TELKOMNIKA Telecommunication, Computing, Electronics and Control
Vol. 18, No. 4, August 2020, pp. 1834~1842
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v18i4.14339

QR code based two-factor authentication to verify paper-based documents

Maysaa Abd Ulkareem Naser, Eman Talib Jasim, Haider M. Al-Mashhadi
Department of Computer Information System College of Computer Science and Information Technology, University of Basrah, Iraq

Article Info

Article history:

Received Oct 17, 2019
Revised Feb 19, 2020
Accepted Mar 27, 2020

Keywords:

Authentication methods
Cloud computing
e-Government
Hash algorithm
QR code

ABSTRACT

Important paper-based documents exposed to forgery such as: official certificates, birth, marriage, death certificates, selling and buying documents and other legal documents is more and more serious and sophisticated. With the purposes of fraud, appropriation of property, job application and assignment in order to swindle public authorities, this forgery has led to material loss, belief deterioration as well as social instability. There are many techniques has been proposed to overcome this issue such as: ink stamps, live signatures, documented the transaction in third party like the court or notary. In this paper, it's proposed a feasible solution for forgery prevention for paper-based documents using cloud computing application. With the application of quick response bidirectional barcode and the usage of hash algorithm. The study aims at developing an electronic verification system for official and issued books (documents, endorsements, and other official books) to/from different sections of the Institute using QR technology.

Corresponding Author:

Haider M. Al-Mashhadi,
Department of Computer Information System College of Computer Science and Information Technology, University of Basrah, Iraq
Email: mashhad01@gmail.com

1. INTRODUCTION

There are many usages and applications where quick response (QR) codes are significantly involved such as commercial products, tracking and monitoring labeled goods, marketing and advertising, identification of business cards, sale of goods, bank accounts, post mailing, virtual store, immigration stamps and entertainment, as a result, in many other circumstances, where sharing data is needed any object is wanted. [1, 2]. With the arise of e-Government and the new view of the automated office that make the office work without papers as possible, despite of this there are some specific types of work that are needed to accomplished by using paper documents. For example, official document-issued and many other legal documents, like a driving license, insurance document, birth certificate, passport, or contract these documents need to some form of authentication to verify the documents. This situations need to specialist to ensure the verification process from this type of documents. The governments established many foundations that can be responsible on work in the field of forensic science. This type of enterprise may use some special tools like a magnifying glass, a UV lamp or an infrared checker [3, 4].

Practically, it is so hard to control considerable quantity of documents quickly using traditional ways for this turn. Tax specialists as a sample, audit various applications, forms, receipt receipts, account statements, documents and other official papers are to be under checking through other agencies and bodies in which professionals are found to validate the legality of such these instruments and documents. [5].

In this study, it is suggested a new cloud computing framework technique that can applyed on traditional way to validate the issuance of document by applying encoding and print the unique QR code on paper to prove the validity of the paper document. This Code of unique symbols are decoded giving same information QR Code include which are able to be read by smart phone and it could have retrieved information its genuine form [6, 7]. The project is consisted of sequenced stages by which it can be validated the legality of document or certified as shown in Figure 1. The summarization of the technique stages is shown in Figure 2.

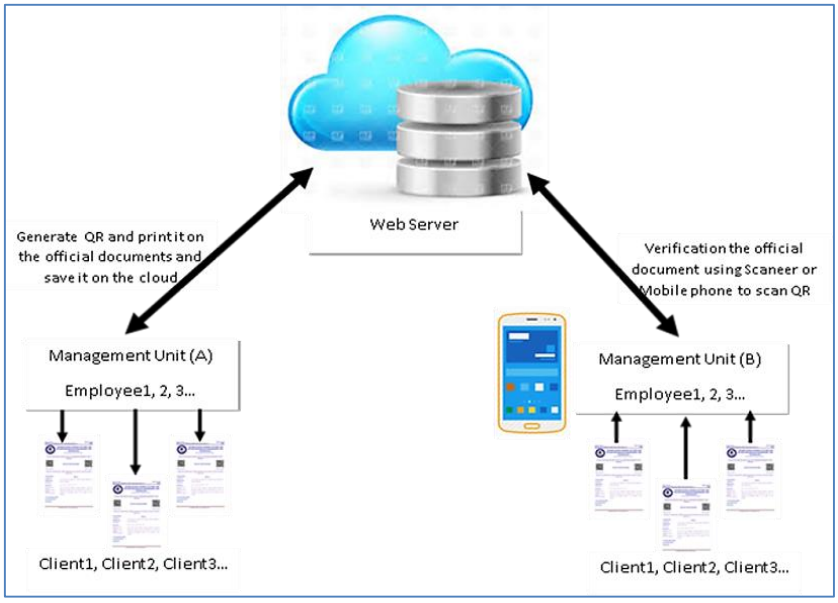

Figure 1. A proposed system for QR code generation and validation using mobile device

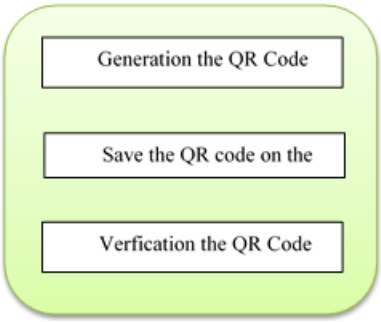

Figure 2. The stages of proposed technique

QR code is very interested code that can be used in authentication and verification operations, because it has the ability to hold many information that can authenticate the official documents. There are many researches that using QR code in authentication fields. In [8] the aim of this work is to examine and analyze the best type of QR code image by calculating the PSNR and MSE values. Using QR Code images with various image file format (PNG and JPG). In [9] the paper proposed new QR code using two storage levels to use it in document authentication. The new QR code, called two-level QR code, has public and private storage levels. The public level is the standard QR code storage level. The private level is arranged by substituting the black squares by some special textured types. It includes information encoded utilizing q-array code with an error correction capability.

In [10] the authors suggested QR code with ECDSA (elliptic curve digital signature algorithm). The propose method using two levels; public level or the standard QR and private level in which adding ECDSA to increase the security of the QR. Furthermore, in [11] the suggest a systematic QR code beautification framework that permit an individual user to personalize the QR code they create (for instant

a QR code containing contact details meant to be printed on a business card) by selecting visually meaningful models. In [12] the original use of QR codes in the automobile industry, QR codes can be used in a number of areas as a means to support interaction in controlled status such as in education. Examples include marking assessment. In this paper, the system creates the official book and generates a QR code for each official book based on a set of data that is read from the contents of the official book and encrypting to ensure confidentiality through a service provider which provides a QR service on the cloud. QR is encoded and sent to the server to be stored in a private database over the cloud framework.

The importance of research lies in:

- Minimizing the fraud and impersonation that can occur as a result of the absence of a precise and precise mechanism to identify the owner of the original book that is related to the data and content of the official book.
- Minimize the human effort in the process of electronic auditing of the book where the system can audit fast and guaranteed and non-error to most of the official books issued and received from and to the administrative units of the University or Institute.
- The data of the book is encrypted before converting it into a QR code so that the data used in the QR coding is not used and the binary verification technology is used for the official book to prevent fraud and impersonation.

Therefore, the method used in this study is very safe and secure, it is also other search benefits through:

- The importance of reducing the human effort in the audit and issuance of the validity of the issue currently in place where the system verifies the validity of the issuance in electronic form and fast does not exceed a few minutes.
- Reducing material costs due to the purchase of equipment or equipment for the coding of official books that must be purchased for each administrative unit.
- Minimize the time lost in the validation process from the official books issued and received.

2. CLOUD COMPUTING

A framework that can provide a fit and demand-driven access network for computing resources (networks, services, applications, servers and storages) that can be provided in quick and minimal configuring efforts or interaction, there are four framworks: private, public, community and hybrid cloud [13]. Cloud computing can be used to store a large amount of data with the ability to access these data by any smart devices such as smart phine, Ipad, tablet and etc from any place in the word using the Internet or Intranet at any time. Most of combanies today have tended to exploit the services provided by cloud computing because of its very benefits such as [14, 15]:

- Very high storage capacity.
- Fast processing capability.
- Ease of use.
- Remote access from anywhere and any time.
- The possibility of using the cloud services offered with low cost.

Cloud computing provide the customers and users to work with platform as a service (PaaS), i.e; different operating systems (OSs) as user nedded, infrastructure as a service (IaaS), i.e; storages, servers and Software as a service (SaaS), i.e.; application level programs. These services models can be provided by many cloud vendors (e.g., amazon web services (AWS) from Amazon.com, Google App Engine from Google.com, and Azure from Microsoft.com) based on payment as much use [16]. The cloud computing service models can be shown in Figure 3.

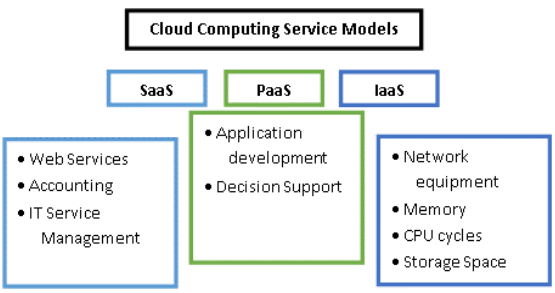

Figure 3. Cloud computing models

2.1. Cloud computing security

Cloud security can be reach by appling different types of security techniques to avoid the breachs and hacking of the cloud data or services this solution can be achieved using cryptography [17]. Cryptography is the science that study the information security and present the information protection techniques against unauthorized access. The cryptography can be applied by converting the critical data into a form that cannot read by attckers if the attackers can get this data. There are many goals of cryptography, the main goal is to maintain data in a secure way to keep it from unauthorized users. By using cryptography, the data such as text, voice, video and image can be stored or transferred on the network from side to side in a secure maner that can not be read from the attackers who may evesdroping of this data. Cryptography provides many security goals such as [18]:

- Authentication: The purpose of the authentication is to ensure user identity. The goal is to prevent unauthorized users from accessing computing resources.
- Confidentiality: The purpose of confidentiality is to grant the access to the data by the authorized persons only to protect data from unauthorized persons.
- Data Integrity: The goal of data integrity is to ensure there are no modification, fabrication, deletion from anauthorized persons.
- Non-Repudiation: the goal is to ensure and prove the person who send or receive the data.
- Access Control: The goal is to grant the permission to access the data to the authorized user only.

3. BASICS OF QR CODE

QR Code is a barcode of two vectors. i.e., it is scanned by two vectors. Vertically and horizontally. It can be kept date more than one vector barcode. Thence, it is suggested QR code needs more developed technology of reading. QR coded is defined by ISO/IEC 18804 Industrial specification. However, it is created and protected by Denso Wave Japanese Corporation 1994. The main aim is to develop this technology is to support users to encode and read their own information easily [19]. As shown in Figure 4.

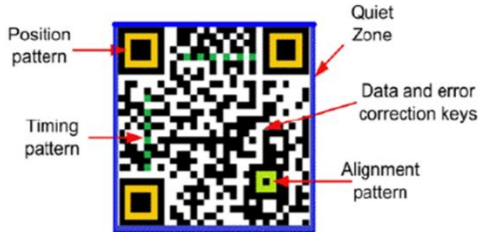

Figure 4. Structure and components of QR code

3.1. Technology

QR code changed the probable usage and purpose of the coded sign [20]. It contains bi-vectors information while the traditional barcode was consisted of tone vector of data; that is, the vertical one. The process to recognize barcode are [21]:

- Detecting outer point
- Recognize shape.
- Identify control bar of barcode.
- Discover barcode aim.
- Vectors and bit intensity to use barcode.
- Computing value of barcode.

The following points are included within QR code;

- Configuration Pattern is used to rectify misstatement in QR code may occur by input codes on curved plans.
- Timing pattern is used to appoint main coordinate of each cell within QR code by black and white units are ordered alternatively for this turn.
- Noiseless Zone: it is a verge space makes detection of QR code most ease. Four cells are to be found for this zone.
- Data area: Within QR code, there is area contains data are encoded by Binary numbers (such as URL) and also include reed-solomon code to correct errors. [22, 23].

3.2. QR code characteristics

(2D) bar codes usually have high-density data storage capacity for a large volume of data within a tiny volume. QR code," is robust since it is application, the application is work on any device and work with any data, and with proceeding characteristics in terms of security, error detection, and correction capability, as well as the ability to encode different languages". [24] QR code is a 2D bar code that was developed by Denso Wave in 1994 for tracking parts in vehicle manufacturing. The decoding is executed automatically and easily: some free add-on software (e.g., Quick Mark and Enigma Readers) can test, read, and decode QR code easily by putting the device before code. [25]. QR is consisted of 360 degree legible black and white quadrangles. The quick response code can be saved in several modes such as communication data, image and video links, plain text, etc. It is also recognized as URL. The storage level of QR codes can be sorted up to 7,089 characters of information, which is very large in comparison with 1D (one vector) barcode. Encoding process able to treat string set of QR code, and Numbers (0-9), Alphabets (uppercase A-Z), Nine Special characters (% * + - / _ $) and Kanji characters [26, 27].

3.3. Advantages of applying QR Code

- Open source techniques
- Free applications.
- Simple running procedure.
- User easy process.

It needs no complex nor special acquaintance of users to apply QR code, like smart phones are need to activate QR code. In addition to QR code scanner, it is also being used to make delivery services that available by informatics libraries. Further, it is also worthy to distribute information and last technology knowledge for all users. It can be used to link instantly with all necessary resources like (institutional digital repository, Web-OPAC, e-Resources, library website, library guide). New access ways and rest of valuable properties of the library quickly and the time of users does not waste, it provides also small space that can be store a huge data size.

4. CRYPTOGRAPHIC HASH FUNCTION

A hash function can be accepting variable-length message and produces constant length hash message digest, it does not need any key in its work [28]. The hash function necessary for security implementations is mentioned to as a Role of Encoding Hash function, that hash function is computationally infeasible to discover a message or the hash value that is identical for two [29]. At most times the hash value is secured by using encryption techniques. The term role of encoding that has been used in computer application from reasonably long time is referred to a role uses string of arbitrary input to a string of fixed length. However, should it meet some extra needs (as detailed further), then it can be applied for encoding applications which is known as role of encoding hash. Roles of encoding hash are one of the most important tools in the field of encoding and are applied to realize group of confidence secure purposes such as authenticity, digital monograms, quasi number generation, digital hiding secret data in sorting mode, and real time stamping, Figure 5 shows the structure of MD5 role of hash function; i.e., it is applied form in the proposed research [30]. The encryption techniques can be adding to encrypt the Hash function; any methods can be used to encrypt the hash function.

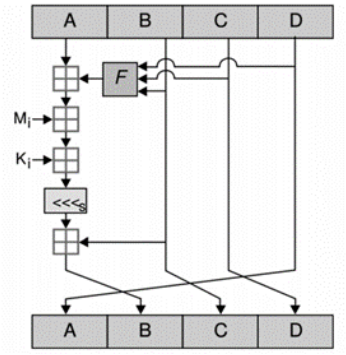

Figure 5. Structure of MD5 hash function

Definition: A hash function is a function h: D → R, where the domain,

D = {0,1} * and R = {0,1} n for some n >= 1 (1)

role of hash function are approximately divided into two kinds; i.e., Maine Roles of hash function; the one that use secret key, and hash without key. The first type is known as message of authentication code. Generally, the term hash functions refer to hash that does not used keys. In this paper, we will focus on hash only not MAC. Hash function (some time also known as MDC-Message Decoding Code) can divided into OWHF (one direction hash function), CRHF (collision resistant hodgepodge) and UOWHF (universal one direction hash function) [31, 32].

5. AUTHENTICATION TECHNIQUE

In this work the data base has been create to hold the data of all documents, the database is stored over the cloud to execute the security processes online. The table of data contains the following fields:

- User name
- Title of the document
- Issue date
- ID Number for document
- The name of the side it may consider
- Random number
- QR Code

5.1. Authentication phase

The system using cloud computing to save the data of official documents and processing the operations for producing the QR, to verification the official documents. By using the QR in the administrative units in the university will provide the ability to save authenticated data in the server on the cloud with secure access to user documents. The Internet conjointly facilitates the exchange of documents with registered external aspect through encrypted QR sharing Code. Table 1 shows the notations used throughout our proposed technique. The steps procedure of the proposed system is as follows:

Input Phase (Create QR)

Step 1: At this stage, information about the document (N, D, AD, AT, X), as Shown in Table 1 are encrypted using Hash algorithm

Step 2: compute $C = (N \parallel D \parallel AD \parallel AT)$

Step 3: In this step, XOR Operation between the name of the person and the random number and the process output is encrypted using the Hash Algorithm Thus ensuring confidentiality of information in the server.

Compute $NP = h(N \oplus x)$

Step 4: After completing the previous step, the document information is encrypted by hash algorithm and the random number is merged in order to store it in QR. because we need it later to encrypted name in the next steps.

Compute $HC = (h(C)) \parallel x)$

Step 5: Generate QR with HC information

Step 6: Print QRon the document

Step 7: Save QR & NP to cloud server.

The hash value h is can be stored in a QR code

Save QR in document's

Table 1. The notations used throughout our proposed technique

Notation	Description	Notation	Description
QR	Quick esponse code	QR'	QR current
N	ID Number of Document	QR_s	QR in cloud server
D	Date of Document	NP	Name of user
AD	Title of Document	NP'	Name of user current
AT	Address To	$\stackrel{?}{=}$	Comparison between two side
$\parallel$	Concatenation operation	x	Random number
$\oplus$	XOR operation		

5.2. Verification phase

Authentication cloud server offers strong authentication and validation of data, the data authenticated is using QR code that allows for the elevated user suitability while maintaining the elevated security. Here concealment secret information based on bit technique cannot change by the attacks. If an attacker obtains the hidden data in the server, it is impossible to recover the secret information.

Step 1: Before verification process the original document is hashed and stored in QR and save it in the cloud server.
Step 2: After Step 1 the verification process needs to scan the QR from the produced documents from step 1 (using scanner or smart phone QR code scan application) and check the result of the scanning QR of the document with the stored QR in the cloud server and then verify that the sending QR corresponds to the document stored in the cloud server.

Scan QR': $m=\{(HC)\}$

Step 3: Compute $NP' = h(N' \oplus x)$
Step 4: In case the two documents (the sender and the stored QR) match, it will be tested if the hash in the document is the same hash in Server.
Step 5: To support the security and to add more security level, the method using the name of the original owner of document to check on the authentication of the document. The name of original owner is stored in server and if any management unit want to verification of the document it using QR beside the name of person. If the two-Name person match, then NP's Document =NP' Server, the document and user are valid. Figure 6 shows the proposed schema.

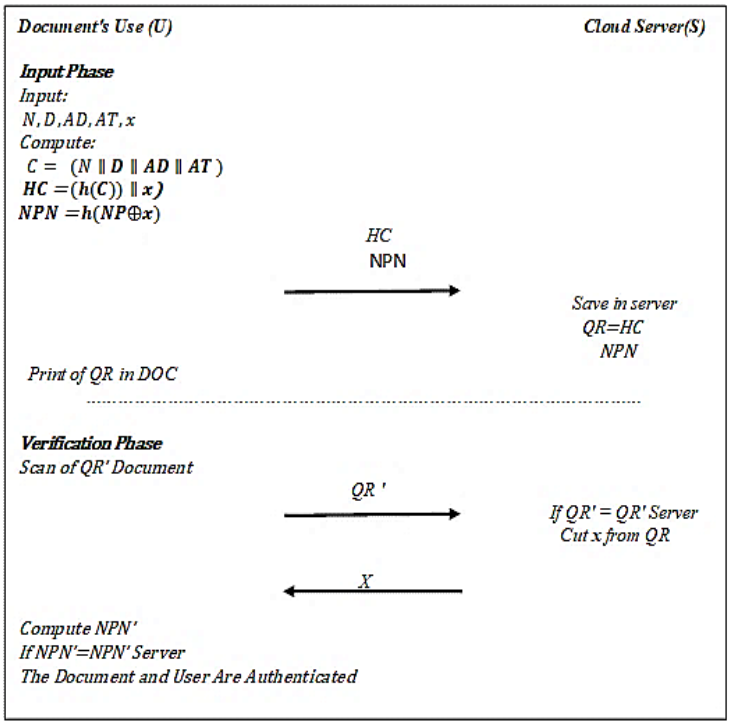

Figure 6. The proposed scheme

6. CRYPTANALYSIS OF THE TECHNIQUE

– User anonymity

In this technique which is based on QR, where all critical information sent to save in cloud server as encryption by hash function after concatenate operation e.g. $C = (N \parallel D \parallel AD \parallel AT)$. The compute $HC = (h(C)) \parallel x)$ from these operations, so sever is difficult to know any information about any the authorization document.

– Forward session

In this situation, If the attacker could reveal the server's secret key x, but it's difficult getting another information after it have been achieved user anonymity, so this attack cannot run with just know x.

– Orgery attacks

An attacker tries to change sensitive data to impersonate as the legal user or server to access the resource on the remote system. As to compute the dynamic NPN its not only used XOR operation but also concatenate operation e.g. $C = (N \parallel D \parallel AD \parallel AT)$, and $HC = (h(C)) \parallel x)$.

– Password guessing attack

It is difficult to guess the sensitive data of document, because this proposal scheme based on QR, hidden D, AD, AT by HC and N by NPN.

– Mutual authentication

To save reliance between Ui and S, the proposed technique based on QR is performed mutual authentication of together communication parties. Where the server S send {HC, NPN} to Ui and Ui calculated the value of NPN by N, x which is only know to Ui and S.

7. CONCLUSION

Authenticity of paper-based documents aims to develop an electronic verification system. Using QR technology. The system creates the official book and generates a QR code for each official book based on a set of data that is read from the content of the official book and encrypted to ensure confidentiality through a service provider working to provide a QR service. The QR is encoded and sent to the server for retention in a private database. In this paper, Book data is encrypted before being converted to a QR code in order not to know the data used in the encoding of the QR and the use of dual verification technology of the official book to prevent fraud and impersonation. Therefore, the method used in this study is very safe and secure.

ACKNOWLEDGMENT

This project is submitted as a study to the Oil Training Institute in the province of Basra in the State of Iraq. It was approved in principle.

REFERENCES

[1] Omar Lopez-Rincon, Oleg Starostenko, "Binary Large Object-Based Approach for QR Code Detection in Uncontrolled Environments," *Hindawi Journal of Electrical and Computer Engineering*, vol. 2017, pp. 1-15, 2017.
[2] ISO/IEC, "Automatic identification and data capture techniques-QR Code bar code semiology specification," *ICS > 01 > 01.080 > 01.080.50*, 2015. [Online]. Available: https://webstore.ansi.org/Previews/PREVIEW.
[3] Robin Ashford, "QR codes and academic libraries reaching mobile users," *College & Research Libraries News*, vol. 71, no. 10, pp. 526-30, 2010.
[4] Mohammad Zainuddin, D. Baswaraj, S. M. Riyazoddin, "Generating SMS (Short Message Service) in the form of Quick Response Code (QR-code)," *International Journal of Computer Science and Mobile Computing*, vol. 1, no. 1, pp.10-14, 2012.
[5] Md. Sanaul Haque, Richard Dybowski, "Advanced QR Code Based Identity Card: A New Era for Generating Student ID Card in Developing Countries*," IEEE First International Conference on Systems Informatics, Modelling and Simulation*, pp. 97-103, 2014.
[6] Maykin Warasart, Pramote Kuacharoen, "Paper-based Document Authentication using Digital Signature and QR Code," *4TH International Conference on Computer Engineering and Technology*, 2012.
[7] J. Z. Gao, "Understanding 2D-barcode technology and applications in M-commerce-design and implementation of a 2D barcode processing solution," *Proc. Int. Conf. on Compute. Software and Applicate*, pp. 49-56, 2007.
[8] Saroj Goyal, Surendra Yadav, Manish Mathuria, "Exploring concept of QR code and its benefits in digital education system," *IEEE International Conference on Advances in Computing, Communications and Informatics, 2016.*
[9] Iuliia Tkachenko, William Puech, Christophe Destruel, Olivier Strauss, Jean-Marc Gaudin, Christian Guichard, "Two-Level QR Code for Private Message Sharing and Document Authentication," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 3, pp. 571-583, 2016.
[10] Neha Malik, Bharti Joshi, "ECDSA Approach for Reliable Data Sharing and Document Verification using Two level QR code," 2nd *International Conference on I-SMAC*, 2018.
[11] Lin Y.-H., Chang Y.-P. & Wu J.-L., "Appearancebased QR code beautifier. Multimedia," *IEEE Transactions on Multimedia*, vol. 15, no. 8, pp. 2198-2207, 2013.
[12] Bhaturkar K. P. & Bagde K. G., "QR code based digitized marksheet," *International Journal of Management, IT and Engineering*, vol. 4, no. 57, 2014.
[13] Peter Mell, Timothy Grance, "The NIST definition of cloud computing," *Special Puplication 800-145*, 2011.
[14] Haider M. Al-Mashhadi, Ala'a A. Khalaf, "Hybrid Homomorphic Cryptosystem for Secure Transfer of Color Image on Public Cloud, *Journal of Theoretical and Applied Information Technology"* vol. 96, no 19, pp. 6474-6486, 2018.

[15] S. Kamboj and M.N. S. Ghumman, "A Survey on Cloud Computing and 1st Types," *IEEE International Conference on Computing for Sustainable Global Development*, vol. 15, pp. 7435-7443, 2016.
[16] N. M. Gonzalez, C. Miers, F. F. Redigolo, M. A. Simplicio Jr, T. C. M. Carvalho, M. Naslund, et al., "A Taxonomy Model for Cloud Computing Services," Proceedings of the 1st International Conference on Cloud Computing and Services Science, pp. 56-65, 2011.
[17] Haider M. Al-Mashhadi, Iman Q. Abduljaleel, "Color Image Encryption using Chaotic Maps, Triangular Scrambling, with DNA Sequences," *IEEE International Conference on Current Research in Computer Science and Information Technology (ICCIT)*, pp: 93-98, 2017.
[18] Passent M. El-Kafrawy, Azza A. Abdo, Amr. F. Shawish, "Security Issues Over Some Cloud Models," *International Conference on Communication, Management and Information Technology (ICCMIT)*, 2015.
[19] Shanthi`Kumaraguru, Prof.Dr.D.S. Bormane, "Identification of QR Code based on Pattern Recognition with Mobile Phones," *International Journal of Modern Engineering Research (IJMER)*, vol. 2, no. 5, pp. 3544-3547, 2012.
[20] José Rouillard, "Contextual QR Codes*," 2008 The Third International Multi-Conference on Computing in the Global Information Technology (iccgi 2008)*, 2008.
[21] Reilly, D., Smolyn, G. and Chen, H., "Toward fluid, mobile, and ubiquitous interaction with paper using recursive 2D barcodes," *Pervasive Mobile Interaction Devices 2007 (PerMID 2007), workshop at Pervasive*, 2007.
[22] Ivan Jelić, Dina Vrkić, "QR codes in library - does anyone use them?" *Conference: Information & Communication Technology Electronics & Microelectronics (MIPRO)*, 2013.
[23] A. Wilson, "QR codes in the library: are they worth the effort? Analysis of a QR code pilot project accesed," *Journal of Access Services*, vol. 9, no. 3, pp. 101-110, 2012.
[24] Kinjal H. Pandya, Hiren J. Galiyawala, "A Survey on QR Codes: in context of Research and Application," *International Journal of Emerging Technology and Advanced Engineering Certified Journal*, vol. 4, no. 3, 2014.
[25] Shintaro Okazaki, "Cross-Media Integration of QR Code: A Preliminary Exploration," *Journal of Electronic Commerce Research*, vol. 14, no. 2, pp. 137-148, 2013.
[26] Hiren R. Kadam, Niketan R. Sutar, Bhumil S. Ugle, Mrs. Kishori Shekokar, "Genuine Automobile Parts Scanner Using QR-Code," *International Journal of Advance Engineering and Research Development*, vol. SIEICON, pp. 1-6, 2017.
[27] Sangeeta Singh, "QR Code Analysis," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 6, no. 5, 2016.
[28] Haider M. Al-Mashhadi, H. B. Abdul-Wahab, R. F. Hassan, "Secure and time efficient hash-based message authentication algorithm for wireless sensor networks," *Conferences: Global Summit on Computer & Information Technology (GSCIT)*, pp. 1-7, 2014.
[29] Goh Khai Hong and Sharad Sinha, "Tracking Vulnerable People Using Body Worn QR Code," A Final Student Application Paper Presented to IEEE Standards Association in Partial Fulfilment of the Requirements for the IEEE Standards University Student Grant Application, 2018. [Online]. Available: https://www.standardsuniversity.org
[30] B. V. Rompay, "Analysis and Design of Cryptographic Hash functions," MAC algorithms and Block Ciphers, Ph.D. Thesis, Electrical Engineering Department, Katholieke Universities, Leuven, Belgium, 2004.
[31] Rajeev Sobti, Geetha Ganesan, "Cryptographic Hash Functions: A Review," *International Journal of Computer Science*, vol. 9, no. 2, pp. 461-79, 2012.
[32] Eman T. Jasim, Hameed A. Younis, "Cryptanalysis and Security Enhancement of a Khan et al.'s Scheme*," IOSR Journal of Computer Engineering*, vol. 17, no. 2, pp. 08-16, 2015.