

# An RFID-based Anti-counterfeiting System

S.H. Choi and C.H. Poon

**Abstract**—RFID facilitates processing of product information, making it a promising technology for anti-counterfeiting. A number of RFID anti-counterfeiting mechanisms have recently been proposed. This paper first compares the strengths and weaknesses of these mechanisms, and evaluates possible impacts of threats to RFID. Subsequently, a track-and-trace anti-counterfeiting system using RFID is proposed. The proposed system is aimed at relatively high-end consumer products, and it helps protect genuine products by maintaining the product pedigree and the supply chain integrity. As such, consumers can safeguard their stake by authenticating a product with RFID readers before making payment. The mechanism is relatively simple and easy to implement.

**Index Terms**—RFID, anti-counterfeiting, track and trace, security analysis

## I. INTRODUCTION

Counterfeiting is generally considered one of the greatest threats to the world economy. In 2006, it was estimated that counterfeit goods accounted for 5% of the world trade, totalling US\$250 each year, and that over the past ten years counterfeiting has destroyed 120,000 jobs each year in the United States, and 100,000 in Europe [1].

The Radio Frequency Identification (RFID) technology is a method of unique items identification using radio waves, typically a reader communicates with tags that hold digital information in microchips [2]. RFID has emerged as a promising tool to combat counterfeiting because it complements the common anti-counterfeiting measures, such as holograms, colour shifting inks, taggants, fingerprints, and chemical markers [3], which do not avail automatic verification of product authenticity.

Several RFID anti-counterfeiting solutions have been proposed in recent years, which would be discussed in detail in section III. While these solutions have not yet been implemented in practice, the United States Food and Drug Administration (FDA) has passed the Prescription Drug Marketing Act (PDMA) in 1999, which requires pharmaceutical wholesalers to track and trace the drugs they distribute. Drug wholesalers are required to supply a “pedigree” in either paper or electronic form which records every entity that has handled the drug since its manufacturing. FDA recommended RFID [4] [5] for such purposes.

However, there are doubts about the security level that RFID can provide in such applications [6]. Thompson et al. proposed a STRIDE model that categorizes different RFID threats [7], while Rieback et al. presented a self-replicating RFID virus that

infects back-end RFID systems [8].

This paper reviews these threats and analyses how they may affect the security of RFID applications in anti-counterfeiting. Subsequently, a track-and-trace system using RFID technologies is proposed for anti-counterfeiting.

## II. THREATS TO RFID

### A. Spoofing

Spoofing is cloning of RFID tags by copying the information of one tag to another. This threatens RFID systems by creating a copy of the supposed-to-be unique, authentic RFID tags. With RFID now being deployed in various areas, such as access control to homes, offices and vehicles, or in electronic payment, victims could include any users of such services [6]. Researchers at Johns Hopkins University and RSA Security demonstrated how the security of the car immobilizers of 2005 model Fords could be tampered with, and that the electronic payment systems of Exxon-Mobil SpeedPass™ could be compromised by cloning the Digital Signature Transponders (DST) manufactured by Texas Instruments [9].

### B. Tampering with data

It refers to a situation when an adversary modifies, adds, deletes, or reorders data in RFID tags. Tampered tags may disrupt the normal operations of the backend system.

### C. Replay attacks

Although the holder of an RFID tag may expect that any readers out of the normal operation range (typically 10cm for Gen 2 tags) cannot retrieve any information from the tag, Kfir et. al. demonstrated that by placing a “ghost” between a reader and a tag, the communication range can be much farther away [10]. This leads to a false perception of safety. A challenge-response type authentication could be a solution to the problem. However, stronger public key cryptography means more expensive tags [11].

### D. Repudiation

Repudiation may result when there is not evidence to prove that a user has actually performed a certain action [7]. Tracking the actions of individual players throughout the supply chain is vital for maintaining the visibility and integrity of the supply chain, which is in turn important in reducing counterfeit gray market distribution [12].

### E. Information disclosure (sniffing)

Sniffing occurs when RFID tags are read without the knowledge of the tag bearer, therefore leaking information to unauthorized users [7] [8]. This does not only destroy the integrity of the supply chain, but also infringes consumers’

S.H. Choi is with the Department of Industrial and Manufacturing Systems Engineering, The University of Hong Kong (email: [shchoi@hku.hk](mailto:shchoi@hku.hk))

C.H. Poon is with the Department of Industrial and Manufacturing Systems Engineering, The University of Hong Kong (email: [ekmanson@hku.hk](mailto:ekmanson@hku.hk))

privacy.

#### F. Denial of service

Denial of Service (DoS) occurs when an RFID system cannot function properly to provide normal services to valid users; it is a common threat to Internet server systems. Service of an RFID system may be denied by “signal jamming”, where the communication between a tag and a reader is clouded or is shielded by a Faraday Cage, which can prevent tags from being read properly. An adversary may also jam the system by generating a return signal stronger than the authentic one to make it unavailable to valid users.

#### G. Elevation of privilege

This occurs when an adversary gains higher privileges in an RFID system than the authorized level. Although the adversary may not disrupt the system operations directly, he may implement some malicious software in the system and thus spread viruses through RFID tags.

#### H. RFID Viruses

Rieback et al. designed an RFID virus that self-replicates, which requires only one virus tag as the initiator. The affected systems run SQL injection codes unintentionally. The codes do not only affect the back-end system, but also spread the virus upon further communications [8]. Although it does not possess propagation capabilities of common computer viruses, it poses a substantial threat to the “trusted entities” within a corporate RFID system.

### III. RFID IN ANTI-COUNTERFEITING

RFID has gained popularity of being an anti-counterfeiting technology in recent years. It has an obvious advantage over other existing anti-counterfeiting technologies, in that it enables efficient and automatic product verification. In such a way, massive checks can be performed at pallet or even item level for product originality verification. Based on this distinct advantage, the following several schemes have been proposed for deploying RFID in anti-counterfeiting.

#### A. Numeric Tokens

Johnston proposed a “Call-in the Numeric Token” (CNT) technique [13]. This technique is relatively low-tech and low-cost, but requires customer participation in authenticating the products they purchase via the phone or the Internet. A random, unique and unpredictable identity number, which is a virtual tag or token, is assigned to each product at item level. The anti-counterfeiting mechanism relies on the difficulties in guessing the valid identity numbers. By setting an appropriate threshold, any items with a high-enough instance of query for validation would be deemed counterfeit.

Although the identity numbers can be printed on the packaging materials of the product item, the supply chain partners can automate the call-in validation process if these numbers are recorded in RFID tags.

#### 1) Security Analysis

Theoretically spoofing is not a threat under this solution, since the CNT technique relies on difficult-to-guess random tokens to make cloning of tags difficult. However, it might give false negative results. Therefore, by carefully controlling the number of counterfeit tags cloned from each genuine tag, an adversary might avoid triggering the call-in system.

If tags without any authentication mechanism are used in the CNT system, tampering and spoofing would become easy. However, random tokens would render tags invalid when they are tampered. Nevertheless, tag tampering could still be a security hole to the supply chain partners who use automated systems to validate tags because the tampered tags may disrupt their normal operations.

As the CNT system does not rely on the movement history of products, repudiation is not a threat. However, this may leave genuine tags unprotected, because if a genuine tag token was sniffed and queried for many times, the real tag would become an counterfeit and there would be no way to prove its authenticity, causing losses to genuine product owners.

The CNT technique poses least requirements on the back-end server operations. Therefore, it is less susceptible to the DoS and elevation of privilege attacks, as well as RFID viruses. Virus writers may turn to infect local systems of those using automated systems to scan the tokens for batch call-in verification. However, this would become less beneficial since individual local systems tend to be different from one another, rendering them ineffective channels to spread RFID viruses.

#### B. Strengthened EPC Tags for secure authentication

The Electronic Product Code (EPC) is a global unique identification service for physical objects [14]. In 2005, EPCglobal, a non-profit making organization that aims to increase visibility and efficiency throughout supply chains, developed the global standards of the EPC Network. It ratified the EPC Class-1 Generation 2 UHF standard, which is expected to be used by most companies in the near future. Commonly known as “Gen 2”, this standard defines the physical and logical requirements for an RFID system operating in the 860 MHz - 960 MHz frequency range [15] [16].

As the Gen 2 standard was developed with little considerations on security and privacy issues [17], Juels proposed a model to strengthen the EPC tags against cloning attacks [18]. The primary assumption is that Gen 2 tags can reliably authenticate product items if they are unique. In the Gen 2 standard, a 32-bit kill PIN is used to make a tag permanently inoperable. Juels proposed another 32-bit access PIN, which is optional in the Gen 2 standard, for some tag commands. Authentication is done by a fix-value mutual-authentication protocol, where the access PIN serves to authenticate the reader, while the kill PIN authenticates the tag. Under this scheme, tag readers are assumed trustworthy.

However, Duc et al. thought that Juel’s solution does not take into account sniffing threat and privacy issues. They proposed another solution that includes security features of authentication, traffic encryption, and privacy protection [17].

Their scheme employs Gen 2 compliant cryptographic features like Pseudo-random Number Generator (PRNG) and Cyclic Redundancy Code (CRC). The scheme makes use of the PRNG to generate a new session key to encrypt each session of tag-to-reader communication, rendering sniffing impossible, while tag authentication is done by the PIN features described in the Gen 2 standard. Since a tag emits a different bit-string in each and every session because of the new session key, even a compatible reader would not be able to track the tag holder's activities for a time longer than the session period.

#### 1) Security Analysis

The primary motivation for developing cryptography for RFID tags is resistance to cloning [19]. When there is such an authentication protocol to prevent cloning, it can also protect tags from tampering, sniffing, virus and replay attacks.

"Secure" tags are obviously beneficial to product stakeholders, as well as to society as a whole. However, product stakeholders never know when adversaries would actually succeed in cracking the system, nor to what extent they would crack it. Therefore, it would be risky to rely solely on the uniqueness of a tag to perform anti-counterfeiting functions, especially in areas of life-threatening consumer products (e.g. pharmaceutical products).

When an RFID tag, and thus the product it attaches to, is assumed unique and secure, efforts can be saved in tracking the product's movements through the supply chain. However, repudiation may become more likely since the product's status is not monitored by the central anti-counterfeiting system throughout its lifespan in the supply chain.

All the secure tag solutions mentioned above rely on a central server for the authentication process. To increase efficiency, a distributed server infrastructure can be used to reduce reliance on a single server. However, it opens up more penetration points for DoS or privilege elevation attacks.

#### C. The Track-and-Trace Approach

Koh et al. proposed a scheme to track and trace products through a supply chain, utilizing the EPC infrastructure [20]. Under this scheme, pallets or cartons are each embedded with an RFID tag that contains an EPC number. The EPC number serves as a pointer to specific product information which may be queried through an Object Name Server (ONS) accessible through the Internet. As the product moves through the supply chain, each node in the supply chain updates the product pedigree information to the central repository. Therefore, the central repository database would contain complete information on the trail of exchange of a product, which includes its origin, destination, timestamp, company names, etc. In such a way, a product can be tracked and traced with a complete product pedigree as it moves from the manufacturer to retailers.

However, Staake et al. thought that Koh's solution is adequate only for some products [21]. They argued that RFID tags, which store the EPC numbers in plaintext, can be easily cloned. Hence the products cannot be sufficiently authenticated. When a counterfeiter does not update the central

repository, nor the customer registers the deal, the counterfeit product may still give an incomplete but plausible history. There may also be other reasons that the central repository may not be updated correctly. Therefore, they suggested extending the EPC Network by adding an EPC Product Authentication Service (EPC-PAS) to allow a secure product authentication in a database-reader-tag environment. A cryptographic unit (CU) is placed behind an RFID reader. Therefore it does not raise new requirements on reader devices. However, RFID tags that support this kind of cryptography are more expensive than normal tags [11], and such secure functionalities do not comply with the EPC Gen 2 standard.

Therefore, Kim et al. proposed another model that authenticates products in mobile RFID environment, utilizing watermarking technologies. It aims at addressing the Gen 2 compatibility problem of Staake's model, as well as the problem of readers' trust level of Juel's model [22] [23]. With digital camera cell phones embedded with RFID devices to come in the near future [2], it may be feasible to require a consumer to scan the product EPC and capture the watermark-embedded image on the product, and then send them over the GSM or CDMA network to the EPC-PAS for authentication. Then it returns a digital certificate with digital signature that states the authentication results.

#### 1) Security Analysis

The primary benefit of the track-and-trace approach is that it does not rely on clone-resistance of RFID tags. Assuming that the tag readers and the partners along the supply chain are all trustworthy, consumers may be protected without any involvement in the anti-counterfeiting mechanism, merely by relying on the credit of the retailers (and of their hardware) for checking the product authenticity. To the manufacturers, this approach best protects their interests, as genuine products will not be deemed counterfeits because of the existence of counterfeit items.

However, a lack of an authentication mechanism between the tags and the reader or the back-end server tends to render tampering or RFID virus attacks more likely. With the standardized EPC structure, it would become easier for a virus to spread around.

Replay and sniffing attacks would be the primary source of problems that lead to intense debates over privacy issues of RFID, which is the primary concern of a lot of consumers' rights groups. Tags without a secure authentication mechanism can practically communicate with any readers, regardless of their trustworthiness. Unencrypted communication between tags and readers may also be sniffed by an adversary. Leakage of sensitive information could possibly be used to produce counterfeit tags or readers, although this is considered impractical in the protected supply chain environment because the adversary devices have to be close enough to the genuine readers and tags [19]. Therefore, this is more than a privacy concern to the end-consumers.

The track-and-trace approach is resistant towards repudiation attacks because all movements of products and

actions of supply chain partners are tracked by the central server. A customer may simply refuse to purchase products without a pedigree or with a suspicious one. This approach relies on the ONS to retrieve pedigree information. The common weaknesses of Domain Name Servers (DNS) of the Internet directly transfer to ONS, because of their similarity in functionalities [24]. As a highly exposed service, the ONS becomes the primary targets of DoS or privilege attacks.

#### IV. THE PROPOSED SYSTEM

##### A. Overview

A number of anti-counterfeiting systems adopting various algorithms and mechanisms have been proposed by many researchers. These systems perform universal functions for virtually all kinds of products. They are generally large in scale with complex functionalities. But they are not without shortcomings: 1. The larger the scale they are, the more the points of penetration vulnerable to attacks; 2. The complex functionalities force host companies to adopt redundant functionalities they do not need; 3. The universal system mandates disclosure of product information to third parties.

To address these problems, this paper proposes an anti-counterfeiting system aimed to provide a product pedigree which supply chain partners and end-consumers can both access. The anti-counterfeiting mechanism is based on the track-and-trace approach, as mentioned in section III(C), with an extra feature that enables end-consumers to verify the products through their own mobile phones.

The system requires various partners along the supply chain to record product transactions using RFID technologies. As such, supply chain integrity is maintained by forming a chain of custody from the product transaction records stored in a central database. All the supply chain partners are expected to verify the incoming products and reject those with a suspicious pedigree, while consumers can verify a product before they make payment with a handheld RFID device, which is expected to be embedded into the mobile cell phones in the foreseeable future; if there is not any valid pedigree or the pedigree is deemed suspicious, payment should be halted.

The system primarily targets at high-end consumer products, such as apparels, handbags, purses, etc. The RFID hardware costs are relatively low compared to the value of these products, and hence the system implementation cost will be justifiable. More importantly, the high values of these products provide enough incentives for end-consumers to verify them before making payment.

##### B. System Design

###### 1) The anti-counterfeiting mechanism

The proposed system performs anti-counterfeiting by maintaining supply chain integrity, the significance of which is twofold. Firstly, the transaction path of a product is clear and its source can be traced accordingly; secondly, product authenticity can be validated.

The pedigree of a product is generated by its transaction

records along the supply chain, which may be retrieved from the host company server through RFID readers and the Internet. With the growing popularity of Internet connection through phone networks and RFID-enabled cell phones coming into market place, the system allows consumers to check the pedigrees of the products they are purchasing.

This mechanism hinders counterfeiters from cloning the products or the tags because of three reasons: 1. Companies have to pre-register before they can access the host company server to record product transactions, and thus excluding counterfeiters from attempting to do so; 2. Suspicious transactions would be screened out accordingly; 3. Consumers will refuse to purchase products without a plausible history.

To customers, making sure that the products are genuine protects their own safety and guarantees value for money. There are indeed sufficient incentives for them to verify product authenticity, given a convenient-enough way to do so. Similarly, since products without a plausible history may not be saleable to end-users or to the next carriers, the current carriers have a stake in recording transactions. In anticipation of the enhanced customer confidence, it would be justifiable for the product producer to host the system. The product producer, who is also the server-hosting company, is responsible for tracking suspicious transactions and tracing through the sources of security breaches in the various supply chains as the product items move along.

###### 2) System Overview

The anti-counterfeiting system can be accessed through the Internet. It is divided into three layers – the Application Server layer, the Data Management layer, and the Client layer. The Application Server layer provides client access to the business logic and user interfaces. The Data Management layer is comprised of the database itself and its database management system. The Client layer can be accessed through the Hyper Text Transfer Protocol (http) or through the Simple Object Access Protocol (SOAP).

On the Data Management layer, the database is the heart of the anti-counterfeiting system. It consists of tables that record the pedigree information, including the company information, the product information, the transaction records, and other system operation information. The database management system updates and retrieves information from these tables according to the instructions given by the Application Server layer, thus integrating the supply chain data systematically and logically to form the product pedigree.

The Application Server layer is where the business logic of the anti-counterfeiting system is stored and executed. The business logic is mainly composed of PHP pages. The server-side PHP scripts are accompanied by the client-side JavaScript codes to perform the operations of the anti-counterfeiting system. A built-in PHP extension is used to access the data stored in the MySQL database in the Data Management layer. HTTP and SOAP are utilized to publish the contents generated by the anti-counterfeiting system. These contents are transferred to the Client layer for users to make

business decisions.

For the Client layer, where a user loads an interface from the Application Server layer to operate a system and to make business decisions, the Hyper-text Mark-up Language (HTML) pages are enhanced by Cascading Style Sheets (CSS) to improve the user-friendliness of the system. The user instructs the Application Server to perform the business logic through the Client layer. The results are transferred to and displayed on the user interface at the Client layer.

Such client-side instructions can also be made through the SOAP. The SOAP communications can be made machine-to-machine without human intervention to suit the fast-moving nature of the supply chain, which is also the reason of employing RFID in the track-and-trace system. This part of the system does not need a user interface, and the associated decisions can be made automatically by the machines.

The Application Server layer is connected to the Data Management layer over a Local Area Network (LAN), where the Application Server interfaces with the Client layer through the Internet. The Application Server layer must be separated from the Data Management layer with a firewall in the middle to protect the latter from outside attacks. An overview of the architecture is depicted in Fig 1.

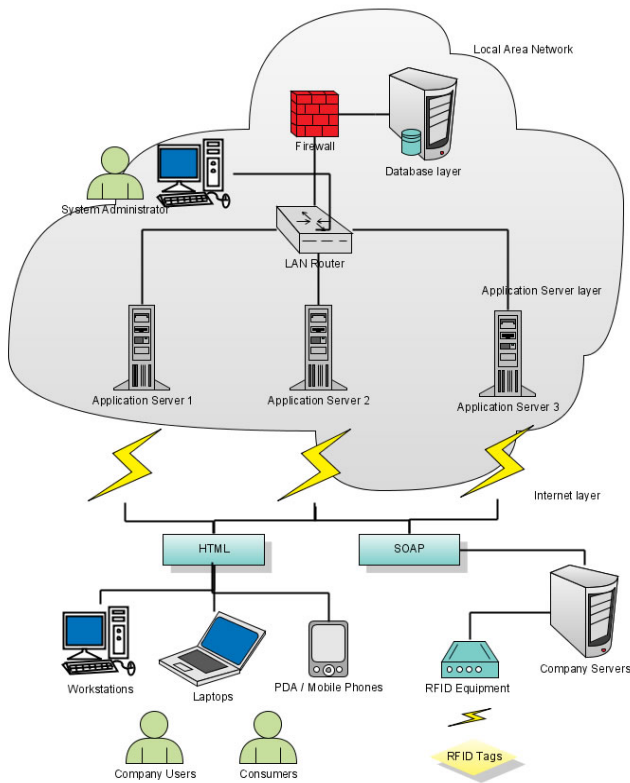


Fig. 1 The overall system architecture

3) System architecture

A system structure flow chart of the anti-counterfeiting system is shown in Fig. 2. The system comprises four servers – the Information Server, the Authentication Server, the Pedigree Server, and the Records Server. The first three servers together

form the Application Server layer, while the Records Server itself is the Data Management layer.

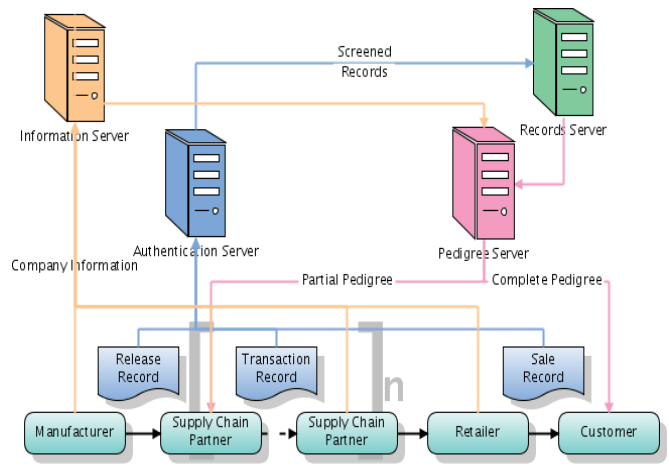


Fig.2 System structure flowchart

The system servers are divided according to the decision activities described in the business process analysis. The Information Server is responsible for information gathering, the Authentication Server for pedigree building, the Pedigree Server for pedigree retrieval, while the Records Server is responsible the system administration.

The Information Server is responsible for collecting company information from the supply chain partners. The information is crucial for the product pedigrees because they form the geographical picture of the product history; it also forms the basis for tracing problems when suspected counterfeits emerge. The information should be pre-registered by the supply chain partners and verified by the host company before the first transaction record was sent to the Authentication Server.

As the products move along the supply chain, each supply chain partner should record each transaction accordingly. The products are identified by the embedded RFID tags. Each tag contains a unique tag ID. It can be read by the RFID readers installed at the partners' sites, supposedly connected to the Internet through a Personal Computer (PC). The tag ID forms the basis of a transaction record, which is sent to the Authentication Server. The Authentication Server verifies the Transaction Records and screens out suspicious activities. The screened records are then sent to the Record Server for storage.

The supply chain partners can verify the partial product pedigree from the point of manufacturing to the previous owners by making requests to the Pedigree Server, which in turn retrieves transaction records from the Records Server as well as company information from the Information Server to generate the required pedigree. They should reject any products with a suspicious partial pedigree.

The Pedigree Server is also responsible for generating complete product pedigrees, through the Internet and the mobile phone network, to end-consumers for verification. When a customer is satisfied that a product is genuine and has

paid for it, the retailer should generate a sale record, which is subsequently sent to the Authentication Server. Any further transactions of the same product after the sale record are deemed suspicious.

C. Individual server structure

1) Information Server

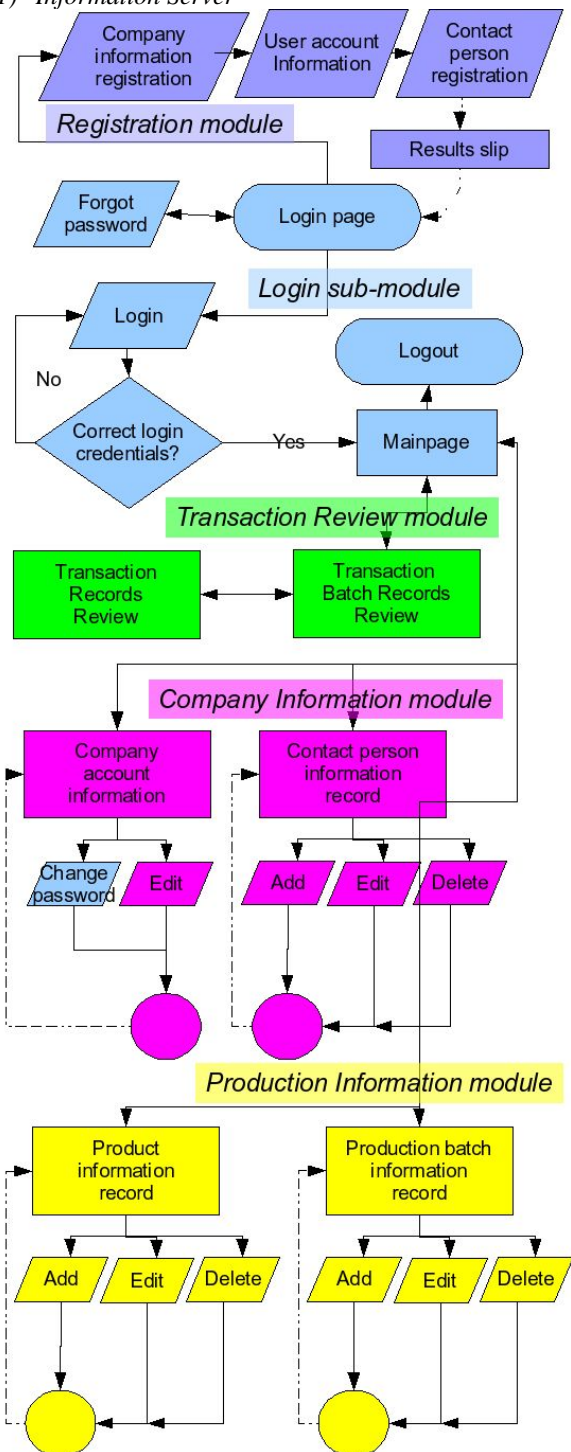


Fig. 3 System structure flowchart of Information Server

Fig. 3 shows the system flow of the Information Server, which consists of five modules – the Registration module, the

Company Information module, the Contact Person module, the Product Information module and the Transaction Review module, plus one sub-module, the Login sub-module, which are represented in five different colours in the figure.

The Registration Module allows a user to access without logging into the system. The user starts with a page to register the information of a company. After filling in the form and submitted it successfully, the user will be redirected to a page with a form that requires the user to enter the information of a contact person. Each company account registration must be accompanied by at least one contact person. Finally the system displays a page that shows the registration result. The company account is not activated until the registration is verified by a system administrator. The system will display a page that shows the summary of registration.

Upon successful account verification, the system administrator will activate the account and the user will be allowed to login to the system. The Login module is responsible for verifying user logins. Logged on users can access the other four modules. The user can edit the company information in the Company Information module, and can manage the list of contact persons in the Contact Person module. The user can add, edit or delete the contact person records but at least one must remain for each company account.

The manufacturers can register new product types and production batches through the Product Information module, which are required before they can update Transaction Records to the system. It is reasonable enough to allow only activated account users to register these two types of information only because only verified manufacturers can start the pedigree update process.

The company users can also review the transaction batches and transaction records they have updated to the Authentication Server from the Transaction Review module. In this module the user can only review the record details but cannot add, modify or delete them because the only way for the company users to interact transaction related records with the system is through the Authentication Server.

2) Authentication Server

The Authentication Server handles the pedigree update requests, as shown in Fig. 4. Before receiving the transaction records, the Authentication Server verifies the status of the company making the SOAP request. If the company account is not in active status, the system will reject the request. The Authentication Server performs basically three kinds of checks to verify the authenticity of these requests. Each of these three checks consists of a series of procedures.

Chain level refers to the order of ownership of a product. Each time when a product is transferred from one company to another, the chain level is incremented by one. The Chain Level Check basically checks two characteristics of the incoming pedigree update request. The first point is whether the current record being handled is transferred from the right previous owner. If the transfer of ownership does not make sense, it is deemed to have violated the records stored in the server,

meaning that an adversary might have been attempting to counterfeit. The second point is whether the current record duplicates another record of the similar kind. Duplicated records lead to suspicions that an adversary may have been trying to clone the product and the tag.

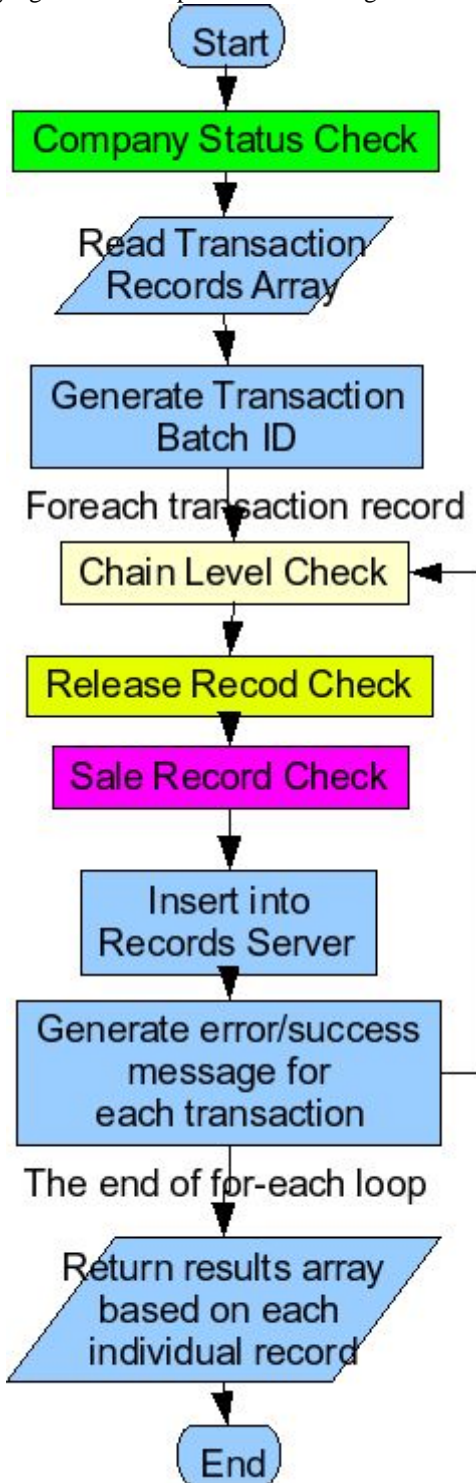


Fig. 4 System structure flowchart of the Authentication Server

The Release Record Check basically checks if the current record being handled originates from an authentic source. Since

all manufacturers issue a “Release Record” (which is indeed a birth certificate) for each product to the anti-counterfeiting system, any product item that goes through the supply chain without a valid Release Record shall be marked suspicious.

When the items are sold, the retailers will update a Sale Record to the system. Therefore, for those that are under transit between the supply chain nodes, which are not supposed to be sold already, should contain no Sale Records from the system. The Sale Record Check marks these after-sale Transaction Records suspicious.

3) Pedigree Server

The Pedigree Server responds to the pedigree requests of pedigree retrievers, the processes of handling such requests are shown from Fig. 5.

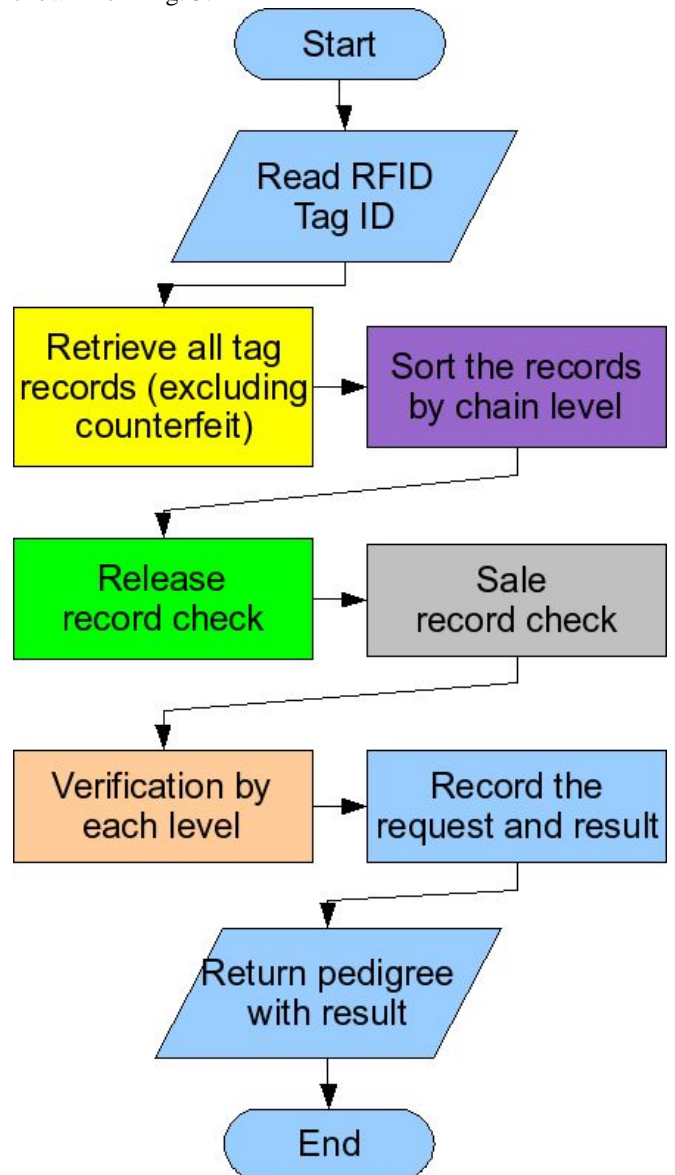


Fig. 5 System structure flowchart of the Pedigree Server

The Pedigree Server retrieves all the relevant records of a product item from the database, and then sorts these records by

the chain level. The records that are marked as “counterfeit” are excluded from retrieval because they play no part in building up the product pedigree. However, those suspicious transaction records are still presented to the pedigree retriever because some of them might still be a part of the authentic product pedigree.

The server then checks if there are a release record and a sale record for the product, which are similar to that performed in the Authentication Server. If either the product item being handled does not originate from the authentic manufacturer, or it is supposed to have been sold already, the Pedigree Server will mark the pedigree suspicious.

Although the pedigree is basically built up with all the records sorted by the chain level, it does not imply that the pedigree is reliable because some of these records might not be authentic. The Pedigree Server checks each of the chain levels and determines if there is a coherent path of non-suspicious transaction along the supply chain for the current product. The request and the result of verification will be recorded into the database.

Apart from logically forming a product pedigree from the retrieved records and return it to the requester, the Pedigree Server also informs the requester of whether the pedigree is reliable or not. When a pedigree retriever (supply chain node companies or customer) receives the response, two simple logics will be used to verify the pedigree. Firstly, if the pedigree is marked as “unreliable” by the Pedigree Server, it means that the product they are currently handling is not reliable and they should refuse to accept it. If the pedigree is reliable, then the retriever should verify the last owner recorded in the pedigree. If they find that the party selling them the product is different from the last owner in the pedigree, the product might also be a counterfeit and should be rejected.

Apart from handling the automatic machine-to-machine SOAP requests, the Pedigree Server also handles manual web interface through HTTP. The system flow of handling these requests is basically the same as mentioned above.

4) Records Server

a) Database structure

Fig. 6 shows the Database structure of the Records Server, which stores the system data in three different databases. This arrangement is solely for the purpose of better categorization and all these data are physically stored in the same machine. It is a relational database and the tables are properly related to avoid confusion and for faster retrieval of data.

The contents and the roles of these databases are discussed below:

(1) The Information database

The Information Database records the company-related information that is not directly used to build up a product pedigree. It consists on four tables, which are listed in the following:

- Company table

- Contact Person table
- Product Type table
- Production Batch table

The kinds of data recorded are basically of once-and-for-all type, which means that the supply chain node companies are only required to register once initially and the data will be reused throughout the product life cycle.

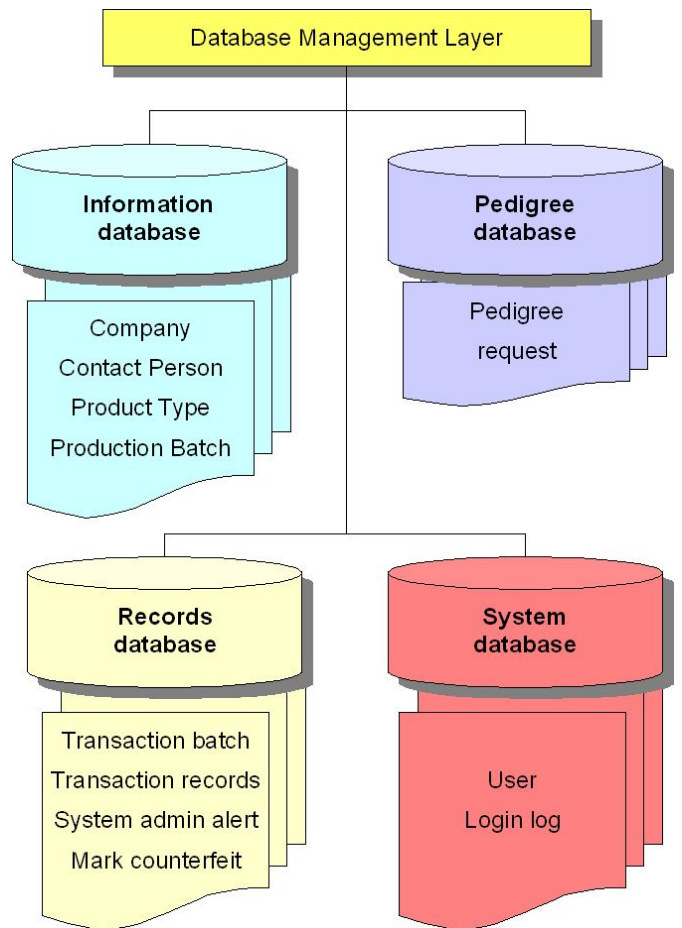


Fig. 6 Database structure diagram of the Records Server

When the supply chain node companies register their information and the first contact person to the system, the information will be stored into the Company table and the Contact Person table respectively. After the company account has been activated, the company can register more contact persons into the Contact Person table, and can also register new product types and production batches into the Product Type table and Production Batch table respectively.

(2) The Pedigree database

The Pedigree database consists of a single table to record all the requests made to the Pedigree Server. The data recorded include the tag ID being requested, the time of request, source IP of requester as well as the result of verification. These data also serve the purpose of problem-tracing.

(3) The Records database

The Records database stores the data that are directly used to produce a product pedigree. There are two tables in it, namely the Transaction Batch table and the Transaction Record table. Since the pedigree updater is expected to update a bunch of items at one time to the system, the “Transaction Batch” concept is introduced to group these transaction records.

Grouping these records into batches enables a more convenient way of problem tracing. Since the pedigree updaters usually process one type of product at a time, if any problems arise, the system administrator can review and manage these records in groups instead of one by one.

This is the database where the Pedigree Server retrieves transaction records from.

(4) The System database

Both the pedigree updaters and the system administrators would have to login the system to perform their business processes. Therefore the system needs a database to manage logins.

In the System database, there is a User table to manage all the system accounts and their privileges in the system. Another login-log table is used to record user logins.

b) System Administration Portal

Fig. 7 shows the flowchart of the System Administration Portal of the Records Server, which provides an interface for the System Administrators to perform the necessary operations. In terms of the anti-counterfeiting mechanism, the system administrators make use of this model to resolve transaction ties and to authorize newly registered companies and production information. There are four modules and one sub-module for the system administrators to manage the system, which is introduced below.

(1) Transaction Management module

Although the Authentication Server is capable of marking unreliable or suspicious transactions under most circumstances, human decision making may be needed to solve some system-undeterminable cases. The transaction record management module provides an interface for the system administrators to review these undetermined records and solve the ties by changing the status of these records; the final decision and the operation of the system administrator will also be recorded into the Records Server through this module.

As the Records Server stores a large number of transaction records, this module also provides an interface for the system administrators to review these records according to different filters and criteria.

(2) Company Information module

This module provides an interface for the system administrator to review the newly registered company information record. The system shows a list of unauthorized company records, from which the system administrator can

choose to review individually and issue a system account for each of these companies. The company users are then allowed to access the system to update transaction records.

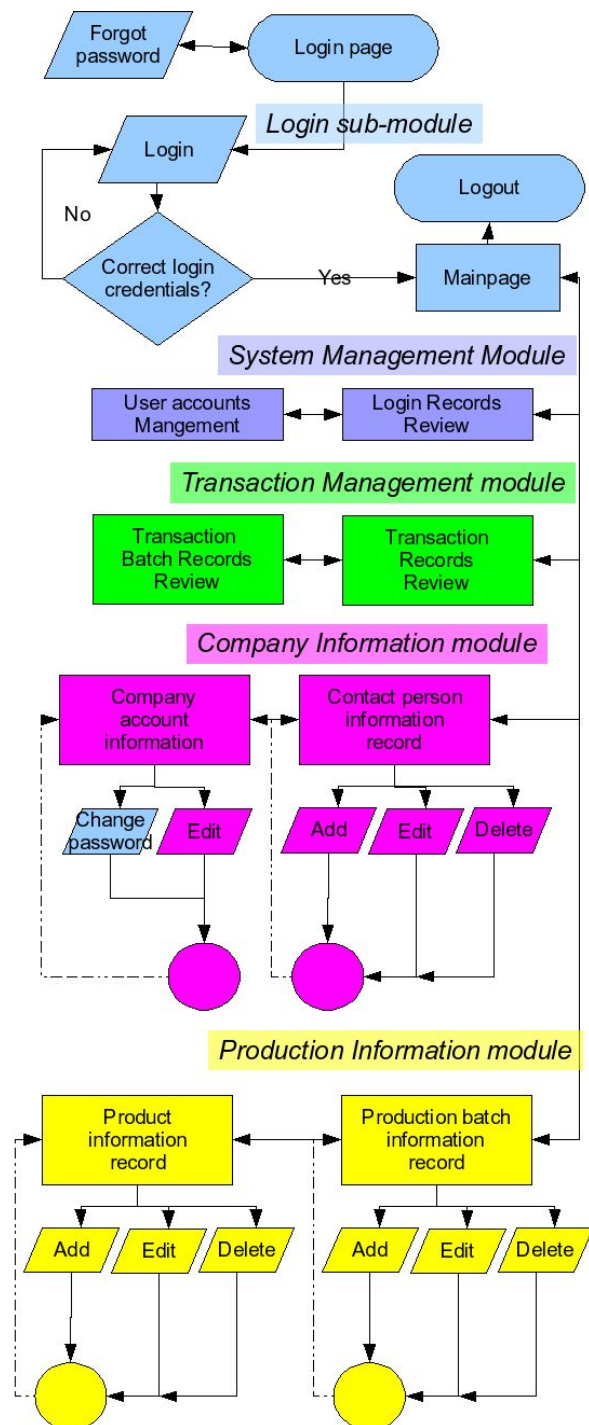


Fig. 7 System structure flowchart of the System Administration Portal

Apart from account issuing and authorization, this module also provides a management console of these accounts. The account details can be edited, and the related contact person, product type, production batch, transaction batch and

transaction records of a single company can be retrieved from here.

(3) Production Information module

Authorized company account users are allowed to register new product type records and production batch records on their own. This module provides a user interface for the system administrator to manage these production-related information records.

(4) System Administration module

This module provides an interface for the System Administrators to manage the registered user accounts as well as the login log of the system.

#### D. SOAP interface design

The pedigree updaters and retrievers communicate with the system in the Remote Procedure Call (RPC) pattern, in which the clients (the updaters and retrievers) send a request message to the server, and the server responds with a message. The information exchange between the clients and the system servers through the SOAP interface will be discussed in the following sections.

##### 1) Authentication Server

The SOAP client of the pedigree updater sends a complete transaction record, including data like the tag ID, production batch ID, transaction time, chain level, type of transaction and previous owner. The number of records for each request is unlimited. Each request corresponds to a transaction batch; the authentication generates a unique transaction batch ID for each request and it also generates a unique transaction record ID for each record. The SOAP server then responds to the client with the generated transaction batch ID, the transaction ID of each product item together with the results of authentication.

##### 2) Pedigree Server

The SOAP client of the pedigree retriever sends a request with a tag ID to the SOAP server. The server then responds with a product pedigree, containing all the transaction records related to that tag ID. The SOAP response also includes a note on whether the retrieved product pedigree is reliable or not.

#### E. System Operation

##### 1) The product flow

As the products move along the supply chain, the system operations are detailed as follow.

###### a) Manufacturers

For both in-house and third-party manufacturers, they are required to generate a Release Record to the Authentication Server before their products can be transferred to the next owner. The Release Record contains the tag ID, the product type, the timestamp of release, as well as the "Chain Level",

which is set to 1 in the Release Record. Its use will be explained in the next section.

The manufacturers also pre-register its company information to the Information Server. The pre-registered information includes the company title, its location, and the product types that they are manufacturing.

This is the first record of the product pedigree. The Release Record serves the purpose of certifying the root source of the product item, which assures the following owners in the supply chain that they are receiving genuine products from the right manufacturer.

###### b) Supply Chain Partners

Upon receiving the product, the supply chain partners should request the partial product pedigree which records the transactions of the item since it was released from the manufacturers. They should only receive products with a plausible history. For suspicious products, they should reject or return to the previous owner, and report to the host company.

The product pedigree must satisfy the following conditions so that a product is considered genuine.

1. *There exists a record of release for the product*
2. *There exists no record of sales for the product*
3. *The recorded previous owner is the party that is selling the product*

After verifying and accepting the product items, the company continues to process the items for value-adding activities. Before the items leave the company, they will have to go through the RFID reader again. There are two jobs for the reader. Firstly, it reads the Chain of Level information (k) from the tag, does an increment (k+1), and then writes it back. Secondly, the reader reads the Product ID (Tag ID) for each product, and together with the Partner ID, the timestamp, and the new Chain Level (k+1), to form a pedigree entry for each item which is sent to the Authentication Server. The pedigree entries from the supply chain partners accumulate to form the complete product pedigree.

###### c) Retailer

Upon receiving the products, the retailer should verify the product pedigrees in the same way described above. The retailer holds a stake in so doing because when the end-consumers find what they have purchased is a counterfeit, its goodwill and reputation would be damaged.

When the end-consumer has paid for a product, the retailer should update the chain level information in the tag by 1 (from n-1 to n), and mark it "sold". The Product ID (Tag ID), the Retailer ID, the timestamp of sale, and the updated chain level (n) together form the sale record, which is sent to the Authentication Server. Any further sale attempts or transactions of supposed-to-be-sold products are deemed suspicious.

###### d) End-Consumers

In order to protect their own stake, customers should verify the pedigrees of the products they want to purchase before making the payment. This can be done by reading the Product

ID (Tag ID) through a handheld RFID device. With RFID-enabled mobile phones are coming to the market [2], and improved Internet connectivity for the mobile networks, this method has the potential to be popular in the foreseeable future. The verification criteria are similar to the above. This allows the customers to verify the product pedigrees by themselves, instead of relying on the retailers.

### 2) *The Authentication Server*

The Release Record, all the Transaction Records as well as the Sales Record must go through the Authentication Server. Therefore, by interacting with the Information Server and the Records Server, the Authentication Server performs an important function in spotting suspicious transactions. It verifies the Transaction Records going through it by spotting for the following items:

1. *Duplicate sales record / transactions after sale*
2. *Duplicate transaction records at the same chain level*
3. *Unreasonable transfer of ownership*

It is not necessary for the Authentication Server to carry out a certain set of activities or to give immediate response on all suspicious activities. Rather, different thresholds can be set for different products for different companies. Based on this information, the host company can set a certain course of actions for different situations to suit their own needs.

## V. CONCLUSION

Counterfeiting poses a great threat to the global economy. It inflicts direct losses to product originators, reduces job opportunities and tax revenues in local economies, discourages investment on research and development, and threatens consumer safety. With the global nature of modern supply chains, it has never been easy to cope with counterfeiters.

Originators of different products around the world have indeed adopted various anti-counterfeiting solutions. However, these solutions do not avail automatic verification of product authenticity. Although product verification along supply chains enhances supply chain integrity, the high cost and the long period of time used outweigh the benefits it may bring about.

RFID has emerged as a promising solution to anti-counterfeiting because of its wireless communication abilities. RFID tags can be read at a distance in large quantities within a relatively short period of time. When products are embedded with RFID tags, mass authentication along the supply chain at item levels becomes possible, and the cost of maintaining the integrity of supply chains would be significantly reduced.

RFID brings about huge potential in enhancing supply chain efficiency, particularly as the Gen-2 standard is expected to be widely adopted in the near future. With a common standard, it would be viable to install an RFID system along the supply chain to enhance efficiency and integrity.

Although RFID is subject to a number of threats and it cannot provide perfect security, it is technically feasible and financially justifiable to integrate RFID with the Internet for

anti-counterfeiting, particularly with consumer participation in the automatic product authenticity verification process.

There have been different approaches proposed for the application of RFID in anti-counterfeiting. Some of them require non-standard, expensive, and secure RFID tags. Although they provide a sound level of security, the high costs and the compliance problem become a barrier for them to be widely adopted in anti-counterfeiting.

The RFID-based anti-counterfeiting system of this research utilizes the track-and-trace approach. It requires the supply chain partners to record all the transactions of a product along the supply chain, which forms a pedigree for the product. Consumers can verify the product authenticity at sale points. This system is characterized by customer participation in verification of product authenticity. Indeed, consumer power provides the ultimate source of incentives for the supply chain partners to maintain supply chain integrity.

The system is simple in architecture. It does not require much sophisticated and expensive technologies, making it relatively easy to implement. The simple system structure and hardware requirements make it cost-effective for companies to host the system. The system can be tailored to suit specific needs of individual companies, saving money on unnecessary functions. In particular, the product pedigrees stored in the system facilitate real-time tracking of problems and further investigations into suspicious activities. As such, a company can afford to host an anti-counterfeiting system without the need to disclose sensitive information to any third parties.

## VI. SUGGESTIONS FOR FUTURE WORK

There are some possible extensions and improvements for future development of the system. These include:

### A. *Interface user-friendliness*

The user interface of both the Information Server and the System Administration Portal can be improved by allowing the user to customize various components and modules. Such flexibility allows the user to perform the anti-counterfeiting related functions in an easier manner.

### B. *Operations logic of the Authentication Server*

In this research, a basic framework on how the system should filter out suspicious activities has been developed. However, the logics behind SOAP request of the Authentication Server are not optimized, and this may lead to unnecessarily long processing of each transaction record. In the future, the logics can be optimized to reduce the processing time and better logic can be developed to reduce the number of cases that require system administrators' decisions. More data fields in different tables might have to be added.

### C. *System administrator logics*

In the anti-counterfeiting system, the administrators are only informed of the system-undeterminable cases, and they are expected to solve these cases by retrieving the related information by themselves. The system can be improved by displaying the related information in a logical way that assists

the system administrator in making decisions. Although the system cannot make a final decision, it can still give suggestions on the unsolved cases.

#### D. Production information suspension mechanism

The system administrators can suspend the company accounts, product types and production batches so as to prevent further related transaction records to be registered. The system administrators make the decision of suspending such records based on memory and experience. The system can be improved by incorporating a mechanism to mark these records as counterfeits. For example, if the system finds that a certain company is constantly registering suspicious transaction records to a certain thresholds, or the transaction records of a certain product are often found to be counterfeit, the system may automatically suspend the company or the product.

#### E. Optimization of data structure

The database of the current system is developed based on the business process analysis as well as the requirements of the user. However, they are not structured in an efficient manner. Future work may include optimizing the database structure to improve the operation capacity of the database management system.

#### F. System operation logging

The system administrators have the final rights to decide on whether a product type should be suspended or a transaction record should be marked as counterfeit. However, such operations are not logged by the system and there will be no way to find the original status of a record in a specified time. Therefore, the system can be improved by adding a logging module to log all changes made to the datasets.

#### G. Error or exceptions handling

The errors and exceptions do not refer to the scripting level problems, but the ignorant and neglectful behaviours of the supply chain node companies. The future development of the system should take these situations into consideration.

#### H. Standard-compliant tag authentication

The operation of filtering out suspicious activities by the Authentication Server can be assisted by ensuring that the tags are reliable to communicate; as such, incompatible tags will be automatically filtered out. The system can be improved by incorporating simple tag-reader authentication mechanisms that are Gen-2 compliant.

- [5] United States Food and Drug Administration, COMPLIANCE POLICY GUIDE 160.900 Prescription Drug Marketing Act – Pedigree Requirements under 21 CFR Part 203. 2006.
- [6] Sparkes, M., Gambling on chips, in IET Manufacturing Engineer. 2006. p. 10-11.
- [7] Thompson, D.R., N. Chaudhry, and C.W. Thompson, RFID security threat model, in Conference on Applied Research in Information Technology. 2006: Conway, Arkansas.
- [8] Rieback, M.R., B. Crispo, and A.S. Tanenbaum. Is Your Cat Infected with a Computer Virus? in Fourth IEEE International Conference on Pervasive Computing and Communications 2006.
- [9] Bono, S.C., et al. Security Analysis of a Cryptographically-Enabled RFID Device. in 14th USENIX Security Symposium. 2005. Baltimore, Maryland, USA: USENIX Association.
- [10] Kfir, Z. and A. Wool. Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems. in 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks. 2005.
- [11] Sarma, S.E., S.A. Weis, and D.W. Engels. RFID Systems and Security and Privacy Implications. in Workshop on Cryptographic Hardware and Embedded Systems (CHES), LNCS 2523. 2003. Springer-Verlag Berlin.
- [12] TransportGistics, I. SUPPLY CHAIN INTEGRITY, A Basis to Upset Gray Market Distribution. 2004 [cited 2006/02/10]; Available from: [http://www.insourceaudit.com/WhitePapers/supply\\_chain\\_integrity.asp](http://www.insourceaudit.com/WhitePapers/supply_chain_integrity.asp).
- [13] Johnston, R.G., Ph.D., CPP, An Anti-Counterfeiting Strategy Using Numeric Tokens. International Journal of Pharmaceutical Medicine 2005. 19(3): p. 163-171.
- [14] Brock, D.L., White Paper: The Electronic Product Code (EPC). A Naming Scheme for Physical Objects 2001, Auto-ID Labs, Massachusetts Institute of Technology.
- [15] EPCglobal Inc., Class 1 Generation 2 UHF Air Interface Protocol Standard Version 1.0.9: "Gen 2". 2005.
- [16] EPCglobal Inc. EPCglobal Homepage. 2006 [cited 2006/12/17]; Available from: <http://www.epcglobalinc.org/home>.
- [17] Duc, D.N., et al. Enhancing Security of EPCglobal Gen-2 RFID Tag against Traceability and Cloning. in The 2006 Symposium on Cryptography and Information Security. 2006. Hiroshima, Japan.
- [18] Juels, A. Strengthening EPC Tags Against Cloning. in ACM Workshop on Wireless Security (WiSe). 2005.
- [19] Lehtonen, M., et al., From Identification to Authentication – A Review of RFID Product Authentication Techniques, in Workshop on RFID Security 2006. 2006, Institute for Applied Information Processing and Communications, Graz University of Technology: Graz.
- [20] Koh, R., et al., White Paper: Securing the Pharmaceutical Supply Chain. 2003, AUTO-ID CENTER, Massachusetts Institute of Technology.
- [21] Staake, T., F. Thiessen, and E. Fleisch. Extending the EPC Network – The Potential of RFID in Anti-Counterfeiting. in ACM Symposium on Applied Computing. 2005. Santa Fe, New Mexico.
- [22] Kim, J. and H. Kim. Anti-Counterfeiting Solution Employing Mobile RFID Environment. in TRANSACTIONS ON ENGINEERING, COMPUTING AND TECHNOLOGY. 2005. Budapest, Hungary.
- [23] Kim, J. and H. Kim. A Wireless Service for Product Authentication in mobile RFID environment. in 1st International Symposium on Wireless Pervasive Computing, 2006. 2006.
- [24] Fabian, B., O. Günther, and S. Spiekermann., Security Analysis of the Object Name Service for RFID. Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2005.

#### REFERENCES

- [1] International Chamber of Commerce Commercial Crime Services, International Guide to IP Rights Enforcement First Edition 2006. 2006, International Chamber of Commerce Counterfeiting Intelligence Bureau.
- [2] RFID Journal. Nokia Unveils RFID Phone Reader. 2004 [cited 2006; Available at <http://www.rfidjournal.com/article/articleview/834/1/13/>].
- [3] United States Food and Drug Administration, COMBATING COUNTERFEIT DRUGS - A Report of the Food and Drug Administration. 2004, U.S. Food and Drug Administration: Rockville, Maryland 20857.
- [4] Editors, FDA Will Begin Enforcing Anti-Counterfeiting Law In December, in Medical News Today. 2006.