PRODUCT AUTHENTICATION USING QR-CODE THROUGH CLOUD

Prof. Sagar Thakare
Assistant Professor,
NCRD's Sterling Institute of Management Studies, Navi Mumbai

Mr. Vighnesh Gadekar
NCRD's Sterling Institute of Management Studies, Navi Mumbai

Mr. Mandar Gharat
NCRD's Sterling Institute of Management Studies, Navi Mumbai

ABSTRACT

The development of a new product or technology always comes with the risk of getting duplicated, something that could affect company revenue and good will. QR codes present themselves as a low cost mobile solution which helps enterprises and consumers identify the authenticity of products. This is a convenient process as it can be deployed on smart phones and other mobile devices .Although the usage of QR codes for this purpose has been prevalent for a while, this POV highlights how companies can derive instantaneous results and detection that goes beyond mere QR code implementation. Product Authentication is one of the fundamental procedures to ensure the standard and quality of any product in the market. Counterfeit products are often offered to consumers as being authentic. Counterfeit consumer goods such as electronics, music, apparel, and Counterfeit medications have been sold as being legitimate. Efforts to control the supply chain and educate consumers to evaluate the packaging and labeling help ensure that authentic products are sold and used. Our work ensures that the task is made as simple with the help of a camera enabled mobile phone supported with QR (Quick Response) Code Reader. We propose a model whereby the application in the mobile phone decodes the captured coded image and sends it through the Cloud Data for authentication. The response received from the cloud enables the consumer to decide on the products authenticity.

KEYWORDS: *QR-code, authentication, counterfeit, security, genuineness, encryption, decryption.*

INTRODUCTION

According to the United Nations, the counterfeit market is worth Us $250 billion a year and growing. Almost every company faces the threat of product duplication as it not only hits revenue but also damages brand reputation. Companies often do not recover their R&D investments due to these losses, thus influencing their potential to create impactful products in the future.

There is also a school of thought that believes that counterfeit products fund organized crime in certain countries. This is something that no company of repute would want to be associated with duplicate puts consumers at risk and certain products can Cause serious health risks or even be fatal. On a strictly economic note, with a highly competitive market and shrinking margins, a counterfeit operation directly hits the top line and bottom line of the company and can be detrimental to business longevity. Authentication is one of the most important process for any consumer to identify whether the product we buy was from an authentic manufacturer or from any fake company. The consumers cannot judge whether the product is original or duplicate on their own by checking the manufactured date and the expired date. The lack of awareness about a products authenticity was well exposed in a recent issue where the consumers faced an issue with the duplication of products. The present authentication systems dealing with the product identification and authentication are Barcode and Hologram. The

drawbacks of the barcode and 3-D hologram technique have led to the evolution of a new technique called the QR code [1][2](Quick Response).

QR Code was created as a step up from a bar code. QR Code contains data in both vertical and horizontal directions, whereas a bar code has only one direction of data, usually the vertical one. QR Code can also correspondingly hold more information and are easily digested by scanning equipment, and because it has potentially twice the amount of data as bar code, it can increase the effectiveness of such scanning. Further QR Code can handle alphanumeric character, symbol, binary, and other kinds of code. All the products we buy will have a (QR) code printed on its cover and it is unique for each product which is going to be used in our authentication system. Then the code is encrypted to add more security to the code and it is sent to the central web server which is in the cloud. The code is searched with a searching algorithm and if it is found, the data in the manufacturer's database is marked as bought and a reply is sent to the central web server that the product is original. If a match is not found then the manufacturer's server will return message stating that the product is duplicate.

SYSTEM INVOLVES

1. Mobile Phone
2. QR-Code Scanner application
3. Server System

RELEATED WORK

Authentication of consumer products can be done with the QR codes it is printed on the cover of the product it is captured as an image through the camera attached with the mobile phone. The image is then opened with the QR code reading application to extract the data from the code and is sent to the central web server. The web server is connected to the cloud with through internet; the web server on receiving the QR code sends the data to the corresponding manufacturer's server in the cloud. The manufacturer's server using a searching algorithm looks for the data in the corresponding database. If the data is found a reply is sent to the central server stating that the product is original and if the corresponding record is not found then the manufacturer's server sends a message to the central server stating that the product is a duplicate one. The web server on receiving the message from the manufacturer's server sends a message to the user stating the status of the product and the user on receiving the message from the central server can then decide on buying the product. The mobile phone is the important device which is used in our proposal as the user needs a device to send the data and receive a reply from the web server. It is found that by the end of 2009, almost every people are using mobile phones and by 2016, that number is projected to grow to 6 billion, which is much more than the personal computer users which show that nearly everyone has a mobile phone. So the same can be used for our process rather than buying a new device for authentication process. The most important advantage in this model by using the mobile phone is; the user can send the data and get the reply without anybody's help or intervention thus the privacy is maintained and The speed of transfer is also high[3].

DEVICE USED & CONCEPT

The mobile phone is the important device which is used in our proposal as the user needs a device to send the data and receive a reply from the web server. So the same can be used for our process rather than buying a new device for authentication process. The most important advantage in this model by using the mobile phone is; the user can send the data and get the reply without anybody's help or intervention thus the privacy is maintained and The speed of transfer is also high . The QR code reader [4] is developed with J2ME to make it work in java

enabled mobiles. The reader is done with the QR code reader library which allows us to decode the data in the QR code

```
decrypt()
{
   if ( image == QR-Code)
     {
       decrypt the code and  get the data;
     }
    else
     {
       return decryption Failed;
     }
}
```

Fig 1: Decryption Concept

```
Reply()
{
  if(data == found )
   {
     return original product
   }
  else
   {
     return fake product
   }
}
```

Fig 2: Reply concept

WHAT COMPANIES DO?

Most companies who value their brand and business have track-and-control mechanisms in place to deter, if not eliminate, counterfeit production and distribution. This includes hologram stickers, watermarks, mass communication, surprise checks, controlled distribution systems, and robust eRP system implementations. The governments also do their bit through central or state regulatory bodies that add another layer of check on counterfeit. On a global scale, United Nations and powerful industry associations work in tandem with local authorities to curb counterfeit activities. However, as the numbers suggest, there is always room for more to be done[2]. This Point of View (POV) presents to you a low-cost mobile solution that adds one more identification layer to the track-and- control process through the use of Quick Response (QR) codes. This simple solution is easy to deploy and takes advantage of today's ubiquitous smartphones and your everyday mobile applications. Though the use of QR codes in counterfeit deterrence is not new, our POV highlights 'closing the loop,' which is necessary for counterfeit detection to be more effective than mere QR code implementation.

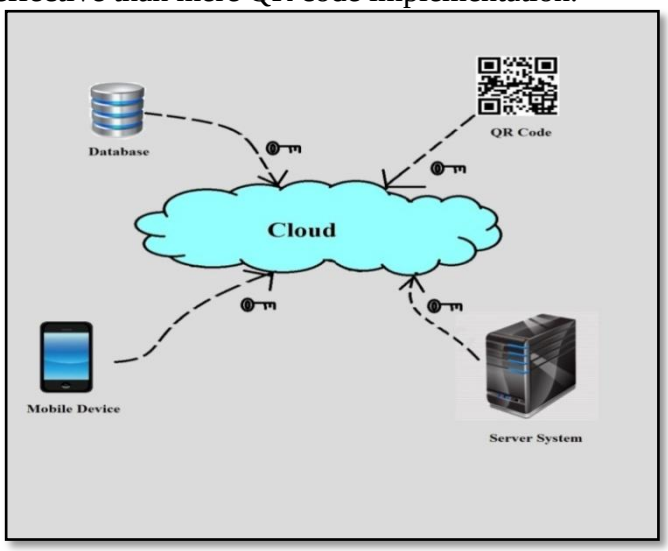

Fig 3: Showing how data is stored & accessed securely through cloud

SECURITY USED FOR MODEL

Attacking the transmitted signal is considerably increased in the recent years. So there is a high probability of hacking the data sent to user and modify it to show that the product scanned is original by the hacker. To avoid such attacks the system should also be able to resist the intrusion. The system is made more secure with the help of applying an encryption algorithm to it. Asymmetric encryption pairs two keys together to encrypt and decryption messages to ensure it is kept secure during a transfer [5]. This method is often considered a better option than Symmetric encryption for larger businesses. According to Microsoft, using this method means "you do not have to worry about passing public keys over the Internet (the keys are supposed to be public). A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message."

Designs of asymmetric encryption schemes rely on tools and ideas different from those underlying the design of symmetric encryption schemes. Namely in the asymmetric case, the basis is (typically) computationally intractable problems in number theory, while for the symmetric case we used block ciphers. Thus, the greater part of the effort in this chapter will be on schemes and their security properties. An asymmetric encryption scheme is just like a symmetric encryption scheme except for an asymmetry in the key structure. The key pk used to encrypt is different from the key sk used to decrypt. Furthermore pk is public, known to the sender and also to the adversary. So while only a receiver in possession of the secret key can decrypt, anyone in possession of the corresponding public key can encrypt data to send to this one receiver.

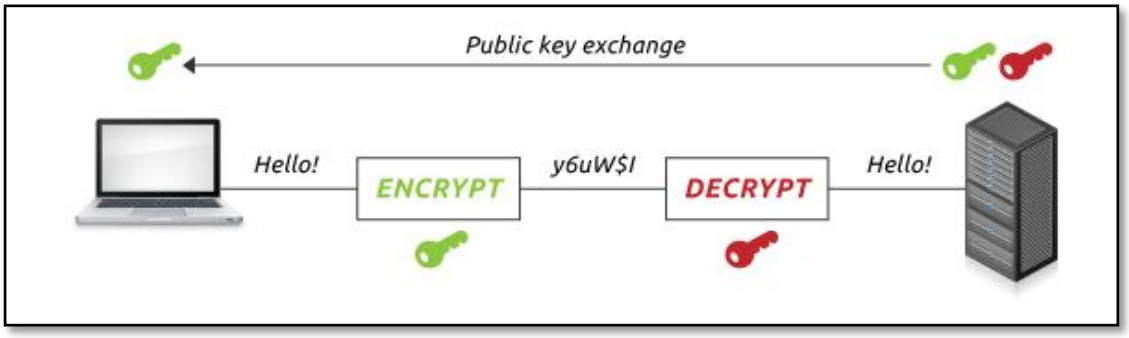

Fig 4: Showing encryption & Decryption process

PROPOSED METHODOLOGY

Counterfeit identification – When a customer sends out the QR code to the predefined server to check product genuineness, it is marked as 'QR registered'. if at a later point in time, multiple data access are received for the same QR code from a different location or city, then it can be as certain that a counterfeit is in circulation. This is counterfeit identification as it will tell the company that someone has circulated mass copies of the same QR code and distributed the 'same label' counterfeits in the market. A genuine product will not encounter multiple QR code checks from different locations. The user will scan the QR Code from his/her smart phone using QR code scanner application. The data which is scanned from that QR Code is then sent to server in encrypted format. The scanned data is then checked at server database whether it is a genuine code or not then appropriate result is sent back to the user which user can see to verify the product's authenticity.

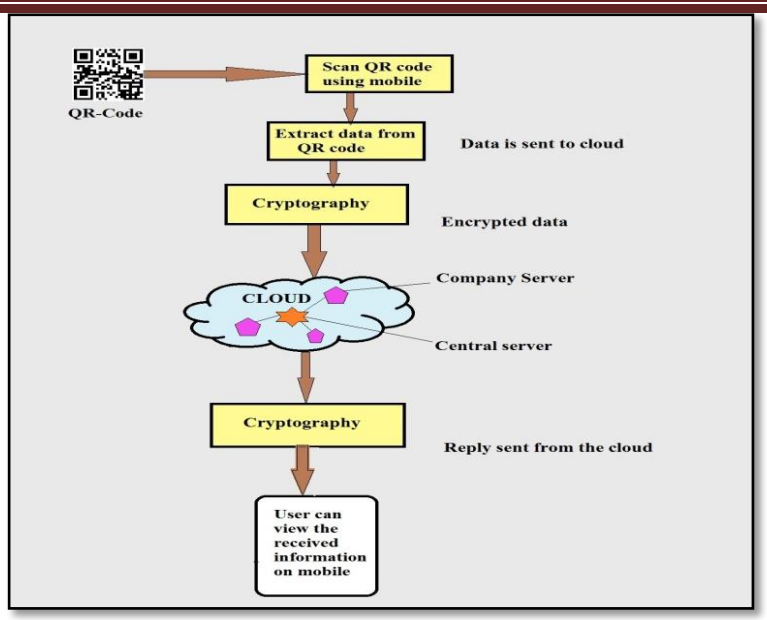

Fig 5: working of model

CONCLUSION

The user must have a device or smart phone through which he will scan the QR-code, using any QR code scanning application. That scanned data will be sent to the cloud. The data which is sent to cloud will be sent in secured manner using cryptography encryption & decryption technique. There data will be decrypted and data is matched with the saved record. All the companies' servers are connected to central server through cloud. So that any person can access the data from anywhere. There inside the server data is decrypted and checked with stored value in database. If record is found in data base reply method will inform user that the product is genuine. Otherwise it will notify the user that product is not valid product. We thus conclude our proposed model saying that this will be a good product Authentication System and can be implemented in day to day life by the people for checking the authenticity of the genuine products. Thus this proposed model will also help companies to find the Counterfeit products.

REFERENCES

[1] The Green Grid Consortium http://www.gridbus.org/cloudsim/

[2] R.Buyya, C.S.Yeo, S.Venugopal, J.Broberg, and I.Brandic. Cloud Computing and Emerging IT platforms : Vision, Hype and Reality for Delivering Computing as the 5th Utility. Future Generation Computer Systems, 25(6):599-616, Elsevier, June 2009

[3] A General Scheme for Extracting QR Code from a Nonuniform Background in Camera Phones and Applications Yu-Hsuan Chang; Chung-Hua Chu; Ming-Syan Chen; Nat. Taiwan Univ., Taipei

[4] Recognition of QR Code with mobile phones Yue Liu ; Ju Yang ; Mingjun Liu ;Sch. of Inf. Sci. & Eng., Univ. of Jinan, Jinan.

[5] "Cryptography and Network Security", Atul Kahate, Third Edition.