Computational Model for Trust Management in RFID Supply Chains

Manmeet Mahinderjit-SINGH and Xue LI

School of Information Technology and Electrical Engineering
The University of Queensland, Australia.
{mkmsingh, xueli}@itee.uq.edu.au

Abstract

Trust management in an open RFID system environment is a nontrivial problem, where different organizations have different business workflows and operate on different standards and protocols. Open RFID systems can only be effective if the systems can trust each other and be collaborative. The open system environment is also constantly evolving. So the trust and the collaborations need to be constantly maintained to cope with changes. RFID is becoming a ubiquitous computing technology imposing security and privacy threats. Counterfeiting in supply chain management is an attack with cloned and fraud RFID tags in order to gain illegal benefits. In this paper we will extend our previous work on a trust framework and construct a computational model for the trust management. The trust evaluation is built into the process of transactions of the data exchange and authorization in order to facilitate a better data sharing and access control. An example of wine counterfeiting will be presented and we will show how our computational trust model helps in reducing fraud brand of wines in supply chain management (SCM).

Index Terms — RFID, Trust Management (TM), Supply Chain Management (SCM), Computational Trust Management (CTM)

I. INTRODUCTION

RFID technology is a revolutionary method to identify and track human and products in applications such as SCM, retails, and healthcare, pharmaceutical and vehicle management [4, 16]. The use of EPC (Electronic Product Code) tags to eliminate counterfeiting is mainly because of two techniques: First, RFID allows for new, automated and secure ways to efficiently authenticate physical items. Second, as many companies invest in networked RFID technology for SCM, the item-level data collection and visibility now becomes possible [17]. Despite of the advantages of visibility and fast identification provided by RFID, the security and privacy threats attributed by limited hardware storage and memory in the RFID tag imposed an issue of counterfeiting [16]. The weakness of RFID technology in this study is considered in SCM only. There are four challenges of applying RFID technology in SCM: (1) tag security, (2) privacy and security of communication channel, (3) automatic transition of tag ownership, and (4) data integration issues [1, 7].

978-1-4244-5113-5/09/$25.00 ©2009 IEEE

Since the cost of tags decrease with the price close to $0.01 (1 cent) each, the storage and memory capabilities on a tag are reduced. As a result, no strong and ultimate security mechanism can be installed on tags [2]. The vulnerability of RFID tags and communication channel increases the risk of security threats such as eavesdropping, skimming, and man–in-the-middle, DOS, and physical attacks [15]. Single attack or a combination of threats contributes to cloning and frauds attacks, which are the main counterfeiting problems in SCM. Consequently, the above security and privacy problems decrease the human trust and confidence in the adoption and implementation of RFID technology [9].

In a typical open network such as SCM, trust counts in selecting partners, software and hardware infrastructure used, and even in the information transmission within a communication system. Together with the list of challenges and vulnerability regarding RFID discussed earlier, public acceptance in RFID implications systems is still an open question. The major question is how can open RFID networks be secured through trust? And how do we derive the existing trust notion to fit into the RFID system and solve the security and privacy issues discussed earlier? Thus the relationship of trust and RFID in the nature of business indicates an interesting research problem, which is to be addressed in this paper.

In our previous work [8], we proposed a novel seven-layer trust framework. Our trust framework provides functions for the trustworthiness of large scale RFID global tracking systems and the usefulness of RFID systems. Our trust framework also functions as a preventive and detective mechanism for security attacks. Based on [9], an RFID cloning and fraud attack is able to be handled with a better data sharing and exchange mechanism. For exchanging information, the need for authorization policies is a must. Hence, the aim of this paper is to construct a Computational Trust Management (CTM) system for our seven-layer trust framework in designing a better data sharing. Our objective is to employ our trust framework for assigning policies for a secure and visible data sharing. The second aim is to show how CTM can be used for RFID based wine counterfeiting handling. Even though our work is concentrated on RFID cloning and fraud attacks, our trust framework and the CTM solution can also be employed for other RFID security attacks.

This paper is constructed as follows. Section II discusses the related work. Section III describes our recent proposed seven-

layer trust framework. Section IV introduces a proposed computational trust management (CTM). Section V illustrates an example of wine counterfeiting and solution using our trust framework and the CTM. Section VI provides the conclusions.

II. RFID SCM TRUST, AUTHORIZATION & AUTHENTICATION

Tackling trust for catering security threats in RFID is a novel approach. Trust decrement among business partners in adoption of RFID-enabled SCM is because of two main issues in RFID technology. First, the security and privacy threats in RFID reduce the trust and confidences especially when RFID tagging is used for anti- counterfeiting purposes. Second, the lack of an attack detection model in the RFID network makes the security and privacy threats go unnoticed. Other reasons that contribute to the decrement of trust in RFID-enabled SCM are as follows:

i) Open System Environment –SCM exists in an open system environment with various types of RFID system interfaces, organisation protocols and communication interfaces [7]. As a result, with multiple data integrations models exist, EDI (Electronic Data Interchange) and Internet Web EDI may widely used. However, when RFID data is involved in the EDI transactions, it risks the propagation non-trusted low level RFID data directly into the high-level EDI transactions. This decreased human trust in RFID adoption.

ii) Non-authentication, authorisation and tracking model – RFID middleware only includes the commonly used standard models for data exchange transactions and data sharing among organisations. Models such as EPC-IS, ONS, EPC-DS only provides common transactions (http://www.epcglobalinc.org). For RFID tracking purposes, e-predigree which is used for drugs industry is the only model [13]. The lack of an authentication model and tracking mechanism to be built into RFID middleware illustrates that the current design of RFID network infrastructures fails to cater for the security and privacy requirements [9].

iii) EPC Trust Service – The current EPC trust model is the only trust model in RFID functions to support authentication and authorisation transactions. EPC-Trust functions use a third party model – CA (Certificate Authority) in authenticating devices and users in a supply chain models VeriSign Inc [22]. By only using PKI architecture namely X.509 certificates [13] as its authentication mechanism, the trust services does not includes any option of selecting any other secure authentication architecture based on application requirements and risks. In addition, we believe that any TM model that only consider hard trust mechanism such as authorization and authentication with no capability of accumulating feedbacks and ratings based on transaction and human experiences fails to preserve its trustworthy functions and are no good.

The trust gaps discussed above impact the RFID SCM business value and causes losses in money and business transactions. For these reasons, the trust management (TM) in RFID requires urgent attention. The importance of authentication and authorization of services and resources is the root of TM [6]. In order to realize the business benefits of RFID, trading partners such as manufacturers, distributors and retailers must be able to exchange data and share data only if authentication and authorization process is carried out. Understanding the requirement of RFID products to be tagged and the data characteristics [8] is the first step before we can design the access control policy for authorization [10]. We believe that RFID tag cloning and fraud attacks can only be eliminated if the policies are assigned at product level or item level. Besides that item level policies are suitable for expensive and high risk products such as jewellery and wines. Role based policy for RFID SCM access control systems [12] can be designed using languages such as SAML, XML, XACML and even WS-Security. In terms of authentication models in RFID, Table 1 provides an analysis on the RFID authentication models according to their performances. Based on Table 1, we conclude that many companies are more comfortable with the usage of CA mainly because the cost and the high security provided. However, one of the disadvantages of this approach is the central authority usage without fault tolerance in hand.

Table 1: RFID Authentication Analysis

	Performances Criteria			
Authentication	Cost	Acceptance	Ease to Use	Security
Tokens [25]	High	Low	High	Low
Digital Cert (CA)[13]	Low	High	High	High
Shared Key [16]	Low	High	High	Low
EPC Trust Services [22]	High	Low	High	High
Reputation System [24]	Low	Low	High	High
Other PKI (RSA, Pairing)	High	Low	Low	High

In contrast, the usage of tokens and shared key approach provides a low security outcome due to the easiness of forged secret keys and its complex management and token distribution. Nevertheless, the limitation of online trust services such as EPC trust services and reputation system in the RFID technologies makes its adoption still at a low rate. As a result, the lack of confidence in RFID authentication schemes, disregarding the availability of excellent security features, causes that many businesses are still at a very early stage of accepting the RFID trust services technologies. Next section will illustrate our seven layer trust framework.

III. RFID TRUST FRAMEWORK

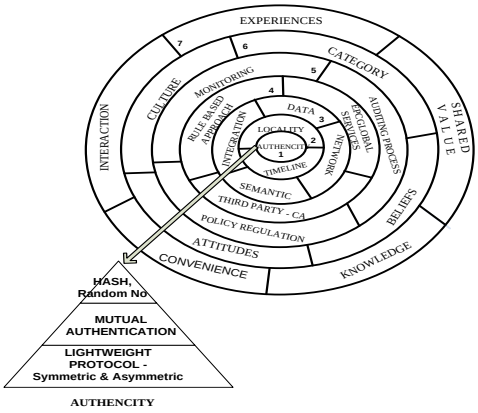


Figure 2: Seven Layer Trust Framework [8]

The deviation of RFID based trust takes places from simple soft trust which includes experiences and reputation up to another higher level known as hybrid trust. Hybrid trust in RFID system is more than just a hard or security trust based on authentication and soft trust as argued by [14]. In our definition, trust for RFID system is defined as a *comprehensive decision making instrument that joints security elements in detecting security threats and preventing attacks through the use of basic and extended security techniques such as cryptography and human interaction with the reputation models*. Since a trust model that dispersed privacy is a weak and non-usable model, our trust framework will ensure privacy and will not compromise security measurements. In addition we argue that a trust model for a technological system should always include human interaction through the usage of a feedback and rating model. Our trust framework provides theoretical solution for all the trust gaps discussed in Section II. In addition, our proposed trust framework (Fig 2) also functions as i) a solution to embrace trustworthiness by employing core functions at three main levels, which are the RFID system physical level (e.g. tags and readers) core functions, including the security and privacy level core functions, and the RFID service core functions at the middleware level by utilizing multiple data integration platforms such as the EPC trust services (http://www.epcglobalinc.org). The third party software system such as intrusion detection systems (IDS) can also be used. Finally the core functions at application level by using reputation system based on user interaction experiences and beliefs ii) to provide guideline for designing trust in solving open system security threats. Section IV demonstrates our trust computational models.

IV. RFID COMPUTATIONAL TRUST MODEL (CTM)

Our trust framework [8] is a combination of prevention, detection, and trust. Fig 3 shows the abstraction of our trust framework.

1)	Application Core(Soft Trust (Vs))	
	Layer 6 & 7 – Experiences (Feedback)	
2)	Service Core (Detection - Hard Trust)	
	Layer 4 – Detection	Layer 5 – Monitoring (Auditing)
3)	Physical Core (Prevention - Hard Trust (Vh))	
	Layer 1 - Authenticity	Layer 2 - Privacy

Figure 3: Seven Layer Trust Framework Abstraction

Our idea in designing our RFID CTM is mainly to calculate trust rate by combining both soft trust and hard trust components based on our trust framework. Once the confidence rate is evaluated, the appropriate access to the information will be given. The value of trust is in the form of binary [0, 1] with 0 means distrust and 1 means trustworthy [23]. Application core (Soft trust) can be denoted as direct trust [14] and meanwhile recommended trust is called indirect trust [14]. The whole process involves three interactions with first, both supply chain partner will need to perform authentication process.

Next our trust framework which resides in the server will calculate the trust rate between the partners (*Vc*). The final phase will provide services such as sharing, modifying and tracking the information based on policies authorized by the trust value.

Similar to the trust computation in [14], the overall trust *Vc* in an RFID SCM is calculated as a combination function *f com*:

$$Vc = f\,com\,(m\,Vh + n\,Vs) \quad (1)$$

Where *m* and *n* are weighting scales for the Hard Trust *Vh* and the Soft Trust *Vs* in the combining function, such that *m, n* ϵ *R, R represents the real numbers m+n <=1.0)* and the formula can be defined as follows:

$$Vc = m\,Vh + n\,Vs \quad (2)$$

In terms of our trust framework, the formula derived from (1) and (2) is:

$$Vc = \frac{w1(Vh(m))(Vh(d) + w2(Vs) + r}{w1 + w2} \quad (3)$$

Vh (m) = Prevention modules
Vh (d) = Detection modules
Vs = Soft trust
r = recommender value
w1, w2 = weight

A) Prevention, Detection and Soft trust notions

i) *Vh (m)* denotes the hard trust notion with *m* is the prevention module.

$$m = |S1 \cap S2| \quad (4)$$

S1 = Tags authentication; if exist value goes to 1, else 0
S2 = Supply chain authentication, if exist value goes to 1, else 0

ii) *Vh (d)* is the notion for hard trust and *d* is detection via intrusion detection system (IDS). False alarm rate (*FAR*) is when genuine products are detected as threat and could reduce the efficiency of a system. Our target is to minimize the *FAR* hit lesser than 5% for our IDS in order to stay trustworthy. Hence, the *d* rate is:

$$\begin{cases} \text{Trustworthy if FAR} \leq 5 \\ \text{Trustworthy if FAR} > 5 \end{cases} \quad (5)$$

iii) *Vs (S)* are the notion for soft trust based sum of partner's knowledge *(P (y))* and successful transaction rate *(F (P, Q))* and compared against soft trust threshold. Thus *S* is:

$$\begin{cases} +S \text{ if FEEDBACK} \geq T \\ -S \text{ if FEEDBACK} < T \end{cases} \quad (6)$$

iv) *r* is the notion for recommender value. This constant value is either 1 or 0 based on either there is a recommender or not. Recommendation notion is an indirect trust utilizes and will be the least priority in the trust computation.

v) *w1* and *w2* are the weighting factors which are assigned based on the risk an application can caused. If the security requirement for an industry is high, the weighting component can be up to 5; else it will be lesser than that.

B) Soft Trust Calculation

In this section we show the design of a computational model for computing feedback. The trust between the partners can be calculated based on the requirement of a supply chain RFID environment. The criteria used here are the 1) Partner Prior knowledge, which reflects the acceptance level of certain partners 2) Past history-based trust whether other partners or own experiences recommend it.

Partner prior corresponds to the partners' trust belief to the whole ubiquitous environment. This matches with our seven-layer trust framework from Layer 1 (security) up to Layer 5 (monitoring). It includes the trust of the co-existence of security and detection capability and the data layer [8]. On the other hand, past history will support our Layers 6 and 7. For instance, if two partners prior shows acceptance for similar need for security both prevention and detection together with openness of different data layers and show to have a pleasant interaction history working together before, the data sharing between them will be mutually authenticated and accepted. Below are the definitions and how the calculation is done.

i) Partner prior Knowledge

Each of the layers (trust framework) from 1 to 5 will have their own trusting scores (1 – 5: with 1 means less important and 5 means highly important). If the trading partners believe that Layer 1; security and layer 2; privacy are important and requires maximum protection, the value assigned is 5 for each. However, if the data integration, detection and monitoring layers are not vital, the value assigned is less than 5.

The functions *P (y) and* P *(n) are* used to denote partner *P* prior probability of acceptance and rejection respectively. Value *k* is the a user-defined importance for each layer.

$$P(y) = \frac{\sum_{5}^{1} k}{m}, \quad m = 25$$

$$P(n) = 1 - P(y) \quad (7)$$

Here *m* is a constant value of maximum importance value which is 25. A partner needs a minimum P(y) > 0.5 to be accepted and able to use to access the information from another partner EPC-IS.

ii) Past Interaction History (Successful transaction)

Past history interaction calculates the successful transaction occur between two partners. The feedback system should be able to calculate. *F (P, Q)* is used to denote the past interaction history between partners *P* and *Q*.

$$F(P, Q) = \frac{n}{n(c-n)} \quad c \neq 0, \text{ where } P \neq Q, n \leq c \quad (8)$$

Here *c* is the total communication times between partners *P* and *Q*. And *n* is the successful communication times between them *F (P, Q)*. If *P* has never communicated with *Q* before, then *F (P, Q) = 0*. If *P* and *Q* have unpleasant interactions history, our model set *F (P, Q) = [-1, 0)*. If out of 5 transactions, 3 transactions provided a good rating and considered successful, then the feedback value is evaluated as 0.5.

iii) Final Decision

The final decision will be to combined both value of partner's knowledge and successful transactions,

$$V_{NB} = P(y) + F(P,Q) \quad (9)$$

When *P* gives a request to *Q*, *h (P, Q)* is used to denote *S* trust decision. The value of threshold, *T* can be set based on security requirements.

Accept=1; Reject=0

$$S = \begin{cases} 1 & V_{NB} \geq T, \\ 0 & V_{NB} < T \end{cases} \quad (10)$$

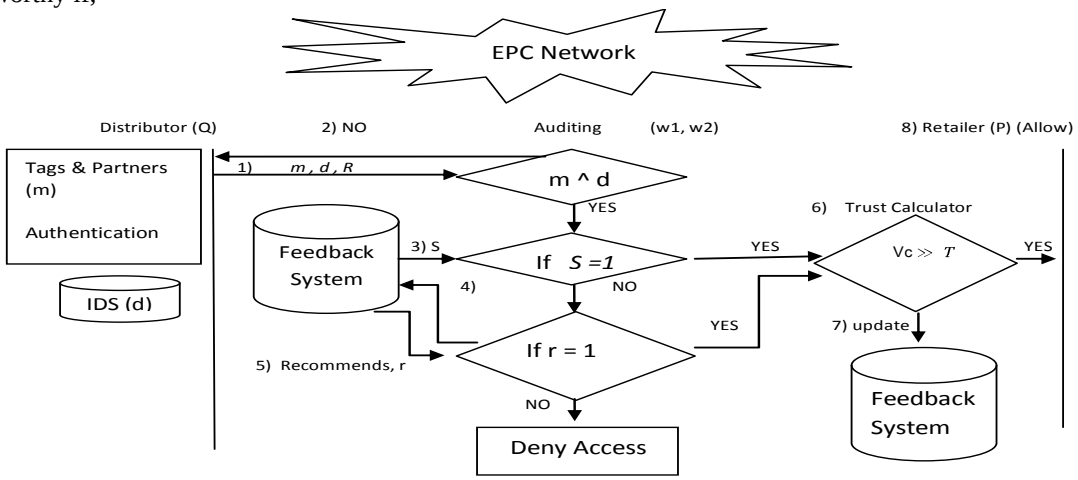
The final decision outcome will be fed into the trust calculator and end results on whether an access is authorized or doe not depend 50% on this value. In the context of an RFID tag cloning and fraud attack, as long as there is a prevention installed on the tags and a detect system is in hand, the system would be only 50% trustworthy. A system is 75% trusted, when the false alarm rate for a system is ≤ 5%. For instances, if 10,000 tags are tested for clones with our IDS, a trading partner should only accept that a previous transaction

is secure, if the cloned tags detected is less than a counting say, 500, then the transaction will be accepted. If the previous observation has achieved positive feedback, the soft trust will be denoted as feedback ≥ *T* or else. Besides, the recommendation value is either *r=0* or *r=1* based on whether any recommendation is given based on other peers. A trading partner is trustworthy if;

(+ m) ^ (d ≤ 5%) ^ (S ≥ T) ^ (r= 0) →Trustworthy

Else,

(- m) ^ (d > 5) ^ (S < T) ^ (r=1) → ⌐ Trustworthy



m: Tags and Partner Auth d : detection rate R : Service request r: recommender value S : soft trust value Vc : calculated trust overall T: minimum trust value for service

Figure 4: Computational Trust Model

Figure 4 denotes our proposed computational trust model and shows on how the trading partners will trust each other. Our trust framework will ensure that only trustworthy trading partners are allowed to access shared information. This protocol is distinguished at Layer 5 of our framework – auditing module [8]. This auditing process requires the authentication between supply chain partners to be performed earlier at Layer 1[8].

It begins with 1) a service request made to access resources and services. This request should be made in order to allow or deny visibility of data sharing between two partners. If the request is allowed, what type of data can be accessed should also be distinguished based on the calculation of trust. The needed prevention value, *m* is vital at this point. If there is no credential provided, the requester will need to ensure that authentication is done upfront and contact previous partners for authentication assistance. Next, the soft trust, *S* is calculated within the feedback system (see formula (10)) and the value is then calculated by (6) Trust calculator.

However, in the example with *S=0*, any recommendation value, *r* is located such as in *(4)* and *(5)*. Once the trust is calculated with the value *Vc*; it is then updated in the feedback system again. By using formula *(3)*, the calculated trust value will be compared against the minimal threshold, *T*. If the value to *Vc* is higher than *T*, then the transaction can be proceed and data sharing mechanism can be accessed. For instance, let assume that the distributor and retailer are authenticated and tags are also authenticated. However the value of *S* is *0* based on formula *(10)*. The recommender value shows that the requester has a good recommendation from other peers. Hence in a scenario of weight 5, the trust value will be 0.6. As we claim that role based policies suited our system, the authorization policies will be in the form of *POL = {role, sub, obj, action, trust value}* and at the item level tracking. The example of the above scenario, since the trust value only made up 0.6, only certain roles and action can be executed. Such as the retailer will only provide the action to read pallets level products with no access to modify and access certain sensitive information. This is done at steps *(8)*. In contrast, if all the steps above cannot be complied, then access to share any information will be denied. Next section will illustrates on how the CTM function on a real case application of RFID tagged wine counterfeiting issue.

V. RFID SCM WINE INDUSTRY

A report by Australian IT [18] showed a study that counterfeit wines brand accounted almost 10 percent of global turnover. One common method of counterfeiting involves replacing the label of expensive wines and pasting it to cheaper wines. Anti-counterfeiting methods include seal over capsules [19], labels on back of bottle and hologram built into the label. However it's possible to purchase copies of many holograms such as done in China [18].

In the wine industry, RFID is able to provide unique identification for tracking not only lots but also at the item-level tagging. Besides assuring product availability, it provides inventory accuracy at far lower expenses. Examples of RFID usage in wine can be explored in a real life business scenario by e-Provenance [20]. However, even though RFID is seen as an anti-counterfeiter tool, there are a few problems when it is tagged on wine bottles such as:

1) *Lack of tag reading accuracy because of wine absorption and radio waves reflection [21].*
2) *Limited lifespan of passive tag battery.*
3) *Tamper-proof seal constraint [19].*
4) *Security problem impose by RFID tags and system.*

Low cost passive tags used are not able to provide ultimate security against counterfeiting derived from RFID tags cloning and fraud. The tag used by e-Provenance [20] for tracking purposes can easily be cloned and all the historical information can be stolen. With this, fraud batches of wine produced with similar historical data may hit the market without checking of the authenticity of the products.

Next we illustrate the computation of the trust value using CTM in order to provide authorization for accessing the EPC-IS information. However, we will not discuss the algorithms and their testing results of our detection and prevention mechanisms for the limitation of the space in this paper.

Let assume Company X produce Chenin Blanc wines and recently it decided to employ RFID as an anti counterfeiting tool. A distributor has transported 1000 Chenin Blanc (white wine) to Retailer Y. Each container of wine is tagged with RFID EPC tag in the format of urn: sgtin: 680001.23456.401. However, on the way, Alice, an employee at the transporter company managed to perform cryptanalysis on 50 wines bottles and performs a brute force to reveal all the secret key of the EPC on the passive tags. The reverse engineering process was able to produce all the information of the EPC data. Alice now injects this information on new empty EPC tags and tagged them to fake brand Chenin Blanc wine. The covert code of the tamper-proof cases was also able to be cracked and imitated. Alice was able to swap the genuine goods with the fake one without anyone noticing it. The fake wines were then shipped to the Retailer. The following assumption is made up front.

i. Wines manufactures creates product and tagged the product with RFID tags
ii. Each local company (supply chain partner) have its own tags- reader, local database and local EPC-IS.
iii. Manufacture stores data in EPC-IS and update in Discovery Service
iv. Manufactures have a list of route need to be taken by each product.
v. Authentication and authorization is done at item-level.
vi. A service observation IDS system to detect clones and fraud tags should be running at each participants supply chain partners.
vii. A feedback observation system is a central registry point and is updated by each partner after a transactions is completed.
viii. Wines movement from each point require product and partner authenticity.
ix. The supply chain partners have employed our trust framework.

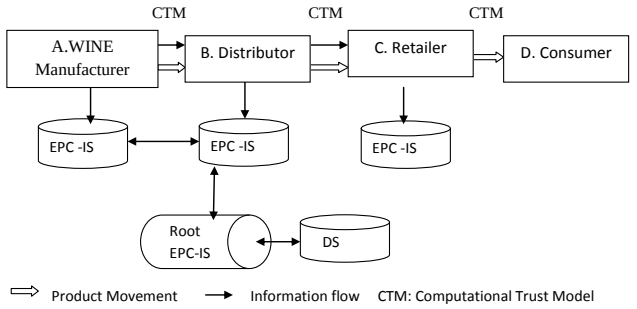


Figure 5: Wine Supply Chain

Our trust framework ensures that only trustworthy supply chain partners are able to access and exchange information regarding the wines tracing and tracking information. By employing the fundamental of both hard trust and soft trust we will show how the CTM is calculated between the wine distributor and retailer in Figure 5. Based on assumption made, all the partners are employing our trust framework which requires both authenticity and detection model in hand. The authentication between these partners can be done via certificates credential x.509 in an encrypted SSL. There are also preventive measurement taken for both tags and readers authenticity. Hence based on formula *4*, the *Vh (m)*; prevention module is calculated to be *m =1*. When wines have reached at the retailer site, the wines information is fed into the clone detection system. The IDS was able to detect the 50 fake wines since the pedigree information of tracking and tracing from EPC-IS does not match and so it triggers hitting in clone detector. The expert system shows the FAR at 1% and the detection formula *(5)* of the system has resulted the *Vh (d)* as 1. There are some previous successful interaction and transaction between the distributor and retailer. Besides that both partners prior probability of acceptance and past interaction history is more than 0.5 based on formula *(9)*. Hence the soft trust, *S* is calculated as 1. There is no need to provide peer recommendation values for the partner. So the *r* value is 0. As the counterfeiting in the wine industry is severe, the weight for the trustworthy is 5 for both *w1* and *w2*.

$$Vc = \frac{w1(Vh(m))(Vh(d) + w2(Vs) + r}{w1 + w2} \quad (3)$$

$$Vc = \frac{5(Vh(1))(Vh(1) + 5(1) + 0}{5 + 5}$$

The system trustworthy threshold is $T \geq 0.75$. Thus *Vc* value is greater than *T*. This proves that the both partners and wines are trustworthy and authentic. Since *Vc* is 1, the distributor and retailer are able to access the shares information in each other local database and EPC-IS server with total access for read, write and modify the shared information. As a result, RFID tagged wine counterfeiting can be handled if each transaction between supply chain partners follows our proposed CTM. Besides, our seven layer trust framework does not only function as a prevention and detection tool, but also provides a mechanism for a better data sharing model and policy authorization between trading partners.

V CONCLUSION

In this paper we have shown how our CTM is able to provide unconditional security in terms of detecting and preventing cloning and fraud attacks by concentrating at the supply chain business information transactions between partners. Our novel trust framework [8] provides a better solution compared to previous trust and authentication - authorization models. RFID tagged wine is used as an example and as a result with our trust framework. This work provides a better prevention, detection, integration and soft

trust model to enhance data sharing and to achieve a secured authorization model between supply chain trading partners. We will extend our prevention model to construct the protocol to authenticate wine bottles in an RFID environment. We will design an expert system to handle the counterfeiting attacks in RFID tagged wine industry. Our research on utilizing trust management in RFID tagged wine industry is currently a novel work that requires further attention.

VI. REFERENCES

[1] Z. A. X. Xingxin(Grace) 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)*, 2004.

[2] 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*.

[3] A. Ilic, F. Michahelles, and E. Fleisch, "Dual Ownership: Access Management for Shared Item Information in RFID-enabled Supply Chains," presented at *Pervasive Computing and Communications Workshops, 2007. PerCom Workshops '07. Fifth Annual IEEE International Conference on, 2007*.

[4] A. Juels, D.Molnar, and D. Wagner, "Security and Privacy Issues in E-passports (2005) " *IEEE SecureComm '05* 2005.

[5] E. Y. Choi, D. H. Lee, and J. I. Lim, "Anti-cloning protocol suitable to EPCglobal Class-1 Generation-2 RFID systems," *Computer Standards & Interfaces*, vol. In Press, Corrected Proof, 2008.

[6] S. R. a. L. Kutvonen, "Trust management survey " , *Proccedings of iTrust 2005, number 3477 in LNCS, pp 77--92 , Springer-Verlag*.

[7] R. Derakhshan, M. E. Orlowska, and L. Xue, "RFID Data Management: Challenges and Opportunities," *presented at RFID IEEE International Conference on, 2007*.

[8] M.M Singh and L.Xue, "Trust Framework for RFID Tracking in Supply Chain Managemen," *Proc of The 3rd International Workshop on RFID Technology - Concepts, Applications, Challenges (IWRT 2009), Milan, Italy, 6-7 May 2009*.

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

[10] Z. Z ,Huang , "*RFID Keeper*: An RFID Data Access Control Mechanism" , *IEEE proceedings GLOBECOM 2007*

[11] D. C. a. C. Ranasinghe, 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 . ISBN 9783540716402*, 2007.

[12] K. Dong Seong, S. Taek-Hyun, and P. Jong Sou, "Access Control and Authorization for Security of RFID Multi-Domain Using SAML and XACML," *presented at Computational Intelligence and Security, International Conference on, 2006*.

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

[14] L. Ching and V. Vijay, "A Hybrid Trust Model for Enhancing Security in Distributed Systems," in *Proceedings of the The Second International Conference on Availability, Reliability and Security*: IEEE Computer Society, 2007.

[15] M.Burmester and B. d. Medeiros (2005). "RFID Security: Attacks, Countermeasures and Challenges.", *Proceedings of the RFID Academic Convocations, The RFID Journals, Conference, 2007*

[16] S.H Choi,. and C. H. Poon (2008). "An RFID-based Anti-counterfeiting System." *IAENG International Journal of Computer Science, 35:1, IJCS_35_1_12*.

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

[18] Australian IT: "RFID to fight wine fraud" [Online]. Available: http://www.australianit.news.com.au/story/0,24897,21355653-15841,00.html (2009 May)

[19] *Jared Sagoff :* New bottle cap thwarts wine counterfeiters [Online].Available:http://www.anl.gov/Media_Center/News/2008/NE080801.html (2008, Aug)

[20] e-Provenance[Online] Available:http://eprovenance.com/WNYUV76B/index.htm? (2008).

[21] Vivian Yeo : "Bedding, wine get a taste of RFID" [Online].Available:http://www.zdnetasia.com/news/communications/0,39_044192,61953022,00.htm (2006, Sep)

[22] Verisign Inc : "EPC Network Architecture" http://interval.hu-berlin.de/downloads/rfid/IT_Infrastruktur/013343.pdf (2004)

[23] S. Marsh. Formalising Trust as a Computational Concept.Ph.D. Thesis. Department of Mathematics and Computer

[24] Wolfe *et al.* "A Trust Framework for Pervasive Computing Environments", 2006 IEEE, Computer Systems and Applications, March 8, 2006 pp. 312 – 319.

[25] G.Johnston, "An anticounterfeiting strategy using numeric tokens. International journal of pharmaceutical medicine", 2007