Evaluation of the WPA2-PSK wireless network security protocol using the Linset and Aircrack-ng tools

Evaluación de seguridad en protocolo de red inalámbrico WPA2-PSK usando las herramientas Linset y Aircrack-ng

Avaliação de segurança em protocolo de rede sem fio WPA2-PSK usando as ferramentas Linset e Aircrack-ng

Fecha de recepción: 13 de septiembre de 2017
Fecha de aprobación: 27 de diciembre de 2017

Alberto Acosta-López*
Elver Yesid Melo-Monroy**
Pablo Andrés Linares-Murcia***

Abstract

Due to the emergence of new techniques and technologies of intrusion, the wireless network protocols have become obsolete; for this reason, this research seeks to violate and evaluate the security of the WPA2 protocol that is widely used by the Colombian service providers. The first section of this paper introduces the WPA2 protocol by describing its operation and the potential attacks it may suffer; the second part details the methodology used to collect the tests data and to carry out the evaluation necessary for the preparation of this article. In addition, we present the Linset and Aircrack-ng tools for auditing wireless networks that were selected to assess the security of the protocol. Finally, we show the results and conclusions.

Keywords: data security; information security; intrusion detection; wireless security.

Resumen

Debido al surgimiento de nuevas técnicas y tecnologías de intrusión, los protocolos de redes inalámbricas quedan obsoletos; para ello se busca vulnerar la seguridad del protocolo WPA2, que es ampliamente usado por los proveedores de servicios colombianos. En la primera parte, el artículo hace una introducción del protocolo WPA2, describiendo su funcionamiento y los ataques de los cuales puede ser objeto; en la segunda parte se muestra la metodología que se usó para recolectar pruebas y realizar la evaluación necesaria para la elaboración de este documento. Se presentan las herramientas para auditoría de las redes inalámbricas Linset y Aircrack-ng, las cuales fueron seleccionadas para la evaluación de seguridad del protocolo. Finalmente, se muestran los resultados y las conclusiones.

Palabras clave: detección de intrusión; seguridad de datos; seguridad de la información; seguridad inalámbrica.

* M. Sc. Universidad Distrital Francisco José de Caldas (Bogotá-Distrito Capital, Colombia). aacosta@udistrital.edu.co.
** Universidad Distrital Francisco José de Caldas (Bogotá-Distrito Capital, Colombia). eymelom@udistrital.edu.co.
*** Universidad Distrital Francisco José de Caldas (Bogotá-Distrito Capital, Colombia). paalinaresm@udistrital.edu.co.

Resumo

Devido ao surgimento de novas técnicas e tecnologias de intrusão, os protocolos de redes sem fio ficam obsoletas; para isso, busca-se vulnerar a segurança do protocolo WPA2, que é amplamente usado pelos provedores de serviços colombianos. Na primeira parte, o artigo faz uma introdução do protocolo WPA2, descrevendo seu funcionamento e os ataques dos quais pode ser objeto; na segunda parte mostra-se a metodologia que se usou para recolher provas e realizar a avaliação necessária para a elaboração deste documento. Apresentam-se as ferramentas para auditoria das redes sem fio Linset e Aircrack-ng, as quais foram selecionadas para a avaliação de segurança do protocolo. Finalmente, mostram-se os resultados e as conclusões.

Palavras chave: detecção de intrusão; segurança de dados; segurança da informação; segurança sem fio.

Para citar este artículo:
A. Acosta-López, E. Y. Melo-Monroy, and P. A. Linares-Murcia, "Evaluation of the WPA2-PSK wireless network security protocol using the Linset and Aircrack-ng tools," *Revista Facultad de Ingeniería,* vol. 27 (47), pp. 73-80, Jan. 2018.

I. Introduction

Cyber-attacks are a growing trend in modern Colombian society. These attacks impact users with information on the Internet [1] because the information traffic generated when files are moved from a computer or cell phone to the Internet, always creates an encryption that allows hiding information frames and packages necessary between the modem and the sending device. For this reason, it is necessary to know how such information packages, which contain important information for the security of our data, are attacked.

A. What is WPA2-PSK?

Among the existent wireless networks that allow interconnecting two or more computers to transmit data, the best known are WPAN (Wireless Personal Area Network), WLAN (Wireless Local Area Network), WMAN (Wireless Metropolitan Network), and WWAN (Wireless Wide Area Network). Each network has an associated protocol and IEEE standard that allow the review and the subsequent communication in a local or global network. We will focus on the WLAN wireless network with WPA2-PSK protocol based on the IEEE 802.11i standard that was released on July 24, 2014 [3-5].

WPA (Wireless Protected Access) originated in the problems detected in the WEP, a previous security system created for wireless networks [6]. WPA2-PSK (PSK acronym for Pre-Shared Key) is the evolution of the WPA protocol; it implements an algorithm based on a key of 8 to 63 characters, which is taken as a parameter, and with this value, a new key is randomly generated [6].

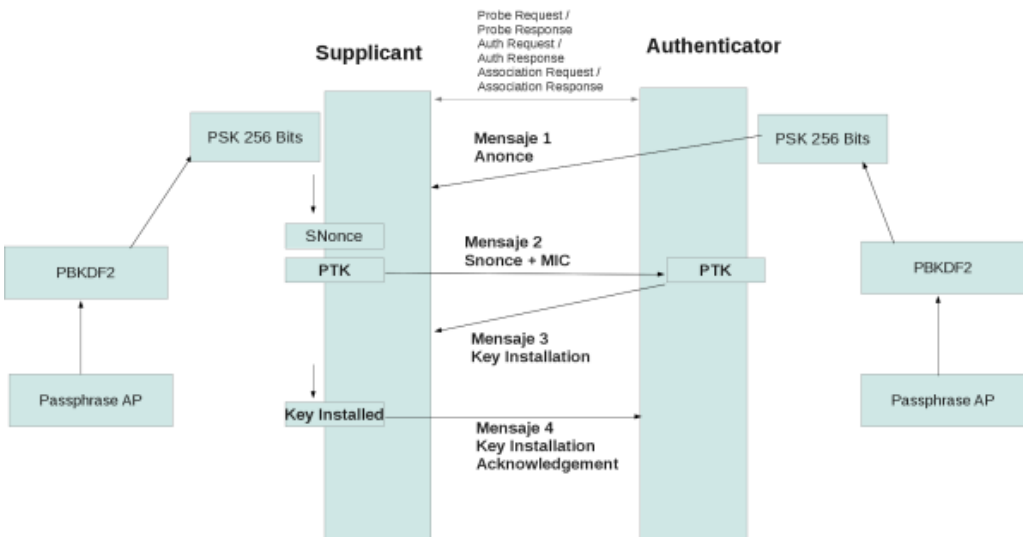

Fig.1 Operation of the protocol WPA2-PSK [6].

The operation of WPA2-PSK involves the following steps (Fig. 1):

1. The authenticator sends a message to the supplicant with a value generated randomly using its PSK key (an arbitrary value with no special meaning). This message is known as an authenticated nonce or simply nonce, because it contains a field called nonce whose value is generated randomly with the PSK key of the authenticator, as shown in Fig. 1, which was captured with Wireshark. In addition, the Replay Counter is an indicator that allows the authenticator and the supplicant to know the number of packages that have been previously sent [6].

2. The supplicant receives the message and generates another message called snonce (supplicant nonce), which is basically of the same type as the received anonce package, but contains a different nonce (an arbitrary text generated randomly using the PSK key of the supplicant) [6].

3. With the previous information, the supplicant creates the Pairwise Transient Key (PTK); this step is extremely important and, therefore, the

reader should pay more attention, because is where the "magic" of PSK and the dynamic generation of keys take place, which was implemented in the beginning to improve the security of WEP against fairly widespread attacks. PTK are the keys generated in each packet exchanged between the supplicant and the authenticator, and are generated using the Pairwise Master Key (PMK), but they are the same PSK code generated in step 1; that is, each PTK is generated dynamically by the supplicant PSK and the authenticator [6].

4. The procedure for generating the PTK key is really important, hence, its understanding is necessary. The PTK is generated by the PMK using a PTK random key generation function that takes the following parameters: 1) anonce, which is the package generated by the authenticator that contains a random text encrypted with its PSK key; 2) snonce, which is the package generated by the supplicant that contains a random text encrypted with its PSK key; 3) MAC authenticator; and 4) MAC supplicant [6].

5. The supplicant sends a packet to the authenticator with the snonce message and a MIC field (field encrypted using the Michael encryption mechanism) that allow performing an integral and consistent check of the packet; this field is generated by the supplicant using the PTK and the PMK [6].

6. With the package sent by the supplicant in step 5, the authenticator derives the PTK key, since it already knows the fields necessary to do the calculation: PMK, which is the same for both the supplicant and the authenticator, anonce, snonce, and the MAC addresses of the authenticator and the supplicant [6].

7. Once the authenticator has generated the PTK with the fields received from the previous packet (with the snonce field), it tries to generate the MIC field, since it has the same PTK and PSK as the supplicant. The MIC generated by the authenticator and the supplicant must be the same, and if that is the case, the authenticator sends a message to the supplicant of the type "Key Installation"; this message can be seen with the "Flag" of the type "Install Flag", which in turn can be seen in the third package exchanged in the authentication process [6].

8. The supplicant sends to the authenticator a "Key Install Acknowledgment" message, which simply confirms that, in this session of package exchange, the same PTK generated in the client and the AP were used. This package contains a "Key ACK" field with a value of zero, indicating that it is the last message sent in the authentication process between the supplicant and the authenticator [6].

Once the function of the WPA2-PSK protocol is understood, we can perform different types of attacks to detect its vulnerabilities.

B. Types of attack

Modems that create wireless networks for their users are vulnerable to several types of attack. The most common attacks are the following:

1. *SYN saturation attack*: flood network traffic. In other words, a single individual makes a large number of requests to the server, in this case the modem, which denies access to the rest of its users [7].

2. *DoS attack*: It is a denial of service attack [8].

3. *DDoS attack:* it is an extension of the DoS attack, but it attacks from different connection points [8].

4. *Identity theft:* Phishing is based on social engineering that focuses on the fact that humans make the greatest errors [8].

5. *Attack by intermediary:* It diverts packet information by changing it and returning altered information, or just checking what information is being handled by the target user [8].

II. Methodology

A. Software

1) WIFISLAX. Operating system based on Linux that can be used as a live cd or boot access on a USB; it was designed by www.seguridadwireless.net, and was adapted for Wireless [9]. This OS is an audit tool for wireless networks that contains a set of tools to function.

2) Linset. Application to audit wireless networks that does not use decryption dictionaries to obtain the access code to the network. With this tool, the cooperation of the user, who is unaware of the attack, is of vital importance, which implies that the user has little or no knowledge of computer security. Linset creates a fake AP with the same ESSID, as the one we are attacking and without any type of encryption; in addition, it authenticates the APs of the legitimate clients, preventing them to authenticate, and making them access the AP created by this tool and enter the password of the network [10].

3) Operation. This tool attack the modem, allowing network users to connect, and then, creating a fake network to which users will connect and provide the network password. Once the password is obtained, the fake network is closed and the modem operation is released.

4) Aircrack-ng. Complete suite of tools that audit wireless Wi-Fi networks. This tool focuses on different areas of security in wireless networks: packet-monitoring, attack, testing, and cracking [11].

5) VMware Workstation PRO (trial version). This tool is one of the industry standard products to run multiple operating systems as virtual machines on a single PC. Thousands of IT professionals, developers, and businesses use Workstation Pro and Workstation Player to improve agility, productivity, and security [12].

6) Windows 8 Pro (trial version). New operating system created by Microsoft. In this case, we will use Windows pro test version for the development of this research.

B. Hardware

Modem ZTE ZXV10 W300E (for home network use)

Desktop computer corei7 16 RAM

Network adapter TP-LINK WN725 (Does not support monitoring)

Network adapter TP-LINK WN722N (Supports packet monitoring)

C. Methods

The modem was configured to generate a wireless network called Security, use the WPA2-PSK protocol, and generate the password for accessing the newly created network. In this case, the network was called PruebaArticulo, and the password was @Prueba@.

We performed the audit using *attack by intermediary* and *DoS attack* (for using decryption dictionaries known as brute force), and run ten tests for each technique.

First, we carried out a brute-force attack, that is, an information package was captured with the wireless network encrypted access key. Afterwards, we carried out an impersonation attack, in which a third network that impersonates the original network is created, while the victim sends the password of his/her wireless network. In both attacks, we evaluated anonymity and waiting time to obtain access.

III. Results

This study allowed us to understand better the use of the audit tools. The focus of our analyses was to highlight the vulnerabilities of the security protocol; for this, we studied the following items: time to obtain the password, method, and visualization of the attack (Table 1).

Table 1
Comparative table between the Linset and Aircrack tools

	Linset	Aircrack
Method	Create an alternate network to capture the access key	Use repositories of dictionaries to make the comparison
Time	The time it takes to obtain a password is related to the lack of technical knowledge or ignorance on the part of the user	The time depends on the type of password security this can last from one to six months
Viewing the network client	It can be perceived by the network client	The network client is not aware of the attack of which he is being victim
Avoidable attack	The attack can be avoided	The attack can not be avoided

Table 2 shows the length (hours) of each of the 10 tests conducted with the Aircrack tool; whereas Table 3 shows the length (minutes) of the attacks with the Linset tool.

Table 2
Length (in hours Approx.) of an attack with Aircrack

Nø Test	Time (Hours)
1	11
2	15
3	10
4	12
5	24
6	16
7	17
8	12
9	14
10	21

Table 3
Length (in min Approx.) of an attack with Linset

Nø Test	Time (Minutes)
1	14
2	7
3	15
4	5
5	11
6	9
7	5
8	7
9	14
10	11

The network attack using Linset was one of the most effective; however, this is not because of the results, but because of the lack of defense methods. Therefore, as long as the attacker has a good network card, the attack is imminent and difficult to avoid if the user is unaware of it.

IV. Discussion

Although companies in Colombia like Digiware are dedicated to computer security, no system is 100 % safe. What is really important for an adequate protection of our data is education; however, how do we obtain this knowledge? Are the supplier companies willing to give us basic training to at least change the password of our wireless network? The truth is that the knowledge we have today is quickly becoming obsolete, particularly in technology; what before lasted a little over a year, nowadays only last for weeks or sometimes days. In the current information age, it is necessary to have a minimum of security in our data, which is why a question arises: who will train us for this?

This article presents two tools to evaluate the security of our wireless networks, and the way the WPA2 security protocol works. Additionally, we provided elementary knowledge about the different types of attacks that currently affect wireless networks. Evidently, besides computer viruses, the attacks to the network infrastructure are problematic because they allow access to the users' sensitive data.

V. Conclusions

Linset employs more advanced techniques than Aircrack, seeking the ingenuousness of the user to appropriate the network´s password. It also uses a technique of alternative creation of networks contrary to Aircrack, which collects identification packages; in terms of time, Aircrack method is more expensive than Linset. Aircrack attacks on vulnerable networks are totally unavoidable, therefore, it would be necessary to find a solution. The delay time that the Linset tool has against Aircrack is limited with respect to time: A Linset attack is limited by the user´s patience who usually does not tolerate more than 15 minutes without giving up the password. An Aircrack attack is limited by the power of the attacking machine; depending on the capacity of the machine, the search can take from days to weeks or even up to one month.

Depending on the management of the company, it is necessary to train the employees to identify the attacks on the networks, and thus avoid providing relevant information so the attacker can access the network. A mechanism to increase the security of entry to a private Wi-Fi network is the authentication through the devices Mac addresses. This mechanism not only allows the known devices to access, but also provide a degree of security.

Author contributions

Alberto Acosta supervised the study. Pablo Linares was the rapporteur of the project, made the first tests, and created the base methodology. Elver Melo helped validating the results and complemented the technical and bibliographic data for the realization of the practice.

Acknowledgments

The authors acknowledge the collaboration and funding from the research group TRHISCUD (Treatment of clinical historical information –Universidad Distrital) of the Engineering School at the Universidad Distrital Francisco José de Caldas. We plan to continue with this collaboration in future studies.

References

[1] D. Lemos, "El secreto en la nube," [Online]. Available: http://www.digiware.net/?q=es/blog/el-secreto-de-la-nube [Accessed Apr. 30, 2017].

[2] R. Juan, "Redes inalámbricas Principales protocolos," 2011. [Online]. Available: http://deredes.net/redes-inalambricas-principales-protocolos/ [Accessed Apr. 28, 2017].

[3] A. Hassan Adnan, "A comparative study of WLAN security protocols: WPA, WPA2," in *International Conference on advances in Eletronical Engineering (IEEE)*, Dhaka, Bangladesh, 2015.

[4] Intel, "Wi-Fi diferentes protocolos y velocidades de datos," 2017. [Online] Aviable: http://www.intel.la/content/www/xl/es/support/articles/000005725/network-and-i-o/wireless-networking.html [Accessed May. 20 2017].

[5] IEEE "802.11-2016 - IEEE Standard for information technology," 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7786995/ [Accessed May 21, 2017].

[6] J. Ruz Maluenda, B. Riveros Vasquez, and A. Varas Escobar, "Redes WPA/WPA2," [Online] Available: http://profesores.elo.utfsm.cl/~agv/elo322/1s12/project/reports/RuzRiverosVaras.pdf [Accessed May. 20, 2017].

[7] Ciberseguridad wikia, "Ataques TCP/IP," 2013. [Online] Available: http://es.ciberseguridad.wikia.com/wiki/Ataques_TCP/IP [Accessed May. 24, 2017].

[8] S. Dietrich, D. Dittrich, and P. Reiher. Denial of Service. *Attack and Defense Mechanisms*. NJ: Prentice Hall. 2004.
[9] Wifislax "Presentación," [Online] Available: http://www.wifislax.com [Accessed Jun. 4, 2017].
[10] A. Maroto, "Crackeando Redes Wi-Fi: WPA y WPA2 –PSK," 2016 [Online] Available: http://www.tic.udc.es/~nino/blog/lsi/reports/wpa.pdf [Accessed Jan. 20, 2017].
[11] Aircrack-ng, "Introduction," [Online] Available: http://www.aircrack-ng.org/doku.php [Accessed Mar. 27, 2017].
[12] VMware, "Workstation pro," [Online] Available: http://www.vmware.com/co/products/workstation.html [Accessed Mar, 30 2017].

Enterprise file synchronization and sharing services for educational environments in case of disaster

Servicios de sincronización y almacenamiento de archivos para entornos educativos en caso de desastre

Serviços de sincronização e armazenamento de arquivos para ambientes educativos em caso de desastre

Ana Isabel Delgado-Domínguez*
Walter Marcelo Fuertes-Díaz**
Sandra Patricia Sánchez-Gordon***

Fecha de recepción: 1 de septiembre de 2017
Fecha de aprobación: 2 de diciembre de 2017

Abstract

Cloud computing is an emerging solution that responds to the concept of Smart University; it aims at offering an intelligent environment of business continuity for the actors of an educational center. This research offers a recovery plan of educational services in case of disaster, through an action research, which analyzed free software for cloud computing, focusing on Enterprise File Synchronization and Sharing (EFSS). To achieve this, the implementation was placed in a local scenario (Linux Apache, MySQL, PHP, LAMP), and stress tests were performed on three applications: Nextcloud, Seafile and Pydio. Nextcloud had more consistent and better results than the other two applications; however, it lacks a system that allows synchronizing two Nextcloud instances. To solve this, we developed a routine aimed at providing an environment that monitors the hot site where the application is hosted and, from time to time, synchronize the instance to avoid data loss during disaster events. Afterwards, we configured a second application on a cold site that is alert to a possible service breakdown, so it can respond and sent immediate alerts. Finally, the usability of the routine was evaluated, and the disaster recovery plan for the EFSS was assembled, to offer a continuity of the educational services that are running in these environments.

Keywords: business continuity; cloud computing; disaster recovery; educational technology; information technology; open source.

Resumen

Las nubes computacionales son una solución emergente que responden al concepto de Smart University, para proporcionar un entorno inteligente de continuidad del negocio para los actores de un centro educativo. Esta investigación propone un plan de recuperación de servicios educativos en caso de desastres, aplicando la metodología de Investigación-Acción, que incluye un análisis de nubes computacionales de software libre, al enfocarse en los sistemas de Sincronización y Uso Compartido de Archivos Empresariales (EFSS). Para llevarlo

* M. Sc. Escuela Politécnica Nacional (Quito, Ecuador). ORCID: 0000-0003-2348-2260. ana.delgado@epn.edu.ec.
** Ph.D. Universidad de las Fuerzas Armadas ESPE (Sangolquí, Ecuador). ORCID: 0000-0001-9427-5766. wmfuertes@espe.edu.ec.
*** Ph.D. Escuela Politécnica Nacional (Quito, Ecuador). ORCID: 0000-0002-2940-7010. sandra.sanchez@epn.edu.ec.

a cabo se diseñó e implementó un escenario local (Linux Apache, MySQL, y PHP, LAMP). Para su evaluación y validación se realizaron varias pruebas de estrés en tres aplicativos: Nextcloud, Seafile y Pydio. Entre los hallazgos se evidenció que Nextcloud tuvo resultados consistentes por encima de las dos opciones restantes; sin embargo, esta solución no tiene un sistema que le permita sincronizar dos instancias de Nextcloud. Para solucionarlo, se desarrolló una rutina con el objetivo de proporcionar un ambiente que monitoree un *hot site* donde está alojado el aplicativo en producción y, cada cierto tiempo, realice sincronizaciones de la instancia para evitar la pérdida de información en caso de desastres. Luego, se configuró un segundo aplicativo en un *cold site* que está atento ante una posible caída del servicio, para su respuesta y alerta inmediata. Por último, se evalúo la usabilidad de la rutina y se ensambló un plan de recuperación de desastres para las EFSS, a fin de ofrecer una continuidad de los servicios educativos que se gestan en estos entornos.

Palabras clave: continuidad del negocio; nube computacional; software de código abierto; recuperación de información; tecnología educacional; tecnología de la información.

Resumo

As nuvens computacionais são uma solução emergente que respondem ao conceito de Smart University, para proporcionar um ambiente inteligente de continuidade do negócio para os atores de um centro educativo. Esta pesquisa propõe um plano de recuperação de serviços educativos em caso de desastres, aplicando a metodologia de Pesquisa-Ação, que inclui uma análise de nuvens computacionais de software livre, ao enfocar-se nos sistemas de Sincronização e Uso Compartilhado de Arquivos Empresariais (EFSS). Para levá-lo a cabo desenhou-se e implementou-se um cenário local (Linux Apache, MySQL, e PHP, LAMP). Para sua avaliação e validação realizaram-se várias provas de estresse em três aplicativos: Nextcloud, Seafile e Pydio. Entre os achados evidenciou-se que Nextcloud teve resultados consistentes acima das duas opções restantes; porém, esta solução não tem um sistema que lhe permita sincronizar duas instâncias de Nextcloud. Para solucioná-lo, desenvolveu-se uma rotina com o objetivo de proporcionar um ambiente que monitore um hot site onde está alojado o aplicativo em produção e, cada certo tempo, realize sincronizações da instância para evitar a perda de informação em caso de desastres. Logo, configurou-se um segundo aplicativo em um cold site que está atento ante uma possível queda do serviço, para sua resposta e alerta imediata. Por último, avaliou-se a usabilidade da rotina e elaborou-se um plano de recuperação de desastres para as EFSS, a fim de oferecer uma continuidade dos serviços educativos que se gestam nestes ambientes.

Palavras chave: continuidade do negócio; nuvem computacional; software de código aberto; recuperação de informação; tecnologia educacional; tecnologia da informação.

Para citar este artículo:
A. I Delgado-Domínguez, W. M. Fuertes-Díaz, and S. P. Sánchez-Gordon, "Enterprise file synchronization and sharing services for educational environments in case of disaster," *Revista Facultad de Ingeniería,* vol. 27 (47), pp. 81-91, Jan. 2018.

I. Introduction

The inclusion of Information and Communication Technologies (ICT) in education has taken a slow and uneven pace, both for their economic and human resources. As a consequence, in disaster situations there is no response that allows continuing the processes linked to administration, documentation, tracking, reporting, and delivery of educational courses. Given this, the computational cloud promises to reduce costs and offer high availability and long-term continuity [1]. The cloud is considered a model of flexible delivery of ICT services that provide systems and networks with high transfer rates [2].

The computational cloud arises from the need to build less complex IT infrastructures in comparison with the traditional technological schemes [3-6], in which the technicians install, configure and improve the software systems, hence, the assets of infrastructure are inclined to quickly become obsolete. Therefore, using these computing platforms is a solution for IT users, as an intelligent technology that responds to the Smart Education model, by offering a robust infrastructure environment.

The vision of Smart University deploys a set of services that focus on large-scale interactions, conceiving the university as a deeply dynamic and innovative place. To achieve this, Smart Education has its foundations on smart devices and emerging technologies [7] that respond to mobile learning. When using devices, it focuses on learner mobility, in contrast to traditional types of education [8]. Ubiquitous technology focused on learning can be used anytime and anywhere, without limitations of time, location, desktop, or mobile environments. Thus, intelligent technologies such as the computational cloud promoted the appearance of Smart Education. In this way, the advent of computational cloud has generated additional options for educators and students, providing them with the means to express their research, studies, and creativity in a distinctive way [9]. Its application not only alleviates the burden of educational institutions to manage the complex IT infrastructure, but also leads to great cost savings [10].

The present study focused on the recovery of services in educational environments, such as storage, communications, sharing, and file synchronization, by combining elements of the computational cloud supported by the Smart Education theory, such as the Synchronization and Use systems: Shared Enterprise File Synchronization and Sharing (EFSS). This allows us to respond to the particularities observed in disaster situations, such as the devastating earthquake of April 16, 2016, which left the education sector in the province of Manabí (Ecuador) out of operation due to the lack of a recovery plan in these eventualities of force majeure.

The rest of the article has been organized as follows: section 2 describes the state of art; section 3 synthesizes the applied research methods and techniques, as well as the activities carried out to bring the work to a successful conclusion; section 4 details the quantitative evaluation of the EFSS platforms; section 5 explains the start-up of the experiment; section 6 describes the experimental results of the EFSS implementations, and the execution of the developed routine in two EFSS instances, the measurement of the quality of use of the routine, and the discussion of the results obtained; finally, section 7 presents the conclusions and lines of future work based on the obtained results.

II. Related work

In various sectors, the use of technology based on file sharing via Internet, among the users of an organization and in collaboration with others, is becoming more and more prevalent [11]; therefore, it requires a careful selection of the solution in terms of administration, security, and costs.

In education, cloud-computing services provide a faster recovery and discovery of information, allowing students to store and share documents in a more flexible environment, and remote access to materials between students and instructors [12]. Computational clouds, in services such as Google Drive, Dropbox, Sky-Drive, and iCloud, offer the user the possibility of storing, reviewing, and accessing files synchronized among various devices [12], with a limiting use license that requires, among other aspects, a subscription fee and content restrictions. The main educational activities conducted in the computational cloud focus on discussing, planning, and using the interactive applications and services that are carried out in colleges and universities around the world [4, 13].

With the advent of computer clouds, disaster recovery of data loss is now possible for the education sector. The traditional techniques used for disaster recovery are very expensive, and the education sector could not afford it due to limited funds [10]. Scientific documentation on free computational clouds is scarce, and it is even more limited on disaster recovery on a free computational cloud. The application of cloud computing in the educational field is at an early stage in the scientific literature [14].

III. Research design

This research focused on implementing a recovery plan in case of disasters by using free computational clouds. To achieve this, we applied the Research-Action methodology, framed in a bibliographical, descriptive analysis, and in a quantitative/qualitative evaluation. In particular, we analyzed several free computational clouds and their relation to the processes that contribute to execute educational programs, when diagnosing the natural environment where the earthquake of April 16, 2016 took place, at the Universidad Laica Eloy Alfaro de Manabí (ULEAM), Ecuador.

The quantitative data were collected from experimental tests performed on each EFSS, which culminated in the development of a routine Shell script under the methodology of Experimental Software Engineering, specifically based on evidence. The main purpose was to improve decision making regarding the development and maintenance of software, integrating the best current evidence of research with practical experiences and human values [15].

To evaluate the EFSS, we carried out two activities. First, we evaluated and implemented three open source options: Nextcloud, Pydio and Seafile. Second, we prepared two test servers with the following characteristics: Intel (R) Xeon (R) CPU E3-1220 v3 @ 3.10GHz with 4 cores; 4 GB RAM memory; Ubuntu Server 14.04 with a kernel 3.13.0-85-64-GNU/Linux Ubuntu; two hard drives of 1 terabyte each. Each EFSS presents a logical layer architecture (Fig. 1), where the client layer is the interface or front-end of the user, with the services offered by the application. Ubiquity is a feature present in EFSS, which allows access from anywhere and at any time.

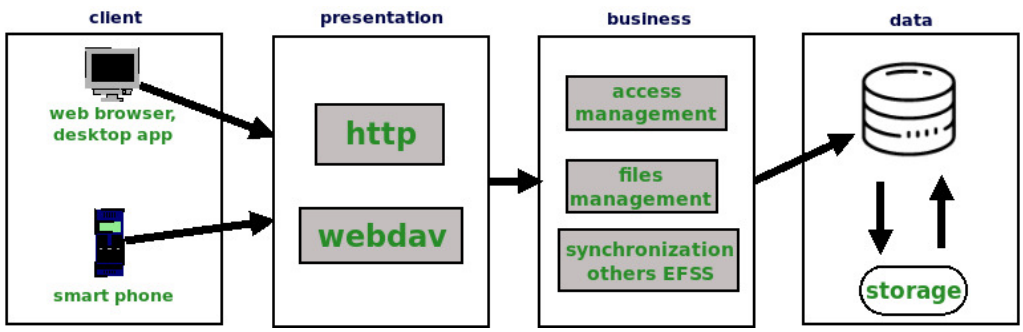

Fig. 1. EFSS logical layers.

IV. Quantitative and qualitative evaluation of the EFSS

According to a thorough review of the state of the art, there are more than 100 commercial EFSS solutions in the market [16]. However, due to the nature of this research, in which the University that served as a diagnosis is public, we framed the analysis in EFSS of free licensing.

Table 1 compares the characteristics of the EFSS, in terms of synchronization and storage. The installation requirements of each EFSS focused on an Apache web server, and the compatibility with databases such as MySQL and the GNU/Linux operating system. The versions of the EFSS analyzed were (a) Nextcloud 11.0.3, (b) Seafile 6.0.9, and (c) Pydio 7.0.4; some of the EFSS depend on packages according to the programming language in which they were developed. After implementing the EFSS, we installed the monitoring applications to obtain accurate data for the evaluation: (a) JMeter, an application written in Java open source, tests the performance and functional behavior of Web applications; we used the 2.13.20 version for GNU/Linux [17]; (b) Cacti, the front-end for RRDTool, stores data that comes from the RRDTool database and shows them graphically, as

well as stores the data in a MySQL database; we used the 0.8.8 version [18]; and (c) Mrtg, the front end for Snmpd (Simple Network Management Protocol), which is a daemon that collects information from the computer to make it available to other users; we used the 2.17.4 version [18].

Table 1
EFSS characteristics: Synchronization and Storage

	Characteristic	Nextcloud	Seafile	Pydio
Synchronization	Portable	√	X	√
	Conflict detection	√	√	√
	Rename and move files	√	√	√
	Version control	√	√	√
Storage	File protection with additional key	√	X	√
	Security / Encryption	ISO/IEC 270001:2013	HTTPS/TLS	Multiple-factor authentication
	Federation Sharing / Integration	√	X	X
	Additional features	A real-time collaborative tool; Calendar Contacts; Audio-video streaming	X (Enterprise)	X (Enterprise)

To carry out the tests, we assigned three (3) user segments of 1000, 6000, and 15000 threads each, which simulate 1000, 6000, and 15000 accesses of concurrent users, respectively. We chose these numbers based on the universe of students enrolled in the ULEAM [19]. JMeter, which is a loading tool to carry out simulations on any software resource, was configured so that the requests were completed by downloading a file with a size of 500 Kb.

V. Experimentation with EFSS in the recovery environment in case of disaster

After evaluating the EFFS, we implemented a synchronization process from the main to the secondary server; in Fig. 2 the broken line from the user to the current server represents the transparency that the user will have when switching from primary to secondary. We focused the tasks on synchronizing the time of the two servers, using as reference the Network Time Protocol (NTP) service of the Oceanographic Institute of the Ecuadorian Navy.

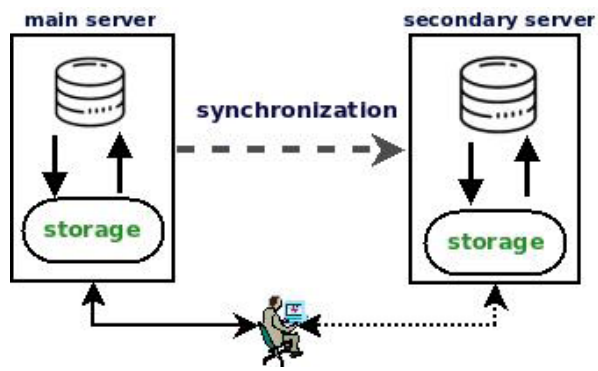

Fig. 2. Desired Architecture.

Subsequently, an SQL file from the database called *dbnc* was generated in the main server, as well as the file *db.md5* in order to check for integrity. We added an entry to the Linux *crontab* file, so it would execute every 10 minutes.

On the secondary server, we run another routine to verify whether the http service of the main server was operating or had failed, and to take the appropriate measures, checking integrity, transferring data, sending alert messages, and raising the http service. Finally, we added an entry in the *crontab* file of the secondary server, so it would execute every 10 minutes (Fig. 3).

```
#!/bin/bash
#Script que verifica que el estado del servicio del servidor principal
#y levanta el secundario, ademas se asegura de tener una ultima
#copia de base de datos.
# En los comentarios de este script se han eliminado
# intencionalmente las tildes y los caracteres especiales
# Elaborado por Ana Isabel Delgado Dominguez
FECHA=$(date +%d%m%Y-%H%M)
cd /var/www/html/nextcloud/
rm -rf dbnc.sql
rm -rf dbnc_comparar.md5
rm -rf dbnc.md5
rsync -apvr root@a.b.c.d:/opt/scripts/dbnc.* .
md5sum dbnc.sql > dbnc_comparar.md5
md5_comparar=$(cat dbnc_comparar.md5)
md5=$(cat dbnc.md5)
if [ "$md5_comparar" = "$md5" ];
then
   rsync -apvr root@a.b.c.d:/var/www/html/nextcloud/* .
   #Verificar estado del servicio http del servidor principal
   ESTADO=$(nmap 67.205.112.196 -p 80 | grep -o open)
   echo $ESTADO
   if [ "$ESTADO" != "open" ];
   then
        echo "servidor entra en produccion"
        #Se debe implementar funcion de envio de correo de notificacion
        echo "Servidor secundario ingresa a produccion" | mail -s "Alerta
NextCloud" anadelgado@gmail.com -r "administrador"
        mysql --user=userncdb --password=administrador ncdb <
ncdb.sql
        service apache2 start
    else
         service apache2 stop
    fi
else
    echo "Error al verificar integridad de transferencia verificar lo más
pronto posible" | mail -s "Alerta NextCloud" anadelgado@gmail.com
-r "administrador"
fi
```

Fig. 3. Routine Shell script for the recovery of an EFSS, in case of disaster.

Disaster recovery plan incorporating the routine (fragment)

To include the development of the routine within a disaster recovery plan for EFSS, we worked based on the ISO/IEC 22301 [20] standard, which focuses on Business Continuity Systems. From the gathering of information to the Central Computer Coordination Unit of the ULEAM, the planning to mitigate and prevent disasters on the services around the EFSS was completed in detail. The Government of Alberta (Canada) developed the template [21].

A. Authorization for the disaster recovery plan}

To elaborate this plan, we informed the highest authority of the Central Computer Coordination Unit.

Policies: Due to the lack of policies in the Central Computer Coordination Unit of the ULEAM before the earthquake of April 16, 2016, each department had its own Internet provider, its own IT staff, and an independent infrastructure depending on the area. However, the effects of the earthquake were evident, not only in material losses, but also in school desertion.

B. Scope of the disaster recovery plan

Table 2 describes the critical services in the EFSS.

Table 2
Critical services in the Efss

Level of Service	IT Service or Application Name	Recovery Time Objective, (RTO)	Recovery Point Objective, (RPO)
0	Authentication service	10 min	0
0	Download and upload service	10 min	0
0	File sharing service	10 min	0
1	Federation service with other EFSS	10 min	60 min
0	Instance synchronization service	10 min	0

- Assumptions

The Disaster Recovery Plan intends to provide the authorities with the information necessary to resume the EFSS service in an appropriate and timely manner, for the following scenarios:

- EFSS server hard drive failures
- Power failures of the data center or the servers cold room
- Corrupt database
- No Apache service (HTTP)
- Total disqualification of the data center, due to any type of disaster
- During the failure of the previous points, the secondary server located outside the institution will be enabled, either in a national or international data center.

The recovery procedures and the estimated time for the RTO (Target Recovery Time) and the RPO (Time Recovery Point) are based on assumptions that need validation:

- Implementation of a secondary server outside the institution with physical characteristics like those of the main server and equal software configurations
- Transfer of new files every 10 minutes from the main server to the secondary server
- Backup and verification of the integrity of the database
- The generated script for the transfer and treatment of the database generates alerts that should be taken seriously.
- Test period to make sure that the solution remains in operation.

C. Test plan

- Roles and responsibilities

The Disaster Recovery team, taking into consideration the current IT organization chart, will conform as follows (Fig. 4):

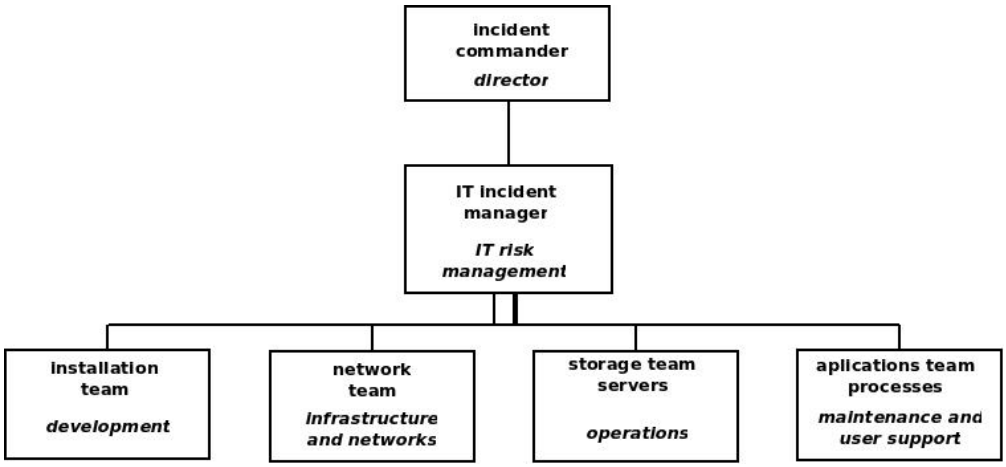

Fig. 4. Adapted IT organization chart.

The order of the individual tests performed before and after the interruption of the service must be the following:

- DNS and response times tests
- Integrity of database
- Integrity of data
- Apache services, MySQL without new features at startup
- User authentication service
- File download and upload service
- Directory and file sharing services

B. Verification of usability

In order to measure Usability, this research was based on the ISO/IEC 25000 series [22], also known as SQuaRE (System and Software Quality Requirements and Evaluation), which aims to help developing and acquiring products that fulfill the quality requirements and their evaluation [23]. Subsequently, we defined metrics of quality of use and weighted according to the studied reality. The evaluations of these metrics started from the definition of the evaluator (independent technician) and the scenario of the control tests in the main and secondary servers.

VI. Results and discussion

A. Results of EFSS

The JMeter, Cacti, and Mrtg tools evaluated the performance of each implemented EFSS, to obtain concrete results on homogeneous samples. Subsequently, the EFSS that generated the best results was subjected to the routine Shell script developed within the test servers. The routine monitored the main instance and executed backups in the secondary instance.

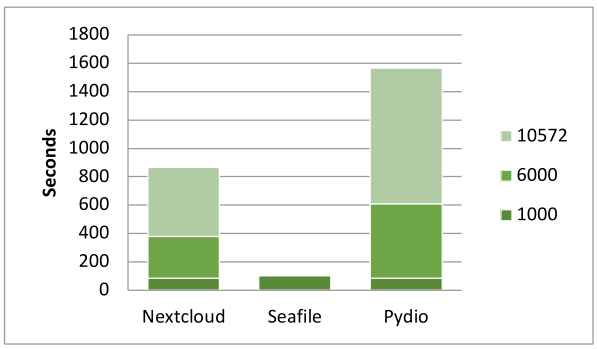

Fig. 5. Time for all samples.

The results focused on three elements: (a) the total and mean (μ) performance time used for all samples requested with a certain number of concurrent users; (b) concurrent users supported by the EFSS before collapsing; and (c) performance aspects in the server processor. In this way, Figure 5 shows the mean (μ) time (in seconds) that the EFSS took to execute the set of assigned requests; Figure 6 shows the number

of concurrent users that the EFSS supported when executing the assigned requests; Figure 7 depicts the average CPU consumption of each EFSS after 1, 5 and 15 minutes of execution; and Figure 8 details the average consumption of RAM memory for the execution of 6000 assigned requests.

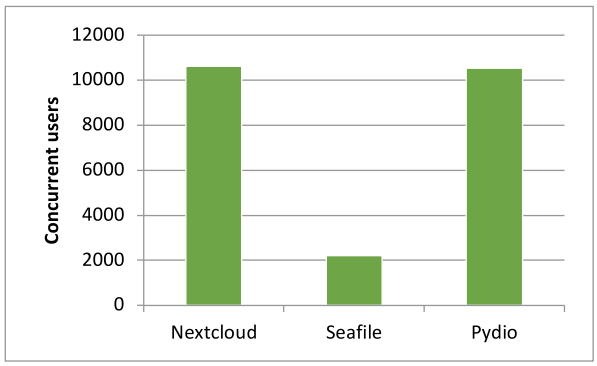

Fig. 6. Tolerance of user concurrence.

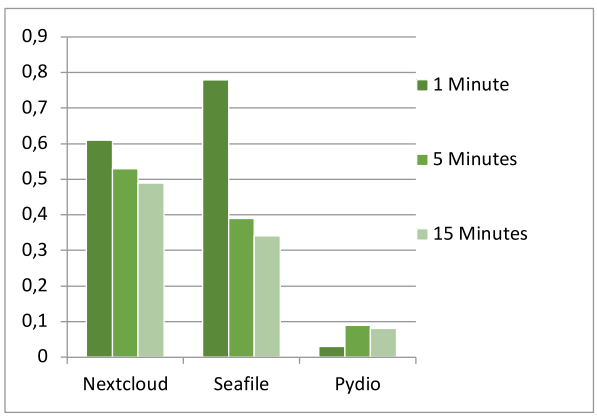

Fig. 7. CPU consumption.

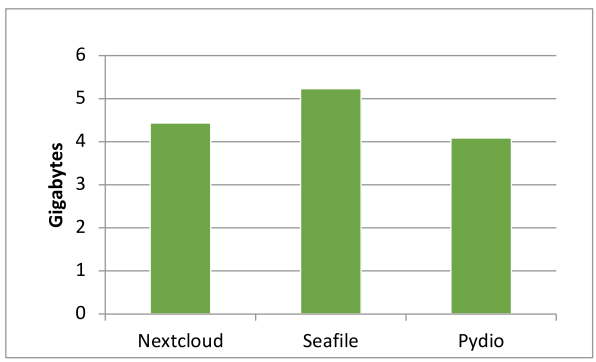

Fig. 8. Memory consumption.

Nextcloud was the EFSS with the best response rate, with a mean (μ) response time per request of 60 ms. Likewise, the number of defined users demonstrates the EFSS behavior for each group. Nextcloud maintained its response time, while Pydio increased considerably its response times as the stress test ran. Regarding the tolerance of concurrent users, Seafile was the first EFSS that did not support the stress test, with a number inferior to 2300 concurrent users downloading a 500 Kb file. In contrast, Nextcloud had a greater tolerance with the load of 10603 concurrent requests, maintaining the response time in all the scenarios. Finally, Pydio responded to no more than 10500 concurrent users with an equitable response time for each user group.

B. Usability of the routine

When selecting metrics on the Quality of Use, we used log monitoring applications on the main processes of the routine. The results showed that the developed routine meets the requirements and generates a high degree of satisfaction (Table 3). These results come from the following metrics: (a) Effectiveness; (b) Efficiency; (c) Satisfaction, and (d) Freedom of risk.

Table 3
Valuation of the usability of the routine

Quality	Quality of the routine	Score level	Degree of satisfaction
Use	9,00	Meets the requirements	Very satisfying

C. Discussion

The data indicate that Nextcloud performed remarkably better than its competitors, which have restricted certain modules and have a technical team under a business structure, instead of community and educational features such as those found in Nextcloud. On the other hand, the lack of a module that allows synchronizing the instances in Nextcloud was notorious. This motivated the implementation of a routine that added this feature, which we later verified in terms of functionality and usability, yielding very satisfactory data (Table 3).

In general, the test plan contemplated three clearly differentiated milestones. The initial phase corresponded to the preparation of the necessary environment, and the implementation and configuration of the necessary tools. The next phase

was the execution of the control tests, following the designed plan. The final phase was the data analysis, in which all the data obtained during the previous executions were studied to present them in such a way that they provide as much information as possible. From there, we proceeded to develop a routine to synchronize and remove the backup instance, product of the absence of this functionality in Nextcloud. The concept tests were carried out and the usability was evaluated. As a final product, the Disaster Recovery Plan was elaborated.

The opportunities found in Nextcloud are based on the nature of the project, which is completely open source, allowing us to detect a growth opportunity and thus develop a Bash routine to offer the continuity of storage and synchronization services. However, this implies a future development, which allows incorporating an emergency module and/or continuity in the configuration panel of the EFSS.

VII. Conclusions and Future Work

In the present study, we configured three computational clouds EFSS under free licensing, and evaluated them quantitatively by measuring the time they used to respond all the requests and each individual request, as well as the number of concurrent users supported and the consumption of CPU and RAM resources. The results of these tests determined that Nextcloud is the best EFSS to implement in an educational scenario, taking into account the impact it generates and its real-time collaboration features. Subsequently, and given the absence of a synchronization functionality of Nextcloud instances, it was necessary to develop a routine that allows business continuity in the face of a disaster. This routine and subsequent Disaster Recovery Plan were prepared based on the ISO/IEC 25000 and 22301 standards. As future work, we plan to include the routine as a back-end package within the EFSS, for its implementation in GNU/Linux distributions.

Authors' contributions

Delgado-Domínguez conducted the search, the recompilation, and the analysis of the papers referenced in this article, and contributed to write the manuscript. Fuertes-Díaz was the advisor of the project, and supervised the development of the DRP. Sánchez-Gordón contributed to write the manuscript and reviewed it. All authors read and approved the final manuscript.

References

[1] F. Daryabar, A. Dehghantanha, and K.-K. R. Choo, "Cloud storage forensics: MEGA as a case study," *Aust. J. Forensic Sci.*, pp. 1–14, Apr. 2016. http://doi.org/10.1080/00450618.2016.1153714.

[2] L. Yang, "Education Cloud: New Development of Informationization Education in China," in *Frontier and Future Development of Information Technology in Medicine and Education*, 2014. DOI: http://doi.org/10.1007/978-94-007-7618-0_131.

[3] S. Kamada, T. Ichimura, T. Shigeyasu, and Y. Takemoto, "Registration system of cloud campus by using android smart tablet," *Springerplus*, vol. 3 (1), pp. 761–774, 2014. DOI: http://doi.org/10.1186/2193-1801-3-761.

[4] T. Dong, Y. Ma, and L. Liu, "The Application of Cloud Computing in Universities' Education Information Resources Management," in *International Conference on Information Engineering*, 2012. DOI: http://doi.org/10.1007/978-1-4471-2386-6_122.

[5] Chrysikos and R. Ward, "Cloud Computing Within Higher Education: Applying Knowledge as a Service (KaaS)," in *Continued Rise of the Cloud: Advances and Trends in Cloud Computing, Z*, 2014. DOI: http://doi.org/10.1007/978-1-4471-6452-4_13.

[6] D. C. Wyld, and R. L. Juban, "Education in the Clouds: How Colleges and Universities are Leveraging Cloud Computing," in *Technological Developments in Networking, Education and Automation*, 2010. DOI: http://doi.org/10.1007/978-90-481-9151-2_1.

[7] J. Zhang, S. Sagar, and E. Shihab, "The Evolution of Mobile Apps: An Exploratory Study," in *International Workshop on Software Development Lifecycle for Mobile*, 2013. DOI: http://doi.org/10.1145/2501553.2501554.

[8] J. C. Augusto, "Ambient intelligence: opportunities and consequences of its use in smart Classrooms," Innov. Teach. Learn. Inf. Comput. Sci., vol. 8, no. 2, pp. 53–63, Jun. 2009. DOI: http://doi.org/10.11120/ital.2009.08020053.

[9] Y. Shi, H. H. Yang, Z. Yang, and D. Wu, "Trends of Cloud Computing in Education," in *7th International Conference Hybrid Learning*, 2014. DOI: http://doi.org/10.1007/978-3-319-08961-4_12.

[10] K. B. Nayar, and V. Kumar, "Benefits of Cloud Computing in Education During Disaster," in *International Conference on Transformations in Engineering Education: ICTIEE*, 2014. DOI: http://doi.org/10.1007/978-81-322-1931-6_24.

[11] Gregus, and V. Karovic, "Practical Implementation of Private Cloud Based on Open Source ownCloud for Small Teams - Case Study," 2016, pp. 183–187.

[12] I. Arpaci, "Antecedents and consequences of cloud computing adoption in education to achieve knowledge management," *Comput. Human Behav.*, vol. 70, pp. 382–390, May. 2017. DOI: http://doi.org/10.1016/j.chb.2017.01.024.

[13] V. Paranjape, and V. Pandey, "An Innovation in Education Through Cloud Computing," in *All India Seminar on Biomedical Engineering*, 2012.

[14] X. Wang, and Q. Cai, "The Analysis of the Application of Cloud Computing in the Field of Basic Education," in *Second International Conference Technology in Education*, 2015. DOI: http://doi.org/10.1007/978-3-662-48978-9_16.

[15] S. Pizard, F. Aceranza, V. Casella, S. Moreno, and D. Vallespir, "Conceptos de Ingeniería de Software Basada en Evidencias," *Reporte Técnico*, RT 15-08, 2015.

[16] M. Basso, C. Smulders, and J. Mann, "Magic Quadrant for Enterprise File Synchronization and Sharing Market," *Gart. Inc.,* Jul. 2015, pp. 16, 2014.

[17] F. J. Díaz, C. M. Banchoff Tzancoff, A. S. Rodríguez, and V. Soria, "Usando Jmeter para pruebas de rendimiento," in *XIV Congreso Argentino de Ciencias de la Computación*, 2008.

[18] S. Powers, "Graph Any Data with Cacti!," *Linux Journal*, vol. 271. pp. 50–68, Nov. 2016.

[19] ULEAM, "Reporte de matriculados 2016 y 2017," Universidad Laica Eloy Alfaro de Manabí, 2017.

[20] ISO/IEC, "ISO/IEC 22301:2012 Societal security -- Business continuity management systems --- Requirements," 2012.

[21] Alberta Education, "IT Disaster Recovery Planning Guide", 2016. Available in: http://education.alberta.ca/media/3272747/2-it-disaster-recovery-planning-guide.pdf.

[22] ISO/IEC, "ISO/IEC 25010 (2011) - Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models," 2011.

[23] K. Esaki, "Verification of Quality Requirement Method Based on the SQuaRE System Quality Model," *Am. J. Oper. Res.*, vol. 3 (1), pp. 70–79, 2013. DOI: http://doi.org/10.4236/ajor.2013.31006.