CLOUD BASED GRADUATION CERTIFICATE VERIFICATION MODEL

[1]OSMAN GHAZALI, [2]OMAR S. SALEH

[1,2]School of Computing, College of Arts and Sciences, University Utara Malaysia, 06010 UUM Sintok, Kedah, Malaysia
E-mail: [1]osman@uum.edu.my, [2]omer.saad10@gmail.com

Abstract- The graduation certificate issued by universities and other educational institutions is one of the most important documents for a graduate. It is proof of the graduate's qualification and can be used anywhere. However, due to advances in printing and photocopying technologies, fake certificates can be created easily and the quality of a fake certificate can now be as good as the original. The certificates issued by many prominent universities have been forged and these forgeries are difficult to detect. Moreover, many factors have led to reduced operational efficiency in student services at universities. One of the most significant factors that has had a detrimental effect on the quality of university services is the verification process for educational certificates and related documents. Yet, certificate verification is essential in order to ensure that the holder of the certificate is genuine and that the certificate itself comes from a real source. However, the verification of graduation certificates is a challenge for the verifier (the prospective employer who wants to verify the certificate). To address this issue, a cloud-based model for certificate verification is proposed. The university, the graduate and the verifier are the three parties involved in the proposed solution in order to accomplish accurate certificate verification. Three key aspects – security, validity and confidentiality – are considered in the proposed model. Several internal and external benefits can be obtained by using the proposed model. Internal benefits include improved work processes and ease of use for university staff due to the digitization of the verification process. External benefits include the receipt of faster and more efficient verification results by students/alumni and employers. The proposed model could also improve the links between universities and government entities.

Keywords- Cloud Computing, Graduation Certificate Verification, Data Security, Information Confidentiality.

I. INTRODUCTION

Institutions issue certificates to those who have successfully completed the requirements for graduation. A graduation certificate is still in the form of a paper-based document because, as yet, an electronic document cannot effectively replace a physical certificate [1].

However, due to the presence of advanced and cheap scanning and printing technologies, the forgery of certificates has increased, which threatens the integrity of both the certificate holder and the university that has issued the certificate [2],[3]. Moreover, the growing student numbers

Therefore document validation and verification has become an important task. In this context, it is the process of ensuring that the graduation certificate presented by a prospective employee is genuine and that the holder is the rightful owner. Moreover, a graduation certificate has to be verified to ensure that its content is true and also to ensure that the issued certificate comes from a real source [4].

Educational establishments try to combat fraud and forgery in several ways; however, most of the methods are time consuming because they are manual and involve human interaction [5]. A lot of the time is spent in either reaching out to the university to verify a certificate or in awaiting a reply from the university that the certificate is valid and true. This process can be extremely laborious and expensive especially if a company needs to check the certificates of several hundreds of applicants. Hence, this research attempts to model a cloud-based service to verify graduation certificates and preserve the confidentiality of the information in them.

II. ISSUES IN CURRENT PROCESS OF DOCUMENT VERIFICATION

The graduation certificate is one of the most important documents issued by universities and other educational institutions. It is proof of a graduate's qualification. However, due to advances in printing and photocopying technologies, fake certificates can be created easily and the quality of a fake certificate can now be as good as the original. The certificates of many prominent universities have been forged and these forgeries are very difficult to detect. Moreover, many factors have led to reduced operational efficiency in student services at universities. One of the most significant factors that has had a detrimental effect on the quality of university services is the verification process for educational certificates and related documents. Yet, certificate verification is essential in order to ensure that the holder of the certificate is genuine and that the certificate itself comes from a real source.

However, manual verification is a tedious task for any organization and its inaccuracy is one of the key reasons that document forgeries continue to be made and go unnoticed. The manual verification process can consume a lot of the resources (time and money) of both the issuer and the verifier and it imposes an extra burden on the university or college [6]. For example, the verifier may call the university to

request a check of a certificate and the university then has to consult its records and reply to the verifier.

III. CLOUD-BASED CERTIFICATE VERIFICATION

To meet the demands posed by the huge growth in educational content, resources and student numbers, a suitable environment needs to be adopted that can accommodate such advancements in the educational sector. The introduction of a cloud-based certificate verification process would be an important contribution to developing a proper educational environment. Cloud computing is one of the technologies that could enable such an environment; it is intended to help in providing a highly scalable IT platform and infrastructure. Cloud computing infrastructure and services can add value to the existing learning environment of an educational system [7].

According to technology experts, most institutions and companies will move to the cloud by 2020, and this should help to eliminate dependency on individual desktop-based systems [8],[16]. Cloud computing has been used in different domains to resolve various issues. In brief, it is an Internet-based technology that provides computational resources via a computer network and it offers scalable, flexible and on-demand services to end users by centralizing storage and network bandwidth as well as memory processing. Cloud computing relies on large data centres that permit the sharing of resources across hosted applications, which leads to economies of scale at both the hardware and software level [9]. Cloud computing has many of characteristics and its benefits can be summarized as follows [8],[14],[15]:

1. Cloud infrastructure is generally provided by third parties; however, the user can access data and applications via a browser anytime, anywhere;

2. Cloud computing allows for efficient utilization of resources;

3. Applications in the cloud can be easily maintained;

4. Cloud computing is scalable and affordable;
5. Performance monitoring is easily executed;
6. Fewer IT skills are required in order to implement the cloud;
7. The security of the cloud infrastructure can be better than the security of traditional systems.

IV. GENERAL PROCESS OF CERTIFICATE VERIFICATION

At present, the process of certificate verification involves three parties, the university, the owner (graduate) and the verifier (company/prospective employer) [17] as shown in Fig.1

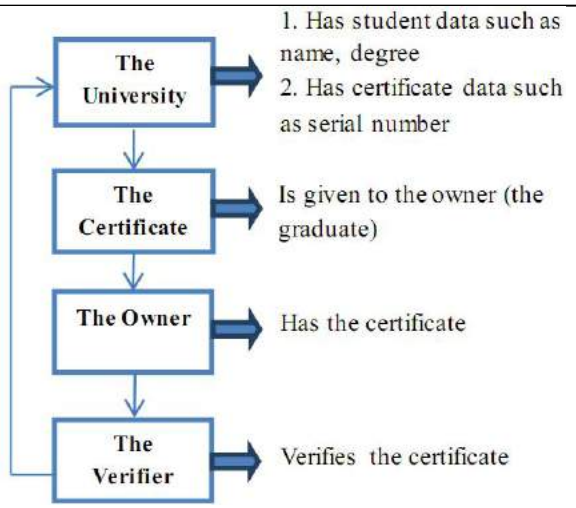

Fig.1. General process of certificate verification

It is clear from Fig.1 that the verification process for a graduation certificate involves several steps that need to be taken by each of the three key parties in order to successfully accomplish verification and that three key parties are involved in that process. This research aims to enhance the certificate verification mechanism by proposing a cloud-based model in order to combat the forgery of such certificates and preserve the confidentiality of the information in them.

V. PROPOSED PROCESS FOR CERTIFICATE VERIFICATION

Fig.2 shows how the general process of certificate verification can be enhanced. As mentioned above, three parties should be involved in the process in order to successfully complete certificate verification. To enhance certificate verification, it is proposed that the university generates a secret key for each graduate. To ensure confidentiality, this key is given to the graduate when he/she has received his/her certificate. The details on how to generate a secret key for a graduate and on how to ensure the security, validity and confidentiality of the issued certificate are described in Section 7.

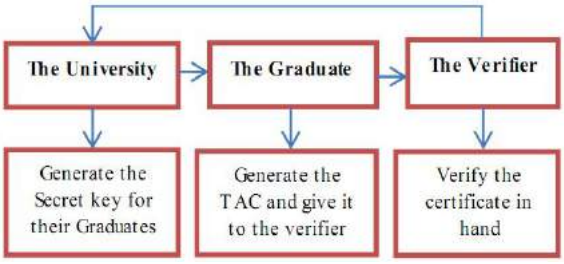

Fig. 2. Suggested process for certificate verification

VI. PROPOSED MODEL FOR CERTIFICATE VERIFICATION

Over the years, universities have increased in size substantially to accommodate the huge growth in the student base, faculty base and other related entities.

This has resulted in operational challenges for university officials and staff, and providing services to large student and alumni communities has become a herculean task. Gradually, it has started to affect the quality of service provided to the student and alumni network. Many factors have led to reduced operational efficiency in student services at universities. One of the most significant factors that has had a detrimental effect on the quality of university services is the verification process for educational certificates and related documents. Hence, the proposed model shown in Fig. 3 aims to enable universities to provide the best service possible to their large student and alumni communities. The proposed model addresses three main issues – security, validity and confidentiality – which are discussed in more detail below.

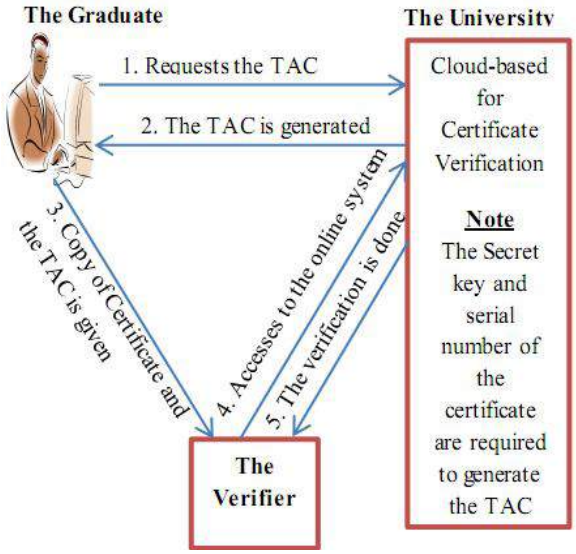

Fig.3. Proposed Model (Cloud- based model for Certificate Verification)

VII. DISCUSSION

Several methods can be used to verify a document and can guarantee the originality and confidentiality of a document, including cryptography techniques and cloud services [1],[6]. Both cryptography techniques and cloud services are incorporated into the suggested solution. This section describes how the proposed model can improve the security, validity and confidentiality of the certificate validation process.

7.1 Security

Cryptography is a process that is designed to address several security objectives such as confidentiality, data integrity, non-repudiation and authentication. Confidentiality means that the information can be understood just by the intended people while data integrity refers to the information being impervious to being altered illegally. Non-repudiation means that neither the sender nor the receiver can deny the creation or transmission of the information, while authentication refers to the bone fide nature of all parts of the document. Each type of cryptography has a pair of keys, one for encryption and another one for decryption. A key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm or cipher [10],[11].

There are two basic techniques in cryptography: symmetric (secret key) encryption and asymmetric (public-key) encryption. The former is considered in the suggested solution because it is faster and computationally cheaper than asymmetric key cryptography [12].

Symmetric key cryptography is also called shared key cryptography because the same key is used for encryption and decryption, i.e. both the sender and the receiver know the same key. Several kinds of symmetric key cryptography algorithm have been developed, such as DES, 3DES, AES, etc. When using a symmetric cryptography algorithm, the sender encrypts the message using the key and the receiver decrypts the message using the same key [12]. The process is shown in Fig.4.

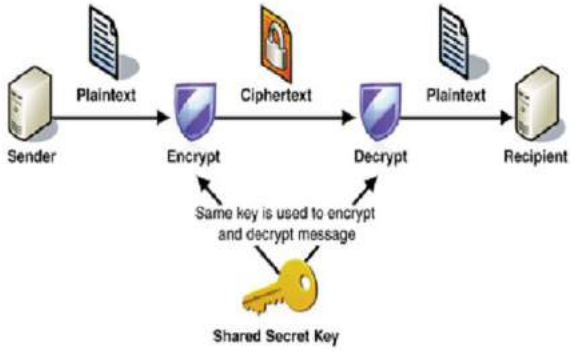

Fig. 4. Process of secret key (shared/symmetric) cryptography

Since the university is solely responsible for issuing certificates for their graduates, the security aspect has to be considered and ensured by the university itself. Unquestionably, all universities should apply a security mechanism when issuing certificates for their graduates. Educational institutions should have a mechanism to combat fraud both in the misuse of their name or to identify fake documents. The increasing incidence of fake documents has led to the introduction of many techniques such as holograms, stamps and wet-signatures. However, these techniques can easily be duplicated to create forged documents. Hence, the proposed model includes a step to generate a transaction authorization code (TAC). A TAC can be generated easily by using the proposed system because it is an online cloud-based system that is hosted on the university's own website. When a graduate wishes to apply for a job, they can request a TAC that can be used by their potential employer to verify and validate their graduation certificate. To successfully generate the TAC, the graduate must provide the system with two main inputs, a secret key and the serial number on their certificate. A secret key is generated by the university for all graduates when they receive their original certificate. When the secret key and the serial number are input into the system, a TAC is generated, but for

security purposes, the TAC that the verifier needs is only valid for a specific duration of time (e.g., 30 minutes, 1 hour or 24 hours), which is determined by the certificate owner.

7.2 Validity

Here, validity means that the issued certificate has been checked to ensure that it comes from a real source and also that the content of the certificate is true. This aspect is the main concern of the verifier (prospective employer/company/university). Clearly, the verifier will have been given a copy of certificate and will want to validate it. The potential inaccuracy of manual verification is overcome by allowing the verifier easy access to the proposed online system. To verify and validate the certificate the verifier must access the online system available on the university's website. The verifier has to provide two inputs in order to successfully verify and validate the certificate. The first input is the TAC mentioned above, which must be acquired from the graduate him/herself, and the second input is the serial number on the certificate that can easily be taken from the certificate in hand.

7.3 Confidentiality

Degree certificates and transcripts contain information that is confidential to the individual concerned and should not be easily accessible to others. Hence, there is a high need for a mechanism that can guarantee that the information in such a document is original, which means that document has originated from an authorized source and is not fake. In addition, the information in the document should be confidential so that it can only be viewed by authorized persons. Confidentiality is the most important feature of information security [13]. Therefore, it is crucial to ensure the confidentiality of information on the certificate and this aspect is taken into consideration in the proposed solution.

Let us assume that a copy of a certificate comes into the hands of an unauthorized person or entity such as a fake company and that they want to use the certificate illegally. The above-mentioned secret key can prevent this from happening. The secret key is required in order to verify and validate the certificate. However, it is impossible for unauthorized people to verify and validate the certificate because that secret key is unavailable to them. As a result, the certificate is useless to them.

VIII. BENEFITS OF PROPOSED MODEL

The proposed model has several benefits that can be classified into internal benefits and external benefits. Internal benefits include improved work processes and ease of use for university staff due to the digitization of the verification process. External benefits include the receipt of faster and more efficient verification results by students/alumni and employers. The proposed model could also improve the links between universities and government entities such as the Secretariat, gaining more reputation in the far-sightedness.

A specific benefit for universities would be that some staff and hardware resources would no longer be required as the time-consuming manual verification process would be eliminated. An important benefit for the graduate would be that the information in his/her certificate would be confidential making it difficult for unauthorized persons or entities to use their certificate illegally. A key benefit for the verifier would be that less resources such as time and money would be needed for verification as, for example, there would no longer be a need for the verifier to call the university and for the university to consult its records and reply to the verifier.

CONCLUSION

In this paper a cloud-based model for certificate verification was proposed in order to enhance the verification mechanism and thereby reduce the incidence of certificate forgeries and ensure that the security, validity and confidentiality of graduation certificates would be improved. By using the proposed model, some of the factors that result in reduced operational efficiency in student services at universities can be addressed and this should have a positive impact on the quality of services provided by universities. Internal benefits of the proposed model include improved work processes and ease of use for university staff due to the digitization of the verification process. External benefits include the receipt of faster and more efficient verification results by students/alumni and employers. The proposed model could also improve the links between universities and government entities.

ACKNOWLEDGMENTS

This research is funded by FRGS Research Grant Project no. 13144 (2014). The authors would like to thank Universiti Utara Malaysia and Ministry of Higher Education for supporting this research

REFERENCES

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

[2]. Z. Chen, "Anti-Counterfeit Authentication System of Printed Information Based on A Logic Signing Technique."

[3]. 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.

[4]. S. Balsubramanian, R. Prashanth Iye, and S. Ravishankar, "Mark sheet verification," 2009 3rd Int. Conf. Anti-counterfeiting, Secur. Identif. Commun. ASID 2009, 2009.

[5]. A. Singhal, "Degree Certificate Authentication using QR Code and Smartphone," vol. 120, no. 16, pp. 38–43, 2015

[6]. J. van Beusekom, F. Shafait, and T. M. Breuel, "Text-line examination for document forgery detection," Int. J. Doc. Anal. Recognit., vol. 16, no. 2, pp. 189–207, 2013.

[7]. 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.
[8]. T. Ercan, "Effective use of cloud computing in educational institutions," Procedia - Soc. Behav. Sci., vol. 2, no. 2, pp. 938–942, 2010.
[9]. M. A. Alahmad, I. Alshaikhli, and B. Jumaah, "Protection of the digital holy quran hash digest by using cryptography algorithms," Proc. - 2013 Int. Conf. Adv. Comput. Sci. Appl. Technol. ACSAT 2013, pp. 244–249, 2014.
[10]. G. Product and A. Service, "Brand protection through the cloud."
[11]. A. J. Abboud, "Protecting Documents Using Visual Cryptography," vol. 3, no. 2, pp. 464–470, 2015.
[12]. Y. Rajput, D. Naik, and C. Mane, "An Improved Cryptographic Technique to Encrypt Text using Double Encryption," vol. 86, no. 6, pp. 24–28, 2014.
[13]. J. Talbot and D. Welsh, "Complexity and Cryptography," pp. 1–9, 2006.
[14]. Y. Jadeja, "Cloud Computing - Concepts , Architecture and Challenges," pp. 877–880, 2012.
[15]. R. S. R. Pandian and K. S. Kasiviswanathan, "Effective use of cloudcomputing concepts in engineering colleges," Proc. - IEEE Int. Conf. Technol. Educ. T4E 2011, pp. 233–236, 2011.
[16]. K. Popović, "Cloud computing security issues and challenges," MIPRO, 2010 Proc. 33rd …, no. 3, pp. 247–255, 2010.
[17]. U. Garain and B. Halder, "On automatic authenticity verification of printed security documents," Proc. - 6th Indian Conf. Comput. Vision, Graph. Image Process. ICVGIP 2008, pp. 706–713, 2008.

★★★