Volume : 4 | Issue : 9 | Sept 2015 • ISSN No 2277 - 8179

Research Paper

# Dynamic Authentication System for Consumer Product Using Quick Response Code in Mobile Cloud Computing Environment

Computer Science

**KEYWORDS :** Cloud Computing, QR codes, Authentication, 2D Codes, Security as Services.

**MS.V.MALATHI** — M.PHIL Research Scholar, PG & Research Department of computer science,Hindusthan college of arts and science, coimbatore.

**MRS.M.HEMALATHA** — assistant Professor, PG & Research Department of Computer Application,Hindusthan college of arts and science,coimbatore.

## ABSTRACT

*The objective of the work is to propose dynamic authentication system for consumer product using quick response (QR) code in mobile cloud computing environment. 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. In recent years, extensive research has been carried out on vision-based automatic identification technology that recognizes image codes using a camera phone, and then provides various services. A novel method 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 Management Interface for authentication. The system then forwards the message to product manufacturer's data center or any central database and the response received from the cloud enables the consumer to decide on the products authenticity.*

## INTRODUCTION

Authentication is one of the most important processes for any consumer to identify whether the product we buy was from an authentic manufacturer or any fictions company and also to ensure that the product is well within the limit of its expiry. In the recent times there are a lot of duplicate and expired products present in the market, the duplication of products has penetrated into many products starting from basic provisions to more important pharmaceuticals. 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 medicines. It has been found that many expired medicines has been recycled and sold in the market as new ones. This problem occurred mainly because of improper authentication system to find whether the product is an original one.

Thus to prevent this from happening again in this pharmaceuticals field or with any other consumers product, a proper effective authentication system must be implemented which prevents the shop keepers or the stockiest to modify any of the records regarding the originality of the product. Hence we, try to make use of the next generation paradigm i.e., cloud computing to ensure the products identity.

## EXISTING PRODUCT AUTHENTICATION METHODS

The present authentication systems dealing with the product identification and authentication are Barcode and Hologram. Barcodes are the most common form of identify establishment technique where a series of black vertical lines of various widths associated with numbers is printed on every product. Being an age old technique this is quite easily duplicated the second and most efficient technique is the Holograms. Holograms are photographic images that are three-dimensional and appear to have depth. The hologram is printed onto a set of ultra-thin curved silver plates, which are made to diffract light, and these thin silver plates are pasted on to the product for its authenticity. But the technique of hologram stickers are a bit expensive because of its cost of manufacturing and hence authenticating a low price consumer goods would not be a feasible solution. The draw backs on the above techniques are that on the one end the bar code can be easily duplicated and on the other extreme the hologram stickers are quite sophisticated for normal consumers to identify the intricate details and come to a conclusion about the originality of the product.

## PROPOSED SYSTEM

The drawback of the barcode and 3-D hologram technique has led to the evolution of a new technique called the QR code (Quick Response). It is a plain old matrix code manufactured with the intent of decoding it at very high speed. 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. QR Code also has an error- correction capability, whereby the data can be brought back to full life even if the symbol has been trashed. All of these features make QR Code far superior to bar 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. This application reads the codes printed on the external cover of the product and it is encoded to get the data stored in the code. 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 through SMS (Short Messaging Service). The data can also be sent through WAP (Wireless Access protocol) and MMS (Multimedia Messaging Service). The central server collects the data and checks the data in the manufacturer's server for the products code. 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. The web server can convey the message to the user.

## PRODUCT AUTHENTICATION USING QR CODE

Thus 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 as an SMS. The web server is connected to the cloud with through internet; the web server on receiving the SMS sends the data to the corresponding manufacturer's server in the cloud.

Volume : 4 | Issue : 9 | Sept 2015 • ISSN No 2277 - 8179

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.

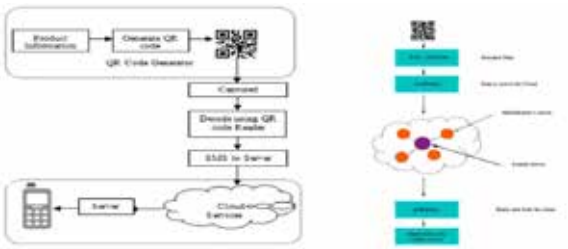

Figure 1: Proposed System Architectures

The QR code which is used in our model is better than the present Barcode and holograms as the QR codes are not in human understandable form, as no one can make changes to make it look original it can only read by the QR code readers. In this model the verification process is done by the user itself and there is no shop keepers hand in the complete authentication process. The user sends the captured image and the final result is also received only by the user with the help of the QR code reader which helps in reading the data printed in the form of QR code.

In our model the computing technology used to connect the mobile devices with central web server is Cloud Computing which allows the users from various locations to access the web server to check the product's originality. Cloud computing helps in easy access to all the remote sites connected in the internet. The central server sends the reply from the manufacturer's server to the user who requests with a QR code to find the originality of a product. The central server can send the solution to the user in two ways; it can either send a SMS with details about the originality of the product or the web server can send a voice message to the user about the originality, the option of sending the reply is based on the user's selection while registering to the web server in the beginning.

**MOBILE DEPLOYMENT MODEL**

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, 4 billion people are using mobile phones and by 2013, 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 mobile phones service providers have also reduced the cost charged for SMS which reduces the cost for the data transfer when using a mobile phone. 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 when compared with MMS. The data from the mobile device to the central web server is through the SMS as it is more economic than the other data transfer modes like MMS and WAP.

**CLOUD COMPUTING FOR AUTHENTICATION**

Cloud computing has now come into the mobile world as "Mobile Cloud Computing", the cloud computing provides general applications online which can be accessed through a web browser while all the software and data resides in the server and the client can access those applications and data without the complete knowledge about the infrastructure.. Cloud Computing should be capable of providing the end-user, services for each component of end-to-end application lifecycle,

- Available over the internet,
- Using pay-as-you-go payment model,
- Highly flexible for user-specific requirements,

It can be explained in a simple way as it is a Client-Server architecture where the clients request a service and not a server. In general the cloud computing users do not own their data, all the data is placed in the cloud and the user can access the data through a computer or a mobile device. In our model cloud computing is chosen because the manufacturer's server will be located in various locations and will have a huge amount of data related to the products. In normal computing technology we need to load the data in from the server and check it for the required record in the client machine. With the help of cloud computing we can directly access the data present in the manufacturer's server and get the data; this reduces the accessing time of the data and increases the speed of the process. In our model the manufacturer's server and our central server is located in the cloud and the user can access the central server from any location in the country and get the authentication information. The central web server in the cloud searches for the corresponding manufacturer's server and sends the data to it. As all the servers are in the cloud the searching process is simple.

**MOBILE CLOUD COMPUTING**

Mobile Cloud Computing (MCC) refers to an infrastructure where both the data storage and processing happens outside the mobile device. Mobile Cloud Applications move the computing power and data storage away from the mobile devices and into centralized and powerful computing platforms located in clouds, which are then accessed over the wireless connection based on a thin native client.

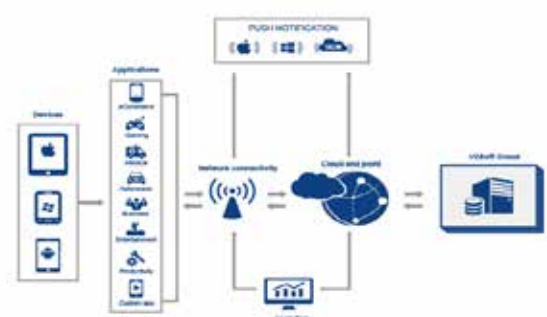

**Figure 3: mobile cloud architecture**

**SECURITY AGAINST ATTACKERS**

The authentication system uses SMS to transfer the data from the mobile phone to the server in the cloud. The data is transferred through the wireless medium using the Signalling System No 7 protocol. This protocol is used to send the SMS, MMS from the mobile phone to any other phone. Attacking the transmitted signal is considerably increased in the recent years. So there is a high probability of hacking the data sent through the SMS 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. The algorithm

used is a normal public key encryption algorithm which uses the same key to encrypt and decrypt the message. With the help of this encryption system the message is encrypted before sending from the mobile and in the server after receiving the message from the mobile it is decrypted to get the actual message. The QR code along with an encryption algorithm increases the security of the whole system which makes it more difficult to attack the system and get the data transmitted.

**IMPLEMENTATION AND RESULTS**

The authentication system is implemented in a mobile phone for a few reasons; the most important is that, everybody now possesses a mobile phone. So no special device is needed to implement the system and it is cost effective. The various steps involved in the process of authenticating the products are as follows. First the QR code is captured with the camera attached to the mobile device and the captured image is then encoded with the decode () function. Then the encoded data is then sent to the central server in the cloud through SMS with the help of the send Encoded () function. The central server on receiving the data from the mobile searches the respective server and checks for the record. The reply is then sent to the central server and then the server sends the reply to the mobile device with the help of the send Reply() function. The figure shows the process in a sequence. The QR code reader 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.

The SMS is sent to the server in the cloud through the Message Connection and Text Message classes available in the Messaging package. By creating instances the SMS can be sent from the mobile to the cloud.

**CONCLUSION**

We thus conclude our proposed model saying that this will be a good product Authentication System and can be implemented in day to day products at low cost which is equivalent to printing a image on the outside cover of the product.

## REFERENCE

[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 Non-uniform 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] Byung-Gon Chun, Petros ManiatisAugmented Smartphone Applications Through Clone Cloud Execution. | [6] M. Satyanarayanan et al. Pervasive personal computing in an internet suspend/resume system. IEEE Internet Computing, 2007. .