Hardware-Enabled Pharmaceutical Supply Chain Security

KUN YANG, HAOTING SHEN, DOMENIC FORTE, SWARUP BHUNIA, and MARK TEHRANIPOOR, University of Florida

The pharmaceutical supply chain is the pathway through which prescription and over-the-counter (OTC) drugs are delivered from manufacturing sites to patients. Technological innovations, price fluctuations of raw materials, as well as tax, regulatory, and market demands are driving change and making the pharmaceutical supply chain more complex. Traditional supply chain management methods struggle to protect the pharmaceutical supply chain, maintain its integrity, enhance customer confidence, and aid regulators in tracking medicines. To develop effective measures that secure the pharmaceutical supply chain, it is important that the community is aware of the state-of-the-art capabilities available to the supply chain owners and participants. In this article, we will be presenting a survey of existing hardware-enabled pharmaceutical supply chain security schemes and their limitations. We also highlight the current challenges and point out future research directions. This survey should be of interest to government agencies, pharmaceutical companies, hospitals and pharmacies, and all others involved in the provenance and authenticity of medicines and the integrity of the pharmaceutical supply chain.

CCS Concepts: • **Security and privacy → Hardware security implementation**;

Additional Key Words and Phrases: Pharmaceutical supply chain, security, privacy, traceability, authentication

ACM Reference format:
Kun Yang, Haoting Shen, Domenic Forte, Swarup Bhunia, and Mark Tehranipoor. 2017. Hardware-Enabled Pharmaceutical Supply Chain Security. *ACM Trans. Des. Autom. Electron. Syst.* 23, 2, Article 23 (December 2017), 26 pages.
https://doi.org/10.1145/3144532

1 INTRODUCTION

The pharmaceutical supply chain, which spans many geographical regions and involves numerous parties, is the pathway through which prescription and over-the-counter (OTC) drugs are delivered from manufacturing sites to patients. GlobalData predicts that the estimated value of the US pharmaceutical market will increase from $395.2 billion in 2014 to $548.4 billion by 2020, which represents a compound annual growth rate (CAGR) of 5.6% [26]. The complexity of the pharmaceutical supply chain has correspondingly increased in recent years thanks mainly to the appearance of new drugs, technical advances, more supplies and locations in the chain, and evolving regulatory requirements. Increased complexity of the pharmaceutical supply chain implies

Authors' addresses: K. Yang, H. Shen, D. Forte, S. Bhunia, and M. Tehranipoor, Florida Institute for Cybersecurity Research, University of Florida, 601 Gale Lemerand Dr., P.O. Box 116550, Gainesville, FL 32611; emails: {k.yang, htshen, dforte, swarup, tehranipoor}@ufl.edu.

https://doi.org/10.1145/3144532

increased difficulty in maintaining its security. Today's pharmaceutical supply chain suffers from three major challenges: (i) theft of authentic medicines; (ii) appearance of counterfeit medicines; and (iii) contamination of medicines during manufacturing, storage, or distribution. These issues not only adversely impact the economic benefits and reputations of pharmaceutical manufacturers, distributors, and retailers, but also jeopardize patient safety and public health. In 2013, the average loss per pharmaceutical theft incident was $261,819 [34].

Theft and/or diversion of pharmaceutical products pose severe threats to public health because provenance and authenticity are difficult to verify for products that leave—and are later reintroduced to—the legitimate supply chain. A counterfeit drug is a pharmaceutical product that has been deliberately manufactured and sold with the intent to fraudulently represent its source, authenticity, or efficacy [52]. A counterfeit drug may contain none or an inappropriate dosage of active ingredients, may be improperly processed within the body, may contain constituents that are not on the label (which may or may not be harmful), or may be supplied with inaccurate or fake packaging and labeling. Counterfeit drugs yielded an estimated revenue of $75 billion in 2010 alone according to the National Association of Boards of Pharmacy [25]. The 2008 case of the counterfeit blood thinner heparin is one example of tragedies caused by counterfeit drugs in the United States [79]. In this case, the active ingredient in heparin was replaced with a cheaper counterfeit substitute, causing a series of adverse reactions and a nationwide range of recalls. The counterfeit drugs were eventually suspected to be the cause of as many as 81 deaths. In addition, contamination of medications leads to grave consequences. Medicine contamination refers to the introduction of an unwanted constituent, contaminant, or impurity to pharmaceuticals during manufacturing, packaging, storage, or distribution. During late January 2012, tainted cardiac medicines killed more than 200 people in Pakistan and sickened around 1000 [57].

The integrity of the pharmaceutical supply chain may be compromised intentionally by economically motivated adversaries or inadvertently by ignorant employees. Pharmaceuticals originate from raw material suppliers; are manufactured in pharmaceutical factories; transferred to wholesalers; stocked at different types of pharmacies (e.g., retail, mail-order, etc.); susceptible to price fluctuations and processed by pharmacy benefit management companies (PBMs) according to quality and utilization management screens; dispensed by pharmacies; and eventually delivered to and taken by patients. Every abovementioned supply chain stage is vulnerable to adversarial activities. Unscrupulous suppliers may sell fake, inferior, spoiled, adulterated, or contaminated raw materials to pharmaceutical manufacturers. Illicit pharmaceutical manufacturers may replace active ingredients with cheaper counterfeit substitutes; change quantities of active ingredients (usually reducing the dose to lower the cost); knowingly or unknowingly use fake, inferior, spoiled, or contaminated raw materials; or mislabel finished drugs. Rogue distributors may mix genuine drugs with counterfeit ones. Dishonest pharmacies may purchase medications from illegal channels and dispense them to patients. Expired medications may continue to be dispensed by dishonest pharmacies. Illicit online pharmacies have the opportunity to sell counterfeit drugs massively, directly to patients, bypassing all highly regulated distribution channels. Some countries have a legalized online drug trade, sometimes even including prescription drugs, which adds difficulty to fighting the battle against the distribution of counterfeit drugs through the Internet [50]. From 2010 to 2014, Interpol's Operation Pangea shut down 57,000 illegal online pharmacies and seized over 30.3 million units of counterfeit drugs [75]. Patients could also purchase medications from gray markets themselves to save money, especially for those high-value drugs (e.g., drugs that cure cancer).

Theft may occur at any stage of the pharmaceutical supply chain. Stolen drugs may be later reintroduced to the legitimate supply chain by dishonest supply chain participants. In addition to economically motivated adversarial activities, medications may also lose their effectiveness due to improper storage or handling (e.g., exposure to sunlight, high temperature, and high humidity)

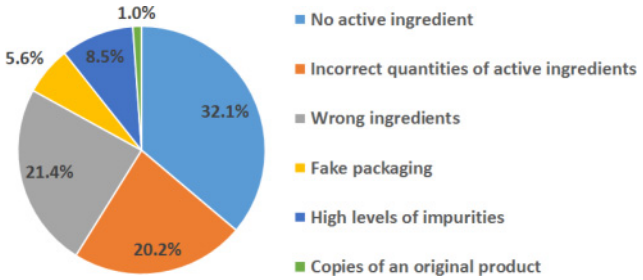

Fig. 1. Percentage distribution of types of identified counterfeit drugs in 2000.

by ignorant employees. Figure 1 illustrates the percentage distribution of types of identified counterfeit drugs according to the World Heath Organization (WHO) statistics collected in 2000 [53]. The top three counterfeit types include counterfeit drugs with no active ingredients, counterfeit drugs containing wrong ingredients, and counterfeit drugs with incorrect quantities of active ingredients. Note that only 1% of identified counterfeit drugs are copies of original products. Most of these counterfeit drugs will be completely ineffective, less effective, or cause severe health issues.

Existing solutions for securing the pharmaceutical supply chain include laws and regulations, track-and-trace techniques, secure packaging, and composition analysis–based authentication. To regulate the pharmaceutical supply chain and protect patients from compromised medicines, a series of laws and regulations have been issued. Two recently implemented regulations include the Food and Drug Administration Safety and Innovation Act (FDASIA) [22] and the Drug Supply Chain Security Act (DSCSA) [21]. By working to understand these regulations, pharmaceutical manufacturers, wholesalers, and dispensers can identify the most appropriate security scheme to protect themselves and their assets against key risks (i.e., counterfeiting, theft, contamination, and so on), while also ensuring regulatory compliance.

To enable dependable visibility into supply chain status, a sequence of track-and-trace techniques have been developed, including barcodes [8], quick response (QR) codes [30], integrated circuit (IC)–based radio frequency identification (RFID) [83], and chipless RFID [88]. To help inspect the integrity of OTC drug products, tamper-evident packaging (e.g., film wrapper, bubble pack, and breakable cap[1]) uses an indicator to imply that tampering has occurred when breached. Introduced by Glaxo in 1989 for its Zantac products, pharmaceutical packaging carrying a holographic image has become a popular approach for assuring consumers of genuineness [15]. The X-ray diffraction (XRD) method recognizes counterfeit drugs by proving the nonexistence of one or more active ingredients and/or particular excipients [44]. Using near-infrared (NIR) spectroscopy for identifying counterfeit drugs has been widely investigated in the past decade [73]. Raman spectroscopy, combined with principle component analysis (PCA), was also proposed to identify counterfeit tablets on the spot without interaction with educated chemists [17]. Quantitative nuclear magnetic resonance (NMR) spectroscopy and diffusion ordered spectroscopy (DOSY) NMR were also proposed to identify and quantify a drug and its related substances as well as to recognize a substandard drug [33]. The authors in [11] proposed to authenticate the contents of packaged medicines using nuclear quadrupole resonance (NQR) spectroscopy. Medicines are authenticated based on the comparison of their measured spectra with references stored within a secure cloud-based database.

In this article, we reflect on the accomplishments and limitations of prior work, highlight the current trends, and discuss future directions for securing the pharmaceutical supply chain. Both generic and hardware-enabled solutions will be investigated. We refer to the approaches

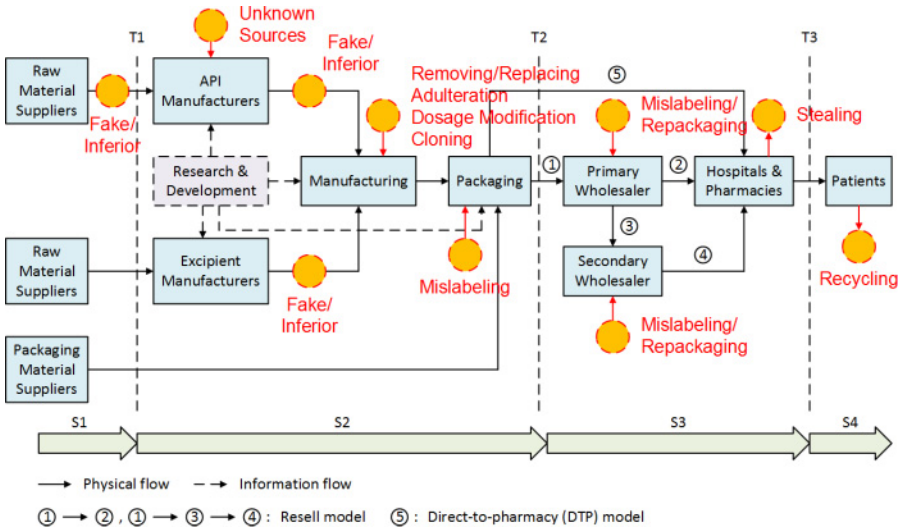

Fig. 2. An overview of the pharmaceutical supply chain.

that integrate electronic components (e.g., RFID tags) or rely on testing facility (e.g., spectrum analyzer) as hardware-enabled solutions.

The remainder of the article is organized as follows: Section 2 describes the framework and properties of the pharmaceutical supply chain and analyzes the risks and vulnerabilities associated with it. We also define the adversarial model in this section. Section 3 and Section 4 discuss existing approaches for securing the pharmaceutical supply chain, categorize them, and compare their advantages and disadvantages. In Section 5, we point out the directions for future research. We present our conclusions in Section 6.

2 PHARMACEUTICAL SUPPLY CHAIN

The pharmaceutical supply chain is analyzed and discussed in this section. First, we describe the framework and properties of the pharmaceutical supply chain and analyze the risks and vulnerabilities associated with it. Next, we define the adversarial model to make preparations for discussion of countermeasures in the next section.

2.1 Framework, Properties, and Risks

We divide the pharmaceutical supply chain into four states (S1, S2, S3, and S4) and there are three state transitions (T1, T2, and T3) between them, as shown in Figure 2. Each state is described in detail in the following.

2.1.1 S1. Raw/Packaging Material Sourcing. The lifecycle of a pharmaceutical product starts from this state, in which active pharmaceutical ingredient (API) [55] manufacturers and excipient [51] manufacturers select raw material suppliers globally and procure raw materials that meet the specifications. Pharmaceutical companies also purchase packaging materials in this state. All incoming materials are sampled and tested in this state per internal requirements of API/excipient manufacturers. The inspection confirms that the raw materials meet the specifications and quality standards that pharmaceutical companies expect from their suppliers upon receipt. Raw-material availability and quality have a significant impact on the capability of a pharmaceutical company to manufacture drugs for the market.

Raw material supply from the main supplier may suddenly discontinue because of various reasons, such as natural disasters, electricity shortage, breakdown of machinery, internal management problems, supplier going out of business, and government restrictions. The first mitigation strategy is to purchase necessary raw materials from secondary suppliers to meet demand. The second mitigation strategy is to maintain large stocks of key raw materials at all times. Raw materials and/or packaging materials may be stolen while in transit or storage. Quality of raw materials belonging to different batches or originated from different suppliers may be inconsistent. Raw materials may be contaminated during manufacturing or while in transit or storage. Unscrupulous suppliers may sell fake, inferior, spoiled, adulterated, or contaminated raw materials to API/excipient manufacturers. Raw materials and packaging materials would subsequently move forward to the next vulnerable state. We denominate this transition T1.

2.1.2 S2. Manufacturing. In this state, raw materials are processed into APIs and excipients, which are further synthesized and packaged into finished drugs. Task processing times of the pharmaceutical manufacturing process are often long and rounded to multiples of shifts. Plenty of inventory is often kept between stages where multistage processes are operated. Before being allowed for downstream use, materials from one intermediate stage must undergo some sort of quality inspection, which will incur additional delays. The manufacturing process for most pharmaceutical products can be divided into two phases: primary API manufacturing (often multistage chemosynthesis or bioprocess) and secondary (formulation) manufacturing [24]. The primary manufacturing phase consists of either a few chemical synthesis and separation steps to create the complex molecules or fermentation, product recovery, and purification in the case of bioprocess. API manufacturing typically comprises a few stages of reactions in which different functional operations are applied to the initial raw materials. We refer to the semifinished products produced after each stage of reaction as intermediates. The final reaction mixture (i.e., mother liquor) undergoes multiple steps of downstream processing to generate the desired active ingredients in solid form. These steps usually include filtration, distillation, precipitation (reactive crystallization), crystallization, drying, and milling [46]. The secondary manufacturing phase adds excipient inert materials to the active ingredients produced at the primary site. The final drugs are produced after further processing (i.e., blending, granulation, drying, compression, tabletting, capsulation, and so on) [70] and packaging.

Raw materials, packaging materials, intermediates, and/or finished drugs may be stolen while in transfer or storage. The quality of finished drugs belonging to different batches or manufactured by different CMOs may be inconsistent. Raw materials, intermediates, and/or finished drugs may be contaminated during manufacturing or while in temporary storage or transfer between stages. Illicit pharmaceutical manufacturers may replace active ingredients with cheaper counterfeit substitutes, change quantities of active ingredients (usually reduce the dosage to lower the cost), knowingly or unknowingly use fake, inferior, spoiled, or contaminated raw materials, or mislabel finished drugs. In addition to economically motivated adversarial activities, medications may also lose their effectiveness due to improper storage or handling (e.g., exposure to sunlight, high temperature, and high humidity) by ignorant employees. Finished drugs would subsequently move forward to the next untrusted state. We denominate this transition T2.

2.1.3 S3. Distribution. In this state, finished drugs are delivered from pharmaceutical manufacturers to patients through different paths. There are two basic distribution models: the traditional asset-based resell model and the recently proposed nonasset-based direct-to-pharmacy (DTP) model [38].

- **Resell model:** In the resell model, as shown in Figure 2, pharmaceutical manufacturers will first sell drug products to primary wholesalers. Primary wholesalers can either directly resell drug products to the final drug dispensers or resell drug products to the secondary wholesalers. The latter will eventually resell drug products to the final drug dispensers.
- **DTP model:** As shown in Figure 2, pharmaceutical manufacturers bypass wholesalers and directly sell drug products to the final drug dispensers.

The secondary wholesale market is believed to be the weakest link in the US drug distribution chain [27]. Security will be improved if the number of transactions in the drug distribution chain can be reduced. The DTP model has some distinct advantages. First, it can increase the efficiency of the supply chain. Second, it is more difficult for counterfeit drugs to enter the supply chain in the DTP model due to enhanced capability to track and control drug products.

Adulterated and counterfeit drugs may be introduced into the US drug distribution chain through importation/reimportation. Pharmaceutical products may be stolen at any intermediate distribution stage and reintroduced into the legitimate supply chain. Drug products that leave the prearranged distribution path are referred to as diverted drugs [27]. It is difficult to verify the quality and integrity of diverted drugs because there are no records indicating their handling or storage conditions. It is also hard to trace their provenance. Wholesale distributors frequently repackage containers of individual batches for final sale or even repackage pharmaceutical products with every sale. Anticounterfeiting measures integrated in the original packaging and labeling may be destroyed by repackaging. Repackaging makes it more difficult to authenticate expired, adulterated, or counterfeit drugs since they can be repackaged in a way that makes them appear to be legitimate products. Legitimate and fake drugs may be mixed by wholesale distributors. This process is called salting [27]. The fake drugs may gain authentic labels through repackaging in the process of salting. Salting may be performed unknowingly. For example, when primary wholesalers purchase pharmaceutical products from other intermediaries, they may accidentally launder fake drugs, package them with authentic labels, and distribute them to pharmacies. In addition to economically motivated adversarial activities, medications may also lose their effectiveness due to improper storage or handling (e.g., exposure to sunlight, high temperature, and high humidity) by ignorant employees. Pharmaceutical products would ultimately move forward to the last vulnerable state. We denominate this transition T3.

2.1.4 S4. Dispensing. Eventually, pharmaceutical products will be dispensed to patients at the point of dispensing (i.e., hospital, clinic, pharmacy, the doctor's office). Counterfeit, contaminated, diverted, or expired medications may continue to be dispensed by dishonest pharmacies, especially for those prescription drugs whose packages are not visible to patients. Patients could also purchase medications from gray markets themselves to save money, especially for those high-value drugs (e.g., drugs that cure cancer). Dispensing errors may lead to fatal consequences [56]. Theft may also occur at the point of dispensing.

2.2 Adversarial Model

Goals of the Adversary. The adversarial goals that we are concerned with here include (i) stealing authentic raw materials, packaging materials, and/or finished drugs from the supply chain; (ii) injecting counterfeit, contaminated, diverted, and/or out-of-date drugs into the supply chain; (iii) recycling unwanted, substandard, and/or expired medications and returning them to the legal supply chain or selling them in the gray market; and (iv) diverting the distribution path of legal pharmaceutical products. The adversaries would try their best to compromise the integrity of the pharmaceutical supply chain to gain economical benefits.

Capabilities of the Adversary. The adversary may perform any of the following actions against the hardware-enabled pharmaceutical supply chain.

- *Removing/Replacing:* The adversary may remove active ingredients of pharmaceutical products or replace them with cheaper counterfeit substitutes.
- *Adulteration:* The adversary may add extra ingredients to pharmaceutical products.
- *Dosage modification:* The adversary may change quantities of active ingredients contained in pharmaceutical products.
- *Mislabeling:* The adversary may misidentify the drug in the container, print improper use instructions on a drug label, or include insufficient or invalid warnings surrounding the use of the drug.
- *Repackaging:* The adversary may compromise anti-counterfeiting features integrated in the original packaging and labeling of pharmaceutical products. Expired, adulterated, or counterfeit drugs may be repackaged expertly enough to appear to be authentic products.
- *Cloning:* The adversary may make copies of original pharmaceutical products.
- *Recycling:* The adversary may recycle unwanted, substandard, and/or expired medications. The adversary may also recycle the packages of authentic drugs.
- *Stealing:* The adversary may steal authentic raw materials, packaging materials, and/or finished drugs from the supply chain.
- *Diverting:* The adversary may modify the distribution path of legal pharmaceutical products.

All kinds of measures may be taken by the adversary to defeat or bypass the defense mechanisms integrated into the pharmaceutical supply chain. Some advanced attacks may be performed with the help of sophisticated equipment. Some adversaries may have the knowledge of pharmaceutical manufacturing and pharmaceutical supply chain management and protection. Rogue employees may have confidential knowledge of the pharmaceutical supply chain, such as distribution paths. Rogue employees may collude with external adversaries to perform attacks for economic gains. Rogue employees in different supply chain parties may also collude with each other.

We assume that the adversary is, however, restricted in two key aspects:

- *No access to the centralized database:* The adversary cannot read or modify data stored in the centralized database. This is a fair assumption since the database is always protected with strong authentication protocols.
- *No authentication apparatus compromising:* The adversary cannot compromise the authorized authentication apparatus (e.g., RFID reader, barcode scanner, smartphone). This is a fair assumption since those authentication apparatuses are usually equipped with advanced protection mechanisms. In addition, the adversary usually does not have physical access to those authentication apparatuses.

3 GENERIC SOLUTIONS

In this section, we investigate the generic solutions for securing the pharmaceutical supply chain. We divide the generic solutions into three categories, as shown in Figure 3, discuss their principles, and compare their advantages and disadvantages.

3.1 Pharmaceutical Supply Chain Regulations

To regulate the pharmaceutical supply chain and protect patients from illegal medicines, a series of laws and regulations have been enacted, as listed in Table 1. Two recently implemented regulations include the Food and Drug Administration Safety and Innovation Act (FDASIA) [22] and the Drug Supply Chain Security Act (DSCSA) [21]. The FDASIA expanded the authority of the FDA

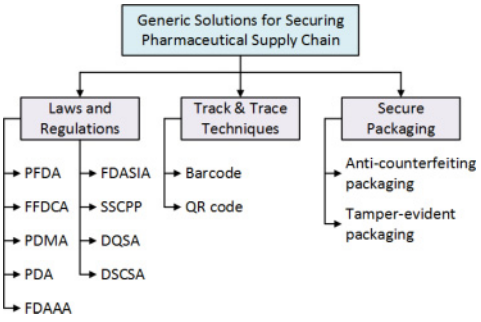

Fig. 3. Taxonomy of generic solutions for securing the pharmaceutical supply chain.

Table 1. Pharmaceutical Supply Chain Regulations

Issue date	Laws, acts, and rules
June 23, 1906	Pure Food and Drug Act (PFDA) [49]
1938	Federal Food, Drug, and Cosmetics Act (FFDCA) [13]
1987	Prescription Drug Marketing Act (PDMA) [48]
1992	Prescription Drug Amendments (PDA) [48]
2003	Florida Paper-Based Pedigree Law [68]
2004	California E-Pedigree Law [31]
Sept 27, 2007	Food and Drug Administration Amendments Act [35]
July 9, 2012	Food and Drug Administration Safety and Innovation Act (FDASIA) [22]
Aug 20, 2013	Secure Supply Chain Pilot Program (SSCPP) [23]
Nov 27, 2013	Drug Quality and Security Act (DQSA) Title II: Drug Supply Chain Security Act (DSCSA) [21]

across manufacturer registration, facility examination and drug importation in 2012 to deal with upstream risks from the supplier of raw materials to the pharmaceutical manufacturer. It allows the FDA to detain an imported drug if its manufacturing facility examination is invalid; increase penalties for suppliers of counterfeit drugs; and require both domestic and foreign facilities to provide a unique manufacturing facility identifier. DSCSA (i.e., Title II of the Drug Quality and Security Act (DQSA)) was issued in 2013 to deal with downstream risks from the pharmaceutical manufacturer to the patient. It enables drug legitimacy verification, enhances illegitimate product detection, and enables more efficient recalls by facilitating the exchange of drug history information. By working to understand these regulations, pharmaceutical manufacturers, wholesalers, and dispensers can identify the most appropriate security scheme to protect themselves and their assets against key risks (i.e., counterfeiting, theft, contamination, and so on), while also ensuring regulatory compliance.

3.2 Generic Track-and-Trace Techniques

A track-and-trace technique is a mass serialization solution for pharmaceutical companies that attach a unique identifier to each packaged drug product, which secures the pharmaceutical supply chain by helping build an accurate drug pedigree (i.e., a record of the chain of product custody as it moves through the supply chain from manufacturer to dispenser) and ensuring that drug products can be easily and correctly identified. Enabling secure and reliable track-and-trace capabilities across diverse touch spots throughout the supply chain is critical for addressing the challenges

Table 2. Comparison Between Different Track-and-Trace Techniques

Metric	Barcode [8]	QR code [30]	IC-based RFID [83]	Chipless RFID [88]
Cost	Low	Low	High	Low
Read range	Short	Short	Long	Long
Read rate	Small	Small	Large	Large
Line of sight	Yes	Yes	No	No
Human capital	High	High	Low	Low
Read/write capability	R	R	R/W	R
Durability	Low	Low	High	High
Security	Low	Low	High	Medium
Event triggering	No	No	Yes	No
Unique identification	No	No	Yes	Yes
Technology	Optical	Optical	RF	RF
Interference	Obstruction	Obstruction	Metal	Metal
Printability	Yes	Yes	No	Depends
Encryption capability	No	Yes	Yes	No
Information capacity	Very small	Large	Very large	Small

(i.e., counterfeiting, theft, diversion, and recalls) faced by the pharmaceutical industry. In this section, we will investigate two generic track-and-trace techniques (i.e., barcode and QR code). Table 2 summarizes the pros and cons of different track-and-trace techniques. Note that all track-and-trace techniques cannot address the attack scenario in which the original pharmaceutical manufacturer is dishonest and will perform removing/replacing, adulteration, dosage modification, and/or mislabeling, as discussed in Section 2.2.

3.2.1 Barcode. Barcodes [8] have commonly been employed to track and trace assets across the supply chain. A barcode is an optical, machine-readable label that describes the item that carries it. Information is methodically encoded into linear or one-dimensional (1D) barcodes by altering the widths and spacings of parallel lines [74]. Barcodes are vulnerable to cloning due to visibility and controllability of encoded information and easy access to printing facilities. Other drawbacks (e.g., requirement of individual scanning, human involvement, direct line-of-sight, and close proximity to scanner, lack of writing capability once printed, low durability), as shown in Table 2, considerably limit their overall utility. Consequently, it is very easy for the adversary to repackage expired, adulterated, or counterfeit drugs; make copies of original pharmaceutical products; and recycle unwanted, substandard, and/or expired medications if the pharmaceutical company only employs barcodes for track-and-trace and anticounterfeiting purposes. It is also very easy for the adversary to avoid detection by the cashier for theft purposes or perform a denial-of-service attack by hiding or removing barcodes on the packages of pharmaceutical products.

3.2.2 QR Code. The QR code is a one-matrix or two-dimensional (2D) barcode originally designed for the automobile industry in Japan [59]. The QR code can be regarded as the upgraded version of the linear barcode and in essence is also an optical, machine-readable label bearing information about the object that carries it. A QR code is typically composed of black squares scattered in a square grid against a white backdrop, which allows access by any smart device equipped with a camera. Original information usually has to be processed using an error correction algorithm (e.g., Reed-Solomon [84]) before being appropriately interpreted. QR codes have become popular because of their larger storage capacities versus linear barcodes. Encryption can prevent

Fig. 4. Overt technologies: (a) transparent hologram [19], (b) color-shift ink [61], and (c) reactive ink [28].

unauthorized access to QR codes [71, 86]. In addition to greater storage capacity, QR codes have the same shortcomings as linear barcodes, as shown in Table 2, which severely impact their overall utility.

3.3 Secure Packaging

Defeating the adversaries in the pharmaceutical supply chain demands a comprehensive, multi-level solution, a component of which is secure packaging. Anticounterfeiting and tamper-evident technologies should be combined to enable optimal security of pharmaceutical packaging.

3.3.1 Anticounterfeiting Packaging. Anticounterfeiting packaging technologies can be divided into two categories: overt and covert technologies. Sometimes, both overt and covert security features that complement each other would be applied to the same pharmaceutical packaging to deliver layered security.

Overt technologies. Overt features applied to pharmaceutical packaging can be instantly validated through visual inspection without requiring expertise. Optically variable design features (e.g., holographic patterns, color-shift inks, and reactive inks) are commonly used to enable fast and effective packaging validation [16]. Secure holograms [47], which are easy to recognize but difficult to accurately duplicate, are widely used as first-level identification features by major pharmaceutical companies. Holograms, as shown in Figure 4(a), are generally placed on the packages of pharmaceutical products in the form of labels, seals, blister foils, or hot-stamped patches [19]. Color-shift inks [61], as shown in Figure 4(b), present two or more unique colors when observed from varying angles. Such features can be easily verified by rotating the object that carries the pattern printed with color-shift ink so that varying colors can be detected. Dr. duo Gautam and his wife Kanupriya Goel have invented a special form of packaging for medications that slowly varies its pattern as the drug expires [28], as shown in Figure 4(c). A particular packaging material that visually "self-expires" over a predefined time period has been used in their solution. Their designed package consists of two layers of information that are isolated by multiple sheets of diffusible material. The foreground displays the medicine label while the background demonstrates a warning message indicating drug expiration. The ink from the background layer will permeate the isolation to display the warning symbols over a designated time period, designed as universally understandable signs of danger.

Covert techniques. Covert security features, such as patterns printed with infrared (IR) and ultraviolet (UV) inks, and microtexts are invisible by the naked eye and hard to detect and clone without a specialist facility and/or material. Figure 5(a) illustrates a push-through-package aluminum foil printed with special ink that allows foreign substances to be detected with IR devices [14]. The left side of Figure 5(a) shows the appearance under a regular visual inspection device; the right side of Figure 5(a) shows the appearance under an IR inspection device. As shown in Figure 5(b), patterns printed with UV inks are only observable under a UV light [77]. UV inks with diverse formulations would be visible under UV lights of different wavelengths. A series of UV colors, ranging from red to yellow to blue, can be chosen to print images and texts. The security of

Fig. 5. Covert technologies: (a) IR ink [14], (b) UV ink [77], and (c) micro-text [14].

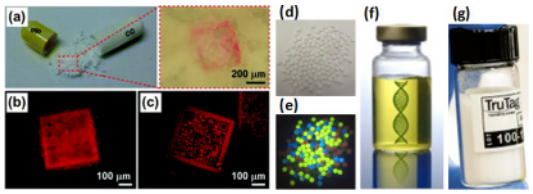

Fig. 6. Forensic techniques: (a) an opened capsule containing the QR-coded micro-taggant (left) and an magnified image of micro-taggant (right) [30], (b) fluorescent image of the QR-coded micro-taggant before washing away drug powder [30], (c) fluorescent image of the QR-coded micro-taggant after washing away drug powder [30], (d) pills that integrate diamond nanoparticles under room light [78], (e) pills that integrate diamond nanoparticles under UV light [78], (f) DNA taggant [66], and (g) TruTag [82].

images printed with UV inks is ensured by strictly controlling the availability of a secure range of inks. By combining a set of colors to construct photographic images, the security level is further enhanced due to the highly specialized originality and printing techniques. Sophisticated printing techniques also enable the creation of fine-line designs as well as colorful and UV micro-texts. Micro-text can also help users confirm the authenticity of a pharmaceutical product. As shown in Figure 5(c), the blue space around the larger symbol is printed in micro-lettering [14]. The level of security with micro-characters is determined by limited access to tspecial printing equipment.

Forensic techniques. Forensic techniques [18] scientifically authenticate pharmaceutical products using sophisticated laboratory or field test kits. Pharmaceutical forensics leverages composition analysis, characterization, and source identification to provide guidance in the mitigation of any pharmaceutical issue. Examples of forensic techniques include:

- *Micro-taggants:* Micro-taggants are tiny particles bearing coded information that uniquely identify each variant. Alphanumeric characters recorded on small flakes or threads, or fragments of multicolored, multilayered laminates with a specific color combination can be used to represent identification information, which can be added to adhesives or directly applied to packaging constitutes as spots or threads. Recently, the authors in [30] developed a drug authentication process, the central player of which is a QR-coded micro-taggant, as shown in Figure 6(a). The fluorescent QR-coded micro-taggant was created by patterning a copolymer of a photocurable polymer and an acrylate modified fluorescent dye. The QR-coded micro-taggant added to a drug capsule can mark individual drug dose and enable on-dose authentication (ODA). As shown in Figure 6(c) [30], the micro-taggant will be observable under a fluorescence microscope after washing away additional drug powder.
- *Chemical taggants:* Chemical taggants may contain indicators that are potentially hydrogen (PH) sensitive or are detectable with precise analytical methods (e.g., IR spectroscopy, X-ray fluorescence). Figure 6(d) shows pills that include diamond nanoparticles when exposed to room light [78]. Figure 6(e) shows the same pills when exposed to UV light [78]. A diamond

Fig. 7. Tamper-evident packaging: (a) folding box [64], (b) self-adhesive seal [65], (c) bubble pack [60], (d) heat shrink band/wrapper [58], (e) breakable cap [2], (f) induction sealing [12], (g) Flexi-Cap [9], and (h) ROPP [29].

is composed of two closely packed interpenetrating, face-centered cubic lattices, with each one shifting from the other by a quarter of its distance along the diagonal. In spite of this regularity, the lattices demonstrate unique variations in structure and light exposure will stimulate them to emit a spectral response associated with them alone, creating a distinct signature.

- *Biological taggants:* Biological taggants, as shown in Figure 6(f) [66], may uniquely identify themselves using specific deoxyribonucleic acid (DNA) strands [85]. An extremely low concentration (units per million) of biological taggant is sprayed onto the product or its package. To verify its existence, the taggant is extracted from a small amount of sample, a few drops of which are then put onto a lateral flow device. After flowing up the slide, the fluid comes into contact with the monoclonal antibody. Visible evidence will appear on the lateral flow device if the taggant is present.
- *Isotope ratios:* Naturally occurring isotopes, which can be accurately detected using laser fluorescence or resonance techniques [54], can be used to trace the provenance of a compound. They can provide a fingerprint of the product components.
- *Silicon taggants:* TruTag developed a type of silicon taggant, as shown in Figure 6(g), which stemmed from a silicon wafer electrochemically etched with a pattern corresponding to a unique spectroscopic signature [82]. TruTag particles are obtained by grounding the wafer into powder. A gram of TruTag particles contains over 12 million tags, each tag carrying information including product type, dosage form, and lot or batch number.

3.3.2 Tamper-Evident Packaging. To help inspect the integrity of OTC drugs, tamper-evident packaging uses an indicator to imply that tampering has occurred when breached. There are dozens of available tamper-evident packaging technologies. Due to the limited scope of this article, we introduce only eight of them, as illustrated in Figure 7, which are either quite popular or recently proposed.

Folding box. A specially constructed folding box, as shown in Figure 7(a) [64], offers a clear first-use visual cue without making it difficult for consumers to open. The new line features die-cut tabs on either side of the assembled box that make it virtually impossible to get to the product contained within without tearing along the perforations. This technique leads to visible, irreversible damage when the box is opened for the first time.

Self-adhesive seal. Self-adhesive seals for first-opening protection, as shown in Figure 7(b) [65], provide an ideal combination of tampering and counterfeiting prevention. The manufacturer's brand logo on the seal intensifies the recognition effect and improves the enforcement of legal

brand protection rights. The seal labels have to ensure the intactness of the sealed component of the packaging. Visible and irreversible damage or alteration of the packaging and the label when opening the pack is the criterion for tamper verification.

Bubble pack. The bubble pack, as shown in Figure 7(c) [60], is usually fabricated by heating the sandwich made up of a thermoformable/heat-shrinkable plastic film, the product, and a hard holding material. The plastic film would be ripped or cracked after removing the product. It is nontrivial to separate the backing material from the bubble or replace it without leaving visible evidence of tampering.

Heat shrink band/wrapper. As shown in Figure 7(d) [58], the shrink band concept is based on the heat-shrinking characteristic of a tenser-oriented polymer, which is fabricated as an extruded, oriented cylinder with a caliber a little larger than the cap and neck ring of the container to be sealed. Bands or wrappers with a distinctive characteristic (e.g., a name, logo, registered trademark, pattern) are shrunk by heat to seal the union of the cap and container. The seal cannot be easily taken off and reapplied without causing visible damage to it.

Breakable cap. As shown in Figure 7(e), the plastic ring of a breakable cap [2] has to be pulled out so that the container can be opened to take out the product, in which case the cap, or a portion thereof, will be broken. The broken cap cannot return to its original state.

Induction sealing. As shown in Figure 7(f), induction sealing technology [12] creates an air-tight, hermetical seal at the opening of the container, which protects the product against cross-contamination and works as an effective tamper-evident layer.

Flexi-Cap. Schreiner MediPharm launched the next generation of its Flexi-Cap, as shown in Figure 7(g) [9], an innovative security feature that irreversibly implies the initial entry to containers to prevent illegally reusing them with counterfeit items. The new Flexi-Cap Plus is characterized by a tear strip running through the label as an integrated element. Upon the first opening, the label will be destroyed and cannot be reemployed with counterfeit substances as a claimed original.

Roll-on pilfer-proof screwcap (ROPP). Guala Closures has launched the first ROPP playing with a tamper-evident band, as shown in Figure 7(h) [29]. A red plastic ring will appear in the narrow space between the glass bottle neck and aluminum closure once the screwcap has been opened.

Tamper-evident packaging is effective at protecting the integrity of pharmaceutical products with a low cost by intuitively indicating whether the package has ever been opened. It is also useful for limiting repackaging and/or recycling of pharmaceutical products to some extent. However, because of relatively low technical barriers and lack of anticloning features, it is not very difficult for the adversary to imitate the tamper-evident packaging and perform a cloning attack.

4 HARDWARE-ENABLED SOLUTIONS

In this section, we investigate the hardware-enabled solutions for securing the pharmaceutical supply chain. We refer to the approaches that integrate electronic components (e.g., RFID tags) or rely on testing facility (e.g., spectrum analyzer) as hardware-enabled solutions. We divide the hardware-enabled solutions into two categories, as shown in Figure 8, discuss their principles, and compare their advantages and disadvantages.

4.1 Hardware-Enabled Track-and-Trace Techniques

In this section, we will investigate two hardware-enabled track-and-trace techniques (i.e., IC-based RFID and chipless RFID), as shown in Figure 9, and compare their advantages and disadvantages. Table 2 summarizes the pros and cons of different track-and-trace techniques. Note that all track-and-trace techniques cannot address the attack scenario in which the original pharmaceutical

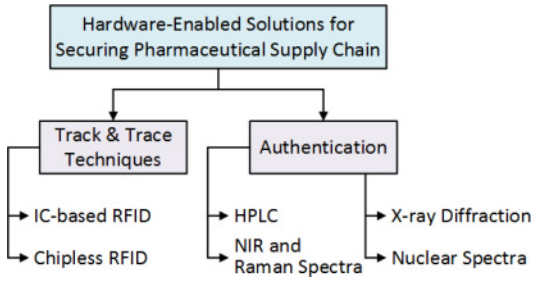

Fig. 8. Taxonomy of hardware-enabled solutions for securing the pharmaceutical supply chain.

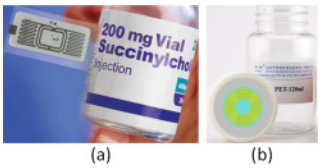

Fig. 9. Hardware-enabled track-and-trace techniques: (a) IC-based RFID [80] and (b) chipless RFID [88].

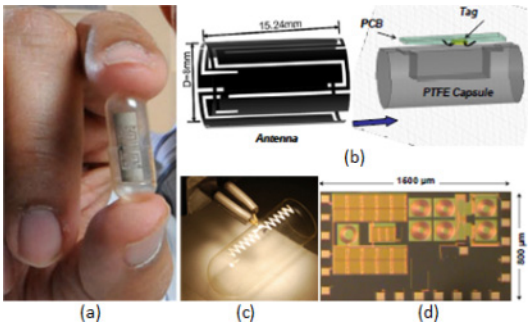

Fig. 10. (a) RFID-enabled drug capsule [76], (b) packaging and assembly of prototype RF capsule tagging [91], (c) capsule antenna prototype [91], and (d) die photo of prototype RF capsule tagging [91].

manufacturer is dishonest and will perform removing/replacing, adulteration, dosage modification, and/or mislabeling, as discussed in Section 2.2.

4.1.1 IC-based RFID. RFID tags, as shown in Figure 9(a), are widely believed to be a promising replacement for traditional linear barcodes and QR codes. The RFID system automatically identifies and tracks tags attached to objects using wireless electromagnetic signals. The tags integrate nonvolatile memories (e.g., EEPROMs) that store product-related information (e.g., manufacturer, expiration date). Unlike optical, machine-readable labels, RFID tags can be embedded in the tracked items since they do not necessarily have to be within the line of sight of the readers.

In order to accurately test the efficacy of a new drug, participants in clinical trials are supposed to take a specific dose of medication at a particular time [76]. To achieve that purpose, pharmaceutical companies would require participants to take the medications under the supervision of a witness to make sure that the drugs are being taken appropriately [76]. To help monitor drug regimen obedience, the authors in [91] developed a passive, ultra-low-power, in-body microsystem for recording when drugs were taken, thereby ensuring that patients or participants in clinical trials comply with the drug regimens. The microsystem, as shown in Figure 10(a) [76], in essence is a

minute RFID tag embedded in a capsule that could communicate sensor data suggesting that the capsule is in a person's alimentary system. The microsystem, composed of a microchip with corresponding software and a digestible antenna, communicates with an RFID reader via low-frequency (LF) signals, taking advantage of the human body's electrical conductivity. A particular sensor integrated in the microchip can detect whether the capsule is in the digestive system. Figure 10(b) and Figure 10(d), respectively, illustrate the packaging and assembly and die photo of the prototype RF capsule tagging system [91]. The passive RFID tag is as small as a grain of sand and carries a unique identifier. The microchip, fabricated with silver nanoparticles, is connected to a digestible antenna that would dissolve in the digestive system. As shown in Figure 10(c) [91], the digestible antenna measures 20mm by 10mm and occupies a little more than half a capsule. The entire system operates as follows: (i) A patient wears a patch that integrates an active RFID reader on the arm or against the abdomen so that the reader's input/output terminals electrically contact the skin. The body is used as a communication system in this way. (ii) Once the capsule is swallowed by the patient, an LF signal emitted by the reader will travel along the body to the digestive tract and power up the tag. The tag replies with its unique identifier and sensor data, which is sent back to the reader relying on the natural conductivity of the human body. The reader will then forward that information to a personal mobile device (e.g., a smartphone) via a Bluetooth connection. The mobile device would eventually send the collected data to a facility's back-end server via a wireless network connection for analysis.

Compared with optical, machine-readable labels, an RFID-enabled system has many advantages—it supports batch scanning and data update, does not require direct line of sight and close proximity to reader for access, and needs less human interaction to capture data—making automatic track-and-trace feasible. A variety of lightweight cryptographic algorithms (e.g., advanced encryption standard (AES), elliptic curve cryptography (ECC)) can be used to increase the security and privacy of RFID communication protocols [7, 32, 41]. However, IC-based RFID tags are not appropriate for the supply chain of low-cost products because of their relatively higher prices.

4.1.2 Chipless RFID. The chipless RFID tag [5], which does not contain a microchip, uniquely identifies itself by reflecting back a particular portion of the reader's signal. Compared with regular IC-based RFID tags, chipless RFID tags have several attractive features: (i) very low price (as low as 0.1 cents) makes them more appropriate for the supply chain of low-cost products; (ii) chipless RFID tags are immune to the denial-of-service (DoS) attack carried out by overwriting tag memory; (iii) it is possible to directly print chipless RFID tags on the products or their packages with conductive inks [92]; and (iv) chipless RFID tags can be used in much harsher environments (e.g., higher temperature, more RF interference) than IC-based RFID tags. Existing chipless RFID tags encode data by removing or shorting some resonators (i.e., spirals or patch slots) on the substrate [62, 63]. Removing or shorting one resonator will either eliminate the resonance point associated with that resonator from the spectrum or shift it outside of the frequency band of interest. Bit 1 corresponds to the case in which a resonance point is detected at a specific frequency, and bit 0 corresponds to the opposite case or vice versa. The manufacturing time/cost has been correspondingly increased due to the extra removing or shorting process. For the same layouts, the IDs generated by conventional chipless RFID tags are deterministic and predictable. It is a trivial task to clone these types of chipless RFID tags. Other drawbacks, such as small ID size (usually not larger than 35 bits) and large area overhead, also make them inappropriate for some application scenarios.

To alleviate the abovementioned shortcomings of traditional solutions and enable dependable visibility into supply chain status, the authors in [88] proposed a novel unclonable chipless RFID (UCR) tag, as shown in Figure 9(b). They make use of the uncontrollable process variations during

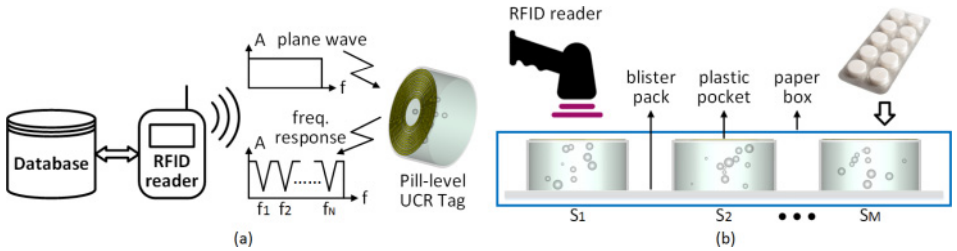

Fig. 11. Pill-level UCR system: (a) working principle and (b) drug authentication without necessarily opening the package.

tag manufacturing to create a unique, unclonable ID that can enable automatic track-and-trace of commodities (e.g., food, beverage, pharmaceuticals) throughout the supply chain. A UCR tag comprises a certain number of concentric ring slot resonators whose resonance frequencies are determined by slot geometric parameters and substrate permitivity that are sensitive to process variations during tag manufacturing. The unique ID of each UCR tag is composed of a set of resonance frequencies susceptible to manufacturing variations. The size of their proposed UCR tag is comparable to a regular QR code. The UCR tag is resistant to cloning attack.

However, their proposed UCR tag does not establish an inseparable connection with the object being identified. As a result, the adversary may successfully perform a repackaging or recycling attack by taking off the UCR tag from the original package of authentic pharmaceutical product and attaching it to the faked new package of repackaged/recycled pharmaceutical product. In addition, the pharmaceutical industry lacks a simple and effective way to enable pill-level traceability. To address these problems, the authors in [87] proposed a new split manufacturing–based, pill-level UCR tag that intrinsically generates a unique ID from multiple entropy sources, as shown in Figure 11. A pill-level UCR tag in essence is a unique object that, upon measurement by an external apparatus, exhibits a small, fixed set of inimitable analog properties that are different from any other entity of the same type. A pill-level UCR tag consists of two parts: (i) a certain number of concentric ring slot resonators integrated on the external surface of each plastic cavity or pocket of blister pack that packages pharmaceutical tablets; and (ii) nontoxic silver particles of random quantity with random diameters filled in random places of each pharmaceutical tablet. A set of resonance frequencies sensitive to manufacturing variations and randomnesses of silver particles will be captured and used as the unique ID of each pill-level UCR tag. Each pharmaceutical tablet has its own unique signature. The signatures of all pharmaceutical tablets within the same blister pack would be bound together to add one more layer of security and be resistant against illegal tablet replacement. This is the first unclonable chipless RFID tag that builds up an inseparable connection with the object being identified.

4.1.3 Application Scenario. Figure 12 illustrates the communication flow of the track-and-trace system in the real application scenario. A barcode and QR code can only be printed on the external package of pharmaceutical products since a light signal can hardly penetrate through plastic or paper material. In contrast, an IC-based RFID tag and chipless RFID tag can be placed inside the package (e.g., on the back side of a bottle cap). A barcode scanner, RFID reader, or smartphone that integrates the necessary hardware (i.e., camera for optical signal or antenna for RF signal, analog front-end, analog-to-digital converter) can be used to read the barcode/RFID tag and download label or tag-related information from the database server. The basic communication flow of the track-and-trace system is as follows:

Fig. 12. Communication flow in the real application scenario.

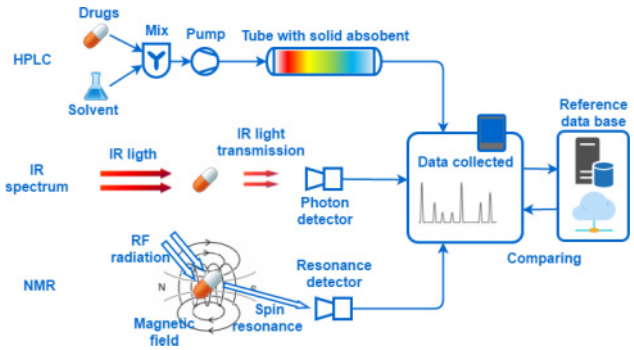

Fig. 13. Working principles of authentication techniques.

Step 1: A barcode scanner, RFID reader, or smartphone stimulates the label/tag with a light or an RF signal.

Step 2: The scanner/reader or smartphone captures the ID or uniform resource locator (URL) associated with the label/tag.

Step 3: The scanner/reader or smartphone sends the ID or URL to the database server for authentication.

Step 4: The database server sends the authentication result and corresponding product information (e.g., manufacturer, ingredients, product description, expiration date) to the scanner/reader or smartphone.

Note that for the IC-based RFID system, there probably would be much more complex cryptographic computation and authentication process involved.

4.2 Authentication

In addition to track-and-trace techniques and secure packaging, composition analysis is another approach for combating counterfeit drugs. As materials, processes, and recipes used for drug manufacturing vary across manufacturers, the API and/or excipient components and the component ratios of pharmaceutical products supplied by different companies will be different. The information obtained by composition analysis can thus be useful for authentication. For efficient and effective on-site authentication, the analytical techniques should be accurate, reliable, fast, and affordable. Candidate techniques include high-performance liquid chromatography (HPLC) [40], NIR spectroscopy [43], Raman spectroscopy [81], XRD [6], NMR spectroscopy [42] and NQR spectroscopy [11]. Figure 13 illustrates the working principles of HPLC, IR, and NMR. The working principles of the other techniques are similar and omitted in Figure 13 for brevity.

4.2.1 HPLC. HPLC is an advanced chromatography technique, which refers to the separation of components in mixtures. To use HPLC, the sample to be tested is first mixed with a proper liquid solvent. Then, a pump is employed to pass pressurized liquid solvent to a tube filled with solid phase absorbent materials to react with sample components. Different compounds in different drugs have different reaction rates with the absorbent materials. Therefore, different components in the test sample will leave the tube sequentially and can be identified by counting the time they consumed to pass through the tube. Although compared with traditional chromatography techniques HPLC has improved the test efficiency by exploiting a pump to increase the flow rate in the tube, thus obtaining the test result in a shorter time, it still takes hours to finish a single test.

4.2.2 NIR and Raman Spectra. Both NIR and Raman spectra can be considered as molecular vibrational spectra. For all molecules containing multiple atoms, there are chemical bonds with vibration modes sensitive to the variations of molecular structures. The vibration modes of different molecules have their own specific energy levels, which can be used for drug composition analysis. For NIR spectroscopy, a test sample is exposed to NIR photons with wavelengths ranging from 780nm to 2500nm. The photon energy is absorbed by sample molecules, changing their vibration modes. By recording the peaks of energy absorption, molecular information is obtained. For Raman spectroscopy, a test sample is exposed to monochromatic photons, usually emitted from a laser source. The photons are scattered by the molecules in the test sample, exciting the molecules to higher virtual energy levels. The excited molecules are unstable and will jump back to lower energy levels, releasing energy by emitting photons. The wavelength of emitted photons corresponds to the gap between the initial and final vibration modes of the sample molecule, providing similar information to that of NIR spectroscopy.

4.2.3 XRD. XRD is a powerful technique to collect atomic-level structure information crystal materials. A sample to be tested by XRD is usually prepared as powder and exposed to X-ray. The X-ray reflected by the sample is measured. When the X-ray is reflected by the sample, it is diffracted into specific directions. Because of the periodic atom arrangement in crystal materials, the X-ray is diffracted into specific directions, which can be well described by Bragg's law. This phenomenon can be observed on some amorphous materials with short-range order as well, which makes XRD-based authentication useful for many drugs that contain amorphous components. By analyzing the angle between the incident X-ray and reflected X-ray, and the corresponding X-ray intensity, structural information of sample materials can be readily obtained and the materials can be identified.

4.2.4 Nuclear Spectra. The nuclear spectra discussed in this section include NMR and NQR spectra, both of which measure the information about the spins of nuclei in materials. As nuclei carry charges, they have different spins based on the number of protons and neutrons contained in them. For NMR spectroscopy, the sample to be tested is placed in a magnetic field. With the given magnetic field, nuclei in the sample molecules with nonzero spin have a magnetic dipole moment, generating their own spin energy levels according to the material structure. Given another electromagnetic radiation, only specific energy from the radiation that corresponds to these energy levels can be absorbed by the nuclei. The absorption can be detected to provide the information about the nuclei. Based on this information, the structures of components in drugs can also be revealed. The working principle of NQR spectroscopy is similar to that of NMR spectroscopy, in which an electric field instead of magnetic field is employed. Nuclei with spin equal to or larger than 1 have an electric quadruple moment, generating their own spin energy levels according to the material structure. Such energy levels can be detected by radiation energy absorption to provide information regarding drug composition, just like NMR spectroscopy.

4.2.5 Comparison of Authentication Techniques. HPLC is widely used by many practitioners because of its flexibility, accuracy, and reliability. However, this technique has its own limitations: it is destructive and the sample preparation requires specialist knowledge. The NIR and Raman techniques are very promising for on-site pharmaceutical characterizations, as they enable rapid and nondestructive measurements and the measurements virtually do not require sample preparation. In addition, the cost of their testing facility is comparably lower. One challenge for NIR and/or Raman spectroscopy is that some materials do not present NIR/Raman resonance. It is also challenging to use NIR/Raman spectroscopy to discriminate components with similar molecular structures. XRD analysis can be performed rapidly and the sample preparation is simple, providing precise and reliable analysis results. However, XRD analysis cannot be used for liquids. The relatively higher price and larger tool size also limit its utility. For NMR spectroscopy, the extremely sensitive spin resonance to an environmental electromagnetic field and the higher measurement accuracy make it very powerful in pharmaceutical composition analysis, but it is very expensive. Compared with NMR spectroscopy, instrumentation required by NQR spectroscopy is simpler and cheaper as no magnetic field is necessary, making it more appropriate for drug authentication. Admittedly, the accuracy of measurement results obtained using NQR spectroscopy is consequently lower than that obtained using the NMR approach.

4.3 Comparison of Hardware-Enabled Solutions

Table 3 compares the advantages and disadvantages of existing solutions for securing the pharmaceutical supply chain. None of the listed techniques beat others in every aspect. Different techniques are suitable for different application scenarios and requirements. Sometimes two or more techniques could be combined to reach the optimal performance and security.

5 FUTURE RESEARCH DIRECTIONS

It is quite challenging to completely defeat the economically motivated adversaries, but a comprehensive, defensive pharmaceutical supply chain system could be devised so that it would be quite time consuming, difficult, and expensive for the adversaries to compromise its security. Although a large quantity of recent research and new developments have emerged on anticounterfeiting and track-and-trace techniques for ensuring the security and integrity of the pharmaceutical supply chain in the past two decades, many open problems still exist that require additional research in the future. Compared with generic solutions, hardware-enabled solutions are believed to be more promising because of their higher level of security and thus require more research effort. In the following, we list some important issues that still need to be addressed.

- **Comprehensive solution.** Solutions for securing the pharmaceutical supply chain exist in isolation. Scholars in different fields of research (e.g., the Internet of Things (IoT) [37], RFID [4], artificial intelligence (AI) [69], wireless sensor network (WSN) [67, 90], pervasive computing [72], big data [45], cloud computing [3], biometric [36], machine learning [10], spectrum analysis [39]) could work together to develop a comprehensive solution for defending the pharmaceutical supply chain from different aspects of security breaches.
- **Smart supply chain.** Although RFID readers and tags, surveillance cameras, and different types of sensors (e.g., temperature sensor, humidity sensor) have been implanted into the pharmaceutical supply chain to enable asset monitoring and tracking, the current pharmaceutical supply chain is still nonintelligent. Deployed sensors can only passively capture environmental variances and send them to the remote server for processing, in which case the responsiveness is often postponed. In addition, information provided by

Table 3. Comparison of Existing Solutions

Technologies	Advantages	Disadvantages
Track and Trace [5, 30, 74, 83, 88]	1. Provides drug provenance and history information, and helps establish e-pedigree. 2. Helps eliminate dispensing errors and accelerates recall of defective drugs. 3. Enables remote authentication by connecting scanner/reader to server via Internet. 4. Low cost.	1. Vulnerable to split attacks (i.e., separating label/tag from product, swapping labels/tags, etc.) 2. Reliability issues arise when labels/tags are damaged in transit. 3. Uniform standards are required for access control and management in different markets.
Overt Techniques [16, 19, 28, 47, 61]	1. Enable instant primary feature verification through visual inspection without requiring specialist knowledge and skill. 2. Extremely low cost.	Distinct features are easily recognized and replicated.
Covert Techniques [14, 77]	1. Distinct features are hidden. 2. Implementation is simple and cost-effective. 3. Facilitate easy addition and modification.	1. Require specialist equipment to detect hidden features. 2. Security relies on limited access to special materials or printing equipment.
Forensic Techniques [18, 30, 54, 66, 78, 82, 85]	1. Taggants are implanted in drugs and cannot be easily separated. 2. Resistant to recycling of pharmaceutical packaging. 3. Enable identification of an individual pill.	1. Have to change the composition of drugs. 2. Require specialist equipment to detect taggants. 3. Detection of taggants is slow and expensive.
Authentication Techniques [6, 11, 40, 42, 43, 81]	1. Provide a higher level of security and authentication accuracy. 2. Do not need to change composition of drugs or their packages, thereby also applicable to legacy products.	1. Authentication requires specialist equipment and expertise. 2. Authentication process is very slow and very expensive.

current deployed cameras/sensors is usually partial and incomplete because of the fact that only limited categories of sensors have been deployed and blind zones still exist. In the future, we could tap the power of the Internet of Things (IoT) and artificial intelligence (AI) to create a much smarter pharmaceutical supply chain, in which case a multifaceted combination of sensors and actuators will be provisioned, environmental variances will be sensed and processed locally in real time, decisions will be made instantly, information and computing resources will be shared among IoT nodes, and data will be backed up in the cloud to help build the electronic pedigrees (e-pedigrees) of pharmaceutical products. Against the backdrop of a smart pharmaceutical supply chain, habitual bad actors that impact product quality and introduce vulnerabilities could be easily identified and positioned in the first place, and corresponding measures would be taken timely. Recalls of pharmaceutical products would be more efficient. Complete e-pedigrees of pharmaceutical products would be established to enable tracing the provenance of suspicious medicines.

Specifically, a variety of sensors could be deployed in the pharmaceutical supply chain to dynamically monitor not only the status of intermediates and finished drugs, how they are handled and how long they stay in each stage, but also the environmental conditions (i.e., temperature, humidity, light intensity, and so on). Images of pharmaceutical products and their packages as well as spectral information of medicines would also be collected.

All this information will be sent to an AI machine for analysis and processing. IP cameras, barcode scanners, and/or RFID readers would report logistics (e.g., receiving, stocking, shipping, selling) to the AI machine. Human errors, medical accidents, and security issues (e.g., thefts, appearance of counterfeits, contamination of medicines) will also be reported to the AI machine. All the aforementioned information will be synthesized, learned, analyzed, and processed by the AI machine to achieve the following three goals: (i) the AI machine will make a comprehensive judgment about the authenticity of pharmaceutical product based on the fusion of various types of information; (ii) the AI machine will determine vulnerabilities associated with the pharmaceutical supply chain; and (iii) the AI machine will send commands to the actuators deployed in the pharmaceutical supply chain to adjust system parameters (e.g., supplier selection, manufacturing and storage conditions, inventory time, distribution path) and mitigate corresponding vulnerabilities. It would be very difficult for the adversaries to tamper with the integrity of a smart pharmaceutical supply chain since information is highly transparent and shared.

Compared with the traditional pharmaceutical supply chain, the additional cost for a smart pharmaceutical supply chain would include the following four parts: (i) The cost of gadgets that are attached to or placed inside the package of pharmaceutical product. The gadgets could include hardware that generates a unique identifier (e.g., IC-based RFID tag or chipless RFID tag) and tiny devices that track history information (e.g., previous storage conditions, such as temperature and humidity, elapsed time since manufacturing) of pharmaceutical product. (ii) The cost of sensors, actuators, RFID readers, and IP cameras that are deployed in the pharmaceutical supply chain to monitor and track the status of pharmaceutical products and execute the commands issued by the AI machine. (iii) The cost of developing an intelligent agent. (iv) The cost of data communication and database maintenance. To transform the traditional pharmaceutical supply chain into a smart one, the cost added to each pharmaceutical product would be around 20 cents, which is quite acceptable.

- **Tracking storage conditions.** Existing track-and-trace techniques can only provide a unique ID for tracking location information and binding pharmaceutical product to a database record that contains information regarding manufacturer, place of origin, product category, expiration date, and so on. Although different types of sensors have been deployed along the pharmaceutical supply chain, information collected by those sensors are susceptible to damage and loss. Information encryption/decryption, communication, storage, and sharing among multiple supply chain participants is also a challenge and causes additional cost. In addition, information provided by deployed sensors is usually specific to a batch of pharmaceutical products rather than a single bottle (or pack) of pills (or capsules). Sensor information is not closely bound to the pharmaceutical product. The pharmaceutical industry requires a cost-effective solution for tracking storage conditions (e.g., temperature, humidity, exposure to light) and elapsed time of pharmaceutical products. That tracking information should be closely bound to each bottle (or pack) of pills (or capsules) or even each single pill (or capsule) and have the capability to be easily extracted without the need to query the centralized database. In addition, this drug-related history information should be resistant to tampering and fabrication.
- **Trace back to raw materials.** Existing track-and-trace techniques can only trace back to the manufacturing stage in which drugs are packaged and finished. However, there is no solution that can trace back to the supplies of raw materials. This is important due to the following probable scenario. Imagine that a batch of pharmaceutical products in the

market is found to cause severe adverse side effects to human health and the contaminated raw materials used to manufacture the APIs are blamed for it. The public will want to know not only which site manufactured this batch of drugs but also which supplier provided the raw materials.

- **Anticloning packaging.** Current secure packaging–based anticounterfeiting techniques are vulnerable to either replicating or recycling of pharmaceutical packages. Self-destructive packaging design with anticloning features could significantly improve the secure packaging–based anticounterfeiting techniques.
- **Automatic and remote authentication.** Current composition analysis–based authentication techniques rely on sophisticated laboratory equipment and professional knowledge. In addition, they do not support automatic and remote authentication. The authentication process is slow and expensive. An optimized authentication technique that relies on hardware and software embedded in smartphones and that enables automatic and remote authentication could significantly broaden the application areas of this type of solution.
- **Blockchain technology.** One of the primary reasons that the pharmaceutical industry has failed to develop an effective solution to counterfeiting is that the most effective solutions require close collaboration among supply chain participants, which inevitably involves significant information sharing. However, the vast majority of supply chain participants are reluctant to collaborate because they do not want to expose competition-sensitive information, such as purchases and sales transactions. Additionally, the pharmaceutical industry has a demand that drug-related records are immutable once verified and can endure the lifetime of pharmaceutical products.

  The blockchain technology can efficiently address these two problems. A blockchain [20] is a distributed database that is used to maintain a continuously growing list of records (i.e., blocks). Each block contains a timestamp and a link to a previous block. A blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. Blockchains are inherently resistant to data modification. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks and a collusion of the network majority. Functionally, a blockchain can serve as an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. The ledger itself can also be programmed to trigger transactions automatically. Blockchains are secure by design and are an example of a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been achieved with a blockchain. This makes blockchains potentially suitable for tracking pharmaceutical products and verifying their provenance. A blockchain allows the pharmaceutical industry to identify the party responsible for introducing counterfeit and substandard products into the supply chain. Encryption and digital signature techniques inherent in a blockchain contributes to the privacy of transaction data and help create an immutable historical record.
- **Printable electronic devices.** The high cost of current hardware (e.g., RFID tag) bound to pharmaceutical products limits its mass adoption. Cost-effective printable electronic devices [89] have the potential to be widely deployed in the pharmaceutical supply chain to enhance security. All gadgets (e.g., RFID tag, temperature sensor, humidity sensor, passive timer) that are attached to or placed inside the package of a pharmaceutical product can be directly printed using a 3D printer with a variety of materials. This can not only reduce costs and save assembly space, but it can also make it more difficult for the adversary to separate the gadgets from the pharmaceutical product.

6 CONCLUSION

In this article, we have described the framework and properties of the pharmaceutical supply chain and analyzed the risks and vulnerabilities associated with it. We have also defined the adversarial model. Existing solutions for securing the pharmaceutical supply chain have been classified and elaborately discussed in terms of their implementations, properties, costs, advantages, and disadvantages. Compared with generic solutions, hardware-enabled solutions are recommended because of their higher level of security. Since pharmaceutical supply chain security relates to public health and patient safety, this work should raise awareness of present state-of-the-art capabilities and provide motivation for the research and development of new, low-cost, and robust security strategies. Finally, we specify future directions for enhancing the state-of-the-art for securing the pharmaceutical supply chain.

REFERENCES

[1] Australian Government Department of Health Therapeutic Goods Administration. 2017. Code of practice for the tamper-evident packaging (TEP) of therapeutic 800 goods. Retrieved November 11, 2017 from https://www.tga.gov.au/sites/default/files/code-practice-tamper-evident-packaging-therapeutic-goods.pdf.

[2] Albert J. Agbay and Ralph H. Thomas Sr. 1987. Tamper resistant and tamper evident closures. (March 3 1987). US Patent 4,646,926.

[3] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and others. 2010. A view of cloud computing. *Commun. ACM* 53, 4, 50–58.

[4] Bilal Aslam, Umar Hasan Khan, Muhammad Awais Azam, Yasar Amin, Jonathan Loo, and Hannu Tenhunen. 2017. A compact implantable RFID tag antenna dedicated to wireless health care. *International Journal of RF and Microwave Computer-Aided Engineering* 27, 5, e21094.

[5] Bilal Aslam, Umar Hasan Khan, Ayesha Habib, Yasar Amin, and Hannu Tenhunen. 2015. Frequency signature chipless RFID tag with enhanced data capacity. *IEICE Electronics Express* 12, 17, 20150623–20150623.

[6] Simon Bates, George Zografi, David Engers, Kenneth Morris, Kieran Crowley, and Ann Newman. 2006. Analysis of amorphous and nanocrystalline solids from their X-ray diffraction patterns. *Pharmaceutical Research* 23, 10, 2333–2349. DOI: http://dx.doi.org/10.1007/s11095-006-9086-2

[7] Lejla Batina, Jorge Guajardo, Tim Kerins, Nele Mentens, Pim Tuyls, and Ingrid Verbauwhede. 2007. Public-key cryptography for RFID-tags. In *5th Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops'07)*. IEEE, 217–222.

[8] Tricia Bishop and Baltimore Sun. 2004. UPC bar code has been in use 30 years / Once-controversial technology is now ubiquitous. Retrieved November 11, 2017 from http://www.sfgate.com/business/article/UPC-bar-code-has-been-in-use-30-years-2744217.php.

[9] Blauvelt. Schreiner MediPharm Introduces Flexi-Cap Plus with Integrated Tear Strip for Enhanced Security. (2016). Retrieved October 23, 2017 from https://www.schreiner-group.com/en/press/detail-smp-usa/404.html.

[10] Jaime G. Carbonell, Ryszard S. Michalski, and Tom M. Mitchell. 1983. An overview of machine learning. In *Machine Learning*. Springer, 3–23.

[11] Cheng Chen, Fengchao Zhang, Jamie Barras, Kaspar Althoefer, Swarup Bhunia, and Soumyajit Mandal. 2016. Authentication of medicines using nuclear quadrupole resonance spectroscopy. *IEEE/ACM Transactions on Computational Biology and Bioinformatics* 13, 3, 417–430.

[12] John W. Collins III. 1978. Induction heat sealed containers. (Aug. 29, 1978). US Patent 4,109,815.

[13] U.S. Congress. 1938. Federal Food, Drug, and Cosmetic Act (FFDCA). Retrieved November 11, 2017 from https://www.fda.gov/RegulatoryInformation/LawsEnforcedbyFDA/FederalFoodDrugandCosmeticActFDCAct/default.htm.

[14] UACJ Foil Corporation. 2017. Push-through-package Aluminum Foil for Pharmaceuticals. Retrieved November 11, 2017 from http://ufo.uacj-group.com/en/products/medical.html.

[15] Lorenzo Cozzella, Carla Simonetti, and Giuseppe Schirripa Spagnolo. 2012. Drug packaging security by means of white-light speckle. *Optics and Lasers in Engineering* 50, 10, 1359–1371.

[16] Martin Dallas. 2014. Anticounterfeiting Packaging 101—Packaging technologies play key role in product protection. Retrieved November 11, 2017 from http://www.pharmtech.com/anticounterfeiting-packaging-101.

[17] Marleen de Veij, Annelien Deneckere, Peter Vandenabeele, Dries de Kaste, and Luc Moens. 2008. Detection of counterfeit Viagra® with Raman spectroscopy. *Journal of Pharmaceutical and Biomedical Analysis* 46, 2, 303–309.

[18] Klara Dégardin, Yves Roggo, and Pierre Margot. 2015. Forensic intelligence for medicine anti-counterfeiting. *Forensic Science International* 248, 15–32.

[19] Packaging Digest Staff in Smart Packaging. 2008. How holograms can stop counterfeiting. Retrieved November 11, 2017 from http://www.packagingdigest.com/smart-packaging/how-holograms-can-stop-counterfeiting.
[20] The Economist. 2015. Blockchains: The great chain of being sure about things. Retrieved October 23, 2017 from https://www.economist.com/news/briefing/21677228-technology-behind-bitcoi%n-lets-people-who-do-not-know-or-trust-each-other-build-dependable.
[21] Food, Drug Administration, and others. 2013. Drug Supply Chain Security Act (DSCSA). Retrieved November 11, 2017 from https://www.fda.gov/Drugs/DrugSafety/DrugIntegrityandSupplyChainSecurity/DrugSupplyChainSecurityAct/.
[22] Food, Drug Administration, and others. 2013. Food and drug administration safety and innovation act (FDASIA). Retrieved November 11, 2017 from https://www.fda.gov/RegulatoryInformation/LawsEnforcedbyFDA/SignificantAmendmentstotheFDCAct/FDASIA/default.htm.
[23] U.S. Food and Drug Administration. 2013. Secure Supply Chain Pilot Program. Retrieved November 11, 2017 from https://www.fda.gov/Drugs/DrugSafety/DrugIntegrityandSupplyChainSecurity/ucm365626.htm.
[24] Shayne Cox Gad. 2008. *Pharmaceutical Manufacturing Handbook: Production and Processes*. Vol. 5. John Wiley & Sons, Hoboken, NJ.
[25] Felix Gillette. 2013. Inside Pfizer's Fight Against Counterfeit Drugs. Retrieved October 23, 2017 from http://www.bloomberg.com/news/articles/2013-01-17/inside-pfizers-fight-against-counterfeit-drugs.
[26] GlobalData. 2015. US Pharmaceutical Market Value Will Approach $550 Billion by 2020, says GlobalData. Retrieved November 11, 2017 from https://www.dddmag.com/news/2015/03/us-pharmaceutical-market-value-will-approach-550-billion-2020-globaldata.
[27] Lawrence O. Gostin, Gillian J. Buckley, and others. 2013. *Countering the Problem of Falsified and Substandard Drugs*. National Academies Press, Washington, DC.
[28] Alyn Griffiths. 2013. Self Expiring packaging by Kanupriya and Gautam Goel. Retrieved November 11, 2017 from https://www.dezeen.com/2013/08/14/self-expiring-packaging-by-kanupriya-and-gautam-goel/.
[29] Guala Closures Group. 2010. NEW TAMPER EVIDENT CLOSURE FROM GUALA CLOSURES. Retrieved October 23, 2017 from http://www.gualaclosures.com/guala-closures-lancia-roll-on-te/.
[30] Sangkwon Han, Hyung Jong Bae, Junhoi Kim, Sunghwan Shin, Sung-Eun Choi, Sung Hoon Lee, Sunghoon Kwon, and Wook Park. 2012. Lithographically encoded polymer microtaggant using high-capacity and error-correctable QR code for anti-counterfeiting of drugs. *Advanced Materials* 24, 44, 5924–5929.
[31] Virginia Herold. 2013. California E-Pedigree Update. Retrieved October 23, 2017 from https://www.gs1.org/docs/healthcare/Wed_9h05_VirginiaHerold_ePedigree.pdf%.
[32] Cédric Hocquet, Dina Kamel, Francesco Regazzoni, Jean-Didier Legat, Denis Flandre, David Bol, and François-Xavier Standaert. 2011. Harvesting the potential of nano-CMOS for lightweight cryptography: an ultra-low-voltage 65 nm AES coprocessor for passive RFID tags. *Journal of Cryptographic Engineering* 1, 1, 79–86.
[33] Ulrike Holzgrabe and Myriam Malet-Martino. 2011. Analytical challenges in drug counterfeiting and falsification: The NMR approach. *Journal of Pharmaceutical and Biomedical Analysis* 55, 4, 679–687.
[34] Don Hsieh. 2014. Pharmaceutical Supply Chain Security Best Practices. Retrieved November 11, 2017 from https://www.tycois.com/blogs/business-security/pharmaceutical-supply-chain-security-best-practices.
[35] P. C. Hyman and Phelps McNamara. 2007. Food and Drug Administration Amendments Act of 2007. (October 2007).
[36] Anil K. Jain, Arun Ross, and Salil Prabhakar. 2004. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology* 14, 1, 4–20.
[37] Arun Kanuparthi, Ramesh Karri, and Sateesh Addepalli. 2013. Hardware and embedded security in the context of Internet of Things. In *Proceedings of the 2013 ACM Workshop on Security, Privacy & Dependability for Cyber Vehicles*. ACM, 61–64.
[38] Yao Zhao and Kathleen Iacocca. 2015. Resell vs. Direct Models: US Branded Drug Distribution in the Future. Retrieved October 23, 2017 from http://www.pharmexec.com/resell-vs-direct-models-us-branded-drug-distribution-future.
[39] Steven M. Kay and Stanley L. Marple. 1981. Spectrum analysis: a modern perspective. *Proceedings of IEEE* 69, 11, 1380–1419.
[40] Yuri V. Kazakevich and Rosario Lobrutto. 2007. *HPLC for Pharmaceutical Scientists*. John Wiley & Sons, Hoboken, NJ.
[41] Yong Ki Lee, Kazuo Sakiyama, Lejla Batina, and Ingrid Verbauwhede. 2008. Elliptic-curve-based security processor for RFID. *IEEE Transactions on Computers* 57, 11, 1514–1527.
[42] Christopher A. Lepre, Jonathan M. Moore, and Jeffrey W. Peng. 2004. Theory and applications of NMR-based screening in pharmaceutical research. *Chemical Reviews* 104, 8, 3641–3676. DOI: http://dx.doi.org/10.1021/cr030409h
[43] J. Luypaert, D. L. Massart, and Y. Vander Heyden. 2007. Near-infrared spectroscopy applications in pharmaceutical analysis. *Talanta* 72, 3, 865–883. DOI: http://dx.doi.org/10.1016/j.talanta.2006.12.023
[44] Jan K. Maurin, Franciszek Pluciński, Aleksander P. Mazurek, and Zbigniew Fijałek. 2007. The usefulness of simple X-ray powder diffraction analysis for counterfeit control: The Viagra® example. *Journal of Pharmaceutical and Biomedical Analysis* 43, 4, 1514–1518.

[45] Viktor Mayer-Schönberger and Kenneth Cukier. 2013. *Big data: A Revolution That Will Transform How We Live, Work, and Think*. Houghton Mifflin Harcourt, Boston, MA.
[46] Matthew J. Mollan Jr. and Mayur Lodaya. 2004. Continuous processing in pharmaceutical manufacturing. *Pharmaceutical Manufacturing Magazine* 1–9.
[47] Takanori Nomura, Atsushi Okazaki, Masashi Kameda, Yoshiharu Morimoto, and Bahram Javidi. 2005. Image reconstruction from compressed encrypted digital hologram. *Optical Engineering* 44, 7, 075801–075801.
[48] U.S. Department of Health, Food Human Services, Center for Drug Evaluation Drug Administration, and Office of Regulatory Affairs Research, Office of the Commissioner. 2006. GUIDANCE FOR INDUSTRY Prescription Drug Marketing Act (PDMA) Requirements. Retrieved October 23, 2017 from https://www.fda.gov/downloads/drugs/guidancecomplianceregulatoryinformation/guidances/ucm134399.pdf.
[49] U.S. House of Representatives. 1906. The Pure Food and Drug Act (PFDA). Retrieved November 11, 2017 from http://history.house.gov/HistoricalHighlight/Detail/15032393280.
[50] International Institute of Research Against Counterfeit Medicines. 2013. FAKE DRUGS ON THE WEB. Retrieved November 11, 2017 from http://www.iracm.com/en/thematic-observatory/fake-drugs-on-the-web/.
[51] World Health Organization. 1999. Good manufacturing practices: supplementary guidelines for the manufacture of pharmaceutical excipients. Retrieved October 23, 2017 from http://www.who.int/medicines/areas/quality_safety/quality_assurance/SupplementaryGMPPharmaceuticalExcipientsTRS885Annex5.pdf.
[52] World Heath Organization. 1999. Guidelines for the development of measures to combat counterfeit drugs. Retrieved November 11, 2017 from http://apps.who.int/medicinedocs/en/d/Jh1456e/.
[53] World Health Organization. 2000. General information on counterfeit medicines. Retrieved November 11, 2017 from http://www.who.int/medicines/services/counterfeit/overview/en.
[54] World Health Organization. 2007. Anti-counterfeit Technologies for the Protection of Medicines. Retrieved November 11, 2017 from http://www.fip.org/impactglobalforum/pdf/backgroundinfo/IMPACT%20-%20AC%20Technologies%20v2.pdf.
[55] World Health Organization. 2011. Definition of active pharmaceutical ingredient. Retrieved October 23, 2017 from http://www.who.int/medicines/areas/quality_safety/quality_assurance/DefinitionAPI-QAS11-426Rev1-08082011.pdf.
[56] World Health Organization. 2012. Ensuring good dispensing practices. Retrieved October 23, 2017 from http://apps.who.int/medicinedocs/documents/s19607en/s19607en.pdf.
[57] World Health Organization. 2013. Deadly medicines contamination in Pakistan. Retrieved November 11, 2017 from http://www.who.int/features/2013/pakistan_medicine_safety/en/.
[58] SKS BOTTLE & PACKAGING. Shrink Bands. 2017. Retrieved October 23, 2017 from https://www.sks-bottle.com/Shrink_Band_Info.html.
[59] James J. Jong Hyuk Park, Joseph Kee-Yin Ng, Hwa-Young Jeong, and Borgy Waluyo. 2014. *Multimedia and Ubiquitous Engineering: MUE 2013*. Vol. 240. Springer Science & Business Media, New York, NY.
[60] PHARMA. Global blister pack industry on the rise: It's no longer just film and cardboard anymore. 2017. Retrieved October 23, 2017 from https://www.webpackaging.com/en/portals/webpac/assets/11132746/global-blister-pack-industry-on-the-rise/.
[61] Roger W. Phillips. 1990. Optically variable films, pigments, and inks. In *San Dieg-DL Tentative*. International Society for Optics and Photonics, 98–109.
[62] Stevan Preradovic, Isaac Balbin, Nemai Chandra Karmakar, and Gerhard F. Swiegers. 2009. Multiresonator-based chipless RFID system for low-cost item tracking. *IEEE Transactions on Microwave Theory and Techniques* 57, 5, 1411–1419.
[63] Stevan Preradovic and Nemai C. Karmakar. 2009. Design of fully printable planar chipless RFID transponder with 35-bit data capacity. In *European Microwave Conference (EuMC'09)*. IEEE, 013–016.
[64] Pipi Print and Packaging. Near perfect tamper evidence (TE) on boxes. 2017. Retrieved October 23, 2017 from https://www.webpackaging.com/en/portals/webpac/assets/11130321/near-perfect-tamper-evidence-te-on-boxes/.
[65] ELTRONIS Speciality & Security Printing. 2016. Self Adhesive Tamper Evident Seal. Retrieved October 23, 2017 from https://www.eltronis.com/specialty-products/pharmaceutical-labels/tamper-evident-seal/.
[66] Louie Prost. Fight against fake medicines Degeuser Justine Laure Tiquet Mehdi Cherbatli Christophe Bouchez Guil Hadrian 1. 2017. Retrieved October 23, 2017 from http://slideplayer.fr/slide/1289799/.
[67] K. Ramesh and S. V. Aswin Kumer. 2012. Efficient health monitoring system using sensor networks. *International Journal of Scientific & Engineering Research* 3, 6.
[68] Dirk Rodgers. 2009. The Florida Pedigree Law. Retrieved October 23, 2017 from https://www.rxtrace.com/2009/08/florida-pedigree-law.html/.
[69] Stuart Jonathan Russell, Peter Norvig, John F. Canny, Jitendra M. Malik, and Douglas D. Edwards. 2003. *Artificial Intelligence: A Modern Approach*. Vol. 2. PrenticeHall, Upper Saddle River, NJ.

[70] Stephan Sacher and Johannes G. Khinast. 2016. An overview of pharmaceutical manufacturing for solid dosage forms. *Process Simulation and Data Modeling in Solid Oral Drug Development and Manufacture* 311–383.
[71] Suraj Kumar Sahu and Sandeep Kumar Gonnade. 2013. Encryption in QR code using stegnography. *IJERA International Journal of Engineering Research and Applications* 3, 4.
[72] Mahadev Satyanarayanan. 2001. Pervasive computing: Vision and challenges. *IEEE Personal Communications* 8, 4, 10–17.
[73] Sérgio Henrique Frasson Scafi and Celio Pasquini. 2001. Identification of counterfeit drugs using near-infrared spectroscopy. *Analyst* 126, 12, 2218–2224.
[74] SCANDIT. 2015. Types of Barcodes: Choosing the Right Barcode. Retrieved November 11, 2017 from https://www.scandit.com/types-barcodes-choosing-right-barcode/.
[75] Gena Somra. 2015. Deadly fake Viagra: Online pharmacies suspected of selling counterfeit drugs. Retrieved November 11, 2017 from http://www.cnn.com/2015/08/31/health/counterfeit-medications/index.html.
[76] Claire Swedberg. 2010. University Team Sees Ingestible RFID Tag as a Boon to Clinical Trials. Retrieved November 11, 2017 from http://www.rfidjournal.com/articles/view?7560.
[77] QuickLabel Systems. 2009. QuickLabel Systems Introduces UV Fluorescent Thermal Transfer Ribbon for Printing Covert Marks on Security Labels. Retrieved November 11, 2017 from http://www.quicklabel.ca/news/press-releases/UV-fluorescent-ribbon-security-labels.html.
[78] Taaneh. 2017. The Taaneh solution. Retrieved October 23, 2017 from http://taaneh.com/taaneh_solution.htm.
[79] Paul Toscano. 2011. The Dangerous World of Counterfeit Prescription Drugs. Retrieved October 23, 2017 from http://www.cnbc.com/id/44759526.
[80] Brian Urban. 2015. RFID: From Start To SencorpWhite. Retrieved October 23, 2017 from http://sencorpwhite.com/wp-blog.php/rfid-from-start-to-sencorpwhite/.
[81] T. Vankeirsbilck, A. Vercauteren, W. Baeyens, G. Van der Weken, F. Verpoort, G. Vergote, and J. P. Remon. 2002. Applications of raman spectroscopy in pharmaceutical analysis. *TrAC Trends in Analytical Chemistry* 21, 12, 869–877. DOI: http://dx.doi.org/10.1016/S0165-9936(02)01208-6
[82] Leonora Walet. 2015. Fighting fake drugs tagging technologies may help deter counterfeiting of medicines. *Chemical and Engineering News* 93, 8 (2015), 28–29.
[83] Roy Want. 2006. An introduction to RFID technology. *IEEE Pervasive Computing* 5, 1, 25–33.
[84] Stephen B. Wicker and Vijay K. Bhargava. 1999. *Reed-Solomon Codes and Their Applications*. John Wiley & Sons, Hoboken, NJ.
[85] Charles L. Wilson. 2007. *Intelligent and Active Packaging for Fruits and Vegetables*. CRC Press, Boca Raton, FL.
[86] Yu Xiaoyang, Song Yang, Yu Yang, Yu Shuchun, Cheng Hao, and Guan Yanxia. 2013. An encryption method for QR code image based on ECA. *International Journal of Security & Its Applications* 7, 5.
[87] Kun Yang, Ulbert Botero, Haoting Shen, Domenic Forte, and Mark Tehranipoor. 2017. A split manufacturing approach for unclonable chipless RFIDs for pharmaceutical supply chain security. In *IEEE Asian Hardware-Oriented Security and Trust (AsianHOST'17)*. IEEE, 1–6.
[88] Kun Yang, Domenic Forte, and Mark M. Tehranipoor. 2016. UCR: An unclonable chipless RFID tag. In *IEEE International Symposium on Hardware Oriented Security and Trust (HOST'16)*. IEEE, 7–12.
[89] Li Yang, Amin Rida, Rushi Vyas, and Manos M. Tentzeris. 2007. RFID tag and RF structures on a paper substrate using inkjet-printing technology. *IEEE Transactions on Microwave Theory and Techniques* 55, 12, 2894–2901.
[90] Jennifer Yick, Biswanath Mukherjee, and Dipak Ghosal. 2008. Wireless sensor network survey. *Computer Networks* 52, 12, 2292–2330.
[91] Hong Yu, Chun-Ming Tang, and Rizwan Bashirullah. 2009. An asymmetric RF tagging IC for ingestible medication compliance capsules. In *IEEE Radio Frequency Integrated Circuits Symposium*. IEEE, 101–104.
[92] Lu Zhang, Saul Rodriguez, Hannu Tenhunen, and Li-Rong Zheng. 2006. An innovative fully printable RFID technology based on high speed time-domain reflections. In *Conference onHigh Density Microsystem Design and Packaging and Component Failure Analysis (HDP'06)*. IEEE, 166–170.

Received March 2017; revised August 2017; accepted September 2017