A Study on Product Authentication and Authorization

Mahmuda Khan Moon
Institute of Information Technology
Jahangirnagar University
Savar, Dhaka

Roksana Akter
Dept. of Computer Science and Engineering
Southeast University
Banani, Dhaka

Rashed Mazumder
Institute of Information Technology
Jahangirnagar University
Savar, Dhaka

ABSTRACT

Fake product has become a major concern in the developing countries like Bangladesh. A good number of products found fake or altered now-a-days. Basic information of the product including company-logo, price, manufacturing and expiring date are printed on product-body or packet. Usually, customers believe those information during purchase time. However, these information can be altered in many ways such as generation and distribution of fake product, and changing the tag. Under this circumstances, an idea is generated that can solve the above issues using a cryptographic tool such as authenticated encryption (AE) and Quick Response Code (QR Code). The target point of using AE is to ensure product authentication and authorization. Furthermore, QR code provides user friendly environment. In this paper, encryption is performed based on the product contents using encryption key and can not be altered without key. This encrypted data is used to create a tag. This tag will be based on AES algorithm and converted into QR code. A valid user can get the tag from the QR. In the next step, a valid user will get all information related to that product.

General Terms

Product Authentication, Watefall Model, UML

Keywords

Authentication, QR codes, AES, Encryption

1. INTRODUCTION

The production of packaged products are numerous. However, fake products are produced at a larger amount than that of the genuine products in certain cases. The fraud manufacturers are making pretty good profit actually. In the certain cases, this profit is more than the original manufacturers [2], [5]. Interestingly, packaged products are not limited to beauty products only. Furthermore, different types of altered or fake packaged foods, medicines, and daily-life goods are available in our local market [16]. As a customer, one can think that the products are original and ready to buy it for his personal usage. Under this circumstance, these fake products create a great financial loss to the valid or genuine manufacturers as well as it creates catastrophic damage in the arena of health sectors [19]. However, this is a very challenging issue to verify the originality of the product as well as expensive in the aspect of time and space complexity.

In this 21st century, it is desired that a smart system ensures the users that the packaged products are genuine using the advanced IT infrastructure. Moreover, the manufacturers are also liable to provide their authentic goods to the customers. Hence, the manufacturers should develop such a smart system that ensures the company good-will as well as customers rights. There is another party, the shopkeepers. In certain cases, shopkeepers face the issue of honesty also because of fake product from supplier.

1.1 Motivation

Everyday a large amount of products are being produced, however, how many of them are original or fake. It is very difficult to find the authenticity of the product in efficient manner. A lot of problems are available with the existing system:

(a) Lack of authentication and authorization
(b) Fake QR code can be generated
(c) Original manufacturer faces a lot of negative cash-flow due to fake product
(d) Compromising the quality of product can lead to health issues

Because of these problems customers do not get the benefit as well as manufacturers face a great loss in their businesses. There are a lot of methods to address these issues.

1.2 Backgrounds

In 1951 Norman Joseph Woodland and Bernard Silver invented " Barcode " which was extended to thick and thin bars. It was based on Morse code. It became really popular when it became able to automate supermarket checkouts [9]. Barcode was introduced to make shopping experience more enjoyable while also helping the inventory management [4]. But the problem arose with the growth of technology. People having smart phones can surf internet and can scan any barcode to see the details of a product. If all the information is available in the web and visible to everyone, it is comparatively easier to create thousands of fake barcodes from a single original one.

Another technology was introduced after barcodes known as "RFID (Radio Frequency Identification)". It was introduced to replace barcodes in supply chain management eventually [13]. It attracted a lot of interest because of it's large convergence of lower cost and the increased capabilities of RFID keys. However, there is a major drawback of this system such as threat of security [3].

Moreover NFC (Near Field Communication) can be another solution. However, NFC can work under limited distance such as around 4 inches initially [20]. Later NFC tags overcome this demerit. Now, NFC tags works by encoding data with a secret key. The key is hidden in the database and tags and upon scanning the encoding/decoding is performed dynamically. Though, it sounds quiet secured and reliable. However, there is a small issue with this technology. NFC tags use a mechanism called scanning counter that depends on how many times the tag has been scanned. Hence, the result of scanning changes each time when the tag is scanned [17]. Moreover, the technology gets more complicated to implement and the reliability decreases also. While we need to deal with so many products over internet, an error can occur during scanning period. As a result, it is very much unsuitable for everyday usage that includes large volume of products.

2. OBJECTIVES

The main objective of this proposed system is to solve the mass product adulteration issue. Due to product adulteration consumers do not get the benefit from the products that they are originally supposed to. In fact there might be opposite results like health issues. This system can be used in the field of medicine which can be of great advantage since there is already a good percentage of sufferer of duplicated medicine. Other objective alongside this achieved by this proposed system are:

(1) To provide customer, an easy access to the products details
(2) To prevent customer from paying over price of a product
(3) To prevent customer from buying fake product
(4) To prevent or reduce the loss of manufacturer
(5) To keep a track or record of the product

3. PROPOSED SYSTEM

3.1 System overview

This system uses AES algorithm that will ensure the product details like manufacturing date, expiring date, price etc have not been tampered with. Then, it will generate a QR code. Later, this code will be scanned by the customers. First part of the work is performed by the manufacturers. They can simply feed the information into the system. With the help of the encryption algorithm tag will be generated automatically.

Customer starts with the scanning of the QR code. usually, it is attached or printed on the product. By scanning the QR codes, customers will view the encrypted tag. This tag can be verified with the official website of the manufacturing company along with the product id. The feedback message from the website contains the information like product's validity. In addition, if the product is valid an additional message will return with the validation message. This message then can be used to perform decryption. The ultimate result of the decryption is the description of product.

Verified vendor will be provided with the authority to update the product status once the product has been sold. This will help to verify the original product even if any third party becomes successful to steal the information or to copy the same QR code. Moreover, the customer can easily see that the product is sold out. Hence, duplicate or copied QR code can not help the fraud manufacturers. Figure 1, shows the general structure of the product authentication system. In addition, Figure 2, describes the work flow of the system. Moreover, Figure 4, states the sequence diagram of the system that represents the data flow of the product authentication.

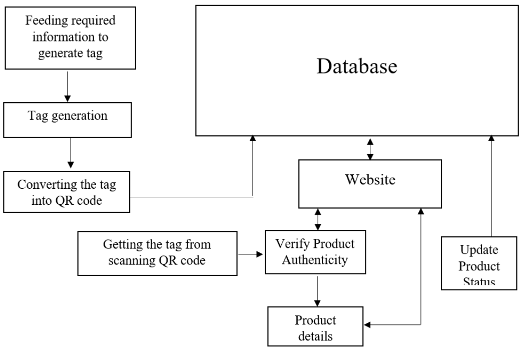

Feeding required information to generate tag
Tag generation
Converting the tag into QR code
Database
Website
Getting the tag from scanning QR code
Verify Product Authenticity
Update Product Status
Product details

Fig. 1. General structure of the product authentication system.

3.2 System module

In this system there are three types of modules such as, **Manufacturer** needs server and stable network connectivity through the business demographic area.

(1) To feed product details into the system to be encrypted
(2) To generate QR codes from the tags created
(3) To update the database with new products
(4) To provide shopkeepers with the authority to update product status

Customer need smart devices.

(1) To read the details of a product
(2) To check if the information mentioned about the product is true or not
(3) To verify with the company if the product really belongs to the mentioned one

Vendor needs high definition machine.

(1) To update about product status after sell of a product

3.3 Procedure

3.3.1 AES algorithm. The AES (Advanced Encryption Standard) is a tool of symmetric encryption that helps to protect the data [8, 6]. It is a symmetric block cipher to protect information. AES can be implemented by software or hardware module to encrypt data [18]. Here, AES-256-CTR has been used to perform encryption. This algorithm first breaks the whole message into blocks of 128 bits. Then a key is used to encrypt this blocks. The key here is of 256 bits. For a 256 bits key length, the block of message will go through a loop of 14 rounds. In each rounds, the block of data goes through 4 phases of data scrambling.

3.4 QR code

Usually, QR code has four types of standardized encoding modes. These modes are used to store data usually [12]. This is very popular tool in the business arena due to the nature of readability and user friendly properties. Moreover, the storage capacity of QR is remarkable [1]. A representation of QR is a black square that can be read by a smart device like smart mobile or else [1].

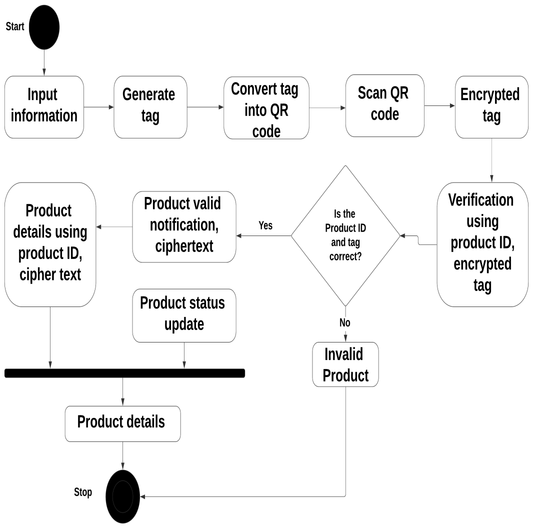

Start
Input information
Generate tag
Convert tag into QR code
Scan QR code
Encrypted tag
Verification using product ID, encrypted tag
Is the Product ID and tag correct?
Yes
No
Product valid notification, ciphertext
Product details using product ID, cipher text
Product status update
Invalid Product
Product details
Stop

Fig. 2. Work flow of the system using Activity Diagram.

4. IMPLEMENTATION OF THE PROPOSED SYSTEM

The implementation of this system is performed in a few sequential steps. These steps are represented as the tasks performed by each user module. Moreover, we use waterfall model to develop the entire system (Figure 3) [11] .

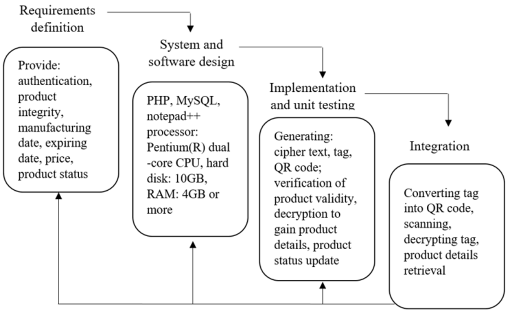

Requirements definition
Provide: authentication, product integrity, manufacturing date, expiring date, price, product status
System and software design
PHP, MySQL, notepad++ processor: Pentium(R) dual -core CPU, hard disk: 10GB, RAM: 4GB or more
Implementation and unit testing
Generating: cipher text, tag, QR code; verification of product validity, decryption to gain product details, product status update
Integration
Converting tag into QR code, scanning, decrypting tag, product details retrieval

Fig. 3. Waterfall model: To develop the product authentication system [14]

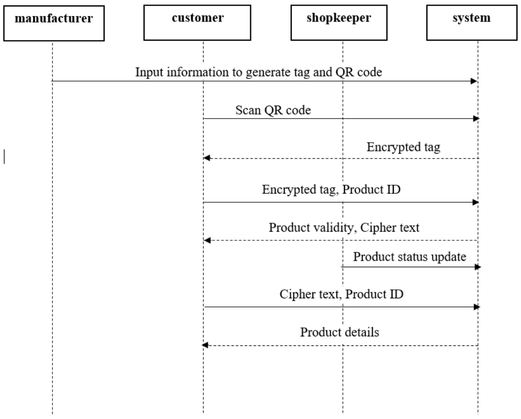


Fig. 4. Sequence diagram of the product authentication system

4.1 Manufacturer module

4.1.1 Tag generation. The first task of the manufacturer is to create a tag for the manufactured products. The tag is a series of binary digits that is created based on the information of the product or product batch. After that, the system generates QR code from the previously generated tag. In addition, that will be stored into the manufacturer's database. As a customer, one can scan the QR code. Later, this will be used to retrieve the main information of the product. Generation of this tag is consisted of three major parts.

(a) **Feeding information.** The initiation of the system is performed with the input of information. Manufacturer module inputs product details like product name, manufacturing date, expiration date, and price. Using encryption key at the system, executes encryption process and generates cipher text.

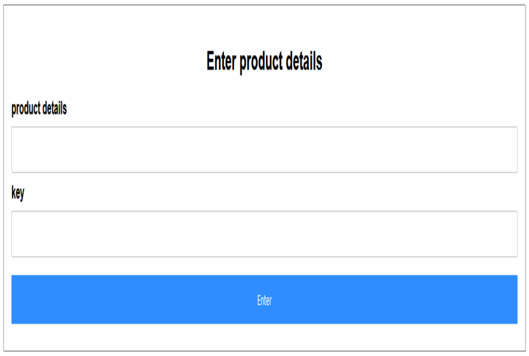
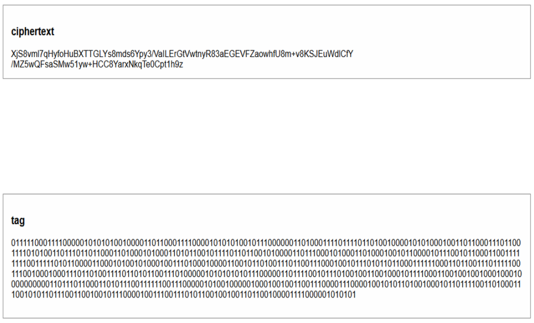


Fig. 5. Entering information into the system.

(b) **Creating cipher-text.** Cipher-text is an encrypted or encoded information that contains the original message in hidden form. Usually, cipher-text is unreadable without the proper key [10]. In this work:
i. AES: Generation of Cipher-text
ii. Key size is 256-bit

(c) **Generating tag.** After creating cipher-text from manufacturer end, a random string will be generated. This random string is the same length as the cipher-text. Then this string will be xored with the cipher-text. This resultant string is converted into binary bit series called as the tag. Figure 6, shows the cipher-text and tag generation after inserting the product information and encryption key.



ciphertext

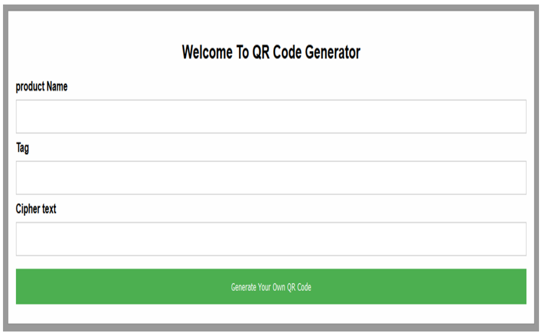
XjS8vml7qHyfoHuBXTTGLYs8mds6Ypy3/VaILErGtVwtnyR83aEGEVFZaowhfU8m+v8KSJEuWdlCfY
/MZ5wQFsaSMw51yw+HCC8YarxNkqTe0Cpt1h9z

tag

0111110001111000001010101001000011011000111100001010101001011100000011010001111011110110100100001010100010011011000111101100
1111010100110111011011000110100010100011010110010111101101100101000011011100010100011010001001011000010111001011000110011111
1111001111101011000011000101001010001001110100010000110010110100111011001110001001011101011011000111111000110110011101111100
111001000100011101101001111011010110011101000001010101010111000001101111001011101001001100100010111100011001001001000100010
000000000110111011000110101110011111100111000001010010000010001001001100111000011100001001010110100100010110111100110100011
10010101101110011001001011100001001110011101011001001001101100100001111000001010101

Fig. 6. Generating cipher-text and tag.

4.1.2 Converting tag into QR code. Once the tag and cipher-text are generated, these information will be entered into the system along with the name of the product. QR will be generated from the above data. In the Figure of 7 and 8, the graphical representation is available.



Welcome To QR Code Generator

product Name

Tag

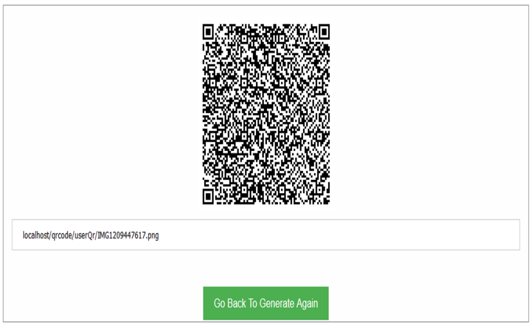
Cipher text

Fig. 7. Conversion: Tag to QR

While generating QR code the system simultaneously stores the information that have been entered into the system (DBMS) previously. Newly generated QR code are also saved at the database in similar clock-time. For each new entry into the database, product status is set as an unsold. In addition, database generates an id for each entry automatically. At last, QR code will be attached to the product along with non-identical id.

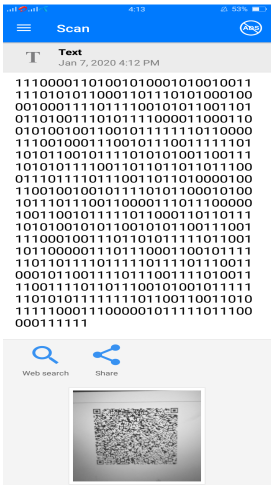
4.2 Customer module

4.2.1 Scanning products. In the customer end, one can get QR-code from product and scan the code using smart device like smart mobile phone. After scanning the QR code, the tag is provided as the scan result. Figure 9 shows the initial view a customer gets after scanning a product.



localhost/qrcode/userQr/IMG1209447617.png

Fig. 8. QR code Generation



Text
Jan 7, 2020 4:12 PM

1110000110100101000101001001 1
1110101011000110111010100010 0
0010001111011110010101100110 1
0110100111010111100001100011 0
0101001001100101111111011000 0
1110010001110010111001111110 1
1010110010111101010100110011 1
1010101111001101101101101110 0
0111011110111001101101000010 0
1100100100101111010110001010 0
1011101110011000011101110000 0
1001100101111110110001101101 1 1
1010100101011001010110011100 1
1110001001110110101111101100 1
1011000001110111000110010111 1
1101101111011111011110111001 1
0001011001111011100111101001 1
1100111101101110010100101111 1
1101010111111110110011001101 0
1111100011100000101111101110 0
000111111

Fig. 9. Output: Scanning QR code

4.2.2 Validity Check of the Product. After getting the tag from scanning the QR code, customer can copy the tag. In the next phase, they can use this tag for verification from manufacturer's central database through web-portal. In this section, a customer can check two types of data set:

(1) Verify Product

(2) Get Product Details

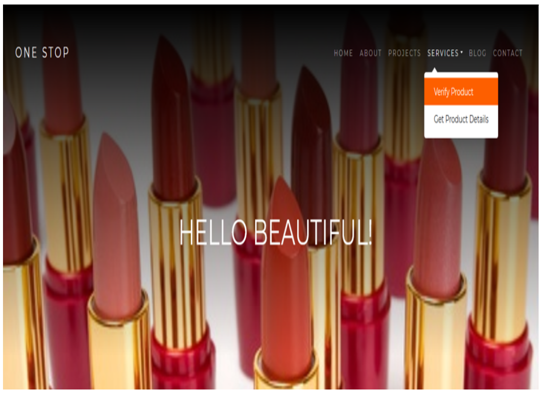
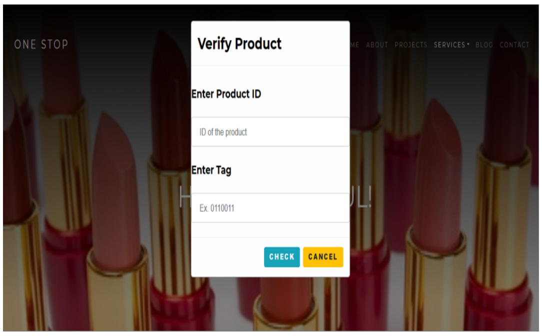


Fig. 10. Product Verification Module

When the customer selects the option of verify-product, a pop up box will ask for ’product-id’ and ’tag’ (figure 11). Hence, customer can simply put the tag copied before and product-id.



Verify Product

Enter Product ID

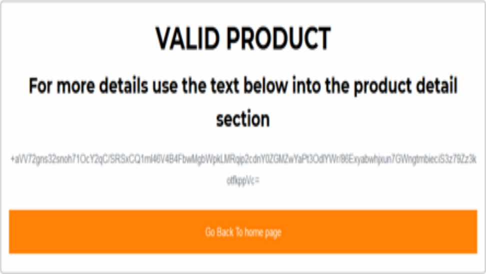
ID of the product

Enter Tag

Ex: 0110011

Fig. 11. Pop up box for product verification.

If the ’product-id’ and ’tag’ are matched with the id and tag of manufacturing company’s database, it is declared as a valid product. Moreover, a cipher-text along with the validation message is returned to the customer. If the customer wants to get more information about the product then one can use this cipher-text into the ’get product details’ option for further procedure. Figure 12 below shows the validation message customer gets.



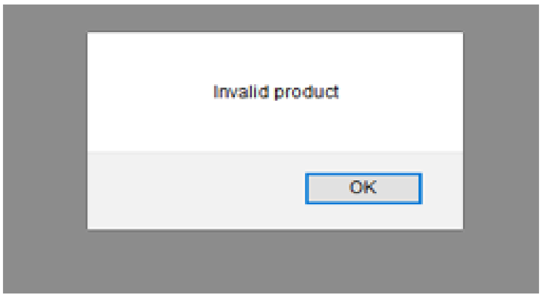
VALID PRODUCT

For more details use the text below into the product detail section

+aVV72gns32snoh71OcY2qC/SRSxCQ1ml46V4B4FbwMgbWpkLMRqjp2cdnY0ZGMZwYaPt3OdfYWr86Exyabwhjxun7GWngtmbieciS3z79Zz3k otfkppVc=

Fig. 12. Valid product.

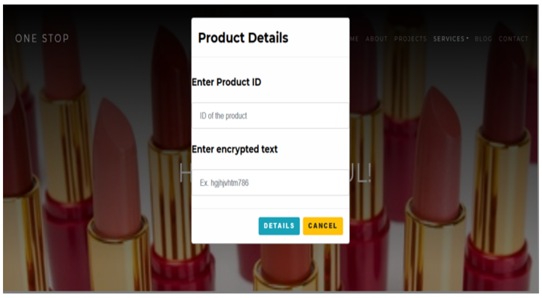
’Product id’ or ’tag’, has chance not to match with the information of manufacturer’s. Under this circumstance, the product is considered to be fake. Hence, an invalid message like figure 13 will show up.



Invalid product

Fig. 13. Invalid product.

4.2.3 Product details. After confirming the authenticity of the product, if the customer wants to verify its integrity, the customer can verify the in-details that is written onto the product surface. A customer needs to get product details, in that case a pop up box will appear. Therefore, customer only has to copy the cipher-text and paste it into the ’Enter encrypted text’ and provide product-id into the ’Enter product id’ section (figure 14).



Product Details

Enter Product ID

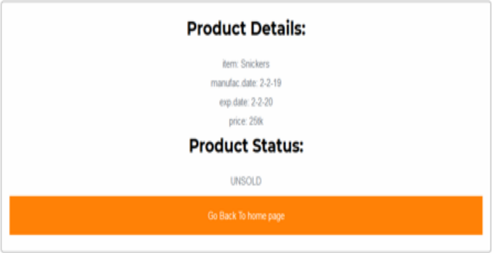
ID of the product

Enter encrypted text

Ex: hghjvhtm786

Fig. 14. Pop up box for product details.

After entering the information, the system will compare the id with the stored value at the database server. The database decrypt the cipher-text using the key by the respective authority. As a result, customer can view the product details as shown in figure 15.



Product Details:

item: Snickers

manufac.date: 2-2-19

exp.date: 2-2-20

price: 25tk

Product Status:

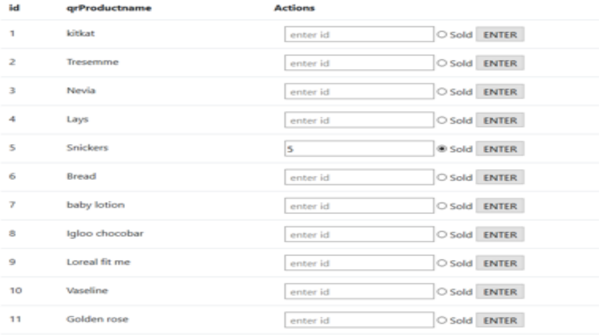
UNSOLD

Fig. 15. Product details.

4.3 Vendor module

A Vendor is responsible to update the information of product. Once the product is sold, an authorized vendor will update the status of the product.

- —The authorization process of vendor module is performed by verified vendors. An authorized vendor will create account under the manufacturer. Hence, the information of Vendors will be stored in the database of manufacturers. The authenticated vendor will log into their account and update status of the product. Figure 16 shows the updating of product status.
- —Vendor can see the individual lists from each manufacturer that contains all the products ’id’ and ’name’
- —In the list, vendor can enter the id of product and notify as a ’sold’



id	qrProductname	Actions
1	kitkat	enter id ○ Sold ENTER
2	Tresemme	enter id ○ Sold ENTER
3	Nevia	enter id ○ Sold ENTER
4	Lays	enter id ○ Sold ENTER
5	Snickers	5 ● Sold ENTER
6	Bread	enter id ○ Sold ENTER
7	baby lotion	enter id ○ Sold ENTER
8	Igloo chocobar	enter id ○ Sold ENTER
9	Loreal fit me	enter id ○ Sold ENTER
10	Vaseline	enter id ○ Sold ENTER
11	Golden rose	enter id ○ Sold ENTER

Fig. 16. Updating product status.

5. PROPOSED SYSTEM SECURITY ANALYSIS

Security analysis is the examination and evaluation of various factors that can affect the security of a system. It is the study that ensures that no intruder or unauthorized individual will be able to access any of the components or data of the system. That is the system will be well protected from any harmful activity. The security of this system is quiet reasonable:

(1) **QR codes.** In current system, the information hold by the tags are written in human language. Which makes it easy to copy them. But QR codes provides an initial level of security. If the information is hidden how fraud manufacturers will copy. However, it is not a strong security measure because of QR code's easy accessibility.

(2) **Tag.** The main security is provided by the tag. The tag is first generated by AES algorithm where the size of key is of 256 bits. After generating the cipher-text, a random string will be xored with the cipher-text. In next phase, this random string is converted into binary bits for getting tag. Hence, the security of tag generation depends on symmetric key size of AES [7]. The security of key is compromised if there is an exchange of keys between the required parties. It can be stolen or even dropped while exchanging the key. But in this system the encryption and decryption both are performed on the manufacturer side. Hence, there is no need for exchange of keys. As a result, it is quiet impossible to have access to the keys without intruder (Man in the Middle Attack).

6. COMPARATIVE STUDIES WITH EXISTING SYSTEMS

Here existing system refers to the regular barcodes that is used for product verification. The points below shows how product authentication system is different from the existing system and why it is better. Product Authentication system uses QR codes(Quick Response Code) as product details accessing mechanism. Using this mechanism gives following benefits over the existing system:

(1) **Additional Information:** Barcodes carries information only in horizontal dimension but QR codes can hold value both in vertical and horizontal dimension and thus can contain more information. Moreover, a QR code memory management is better [15].

(2) **Variety in reading:** A QR code is capable of being read in 360 degrees, from any direction, thus eliminating any interference and negative effects from backgrounds [15].

(3) **Product status:** Previous systems like barcodes do not have any option regarding product status. That is if the product is already sold or not. But this system will show the status of the product. Which will be a great help to ensure the authenticity because after selling of a product, verified authorities will update the database saying the product has been sold. So, when a customer will scan the same product it will show that it's already sold. At that time if the product is in any shopping centre for sell then the customer can be sure of it being a fake one.

(4) **Ensures authenticity:** Using tag generation, the system keeps the information of the product secret. In the final stage of the product purchasing, customer can verify the product is genuine or not.

7. CONCLUSION

In this paper, the problem of fake products has been studied. Ensuring product authenticity is a much bigger concern than it appears at the first glance. In addition, there are certain technological advances which are available in our current world. The proposed method tried to make a bridge between problems and technological solutions. Usually, barcodes are used to ensure authenticity. However, barcodes can be easily copied and it can be re-generated. Hence, proposed model imposes encryption technique for tag and cipher-text generation. A new system has been discussed that would be able to solve the product duplicating issue with existing technology. The proposed model, hides the product information and protects it from copying. Usually, this system is suitable for retail traders. In addition, this system is easy to implement, affordable and suitable for practical uses. This system has been simulated and gives a good result. Therefore, there is a great opportunity to keep the information of the product secret by adopting this proposed system in real life and customer can verify if the product is genuine or not.

References

[1] Denso ADC. "QR Code Essentials". In: (Jan. 2013). Archived from the original on 12 May 2013. Retrieved 12 March 2013.

[2] ADWEEK. *Counterfeit Goods Are a $460 Billion Industry, and Most Are Bought and Sold Online*. https://www.adweek.com/brand-marketing/counterfeit-goods-are-a-460-billion-industry-and-most-are-bought-and-sold-online/. 13 February 2017.

[3] Himja Agrawal and Prof.P.R.Badadapure. "A Survey Paper On Elliptic Curve Cryptography". In: *International Research Journal of Engineering and Technology(IRJET)* 3 (Apr. 2016).

[4] Barcode.com. *History of the Bar Code*. https://barcode.com/20110610585/history-of-the-bar-code.html. [Online, Accessed 2 January, 2020]. 2020.

[5] CNN business. *The 'fakes' industry is worth $461 billion*. https://money.cnn.com/2016/04/18/news/economy/fake-purses-shoes-economy-counterfeit-trade/index.html. 18 April 2016.

[6] BusinessDictionary. *Mechanism*. http://www.businessdictionary.com/definition/mechanism.html. [Online, Accessed 8 January, 2020]. 2020.

[7] Sumanta Chatterjee. *How long will it take to break a 256 bit AES encryption key using brute force?* https://www.quora.com/How-long-will-it-take-to-break-a-256-bit-AES-encryption-key-using-brute-force. [Online, Accessed 12 January, 2020]. 13 June 2017.

[8] Comparitech. *What is aes encryption and how does it work*. https://www.comparitech.com/blog/information-security/what-is-aes-encryption/. [Online, Accessed 8 January, 2020]. 2019.

[9] Wikipedia Contributors. *Barcode*. https://en.wikipedia.org/wiki/Barcode. [Online, Accessed 2 January, 2020]. 21 January 2020.

[10] Wikipedia Contributors. *Ciphertext*. https://en.wikipedia.org/wiki/Ciphertext. [Online, Accessed 12 January, 2020]. 18 December 2019.

[11] Wikipedia Contributors. *WM*. https://en.wikipedia.org/wiki/Waterfall$_{m}odel$. [Online]. Oct. 2021.

[12] Denso-Wave. “QR Code features”. In: (Jan. 2013). Retrieved 3 October 2011.

[13] Christoph Jechlitschek. “A survey paper on Radio Frequency Identification (RFID) trends”. 24 April 2006.

[14] Dejan Baca Kai Petersen Claes Wohlin. *The Waterfall Model in Large-Scale Development*. June 2009.

[15] Mobie-QR-Codes.org. *How are QR codes better than barcodes*. http://www.mobile-qr-codes.org/qr-codes-vs-barcodes.html. [Online, Accessed 11 January, 2020].

[16] Allied Market Research. *Packaged Food Market by Product Type (Ice Creams, Pasta, Cheese, Yogurt, Nuts, Biscuits, Baby Food, Soups, Potato Chips, Instant Noodles, Non-Alcoholic Drinks, Breakfast Cereals) - Opportunity Analysis and Industry Forecast, 2014 - 2020*. https://www.alliedmarketresearch.com/packaged-food-market. July 2015.

[17] Seritag. *NFC tag Authentication*. https://learn.seritag.com/tech/nfc-tag-authentication-explained. [Online, Accessed 3 January, 2020]. 21 June 2019.

[18] TechTarget. *Advanced Encryption Standard (AES)*. https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard. [Online, Accessed 8 January, 2020]. 2020.

[19] Hetty Tullis. *13 Terrifying Dangers Of Counterfeit Makeup*. https://www.thetalko.com/13-terrifying-dangers-of-counterfeit-makeup/. 15 December 2015.

[20] How stuff works. *What’s an NFC tag?* https://electronics.howstuffworks.com/nfc-tag.htm. [Online, Accessed 3 January, 2020]. 2019.