses yearly in the market. Overall, we could conclude that by using WEKA tool, we are able to detect cloned and fraud tags in a supply chain plant. In addition, when various cost files are utilised we are able to reduce the misclassification cost of testing dataset. The important of the above experiment are to show the relationship between false positive rate and false negative rate. The trade-off shows that by increasing cost values, the false negative or the misclassification cost can be reduced. As a result, the false positive rate increase and this reduced the classifier accuracy overall. We also conclude that among the various supervised learners used, J48 is more sensitive to cost effects and outperform other classifiers when used together with Metacost.

In an RFID based wine supply chain, our main concern will be to eliminate the possibility of any counterfeit wine bottle passing through any detection classifier without generating any alarm. We believe the risk of counterfeit wines bottles passing through our detection system is greater than any genuine wines bottles detected as counterfeit one. Thus, even though the overall accuracy of classifiers decreases under the cost effects, we are able to reduce the losses in term of money and trust in RFID technology when used in supply chain. By minimising the counterfeit rate flowing in the market, human trust in this technology increases dramatically.

Next section provides a comprehensive privacy guideline in handling counterfeiting in a supply chain environment.

### 4.3 Privacy - countermeasures in preventing privacy violations

In the clone detector, some ways to prevent privacy violations in a Wine based RFID-enabled supply chain include:

1. The EPCglobal Discovery Service (DS) is equipped with key management mechanisms using ElGamal or RSA encryption algorithms. The clone detector is installed on the DS. The partners that need to access the clone detector will have to go through the DS for authenticity, and only permitted personnel are given permission to access information.

Before using the clone detector, all players obtain the necessary information to establish a connection to each other through the DS, which knows who owns an event on a certain ID and can the bootstrap the network upon a partner request for detecting clones of ID.

2. Distributed network architecture is employed. The distributed network architecture eliminates the problem of information overload and makes it easier to exchange information (VeriSign, 2008). Manufacturers as well as all trading partners create and store their own serialised information about each and every product. The manufacturer will manage and host a database that stores information about the generation of products, while trading partners host and manage similar databases storing information about product movement through the supply chain. Each involved partner will make this information available to authorised parties over the internet. This will ensure minimal sharing of local tracking data (times and places) with the EPC network.
3. The ONS could be used to point to an address on the EPCglobal network where information about the product being questioned is stored. The information stored here should be in minimal granularity that has limited timestamp information. By limiting timestamp accessible data, the effect of data leakage and data privacy can be minimised.
4. Default killing of RFID tags at store exits or password protection of RFID tag content could be set up. This means that the production tag which is used for tagging on the product within the supply chain will be deactivated at the POS exit. This will reduce the possibility of tracking and inventorying for the purposes for profiling done by the supply chain partners especially the manufacturer in learning the behavior of the consumer. In addition, a new tag can be placed on the tag after the purchase of the product that comes along with warranties. This information should be accessible only by the manufacturer and consumer.
5. Partial or no saving of the full EPC serial number should always be applied on RFID tags in an RFID-enabled supply chain environment.
6. There can be rigorous controls and transparency of EPC network access rights. A role-based access control (RBAC) policy should always be implemented together with item-level tagging (Illic et al., 2007). The main purpose of the RBAC policy is allowing only certain individuals to access certain levels of information. By applying this policy, we are able to limit accessible information by different role of personnel in an organisation.
7. Deletion of all product data after a certain period of time. After a while, the entire product data linked by the tag ID and the database should be deleted. This requirement reduces any form of tracking violation and curbs fraud situations from occurring. However, this will stamp out the advantages of an RFID system in a supply chain such as providing visibility and traceability.
8. Any supply chain partner could exercise control over personal information on sold products available on the EPC network. This will limit any misuse of product information by the consumer and competitors in learning about the supply chain partner"s financial gain in forecasting sales information. In addition, a competitor could also use this information in creating cloned tags with similar product information on fake products for future transactions.
9. All RFID transactions and information transmissions in the RFID supply chain require consent from both parties, namely, the business owner and consumer. By complying

with Garfinkel et al' s proposed policy (2005), RFID organisations in a supply chain environment need to be aware of their full rights especially to know when, where and why an RFID tag is being read. To comply with it, organisations could post a sign wherever RFID readers operate. Embedding this policy with a detection system is possible when a tag equipped with memory could count the number of times it has been read.

In preservation of RFID privacy, besides employing user policies in accessing the information in system, ownership transfer between partners can also be supported. By using one of the ownership transfer protocols discussed in Section 2.2, the security of the protocols can be maintained if the communication channel is protected. Another way to ensure a secure transfer of information will be to allow access to information to all the partners in the local EPC-IS without handing out any sensitive information such as sales and forecasting information. The conclusion we could draw here is that by following one or more of the privacy guidelines are able to protect the whole supply chain running on an EPCglobal network platform.

## 5. Conclusion

In this paper, three layers – Layer 1 – Security, Layer 2-Privacy and Layer 5-Detection – from our seven-layer trust framework are investigated for tackling counterfeit problem in a wine industry RFID-enabled supply chain. We have directed the security (prevention and detection of counterfeiting) and privacy preservation by using the RFID-enabled wine supply chain application. In an RFID-enabled supply chain system, privacy concerns require urgent attention especially to control the counterfeit issue. Security principles such as authorisation, authentication and encryption need to be combined with privacy procedures to maintain data integrity and privacy. Protection of privacy is essential for both consumers and business owners in order for a trustworthy relationship to be maintained between them. We have demonstrates that by applying MAC technique and third party services such as CA and KDC service, we are able to protect the low cost tags from being counterfeit.

In addition, we argue that RFID clone detection classifiers must always be correlated with cost since lower cost properties project to lower or zero cloned tags in the system. This also impacts positively in reducing the counterfeit attack which risks billions of dollars in losses every year in the market. We have shown that when the relabelling approach is used, we are able to reduce the misclassification cost and eliminate the scenario of having cloned and fraudulent tags in the system.

Nevertheless, RFID tag cloning and fraud can be detected in a supply chain at an initial stage if there is proper transfer of ownership with secure and authorised information exchange. This is made possible by integrating the monitoring, detection, and security and privacy functions from the seven-layer trust framework model which focuses on reducing risks and increasing benefits such as eliminating counterfeiting tags in SCM systems and boosting supply chain players‟ confidence. In future work, we aim to extend our RFID cloning and fraud detection work by using an outlier detection technique to identify illegitimate RFID tags and designing an improved cost decision model to calculate the damage, response and operational cost for a typical RFID clone detector system in a supply

chain application. In addition, we would like to enhance RFID supply chain privacy and security in terms of context-awareness.

## 6. Acknowledgements

This work is partially sponsored by University Sains Malaysia (USM)

## 7. References

Ayoade, J (2007). Privacy and RFID Systems: Roadmap to Solving Security and Privacy Concerns in RFID Systems. *Computer Law and Security Report*, 23(6):555–561, 2007.

A.J. Menezes, P.C. van Oorschot, S. Vanstone. Handbook of Applied Cryptography, CRC Press , Florida , USA (1996), 780 pages, ISBN 0-8493-8523-7.

Domingos, P. (1999). MetaCost: A general method for making classifiers cost-sensitive. In Proceedings of the Fifth International Conference on Knowledge Discovery and Data Mining, pp. 155-164, ACM Press.

Drummond, C. and Holte, R. (2000). Exploiting the cost (in)sensitivity of decision tree splitting criteria. In Proceedings of the 17th International Conference on Machine Learning, pp.239- 246.

Devadas, S., Suh, E., Paral, S., Sowell, R., Ziola, T., & Khandelwal, V. (2008). Design and implementation of PUF based "Unclonable" RFID ICs for anti-counterfeiting and security applications. In Proceedings of the 2008 IEEE International conference on RFID, 2008 (pp. 58- 64).

Garfinkel, S., Juels, A., and Pappu, R. (2005). RFID Privacy: An Overview of Problems and Proposed Solutions.*IEEE Security and Privacy*, 3(3):pp 34–43, May–June 2005.

Gao, X., Wang, H., Shen, J., Huang, J., Song, B. (2004). "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*.

G.Johnston, "An anticounterfeiting strategy using numeric tokens. International journal of pharmaceutical medicine", pp 163-171 2007

Hargraves, K., Shafer, S. (2004). Radio Frequency Identification (RFID) Privacy The MicrosoftPerspective [Online]: http://www.microsoft.com/twc (2004)

Ilic, A., Michahelles, F., Fleisch, E. (2007). Pervasive Computing and Communications Workshops, 2007. PerCom Workshops '07. Fifth Annual IEEE International Conference on pp. 337-341.

Juels, A. (2006). „RFID security and privacy: a research survey" IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, February 2006, pp. 381-394.

Juels. A. (2005). „Strengthening EPC tags against cloning", in Proc of the 4th ACM workshop on wireless security. 2005, Cologne, Germany, pp. 67-76.

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

Koh, R., *et al.* (2003). White Paper: Securing the pharmaceutical supply chain, Auto-ID Center, Massachusetts Institute of Technology, 2003,

http://www.autoidlabs.org/uploads/media/MIT-AUTOID-WH021.pdf (accessed 5 Nov 2009).

Lehtonen, M., Michahelles, F. and Fleisch, E. (2007). „Probabilistic approach for location-based authentication", Auto-ID Labs White Paper WP-SWNET-020, Auto-ID Labs ETH Zurich. pp. 3-17.

Lehtonen.M (2007) , "Trust and Security in RFID-Based Product Authentication Systems" Systems Journal, IEEE, pp 129 - 144

Lehtonen.M et.al (2006). "From Identification to Authentication – A Review of RFID Product Authentication Techniques." Workshop on RFID Security—RFIDSec,pp 169-181 2006 - Springer

Li, X., Liu, J., Sheng, Q.Z., Zeadally, S., and Zhong, W. (2009), TMS-RFID: Temporal Management of Large-Scale RFID Applications, International Journal of Information Systems Frontiers, Springer, July. 2009 pp.1-20.

Mahinderjit-Singh, M. and Li, X. (2009). "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*.

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

Nochta, Z., T. Staake, and E. Fleisch. "Product specific security features based on RFID technology."in Applications and the Internet Workshops, 2006. SAINT Workshops 2006. International Symposium on, pp 23-27 2006.

Osaka, K., Takagi, T., Yamazaki, K. and Takahashi,O. (2006). "An Efficient and Secure RFID Security Method with Ownership Transfer" Computational Intelligence and Security, 2006, vol. 2, pp. 1090-1095.

Pedro, P.L et al. (2010).Vulnerability analysis of RFID protocols for tag ownership transfer, Comput. Netw. (2010), doi:10.1016/j.comnet.2009.11.007

Potdar.V and Chang.E, "Tamper detection in RFID tags using fragile watermarking," 10th IEEE International Conference onIndustrial Technology (ICIT2006), Mumbai, INDIA, Dec. 15–17,2006

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*

Ranasinghe. D. C and Cole , P.H, "EPC Network Architecture," In: Cole, P.H. and anasinghe, D.C., (eds.) Networked RFID Systems and Lightweight Cryptography: Raising Barriers to Product Counterfeiting. Springer; 1 edition . ISBN 9783540716402, 2007.

Staake, T. Thiesse, F., and Fleisch, E. (2005). „Extending the EPC network: the potential of RFID in anti-counterfeiting", Proc of ACM symposium on Applied computing, Santa Fe, New Mexico, 2005, pp. 1607-1612.

Sarma, S., Ashton, K., Brock, D. (1999). The Networked Physical World, Technical Report IT-AUTOID -WH-001, 1999. http://www.autoidcenter.org/research/MITAUTOID-WH- 001.pdf.

Seong. D et. al , "Access Control and Authorization for Security of RFID Multi-Domain Using SAML and XACML," presented at Computational Intelligence and Security, 2006 International Conference on, pp 1587 - 1590 2006.

Saito, J., Imamoto, K., Sakurai, K.: Reassignment scheme of an RFID tag's key for owner transfer. In: Enokido, T., Yan, L.,Xiao, B., Kim, D.Y., Dai, Y.-S., Yang, L.T. (eds.) EUC-WS 2005. LNCS, vol. 3823, pp. 1303-1312. Springer, Heidelberg (2005)

Song, B.(2008). RFID tag ownership transfer, in Proceedings of Workshop on RFID Security, Budapest, Hungary, July 2008.

Turney, P.D. 1995. Cost-Sensitive Classification: Empirical Evaluation of a Hybrid Genetic Decision Tree Induction Algorithm. Journal of Artificial Intelligence Research 2: pp. 369- 409.

Turney, P.D. 2000. Types of cost in inductive concept learning. In Proceedings of the Workshopon Cost-Sensitive Learning at the Seventeenth International Conference on Machine Learning, Stanford University, California pp. 15-21.

Ting, K.M. (1998). Inducing Cost-Sensitive Trees via Instance Weighting. In Proceedings of the Second European Symposium on Principles of Data Mining and Knowledge Discovery, pp. 23-26. Springer-Verlag.

Turney, P.D. (1995). Cost-Sensitive Classification: Empirical Evaluation of a Hybrid Genetic Decision Tree Induction Algorithm. Journal of Artificial Intelligence Research 2: pp.369- 409.

Verisign - Expanding value of Supply Chain, (2008) http://www.verisign.com/static/DEV044098.pdf

Verisign Inc : “EPC Network Architecture” (2004) http://www.verisign.com/static/DEV044097.pdf

Witten, I.H., and Frank, E. (2005). Data Mining – Practical Machine Learning Tools and Techniques with Java Implementations. Morgan Kaufmann Publishers.

Hall.M and Frank.E et.al (2009); The WEKA Data Mining Software: An Update; SIGKDD Explorations, Volume 11, Issue 1. Mark Frey: "EPCglobal Certificate Profile [online]," Available http://www.epcglobalinc.org/standards/cert/cert_1_0_1-standard-20080514.pdf.

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

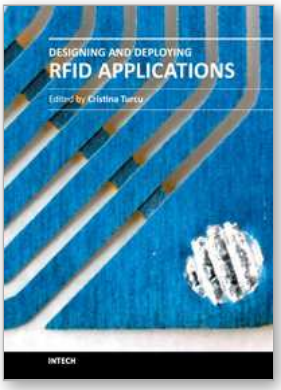
Zadrozny, B., Langford, J., and Abe, N. (2003). Cost-sensitive learning by Cost-Proportionate instance Weighting. In Proceedings of the 3rd International Conference on Data Mining pp. 435-445.(2005) GS1 :

Wine Supply Chain Traceability” [Online] Available:http://www.gs1.org/docs/traceability/GS1_wine_traceability.pdf(2006, Sep)

Vivian Yeo : Bedding, wine get a taste of RFID[Online]. Available: http://www.zdnetasia.com/news/communications/0,39044192,61953022,00.htm(2007 Mar.).

Australian IT, 2009: "RFID to fight wine fraud" [Online]. Available: http://www.australianit.news.com.au/story/0.24897,21355653-I5841,00.html.

Domenitz.L and Kravitz.J (2011); e-Provenance [Online] : Available:
http://eprovenance.com/WNYUV76B/index.htm?
Jared Sagoff : New bottle cap thwarts wine counterfeiters [Online]. Available:
http://www.anl.gov/Media_Center/News/2008/NE0




**Designing and Deploying RFID Applications**

Edited by Dr. Cristina Turcu

ISBN 978-953-307-265-4
Hard cover, 384 pages
**Publisher** InTech
**Published online** 15, June, 2011
**Published in print edition** June, 2011

Radio Frequency Identification (RFID), a method of remotely storing and receiving data using devices called RFID tags, brings many real business benefits to today world's organizations. Over the years, RFID research has resulted in many concrete achievements and also contributed to the creation of communities that bring scientists and engineers together with users. This book includes valuable research studies of the experienced scientists in the field of RFID, including most recent developments. The book offers new insights, solutions and ideas for the design of efficient RFID architectures and applications. While not pretending to be comprehensive, its wide coverage may be appropriate not only for RFID novices, but also for engineers, researchers, industry personnel, and all possible candidates to produce new and valuable results in RFID domain.



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