# PREVENTING COUNTERFEIT PRODUCTS USING CRYPTOGRAPHY, QR CODE AND WEBSERVICE

Cheman Shaik

VISH Consulting Services Inc, 6242 N Hoyne Avenue, Chicago IL 60659, USA

***ABSTRACT***

*Counterfeit production is a threat for every genuine business causing damage to their brand image and stealing their revenues. The aim of this paper is topresenta novel method to prevent counterfeit products using cryptography, QR code and webservice. The method requires that every original product manufacturer obtain a cryptographic key pair, securely store their private key and publish their public key on their website as a QR code. The product manufacturer needs to print a unique item code on their product packs and provide inside the pack a QR code encoding the ciphertext generated by encrypting the item code with their private key. For product verification by buyers, the manufacture is required to provide a QR code scanning app for download on their website, Google Play Store or iPhone App Store. The scanning app should have additional cryptographic functionality to decrypt ciphertext of the item code encoded in the QR code. The manufacturer also needs to launch a simple webservice on his hosting server to accept requests from the mobile app and verify the item code and buyer's name in its database. Technicalimplementation and the verification process are described in detail through figures and flowchart. The method can be implemented even by small manufacturers with nominal cost by obtaining a key pair and creating a scanning app and webservices. We have also tested the method with an actual software code written for cryptographic operations using the Java Cryptography Extension and QR code operations using Google Zxing libraries.*

***KEYWORDS***

*Counterfeit Products, Cryptography, Encryption, Decryption, QR Code, Mobile App, Webservice*

## 1. INTRODUCTION

Counterfeit product is a product that closely resembles the original product it substitutes in the market [1]. These products are poor in quality and sold at pretty much cheaper prices, thereby seriously damaging the brand image of the original product and further impacting its revenues. Another disruptive effect of counterfeit products is the loss of genuine employment with an estimated loss of 2.5 million jobs word wide.

Further, counterfeits seriously discourage innovation because the counterfeiters straight away copy the original designs and reproduce the product without any permissions from those who invent and innovate the product with lot of effort laid in research and development. Moreover, counterfeits badly impact the economy of nations as the business is illegal and their manufacturers do not declare yearly earnings, causing loss of tax to the governments [2].

According to a 2014 report from the Organization for Economic Co-operation and Development (OECD), the cost of counterfeits to the global economy is around $250 billion a year. The most counterfeited products in America are optical media, labels/tags, computers/accessories, electronics, footwear, pharmaceuticals, personal care, apparel, watches, jewelry, handbags and wallets [3].

Genuine American businesses and industries incur a loss of $200 billion approximately every year due to counterfeit products. It is very unfortunate to learn that about 10% of medicines worldwide are counterfeit, which is very detrimental to the health and well-being of the public.

There are no counter measures to stop counterfeits except legal regulations and inspections by anti-counterfeit authorities which often prove insufficient to contain them. Very often it is very difficult for these authorities to differentiate between a genuine and counterfeit product.

More research needs to be conducted to device new technologies to enable consumers detect counterfeit products using software applications, mobile apps and online verification.

## 2. LITERATURE SURVEY

In 2006 World Health Organization (WHO) created the first global partnership known as the International Medicinal Products Anti-Counterfeiting Taskforce (IMPACT) to mitigate the production, trading and selling of fake medicines through coordination and harmonization [4].

In 2008, Steven et al suggested eight ways to combat counterfeits, tightening supply chain, investigating leads fully, establishing excellent Government relations, excellent internal recordkeeping, updated packaging, formulating crisis management plan, and preparing to litigate. However, these are only non-technical measures to mitigate counterfeit operations [5].

In a research paper published in 2010, Suchir et al reported that linear or two-dimensional bar codes assist users to confirm the genuineness of a product pack. However, even high-quality bar codes are easy to replicate. They further reported holograms in the form of shrink sleeves, blister packaging aluminum foil and induction cap seals may be used as security feature on products as these are difficult to reproduce. However, they also reported that more than half the sales of the artesunate drug in South East Asia is forged, despite the presence of the hologram.

Radio Frequency Identification Device (RFID) technology could be helpful in discouraging counterfeits as their high cost of 20 – 50 cents a tag compared to 2 cents a barcode might forbid the counterfeit sellers from implementing it [6]. However, counterfeits generate lot of revenues to their sellers for whom the RFID cost is not a matter of concern.

Later in 2010, Babu et al presented a novel anti-counterfeiting and product security technique which uses a secure optical tag comprising randomly distributed reflective micro particles. The concept is based on embedding invisible random particles into the product's surface or in the document. The micro particles are verified by imaging their reflections with a camera enabled cellphone [7].

All these countermeasures are centered around enterprise strategies or based on the principles of physics and chemistry. No evidences are found in literature on using software techniques, especially using cryptography, QR codes and webservices to detect and prevent counterfeits.

In 2017, Toyoda et al proposed a blockchain-based novel product ownership management system of RFID-attached products for anti-counterfeits that can be used in the post supply chain[8].

In 2018, IjazulHaqet al explained how to use blockchain technology in pharmaceutical supply chain to add traceability, visibility and security to the drugs supply system. They used a permissioned blockchain for storing transactions and only trusted parties were allowed to join the network and push data to blockchain.

In 2019, Hoai Luan Pham et al proposed a novel blockchain-based product ownership management method for anti-counterfeit medicine system to resist the cloning of drug and improve the practical applicability. Their solution is based on Ethereum Blockchain and IPFS networks to provide a tamper-proof, security, and reliable traceability of genuine medicine [9].

However, blockchain is a very complicated and technology fraught with many challenges such as standardization, governance, data privacy and nodes maintenance. Every small manufacturer can not afford blockchain based products and services.

## 3. CRYPTOGRAPHY

Cryptography is a mathematical technique that turns the original data into an illegible form, called ciphertext in other words, using an encryption key, which makes no sense to its unintended reader. The ciphertext is successfully decrypted by the actual intended receiver with a decrypting key. Basically, crypto systems are classified into two categories – symmetric and asymmetric [10].

Symmetric cryptosystems use the same key for encryption as well as decryption whereas asymmetric cryptosystems use different keys for encryption and decryption. While symmetric cryptosystems are used for communication between two known parties asymmetric cryptosystems are used for communication between two unknown parties. Presently the most widely used symmetric cryptosystem is the Advanced Encryption Standard (AES) while the mostly commonly used asymmetric cryptosystems are RSA, ECC and ElGamal [11].

In asymmetric cryptosystems information encrypted with one key can be decrypted only by the other key which should be kept very secret. Any compromise of the decrypting key will result into obtaining the communicated messages in plain text. The public and private keys are mathematically related through the key generation equation of the crypto system. However, deriving one from the other is nearly impossible even with clustered super computers, which is why though the public key is known openly, the private key cannot be derived from it [12].

## 4. QR CODES

QR (Quick Response) code is a two dimensional, mostly square shaped, matrix populated with black data modules on a white background. A QR code can encode data of different forms such as byte, numeric alphanumeric, Chinese, Japanese and Korean characters. The information encoded in a QR code can be decoded with a handheld scanner or a QR code scanner app installed on a smart phone. A QR code can encode as many as 7,089 numeric characters or 2,953 alphanumeric characters [13].

A thick white border called the quiet zone differentiates a QR code from its background images. A QR code structure mainly comprises a finder pattern that allows the decoding software to identify the QR code and determine its orientation, separators to boost the recognition of finder patterns, a timing pattern that determines a single module's width, a format information section that stores data about the QR code error correction rate, and a data section that holds the actual data encoded in the QR code [14].

Nowadays QR codes are used to achieve many things such as to encode business cards, download files, link to a Google Map, show YouTube videos, make mobile payments, connect to a social network and connect to an app store and website [15].

## 5. WEBSERVICE

Webservice is a data exchange system that uses the internet for communication and interfacing between two applications. The data can be exchanged in the form of Extensible Markup Language (XML) or JavaScript Object Notation (JSON). XML is very verbose and consumes more bandwidth while JSON is very concise, light weight and easy to understand [16].

The two broadly used categories of webservices are SOAP (Simple Object Access Protocol) and REST (Representational State Transfer). SOAP services work only with XML data whereas REST services work with plain text, XML, HTML and JSON data. REST services are very easy to implement and access [17].

A REST is service hosted at a Uniform Resource Locator (URL) which consists of four parts, a protocol such as http or https, a domain name, a path to the resource on the domain, and a query string that includes parameters and their values to be passed [18]. Sometimes the parameters may be passed as a JSON object if they contain sensitive information such as a password.

## 6. APPLYING CRYPTOGRAPHY, QR CODE AND WEBSERVICE

In this section, we present a method to detect counterfeit products using cryptography, QR codes and webservice. This method requires that the implementing product manufacturer own a public and private key pair of any public key cryptosystem and publish their public key on their website. It also requires that the product manufacturer print a unique item code on every copy of the product. It may be printed on the outer pack of the product item. The manufacturer should encrypt the item code with the private key and encode the resulting ciphertext in a QR code. The QR code and the item code in plain text must be printed on a paper that should go inside the package. The manufacturer also needs to provide a QR code scanner mobile app for download on their website, Google Play Store and App Store. The app should store the public key in its memory.

For illustration purpose, an LG brand Smart TV is selected and an item code is printed on the packing box. Also, a QR code along with the same item code is printed on a paper that is supposed to go inside the box. Fig. 1 below shows the packing box of the Smart TV.


**Fig. 1** An LG Smart TV using Cryptography and QR Codes to defeat counterfeits


**Fig. 2** QR Code encoding an encrypted LG product item code

Fig.2 below shows a paper with the item code and a QR code printed on it which goes inside the pack.

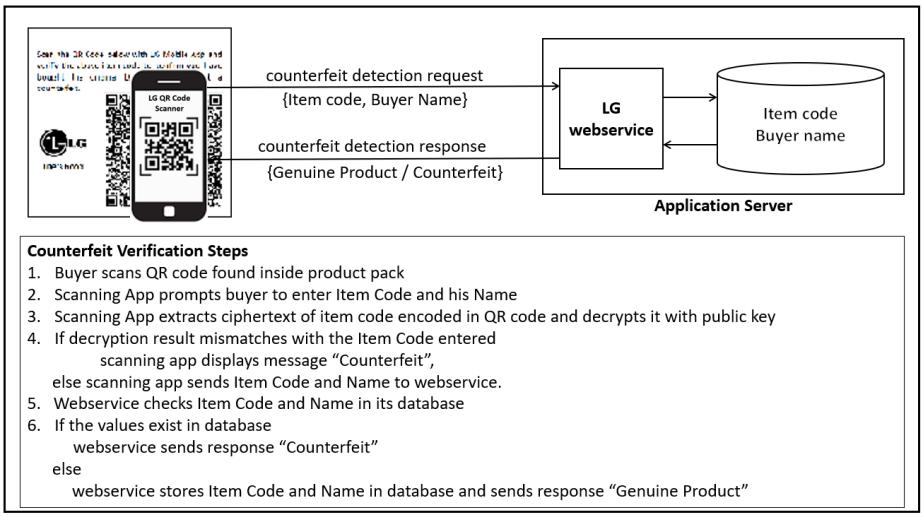


**Fig. 3** LG QR Code Scanner App interacting with their webservice for counterfeit detection

Fig. 3 below shows the LG QR code scanner mobile app interacting with their webservice for counterfeit detection.

When a product buyer scans the QR code on the paper provided inside the pack using the counterfeit detection mobile app, the app prompts the buyer to enter the item code in a text box. Once the item code is entered, the app captures the ciphertext encoded in the QR code and decrypts it using the manufacturer's public key stored in its memory. If the resulting code mismatches with the item code entered, the app raises an alert with a message that the purchased item is a counterfeit. The mismatch clearly implies that the ciphertext encoded in the QR code is not generated by encrypting the plain text item code with the manufacturer's private key.

On the other hand, if the two values match, the app prompts the buyer to enter his name in a text box. Once the buyer enters his name, the app immediately calls a webservice on the manufacturer's application server, passing the item code and the buyer's name. Subsequently, the webservice captures the item code and the buyer's name from the request and checks if a record exists in its database with the two values. If no record exists, it saves the record in its database and provides a response to the buyer with the message that the item is genuine.

In case a record exists with the captured values, the webservice will check if the buyer name in the database and the one received in the request are the same. If the two names are the same, the

webservice will send a response to the buyer with the message that the product is genuine. If any mismatch occurs between the two names, buyer will receive a message in the app that the product is a counterfeit, as it indicates the product is already sold. A possible reason could be a counterfeit manufacturer has purchased a copy of the product and printed the same item code and QR code on two or more counterfeit copies that he produced and sold in the market.

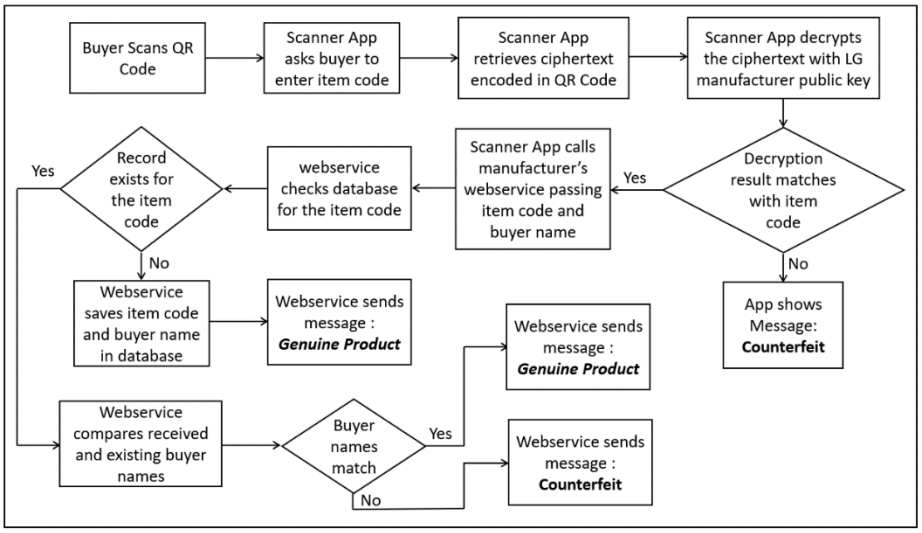


**Fig. 4** Flow chart for genuine product verification through manufacturer's mobile app

Fig. 4 below shows a flow chart depicting various steps involved in counterfeit detection by the QR code scanner app and the webservice.

## 7. RESULT OF RELEASING COUNTERFEITS

When a counterfeit product is released in the market, its manufacturer has two options:

- print their own item code and a QR code encoding the ciphertext of the item code generated by encrypting it with their own private key

  In this case the buyer will scan the QR code with the genuine manufacturer's app downloaded from their website, which will capture the ciphertext from the QR code and decrypt it with their public key. As the counterfeit's private key and the original manufacturer's public key are not mathematically related and fail to satisfy the key generation equation of the crypto system used, the decryption will result in junk text and the app will raise an alert that the purchased product is a counterfeit.

- buy a genuine product from the original manufacturer and copy the same item code and QR code on all their items or product copies

  In this case, when the counterfeit manufacturer bought the original product, they might have verified it using the original manufacturer's app. When a buyer of the counterfeit product verifies it, the app will call the webservice and verify the name existing in the database against the item code. As the names mismatch, the app will raise an alert with a message that the purchased product is a counterfeit.

Alternatively, when the counterfeit manufacturer bought the original product, they might not have verified it and sold their counterfeit product to a buyer. In this case the app will report it as a genuine product as the QR code scan will be successful, and the webservice will save the item code and the buyer name in its database. However, the original manufacturer has nothing lose here as the counterfeit manufacturer has already bought a copy their original product.

Next, when a second buyer buys a second copy of the counterfeit product with the same item code and QR code, the app scan will raise an alert of counterfeit purchase. This means the counterfeit manufacturer will not be able to sell more than one copy of their product. In order to sell a copy of their low-cost counterfeit product, the counterfeit manufacturer needs to buy a high-cost copy of the original product, which will turn their business inoperative and lead them to bankruptcy.

Moreover, practicing this option, that is, releasing multiple product copies with the same item code, will be very risky for the counterfeit manufacturer. The counterfeit controlling authorities in local retail markets, and airports and seaports where shipments are uploaded and downloaded could easily identify the malpractice by verifying the item codes on the product packs.

## 8. ITEM CODE ENCODING IN QR CODE

Item code encryption can be implemented using any public key crypto system such as RSA and ECC. Today, the industry standard for RSA key length is 2048 bits. For example, with RSA encryption, the plain text item code M is encrypted to generate a ciphertext C as below:

$C = M^e \bmod n$ where e is the private key exponent that should be kept secret.

The ciphertext C is encoded into a QR code that will be printed on a paper and provided inside the packing box. When the QR code scanning app of the original manufacturer scans the QR code, it will capture the ciphertext C from it and decrypt it to the original plain text M as below:

$M = C^d \bmod n$ where d is the public key stored in memory of the app.

The key modulus n is common on both sides.

In public key cryptography use cases of ecommerce and online communication, usually the plain text is encrypted with the public key and the ciphertext is decrypted with the private key. However, in this case the process must be reversed, that is, the plain text is encrypted by the private key and the ciphertext is decrypted with the public key.

In RSA crypto system, usually, small numbers like 3 or 65537 are chosen as the encrypting key exponent in order to minimize the ciphertext computation effort. This practice must be avoided for counterfeit verification. The encrypting key exponent used by the manufacturers should be the order of key modulus. Otherwise, brute force attacks will be much easier and the attacker could guess an exponent that would generate the right QR code to be shipped with the counterfeit products.

## 9. A UNIVERSAL MOBILE APP FOR ALL MANUFACTURERS

Download and install of QR code scanning apps of several manufacturers, could be very time consuming and may require lot of hard drive space and memory on buyer's smart phone. In order to make it simple and more practical, a universal mobile app may be developed and placed on Google Play Store and iPhone App Store. The universal app may provide UI screens to add different manufacturers, their corresponding public keys and webservice endpoints to the app memory. When a product buyer wants to scan the product's QR code, he can select the manufacturer or brand from the existing list and focus the camera over the QR code, which would capture and decrypt the ciphertext encoded therein and also make a call to the manufacturer's webservice.

Manufacturers may publish their public keys and webservice endpoints on their respective websites in the form of QR codes so it would be easy for the buyers to capture and store them with the scanning app. Another, better approach is to release the initial version of the app with built-in public keys and webservice endpoints of the most popular manufacturers around the word to avoid time consuming visits to multiple manufacturer websites. Any missing manufacturers may be allowed to join the app later through online registration. The new manufacturers may be added to the already installed apps through over-the-air updates. Alternatively, app users can integrate any missing manufacturers' public keys and webservice end points manually as required when they purchase a product.

## 10. BENEFICIARIES OF THE METHOD

The counterfeit detection method will be useful to a multitude of beneficiaries including:

- original product manufacturers
- end customers buying the products
- counterfeit controlling authorities
- customs authorities in airports and seaports
- general public (by avoiding counterfeit medicines)
- governments losing sale tax on counterfeit products

## 11. ADOPTION AND ENFORCEMENT

Adoption of the proposed solution will grow rapidly once a few manufacturers implement the solution and report their financial gain from the solution. The cost incurred by the manufacturer in rolling out this solution would be so nominal that even a small manufacturer can implement it. The implementation cost involves merely acquiring a certified key, launching a webservice and creating a mobile app for scanning their QR codes and a piece of software code that encrypts their item code, creates a QR code encoding the ciphertext which goes inside their product pack.

An open-source trusted app that can integrate the public keys and webservice end points of manufacturers around the world will become a great thrust for this solution as it relieves the manufactures from the burden of creating their own mobile apps. Also, it would be useful to consumers if branded smart phones provide such a mobile app built into their devices. Ministries of industries around the world may release their national policies mandating shipment of encrypted QR codes with their products.

## 12. ENCRYPTED QR CODES VS BLOCKCHAIN

Blockchain is an open, distributed ledger storing transactions as blocks linked to their preceding block. The blocks are stored on an open network of nodes. In the past few years blockchain has caught rapid momentum in different areas of technology, such as health, IoT, multimedia processing, e-commerce, supply chain management, etc. However, to maintain product sale and transaction records, each manufacturer needs to maintain their own controlled, permissioned blockchain or alternatively they need to join a consortium of product manufacturers to be a part of their common blockchain. This poses lot of technical and management challenges such as maintaining own nodes with efficiency and resiliency, data backup and recovery, rapidly growing storage requirements, ledger pruning and archiving, proper governance and audit capability, data privacy and business confidentiality. All these challenges make the blockchain a very complicated, high cost and heavy weight solution to combat counterfeits [17].

On the other hand, the proposed method provides a very simple, light weight, low-cost solution. Moreover, it mutes the challenges such as data privacy, business confidentiality, governance, audits etc.

## 13. RESULTS AND DISCUSSION

We have run the cryptographic and QR code operations on the actual item code shown in figure 1 and figure 2. Java Cryptography Extension (JCE) for encrypting the item code and decrypting its ciphertext. QR code generation and reading are performed using Google Zxing library. Results are tabulated as shown in Table 1 as shown below.

| Item Code | Time to Encrypt (milli sec) | Time to Generate QR Code (milli sec) | Time to Read QR Code (milli sec) | Time to Decrypt QR Code Content (milli sec) |
|---|---|---|---|---|
| LG 3815-9620-4518-3752 | 734 | 141 | 125 | 628 |

From the above results it can be learnt that the complete process of encrypting the item code and generating a QR code encoding the ciphertext took 875 milliseconds on the manufacturer side where as reading the QR code on the item slip in the product pack and decrypting by buyer took 753 milliseconds. Request and response time with the webservice actually depends on the manufacturer's application server and the internet speed of the buyer's internet connection.

## 14. CONCLUSION

Counterfeit business is a growing concern for the original product manufacturers throughout the world, causing losses of several billion Dollars to genuine businesses every year. In look and feel counterfeit products closely resemble their original products but are sold at low prices with compromised quality. Counterfeit manufacturers create multiple problems to the society, such as discouraging invention and innovation, badly impacting the economy of nations, loss of taxes to governments, and affecting the health and well-being of the public.

In this paper, we present a technical solution to prevent counterfeits using cryptography, QR codes and webservices. The presented solution requires that the original product manufacturers acquire a cryptographic key pair, generate a ciphertext by encrypting the item code with the private key and encode the ciphertext in a QR code, which goes inside the product pack. It also

requires that the original manufacturer launch a webservice that accepts a request from the mobile app when a buyer verifies the originality of the product by scanning the QR code.

When a buyer wants to verify the originality of a product that he purchased, he needs to scan the QR code shipped with the product using the manufacturer's mobile scanning app downloaded on his smart phone, which will capture the ciphertext of the item code, decrypts it with the manufacturer's public key stored in the app memory and compares the plain text item code with the item code printed on the product. The app further sends a request with the item code and the buyer's name to a webservice launched on the manufacturers hosting server. Based on the app's comparison of the item code and the response from the webservice, the app alerts the buyer with a message whether the product is original or counterfeit.

The presented method provides a low cost, light weight solution to the manufacturer, protecting the brand image and saving the business from counterfeit manufacturers. It keeps buyers away from the low-cost traps of counterfeits, increases revenues to the original manufacturers, encourages invention and innovation, surges tax revenues to governments and also improves the efficiency of regulating and controlling authorities in curbing counterfeit markets.

We discussed in detail the implementation procedure with figures and a flow chart. A future work recommendation is to conduct a proof of concept on a selected product, acquiring a key pair, creating a mobile app and a webservice so its benefits can be proved to both manufacturers and buyers.

## DISCLAIMER

The product pack shown in figures is not a real one but copied from the web through a Google search only for the purpose of illustration. Also, the QR code and item code provided on and inside the pack are randomly generated to facilitate a clear understanding of the method

## REFERENCES

[1] Arlee Sowder, "The Harmful Effects of Counterfeit Goods", https://www.athens.edu/journal/spring-2013/asowder-couterfeit/xxx

[2] IP INSIGHTS, "What are the economic effects of counterfeit goods?", https://www.redpoints.com/blog/what-are-the-economic-effects-of-counterfeit-goods/

[3] Thomas C. Frohlich, Alexander E.M. Hess and Vince Calio, "9 most counterfeited products in the USA", https://www.usatoday.com/story/money/business/2014/03/29/24-7-wall-st-counterfeited-products/7023233/

[4] G. Swaminath, "Faking it - II: Countering and preventing counterfeiting of drugs", Indian J Psychiatry. 2009 Jan-Mar; 51(1): 9–11.

[5] Steven Cooper and Gail M. Eckstein, "Eight Ways to Minimize the Risk of Counterfeiting", Intellectual Property Technology Law Journal VOLUME 20 • NUMBER 8 • AUGUST 2008

[6] Ruchir Y. Shah, Prajesh N. Prajapati, Y. K. Agrawal, "Anticounterfeit packaging technologies", Journal of Advanced Pharmaceutical Technology & Research (JAPTR) 2010 Oct-Dec; 1(4): 368–373.

[7] H. U. Babu, W. Stork and H. Rauhe, "Anti-counterfeiting using reflective micro structures - Based on random positioning of microstructures," Advances in Optoelectronics and Micro/nano-optics, Guangzhou, 2010, pp. 1-5, doi: 10.1109/AOM.2010.5767157.

[8] K. Toyoda, P. T. Mathiopoulos, I. Sasase and T. Ohtsuki, "A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in the Post Supply Chain," in IEEE Access, vol. 5, pp. 17465-17477, 2017, doi: 10.1109/ACCESS.2017.2720760.

[9] IjazulHaq and Olivier MuselemuEsuka, "Blockchain Technology in Pharmaceutical Industry toPrevent Counterfeit Drugs", International Journal of Computer Applications (0975 – 8887)Volume 180 – No.25, March 2018
[10] Hoai Luan Pham, Thi Hong Tran, and Yasuhiko Nakashima, "Practical Anti-Counterfeit Medicine ManagementSystem Based on Blockchain Technology", The 2019 Technology Innovation Management and Engineering Science International Conference (TIMES-iCON2019)
[11] binance.com, "Symmetric vs. Asymmetric Encryption", https://academy.binance.com/en/articles/symmetric-vs-asymmetric-encryption
[12] Patrick Townsend, "RSA VS AES ENCRYPTION - A PRIMER", https://info.townsendsecurity.com/rsa-vs-aes-encryption-a-primer
[13] dtos-mu.com"UNDERSTANDING THE BASICS OF PUBLIC KEY CRYPTOGRAPHY", https://www.dtos-mu.com/understanding-the-basics-of-public-key-cryptography/
[14] Scanova Blog, "What is a QR Code: A Beginner's Guide", https://scanova.io/blog/what-is-a-qr-code/
[15] Chinmay Jathar, Swapnil Gurav, and KranteeJamdaade, "A Review on QR Code Analysis", International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 8, Issue 7, July 2019
[16] uQR.me, "30 Things You Should Know About QR Codes", https://uqr.me/blog/things-you-should-know-about-qr-codes/
[17] Adam Hughes, "What Are Web Services? Easy-to-Learn Concepts with Examples", https://www.cleo.com/blog/knowledge-base-web-services
[18] guru99.com, "SOAP Vs. REST: Difference between Web API Services", https://www.guru99.com/comparison-between-web-services.html
[19] sciencedirect.com, "Uniform Resource Locator", https://www.sciencedirect.com/topics/computer-science/uniform-resource-locator
[20] Baohua Yang, "10 Practical Issues for Blockchain Implementations", https://www.hyperledger.org/blog/2020/03/31/title-10-practical-issues-for-blockchain-implementations

## AUTHOR

**Cheman Shaik** is a Research & Development professional in Computer Science and Information Technology for the last twenty years. He has been an inventor in these areas of technology with eight U.S Patents for his inventions in Cryptography, Password Security, Codeless Dynamic Websites, Text Generation in Foreign Languages, Anti-phishing Techniques and 3D Mouse for Computers. He is the pioneer of the Absolute Public Key Cryptography in 1999. He is well known for his Password Self Encryption Method which has earned him three U.S Patents. He has published research papers in the international journals – IJCSEA, IJCIS, IJNSA and the proceedings of EC2ND 2006 and CSC 2008.