ISSN 2278-3091
Volume 8, No.6, November – December 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse10862019.pdf
https://doi.org/10.30534/ijatcse/2019/10862019

Cloud-based Framework for Issuing and Verifying Academic Certificates

ADEL ABDULLAH ABBAS
Ministry of Higher Education and Scientific Research, Baghdad, Iraq
adelamiry1975@gmail.com

ABSTRACT

Verification of certificates is one of the major challenges in every association, school, government, and employers. Most of the employers have been encountering rate of fake certificates. Initially, the traditional based model of verification contributes underway of fake certificates which represent a troublesome in knowing the legitimacy of such scholarly certificates introduced to them because it is highly unlikely they can validate them in a flash. Furthermore, present-day innovation and the ascent of the web are very much advantageous. Document management plays a vital role in securing documents in any organization, such as how the documents are created, reviewed, published and disposed of or retained. Majority if not all universities print graduation certificates and despite the technological advancements digital-based certificates did not yet replace the paper-based. Hence, this research aimed to investigates the techniques that currently being used for document verification. In this research, we proposed a cloud-based framework for issuing and verifying the academic certificates.

Key words: Academic Certificate Verification, Cloud Computing, QR Code, RFID, Watermarking

1. INTRODUCTION

Document verification can be defined as it it is the ability to track the origin of document to a specific person [1]. Verification process is very important to ba tackeled as it would fight the forgery. Document forgery is a real issue as it affect both the holder of the document and the issuer of that document. It also threats the trust and the authenticity [3],[4],[5],[6],[7].

Document forgery is classified into two types: forgery type 1 and forgery type 2 [7], [8]. Forgery type 1 is happened if some part of the original document is changed. Forgery type 2 is happened if both the base substance and the information contained therein is fake. This type of forgery often very difficult to tell whether it is real or fake because the base substance and the style of the document normally look authentic [8].

Academic certificates are one of the most important documents that issued by the university. And as mentioned that document forgery is a real issue, anhancing the verification process of the academic cerificatates become a concern. Verification of certificates is one of the major challenges in every association, school, government, and employers. Most of the employers have been encountering rate of fake certificates. Initially, the traditional based model of verification contributes underway of fake certificates which represent a troublesome in knowing the legitimacy of such scholarly certificates introduced to them because it is highly unlikely they can validate them in a flash. Furthermore, present-day innovation and the ascent of the web are very much advantageous. Document management plays a vital role in securing documents in any organization, such as how the documents are created, reviewed, published and disposed of or retained. Majority if not all universities print graduation certificates and despite the technological advancements digital-based certificates did not yet replace the paper-based [9].Because of some of the reasons like the affordability; the familiarity and the simplicity of paper. The affordability of paper means the paper is low cost, the familiarity of paper means the people are used to it and the simplicity of paper means that the paper does not require special equipment to write or read [10]. Forgery of document is a serious issue and need to be solved. It is affect both the owner or the holder of document and the company or the institution that issue that document[11],[2]. One of the main reasons that lead to the forgery is the lack the verification propoces [2],[3],[4],[5]. The existing verification method consume a lot of resources such as time and money. Hence, a new approach that can ehnace the verification process and overcome the forgery issue is needed. Fo that, the main objective of this research is to propose a framework for issuing university certificates that are hard to forge and easy to verify.

2. DOCUMENTS FORGERY

The documents in hardcopy are nowadays still used like graduation certificates, academic transcript, and contracts, etc.[1]. There are many cases of forgery of hardcopy documents took place over the years. The first case is taking place in New Delhi, it was a report about arresting of five people obtained loans and cheating the banks using fake documents [1]. In Iraq, many forgery cases are happened. This claim was supported by invitagation that conducted about 20,000 government employees. This invistagation reports that some employees have used forged documents to get a job [1]. Not only that, some of the prominent Universities like Newcastle University has been a victim of forged documents. However, almost of (50) students have been told to leave Newcastle University because of that they were used forged certificates. In details, 49 Chinese students with one Taiwanese student had enrolled the course of business studies in September. The lecturers figure out that those students were unable to keep up with their study [12]. In the last ten to fifteen years, the production of fake degrees and diploma become really a worldwide problem because of that the academic qualifications have gained increasing commercial value. The advancements in the printing and scanning technologies resulted in the increasing of the fraud and fake

degrees [13]. Hence, a lot of researches come in to fight the forgery of printed documents

3. ANALYSIS OF CURRENT VERIFICATION TECHNIQUES

There is an obvious gap when the current physical document verification techniques of the day are considered against these three basic principles. The typical system of verification normally involves exchange of mails or posts, which can be a time consuming process. Another common verification technique is through the direct calling of the issuer of the certificate. This is not only time consuming, but also susceptible to interference. If the individuals on the other end do not authenticate the certificate, then there is little one can do in terms of protecting themselves from the risk.

Image verification and change detection is another common technique[14]. This involves the comparison of the subject document with an original image of one held in a storage server. Image verification determines whether a document has been modified, and determines what content may have been added, deleted or otherwise modified [14]. When documents are held in a different server, they normally are in their original format and chances are that they can be modified [15].

Another example is the use of watermarked a quick response (QR) code. Normally, an embedded logo is generated that belongs to the owner of the document. According to Mantoro the logo will normally contain a validation link, which is then linked to a web server and database server through an internet connection. It is scanned over a camera phone or QR code reader, with the result being that the validation can happen real time, and relatively easily as it can be done using simple smartphone technology like Android, iOS and Blackberry [5]

The use of 2D barcode and public encryption systems suggested by the the researcher [1]. This technique traces the origin of the document to a particular person, to the device that produced it or to the place where it was produced. This technique requires the addition of 2D barcodes that contain required information to ensure the integrity of the document [1]. The researchers use cryptographic algorithms like RSA, the Chinese Remainder Theorem and the ElGamal Cryptosystem [1].

There are several techniques which currently being used for fighting fake certificates such as stamps, and wet-signatures and holograms. However, with these techniques, the fake documents can be created easily. 2D barcode, QR code watermarking and RFIDs are dominant approaches that recently proposed for verifying the document. 2D barcode looks like a rectangle that contains many small, individual dots and is readable by a machine. It has the ability to hold a significant amount of data as well as it may remain legible even when printed at a small size or imprinted onto a document; That is why the researcher [16] adopted it as a solution to authenticate paper-based documents. They focused on mark sheets because the mark sheets issued by the university (Amrita University) lacked any standard nor were they secure. Their research suggested a standard framework to generate and authenticate mark sheets, without the need to access any kind of online database; the generation and authentication of mark sheets were using a 2D Barcode that holds the issuer public key for that specific mark sheet. The drawbacks in their solution are that the entity to issue the certificate as well as the entity that verifies the certificate has to have a license to adopt their said solution and is not easily accessible through a cloud service and they also did not specify whether this could be unified across different document issuers. The 2D barcode solution was also adopted by other researchers [2]; however, their proposition is somewhat different than the researcher [16]. They proposed to embed instead of the public key alone the content and layout of the document along with a digital signature generated using the issuer's private key. The end-user or the person to authenticate can then use a smartphone to authenticate the document. Their solution has the advantage over the researcher [16] because it is more portable and can be done on the go however there is a drawback similar to the researcher [16] in that the application license has to be obtained first and also they did not specify if this can be unified across different document issuers.

A system for authenticating paper-based documents based on 2D barcode and smartphone was proposed by the researchers [17] to fight the document counterfeiting and forgery. QR code was proposed to be used and printed on the document. QR code is adopted for two purposes; the first purpose is to hold the content and layout of the document, and the second purpose is to hold a digital signature on the copy of document based on the private key of the issuer. They proposed for document verification is to use a smartphone; it is used to scan the QR code however the extracted document is compared with document copy in hand. The drawbacks in their solution are that both entities; issuer entity that issues the certificate and verifier entity that verifies the certificate must have a license to adopt their said solution. In addition to that, the proposed solution is not easily accessible through a cloud service. Furthermore; they also did not specify whether that the solution could be unified across different document issuers.

A somewhat different method for hardcopy document authentication is presented by the researcher [1]. They proposed a method for document authentication (means document verification) to be adopted between two known users (the issuer and the verifier) over the network. The method is based on using 2D barcode with the public key cryptography techniques. The 2D barcode is proposed to carry some important data of document like the document content, the issuing number, timestamp and sender signature. For document verification, the receiver decrypts the cipher-text, through scan the barcode and compares the extracted data. Their solution has an advantage over the authors [18] because it is has a good level of security for the document in paper format because of that they aware to encrypt the data before keeping it into 2 barcodes. However, there is a drawback similar to [18] in that is no real implementation to prove the validity of the proposed method. In addition to that, the proposed method is proposed to be adopted between two know users. However, the proposed method would be the not proper choice in our case.

Authors [5] suggested to adopt watermarked QR code to hold the logo of the document; the logo is reflected the validation link of the printed document. For document authentication, QR, however, would be scanned using a camera phone or QR code reader. The proposed solution has the advantage of that the printed documents can be easily authenticated using watermarked QR code. However, the drawback is that there is

no real implementation to prove the validity of the proposed method

A method similar to the proposed approach by the researchers [1] based on digital signature and QR code for document authenticating is proposed by the researchers [19]. QR code is proposed to be printed in the document to enhance the document verification mechanism. They proposed that the content of document along with verification code were to be kept in the form of QR. From the content of the document, the hash value is generated to then be encrypted. The digital signature of document content is also be generated using the private key of the sender. Then, the generated digital signature along with the document content are combined, compressed and stored in the QR code, then send the document to the receiver. For document verification, They proposed a somewhat different technique from the researchers [1]. They proposed to employ the OCR technique to compute the hash value from the obtained document then compare it with a hash value that already stored in the QR code. The proposed method has an advantage over the authors [1] because it is a proposed new technique for document verification; they proposed the OCR technique which can automatically compute the hash value. The drawback in the proposed method is that they proposed the method between two known users (known sender and known receiver). Furthermore; there is no real implementation is utilized to prove the validity of the proposed method.

The authors [18] proposed a conceptual method for authenticating the degree certificate issued by the university. The method is proposed based on the QR code and using the smartphone to verify ethe certificate. They aimed in their solution to prevent the degree certificate to be forged. QR code is proposed to hold some important data related to the student like student's name, the ID of the student, the marks obtained, etc.; all of this information are signed by the university. However, for certificate verification, a smartphone is used to scan the QR code then compare the copy in hand with the extracted document copy. The drawbacks in their proposed method are there is no suggested mechanism is proposed to protect the data which kept in QR code. Furthermore; there is no real implementation to prove the validity of the proposed method.

Authors [16] focused on mark sheets verification because of that the mark sheets issued by the university (Amrita University) lacked any standard nor were they secure. Their research suggested a standard framework to generate and authenticate mark sheets, without the need to access any kind of online database. They proposed to verify the mark sheets based 2D Barcode. 2D barcode is proposed to hold the issuer public key for that specific mark sheet. However; for mark sheet verification, the QR code reader is proposed to be used to scan the 2D barcode. The drawbacks in their solution is that the entity to issue the certificate as well as the entity that verifies the certificate has to have a license to adopt their said solution and is not easily accessible through a cloud service (also is it a desktop application) they also did not specify whether this could be unified across different document issuers (also content not secured).

The researchers [20] proposed to utilize the QR code plus the cryptographic hash algorithm. However; they proposed to computationally extract some features from the document image. As a result, the extracted information is processed using an algorithm which identifies the counterfeited areas. The proposed document verification mechanism similar to the document verification mechanism proposed in by others [19],[1]. Their solution has an advantage over the proposed approaches by [19],[1] which is that their solution has more level of security as well as they simulated their proposed method to proof its validity, however, the drawback in their solution is that they did not specify if the proposed method can be implemented in real-time case and whether it can be unified across different document issuers.

The researchers [21] they proposed a different method for using the 2D barcode to authenticate and issue certificates and is to embed biological information like a fingerprint in the 2D barcode. To authenticate the certificate, they suggested something similar to what the researcher [2] suggested and is the use of smartphones. They proposed using the smartphone to acquire a user's fingerprint and compare it the one embedded in the barcode, if it matched is shows a valid certificate. Even though this solution might work however it required investment in a mobile phone that read fingerprints and also requires the presence of the certificate owner to supply his/her fingerprint. The other drawback in the proposed solution is that there is no mechanism to protect the data or authenticate the data, it is mere owner authentication.

The researchers [22] proposed the system based on 2LQR code. Thhe proposed solution did not focus on verification of the content of the document; it focused on the association values in both the textured patterns and the original numerical patterns between Print & Scan for identifying the counterfeited document. The proposed system has an advantage in utilizing new two-level QR however the drawback in the proposed system is that third party was not considered. It means that the proposed system did not pay attention to how the verifier can verify the document they only focused on the printing and copying processes along with 2LQR.

The researchers [23] proposed a system based on utilizing of QR code. For document verification, a smartphone is used to read the information from the QR code. The advantage of the proposed system is that the security of the content of the physical paper documents is somewhat enhanced however the drawback in their system is that they did not specify whether their solution can be adopted across different platforms as well as their solution is desktop system and could not be adopted via cloud services.

The authors [24] proposed that based on identifying the core point of the fingerprint to be kept into the QR code. They proposed to utilize the QR code to carry the extracted feature of the fingerprint of an individual. Even though this solution might work however it required investment in a mobile phone that read fingerprints and also requires the presence of the certificate owner to supply his/her fingerprint. The other drawback in the proposed solution is that there is no real implementation to proof the proposed method.

The authors [3] proposed to append some of information such as tracking number and timestamp. in the barcode. All of these information are hashed using hash algorithm and the generated hash will be kept in the QR code.

For verification, the researcher proposed to use a scanner. The decoding and extracting the hash value from the 2D barcode is accomplished using the decoding algorithm. The proposed solution has the advantage of that it has a good level of security for the document in paper format however the

drawbacks of the proposed system is that it is a desktop system and it is not easily accessible through a cloud service. In addition to that, they also did not specify whether this could be unified across different document issuers (also content not secured)

A conceptual method for ID (identification document) verification is proposed by the researchers [25]. Their method is somewhat different method from the approach of the researcher s [21], they proposed the method based on VSS and QR codes. Their proposed method is to encrypt the binary secret image into two shares to be encoded into two QR codes; a (2,2)-threshold VSS is used to generate the shares. They proposed that one share is printed onto an ID-card, while the other is kept in the database. For ID verification, a smartphone is proposed to be used to scan the QR code and extract the share. After that, compare the extracted share with the one in the database to authenticate the ID. The proposed method has the advantage in the way of generating the shares, they used VSS technique to generate the shares however the drawbacks in the proposed solution is that no real implementation to proof the proposed concepts and there is no security mechanism to protect the share kept in the QR code.

The researchers [26] proposed a method for mark sheet verification based on the QR code. They suggested that the information of the mark sheet is encrypted and stored in QR code. For verification, QR code has to be scanned in order to retrieve the information.The proposed method has the advantage over the approach of the authors [41] because the researcher are well explained the algorithm used (TTJSA decryption) for encryption and decryption however the drawback in the proposed method is that there is no implementation or simulation result to prove the concepts of the proposed method.

The other dominant approach to protecting against counterfeiting and forgery is digital watermarking. Within this approach, some information would be embedded in the cover image. In the verification stage, the information is extracted in order to identify the owner and verify other contents such the copyright. The copyrights of printed documents like in the certificate and ID card is protected by utilizing the digital watermarking [27],[28]. They proposed a method for detecting the noise from the printed documents; the noise can be detected through the printing and scanning the documents. They argue that the with noise detection the identifying the counterfeited printed documents would be easier. The proposed method has an advantage which did not require a database for document verification. The hybrid watermarking method is also proposed [29]. They proposed to combine some important features of signature presented in the document in order to protect the copyright of the document and to detect tampering. They have been used the Stirmark benchmark to prove the validity of their method however their method resulted in obtaining good performance. With the watermarking technique, the embedded information is invisible to human eyes. However, the document with watermarking can be verified through extracting the watermarked information thus the counterfeiting would be very hard. Digital watermarking is a very popular approach and it provides good protection against forgery. However, the drawbacks with digital watermarking are often used in practice, costly and not included in real-life documents [30].

The third common approach is the use of RFIDs. RFIDs is the third approach is the use of. RFID was proposed to be utilized for document verification by several authors [28]. Authors [28] proposed a system based on RFID; they proposed to include some information related to the students in the RFID. An interrogator must be used for authenticating the document and also the verifier should log into the university website in order to download the needed software. The proposed solution is a good approach, however, it is time-consuming and costly and also the original document must be shown the verifier. There is an obvious gap when the current physical document verification techniques of the day are considered against these three basic principles. The typical system of verification normally involves the exchange of emails or posts, which can be a time-consuming process. Another common verification technique is through the direct calling of the issuer of the certificate. This is not only time consuming, but also susceptible to interference. If the individuals on the other end do not authenticate the certificate, then there is little one can do in terms of protecting themselves from the risk. Image verification and change detection is another common technique [14]. This involves the comparison of the subject document with an original image of one held in a storage server. Image verification determines whether a document has been modified, and determines what content may have been added, deleted or otherwise modified [14]. When documents are held in a different server, they normally are in their original format and chances are that they can be modified [15]. Another example is the use of watermarked a quick response (QR) code. Normally, an embedded logo is generated that belongs to the owner of the document. Table1 shows the comparisons among RFID, digital watermarking and QR code

Table 1: Comparisons among RFID, digital watermarking and QR code

Attribute	RFID	Digital Watermarking	2D barcode (QR code)
Installation	Complex	Simple	Simple
Cost	Expensive	Expensive	In expensive
Lifetime	Very limited	Not limited	Not limited
Data hiding	Require a hardware	Not Required	Not required
Data Capacity	100s to 1000 characters	Not available	Up to 7,089 characters
Verification method	Require equipment	Not required	Require a smartphone with Camera
Technology used	RF (radio frequency)	-	Optical (laser)
Information Updating	New information can be written on the old tag	Cannot be updated	Cannot be updated
Information Capacity	More than QR code	Less	Less

TABLE I Comparisons among RFID, digital watermarking and QR code

4. IMPORTANCE OF CLOUD COMPUTING FOR DOCUMENT VERIFICATION

Cloud Computing has been utilized in various sectors. It has been shown its valuability to improve the Education sector. [31],[32],[33],[34].

A study by Gartner identified that Cloud Computing is the first among the top 10 most important technologies[35]. It is considered the fifth generation comes after mainframe computing, personal computing, client-server computing and the web [36]. Google, IBM, Microsoft, and salesforce.com are the biggest companies in the Cloud Computing environment [33]. In 60s years back, large rooms are needed to accommodate the number of computers. As a result, the consumed amount of electricity is very high. Fig.1 shows the perspectives of Cloud computing. Recently, the traditional computing infrastructure became costly and hard to manage because of that the demand for data and online users has been vastly increased. The traditional system integrates software, hardware, and underlying operating system, therefore organizations with adopting the traditional system in their environment need data centers to keep servers so they are required to spend money on power, cooling, and rental space. With traditional computing, it is very difficult to access the data anywhere and at any time hence, cloud computing comes in to overcome the mentioned issues. Cloud Computing can be just limited to a web browser [37],[38]. Cloud computing is categorized into three type: SaaS, PaaS and IaaS [35],[36], [39].[42],[43]. Each type will be discussed in the next paragraph.

Software as a service (SaaS) is located on the top of delivery models of cloud computing. It allows third-party vendors to deploy the applications remotely. It also allows the customer to use the cloud service provider's application (CSP's) running on cloud infrastructure via the internet. SaaS stills keep growing quickly. The most popular examples of SaaS providers are Google App and Salesforce which considered as a collection of remote computing services [31],[40]

Platform as a service (PaaS) is located in the middle of the service model of cloud computing. it delivers the services in various forms such as development tools, architecture, framework, programs, and Integrated Development Environments (IDE). The customers can control the applications without having any meaning in managing the underlying infrastructure. PaaS would be very helpful in the situation that multiple developers located in different physical locations need to work together. The most popular example of a PaaS provider is Google App Engine. It is a Software Development Kit (SDK) which provides an environment that supports Python, Java, and Go programming languages. PaaS is more flexible than the SaaS model because it provides features that are ready for the customer [31],[41].

Infrastructure as a service (IaaS) is located on the bottom of the service delivery model of Cloud computing. It is related to the computer hardware which offers network storage, virtual server/machine, data center, processor, and memory as a service [42]. The first step in providing infrastructure in an abstract manner is in the elasticity of allocating physical or virtual resources, therefore, IaaS provides scalability and provisions so the issues of infrastructure like spending huge amount of funds and time would be removed [31],[43].

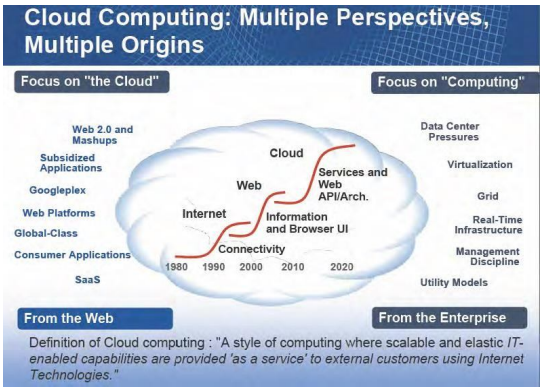

Figure 1: Cloud Computing Perspectives

5. THE PROPOSED FRAMEWORK

The proposed technique that will be investigated in this paper will be based on the three physical characteristics of the unforgeable document outlined by the researchers [8], [44],[45],[46]. It must have a multi-layered structure where

1. The information data in both the external and internal layers are tightly linked
2. The internal information cannot be extracted without the use of a special means to extract
3. The internal information cannot be changeable

Further, it will be geared towards the detection of the two types of forgery, type 1 and type 2. The proposed technique will be a hybrid of already existing techniques, but one which incorporates elements of multi-factor authentication. Verification will involve two simultaneous processes. The first will be scanning of 2D barcodes on the document to reveal a unique identification number from the document. This identification number, together with the certificate owner's fingerprint information will then generate a one-time pin, which is sent to both the institution and the certificate owner via email or SMS. This pin is then used as a login password with an ID to reveal the original document from a storage server for the final stage of comparison of details and structure. The first stage of scanning will detect any type 2 forgery attempt, while the second fingerprinting stage, as well as the final comparison stage, will detect any attempts at type 1 forgery. The proposed framework includes two stages; the first stage shown in fig.2 is proposed to be followed in the issuing process. The second stage shown in fig .3 is proposed to be followed in the verification process. By adopting the proposed framework, both issuing and verification process will be enhanced for better and that would resulted to mitigate the forgery issue.

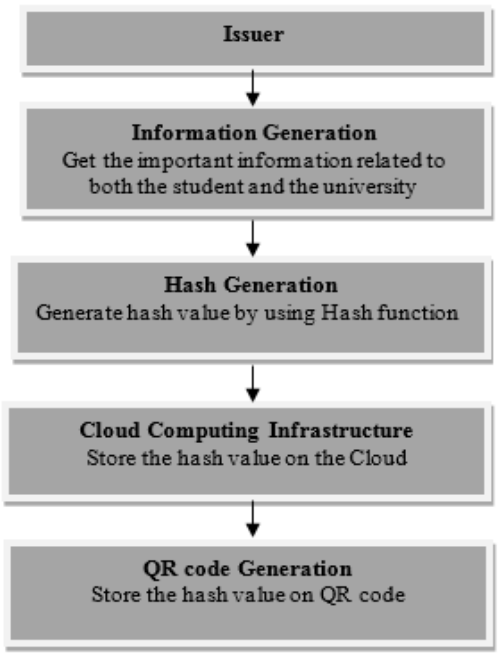

Figure 2: The Proposed Issuing Process

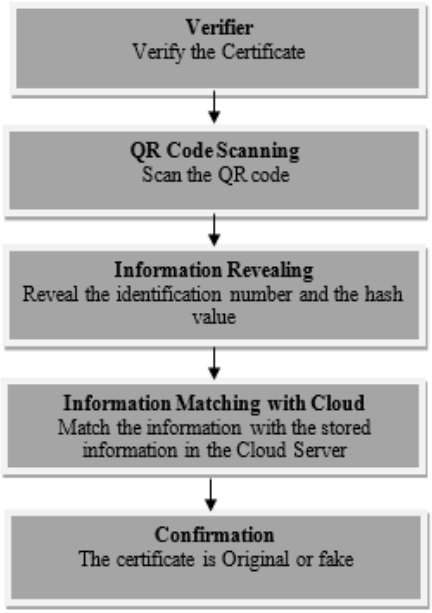

Figure 3: The Proposed Verifying Proces

6. CONCLUSION

In this paper, we critically analyzed the existing techniques that currently being used for document verification. As a result, a cloud-based framework for issuing and verifying the academic certificates. The proposed framework will enhance the issuing and verifying the academic certificates and thereby reduce the
incidence of certificate forgeries and ensure that the security, validity, and confidentiality of graduation certificates would be improved. With the proposed framework, all entities involved in the process of issuing and verifying such as the issuer, the verifier will get benefits. Author is working on the implementation part of the proposed framework and it will be validatied and tested in one of the academic institutions of Iraq.

ACKNOWLEDGMENT

Author would like to thank the Ministry of Higher Education and Scientific Research for supporting this research.

REFERENCES

[1] M. H. Eldefrawy, K. Alghathbar, and M. K. Khan, “Hardcopy document authentication based on public key encryption and 2D barcodes,” Proc. - 2012 Int. Symp. Biometrics Secur. Technol. ISBAST 2012, pp. 77–81, 2012.
https://doi.org/10.1109/ISBAST.2012.16

[2] C. M. Li, P. Hu, and W. C. Lau, “AuthPaper: Protecting paper-based documents and credentials using Authenticated 2D barcodes,” IEEE Int. Conf. Commun., vol. 2015-Septe, pp. 7400–7406, 2015.

[3] M. Salleh and T. C. Yew, “Application of 2D barcode in hardcopy document verification system,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 5576 LNCS, pp. 644–651, 2009.
https://doi.org/10.1007/978-3-642-02617-1_65

[4] O. Ghazal and O. S. Saleh, “A graduation certificate verification model via utilization of the blockchain technology,” J. Telecommun. Electron. Comput. Eng., vol. 10, no. 3–2, pp. 29–34, 2018.

[5] T. Mantoro, M. I. Wahyudi, M. A. Ayu, and W. Usino, “Real-time Printed Document Authentication Using Watermarked QR Code,” pp. 68–72, 2015.

[6] A. Husain, M. Bakhtiari, and A. Zainal, “Printed document integrity verification using barcode,” J. Teknol. (Sciences Eng., vol. 70, no. 1, pp. 99–106, 2014.
https://doi.org/10.11113/jt.v70.2857

[7] P. Documents, “Verification of the Integrity and Legitimacy of Academic Credential Documents in an International Setting,” Coll. Univ., vol. 84, no. 4, 2009.

[8] K. Nozaki, H. Noda, E. Kawaguchi, and R. Eason, “A Model of Unforgeable Digital Certificate Document System,” 2005.

[9] M. Warasart and P. Kuacharoen, “Paper-based Document Authentication using Digital Signature and QR Code,” 202.21.149.33, no. Iccet, 2012.

[10] “Document Authentication System Preventing and Detecting Fraud of Paper Documents.”

[11] Z. Chen, “Anti-Counterfeit Authentication System of Printed Information Based on A Logic Signing Technique,” 2007.

[12] G. Gupta, S. K. Saha, S. Chakraborty, and C. Mazumdar, “Document frauds: Identification and linking fake document to scanners and printers,” Proc. - Int. Conf. Comput. Theory Appl. ICCTA 2007, pp. 497–501, 2007.

[13] A. K. Mikkilineni, G. N. Ali, P.-J. Chiang, G. T. C. Chiu, J. P. Allebach, and E. J. Delp, “Signature-embedding in printed documents for security and forensic applications,” Proc. …, no. 0219893, pp. 455–466, 2004.
https://doi.org/10.1117/12.531944

[14] R. Jain and D. Doermann, “VisualDiff: Document image verification and change detection,” Proc. Int. Conf. Doc. Anal. Recognition, ICDAR, pp. 40–44, 2013.

[15] R. R. B, P. K. C, R. Singh, and R. Selvakumar, "Access Control and Data Security in Online Document Verification System," pp. 0–4, 2016.

[16] S. Balsubramanian, R. Prashanth Iye, and S. Ravishankar, "Mark sheet verification," 2009 3rd Int. Conf. Anti-counterfeiting, Secur. Identif. Commun. ASID 2009, 2009. https://doi.org/10.1109/ICASID.2009.5276942

[17] C. M. Li, P. Hu, and W. C. Lau, "AuthPaper: Protecting paper-based documents and credentials using Authenticated 2D barcodes," IEEE Int. Conf. Commun., vol. 2015-Septe, no. January 2013, pp. 7400–7406, 2015.

[18] A. Singhal, "Degree Certificate Authentication using QR Code and Smartphone," vol. 120, no. 16, pp. 38–43, 2015. https://doi.org/10.5120/21315-4303

[19] M. Warasart and P. Kuacharoen, "Paper-based Document Authentication using Digital Signature and QR Code," no. Iccet, 2012.

[20] M. Al-gawda, Z. Beiji, and N. Mohammed, "Printed Document Authentication Using Two-Dimensional (2D) Barcodes and Image Processing Techniques," vol. 9, no. 8, pp. 347–366, 2015.

[21] S. Liu, "Anti-counterfeit system based on mobile phone QR code and fingerprint," pp. 250–254, 2010.

[22] I. Tkachenko, W. Puech, O. Strauss, C. A. P. Omega, and M. Cedex, "Printed Document Authentication Using Two Level QR Code Authentication," Icassp 2016, pp. 2149–2153, 2016. https://doi.org/10.1109/ICASSP.2016.7472057

[23] P. Wang, X. Yu, S. Chen, P. Duggisetty, S. Guo, and T. Wolf, "CryptoPaper : Digital Information Security for Physical Documents," pp. 2157–2164, 2015.

[24] S. Ambadiyil, K. S. Soorej, and V. P. Mahadevan Pillai, "Biometric based unique ID generation and one to one verification for security documents," Procedia Comput. Sci., vol. 46, no. Icict 2014, pp. 507–516, 2015.

[25] E.-T. a., C.-C. I., N.-M. M., and P.-M. H., "Identity Document Authentication Based on VSS and QR Codes," Procedia Technol., vol. 3, pp. 241–250, 2012. https://doi.org/10.1016/j.protcy.2012.03.026

[26] S. Chavan, S. Gadakh, G. Kanchan, S. Surabhi, and P. D. V Shinkar, "QR code Authentication System for confidential (digital Mark sheet) Encrypted data hiding and retrieval (Decryption)," vol. 5, no. 4, pp. 88–92, 2016.

[27] M. Afrakhteh, S. Ibrahim, and M. Salleh, "Printed document authentication using watermarking technique," Proc. - 2nd Int. Conf. Comput. Intell. Model. Simulation, CIMSim 2010, pp. 367–370, 2010.

[28] S. Ibrahim, M. Afrakhteh, and M. Salleh, "Adaptive watermarking for printed document authentication," Proceeding - 5th Int. Conf. Comput. Sci. Converg. Inf. Technol. ICCIT 2010, pp. 611–614, 2010.

[29] F. Deguillaume, S. Voloshynovskiy, and T. Pun, "Secure hybrid robust watermarking resistant against tampering and copy attack," Signal Processing, vol. 83, no. 10, pp. 2133–2170, 2003.

[30] J. Gebhardt, M. Goldstein, F. Shafait, and A. Dengel, "Document authentication using printing technique features and unsupervised anomaly detection," Proc. Int. Conf. Doc. Anal. Recognition, ICDAR, pp. 479–483, 2013. https://doi.org/10.1109/ICDAR.2013.102

[31] O. Saad and M. Ehsan Rana, "Cloud Computing Adoption for Software Engineering Learning Environment: Set of Guidelines derived through Primary Research."

[32] O. SSaleh and M. Ehsan Rana, "Cloud-Based Learning Environment to Leverage Software Engineering Education."

[33] N. Nagar and P. Jatav, "A Secure Authenticate Framework for Cloud Computing Environment," no. 1, 2014.

[34] X. Ge, J. Yu, C. Hu, H. Zhang, and R. Hao, "Enabling Efficient Verifiable Fuzzy Keyword Search over Encrypted Data in Cloud Computing," IEEE Access, vol. 6, no. c, pp. 45725–45739, 2018.

[35] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," J. Internet Serv. Appl., vol. 4, no. 1, p. 5, 2013. https://doi.org/10.1186/1869-0238-4-5

[36] Y. Khmelevsky and V. Voytenko, "Cloud Computing Infrastructure Prototype for University Education and Research Categories and Subject Descriptors," Computing, pp. 1–5, 2010.

[37] S. Bhayal, "A study of security in cloud computing," Dep. Comput. Eng. Comput. Sci. Calif. State Univ. - Long Beach, vol. 2011, pp. 1–59, 2011.

[38] S. Singh, Y. S. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," J. Netw. Comput. Appl., vol. 75, pp. 200–222, 2016.

[39] O. Saad and M. E. Rana, "Use of Cloud-based Learning Environment in Enhancing the Teaching and Learning Process for Software Engineering Courses," Third Int. Conf. E-Learning E-Technologies Educ., pp. 246–252, 2014.

[40] H. Fan, F. K. Hussain, M. Younas, and O. K. Hussain, "services," Futur. Gener. Comput. Syst., 2015.

[41] D. Sun, G. Chang, L. Sun, and X. Wang, "Procedia Engineering Surveying and Analyzing Security , Privacy and Trust Issues in Cloud Computing Environments," 2011. https://doi.org/10.1016/j.proeng.2011.08.537

[42] Y. A. Younis, M. Merabti, and K. Kifayat, "Secure Cloud Computing for Critical Infrastructure : A Survey," 2013.

[43] F. Lombardi, R. Di, C. Nazionale, D. Informativi, and P. A. Moro, "Journal of Network and Computer Applications Secure virtualization for cloud computing," J. Netw. Comput. Appl., vol. 34, no. 4, pp. 1113–1122, 2011.

[44] L. M. Arjomandi, G. Khadka, Z. Xiong, and N. C. Karmakar, "Document verification: A cloud-based computing pattern recognition approach to chipless RFID," IEEE Access, vol. 6, pp. 78007–78015, 2018.

[45] W. A. Ghumman and J. Lässig, "Verification requirements for secure and reliable cloud computing," Proc. - 2013 IEEE 3rd Int. Conf. Cloud Green Comput. CGC 2013 2013 IEEE 3rd Int. Conf. Soc. Comput. Its Appl. SCA 2013, pp. 143–150, 2013. https://doi.org/10.1109/CGC.2013.29

[46] A. Souri, N. J. Navimipour, and A. M. Rahmani, "Formal verification approaches and standards in the cloud computing: A comprehensive and systematic review," *Comput. Stand. Interfaces*, vol. 58, pp. 1–22, 2018.