ISSN: 2007-5448

Volúmen 6 No. 2

RECIBE

Revista electrónica

DE COMPUTACIÓN, INFORMÁTICA, BIOMÉDICA Y ELECTRÓNICA

PUBLICACIONES
Vol.6 No.2 | Nov 2017 - Abr 2018

Índice

Computación e Informática

Electrónica

Recibido 5 May 2017
Aceptado 22 Sep 2017
ReCIBE, Año 6 No. 2, Noviembre 2017

Aplicación móvil basada en el contexto para promover el aprendizaje del idioma inglés

Context-based mobile application to encourage English language learning

Osiris Montero Ríos[1]
osirismonterorios@gmail.com

Francisco Aguilar Acevedo[1]
aguilar.afco@sandunga.unistmo.edu.mx

Guadalupe Toledo Toledo[1]
gtoledo_1207@hotmail.com

Silvia Reyes Jiménez[1]
chivisza9@sandunga.unistmo.edu.mx

Daniel Pacheco Bautista[1]
dpachecob@bianni.unistmo.edu.mx

[1]Universidad del Istmo

Resumen: La telefonía móvil que en un principio se comercializó como dispositivos de comunicación y entretenimiento, en la actualidad es empleada en sectores tan diversos como la educación. Dentro de los métodos de apoyo al proceso de aprendizaje destacan las aplicaciones móviles y en especial las relacionadas con los idiomas. En su mayoría, estas aplicaciones emplean estrategias de enseñanza universal que sugieren situaciones ajenas al entorno sociocultural del usuario, lo cual podría impactar en su aprendizaje. En este artículo se muestra el desarrollo de una aplicación Android para promover el aprendizaje del idioma inglés basada en información provista por el usuario que le resulta de su interés. Se presenta el diseño del contenido educativo y de la aplicación móvil que permiten al usuario generar su propio material didáctico en base a sus intereses. Como caso de estudio se considera la evaluación de la aplicación para el área de las ciencias computacionales.

Palabras clave: Sistemas basados en el contexto, Android, aprendizaje móvil.

Abstract: Mobile telephony was initially marketed as communication and entertainment devices. It is currently used in different sectors such as education. Mobile applications, especially those related to language, stand out within the methods that support learning. Most applications use universal teaching strategies and propose situations that are unrelated to the user's socio-cultural environment. This is a drawback that may affect learning. This article presents the development of an Android application for the learning of English which is based on the information provided by the user that is of interest to you. The design of both the educational content and the mobile application that allow users to generate their own learning material according to their own interests is also presented. The case study is the assessment of the application within a computer science área.

Keywords: Context-based systems, Android, m-learning

1. Introducción

Saber inglés se ha convertido en una competencia básica de estudiantes de todos los niveles educativos. Pero ¿por qué es tan importante el idioma inglés? Según Calderón (2015), porque hay más de dos mil millones de personas que lo usan regularmente y además se habla en 138 países, porque 4 de cada 5 interacciones en inglés se dan entre personas para las cuales ese idioma no es su lengua materna, porque particularmente en México uno de cada dos empleos con ingreso superior a cincuenta mil pesos exige el uso constante del inglés, y porque hablar una segunda lengua tiene un impacto positivo sobre el desarrollo neurológico. Más aún, muchas de las publicaciones científicas y libros se divulgan en inglés, hecho que acentúa su importancia en la educación, la investigación y la práctica profesional. Sin embargo, en México las marcadas deficiencias en el dominio del idioma inglés, es una problemática en todos los niveles educativos la cual no es privativa de un estado o región; sino de todo el país (Lemus, Duran, y Martínez, 2008).

En respuesta a este tipo de problemáticas, organismos como la UNESCO (Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura), han fomentado iniciativas encaminadas a estudiar de qué manera las tecnologías móviles pueden propiciar la consecución de la educación para todos, señalando que el *m-learning* o aprendizaje móvil proporciona estrategias al proceso de enseñanza- aprendizaje a través del uso de computadoras portátiles, tabletas electrónicas, teléfonos inteligentes (*smartphones*) e incluso teléfonos móviles[i] (UNESCO, s.f.). Dicha organización ha publicado una serie de estudios sobre aprendizaje móvil, cuyo propósito es lograr una mayor comprensión de cómo las tecnologías móviles pueden ser utilizadas para mejorar el acceso, la equidad y la calidad de la educación en todo el mundo. En dicha documentación se señala que a medida que aumenta la cantidad y el tipo de información que pueden recopilar los dispositivos móviles acerca de sus usuarios, este tipo de tecnología será más apta para la individualización del aprendizaje, otorgando a los estudiantes mayor flexibilidad para avanzar a su propio ritmo y seguir sus propios intereses, lo que podría aumentar su motivación para aprovechar las oportunidades de aprendizaje (UNESCO, 2013).

Por otra parte, el popular uso de los dispositivos móviles como smartphones y tablets, han incorporado nuevos paradigmas con el objetivo de mejorar la experiencia del usuario. Numerosas aplicaciones comerciales en las dos plataformas dominantes en el mercado: iOS y Android, son testimonio de estos nuevos paradigmas. Un enfoque para mejorar la experiencia del usuario de una aplicación es realizar un seguimiento del contexto, considerada como aquella información que se puede utilizar para caracterizar la situación de una entidad, donde una entidad puede ser una persona, un lugar u objeto (Kolangade, 2013). El desafío es identificar aquellas piezas de información contextual que son

consideradas más relevantes y que pueden ser obtenidas de manera fiable (Peña, 2016).

Así, en este artículo se presenta el desarrollo de una aplicación para móviles Android que permite al usuario generar su propio material didáctico contextualizado a partir de textos de su interés escritos en idioma inglés, que él mismo provee, fomentando de esta manera su autoaprendizaje. Como caso de estudio se presenta la evaluación de la aplicación para lecturas acordes al tópico de las ciencias computacionales en idioma inglés, considerando que la mayoría del vocabulario técnico que se utiliza en esta área tiene su fundamento en dicho idioma. Es de resaltar que la aplicación muestra un grado de flexibilidad no observado en aplicaciones comerciales.

2. Aplicaciones Basadas en el Contexto

En el campo de la computación se denomina contexto a cualquier información que puede ser usada para caracterizar la situación de una entidad (persona, lugar u objeto), y que es considerada relevante para la interacción entre el usuario y la aplicación (Abowd, et al., 1999). Los sistemas que toman en cuenta el contexto en su interacción con el usuario o con la lógica de procesamiento suelen denominarse sistemas basados en el contexto.

En un sistema de cómputo, las acciones del usuario que se requieren como entrada para determinar la solución, dirección o acción, pueden ser parcial o completamente eliminadas con el uso de contextos (Kolangade, 2013). Esto es especialmente cierto en los sistemas de cómputo móvil donde la naturaleza portátil inherente de los dispositivos permite que exista un gran número de variables influyentes tales como la edad, el género, los gustos, entre otras, que pertenecen al entorno, razón por lo cual, los sistemas basados en el contexto han sido investigados y desarrollados, empleando dispositivos móviles, desde hace más de una década. Por ejemplo, en Zheng, Cheng y Xu (2016) se describe una aplicación de comercio electrónico (*e-commerce*) con una interfaz de usuario que se adapta en función de la información del dominio del usuario como la edad, el género, la categoría del usuario e información de los cambios en el entorno como el nivel de batería y la disposición de Wi-Fi. Un árbol de adaptación es empleado para representar la adaptación de la interfaz de usuario en el dispositivo.

Con propósitos de enseñanza-aprendizaje se han realizado diversas investigaciones. En Wanumen, Cavanzo, y Guevara (2015) se aborda el desarrollo de una plataforma de enseñanza-aprendizaje de conceptos básicos sobre astronomía a través de una aplicación Android con dos modelos de adaptación: uno basado en el perfil de usuario de Facebook y el otro con

atributos pertenecientes al contexto. Los datos de la cuenta de Facebook brindan a la plataforma de enseñanza-aprendizaje la información necesaria para perfilar el rol al que pertenecerá el usuario (ya sea docente o estudiante básico-intermedio-avanzado).

Para el caso del modelo de adaptación basado en el contexto se hace uso de la ubicación del usuario y el tiempo calendario. En el primer caso, la interacción con el usuario se limita a mostrar su cambio de ubicación mediante una brújula en pantalla e indicar cómo llegar a un determinado lugar. El tiempo calendario permite al sistema mostrar las fases de la luna y calcular su fase actual dependiendo de la época del año. Bajo la otra perspectiva, en Gómez, Hernández y Morales (2015) se presenta un sistema de aprendizaje situado capaz de entregar contenidos a estudiantes de ingeniería de acuerdo con el contexto. La arquitectura del sistema se fundamenta en la filosofía cliente-servidor. El cliente se configura para proporcionar un acceso *offline* y *online*. En el caso de la configuración *offline* se hace uso de la realidad aumentada mediante objetos modelados en 3D que son almacenados-presentados en una computadora personal. Mediante el acceso *online* el estudiante puede seleccionar a través de una aplicación móvil, el tipo de lectura a realizar: QR Code (*Quick Response*, Código de Respuesta Rápida) o NFC (*Near Field Communication*, Comunicación de Campo Cercano), mientras el servidor gestiona los contenidos respectivos. Se realizan tres experiencias de aprendizaje con estudiantes de los programas de Ingeniería de Sistemas, Eléctrica y Mecánica.

En lo que respecta al aprendizaje de idiomas, en Morales, Igler, Böhm, y Chitchaipoka (2015) se presenta una aplicación móvil para el aprendizaje de idiomas como apoyo a usuarios que viven en países extranjeros. En primera instancia, la aplicación Android se enfoca en estudiantes de Alemania y Tailandia interesados en programas de intercambio entre estos dos países. La aplicación sugiere vocabulario, frases u oraciones que son útiles para el usuario, considerando atributos tales como el género del usuario, la geolocalización y el lenguaje nativo.

Los resultados reportados estiman que el enfoque propuesto mejora la experiencia de aprendizaje al considerar el contexto de uso, resultando en un proceso de aprendizaje más efectivo. Por su parte, en Sun, Hou, Hu y Al-mekhlafi (2015) se describe un prototipo de sistema para el aprendizaje del idioma Chino dirigida a extranjeros en China cuya nativa o segunda lengua es el inglés. La aplicación proporciona materiales de aprendizaje relacionados con lo que el usuario está haciendo o lo que va a hacer. El sistema propuesto presenta una arquitectura cliente-servidor vía red inalámbrica. La base de datos en el servidor almacena los materiales de aprendizaje, mientras la aplicación móvil cliente provee la interfaz de usuario. El sistema también puede adaptarse a los perfiles

de los estudiantes como muchos sistemas de aprendizaje electrónico (*e-learning*) existentes.

3. Organización del Contenido Educativo de la Aplicación Propuesta

En la Figura 1 se ilustra un proceso seguido por el usuario para solucionar su problema de aprendizaje. En búsqueda de apoyo en su proceso de aprendizaje, el usuario encuentra en la educación presencial una acertada opción cuyo costo sin embargo va en aumento (Jardines, 2010). Por otra parte, se tiene a la educación a distancia que mediante el uso de la tecnología busca maximizar la interacción profesor-alumno, enfatizando en la autonomía del estudiante. Desprendida de esta instrucción a distancia se encuentra el aprendizaje móvil, como un método de apoyo al proceso de aprendizaje mediante el uso de los ahora comunes dispositivos móviles. El elemento final de este proceso señala la atención al usuario mediante aplicaciones con estrategias de enseñanza que tienen mucho de universal, al sugerirle situaciones ajenas a su entorno sociocultural, lo cual podría impactar en su aprendizaje.

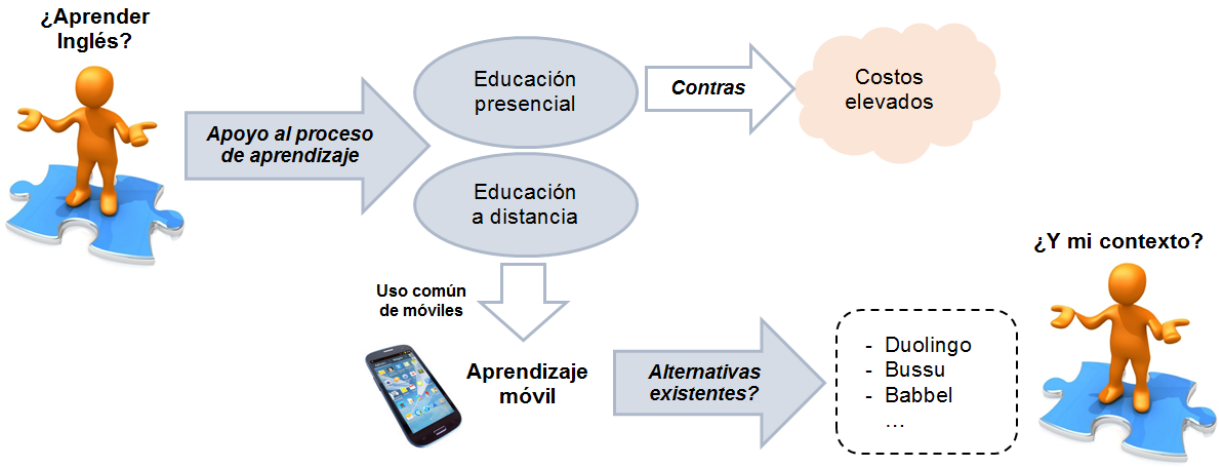

***Figura 1**. Necesidad del usuario.*

3.1. Contenido Educativo

Sobre el uso y aprendizaje de lenguas, el Consejo de Europa (2002) señala: “Las personas utilizan las competencias (generales y comunicativa) que se encuentran a su disposición en distintos contextos y bajo distintas condiciones y restricciones, con el fin de realizar actividades de la lengua que conllevan procesos para producir y recibir textos (hablados o escritos) relacionados con temas en ámbitos específicos,…”. En este sentido, el contexto se refiere al: “conjunto de acontecimientos y de factores situacionales (físicos y de otro tipo), tanto internos como externos a la persona, dentro del cual se producen los actos

de comunicación". Para el caso particular de esta aplicación se plantea el contexto en términos de las lecturas en inglés que el usuario proporciona y que se antepone reflejan sus intereses, cualesquiera que estos sean, lo que le permitirá generar material didáctico personalizado.

Las competencias generales son las que no se relacionan directamente con la lengua, mientras las comunicativas son las que posibilitan a una persona actuar utilizando específicamente medios lingüísticos. La competencia comunicativa se describe como un conjunto de competencias interrelacionadas, que incluyen competencias lingüísticas, sociolingüísticas y pragmáticas, integradas con las competencias generales del individuo. Las competencias lingüísticas incluyen los conocimientos del sistema fonético, vocabulario y sintaxis de la lengua. Las competencias sociolingüísticas hacen referencia a la capacidad de una persona para producir y entender adecuadamente expresiones lingüísticas en diferentes contextos de uso. Las competencias pragmáticas tienen que ver con el uso funcional de los recursos lingüísticos sobre los escenarios de intercambios comunicativos (Consejo de Europa, 2002).

Desde el punto de vista del diseño de instrucción la aplicación presentada se desarrolla bajo un enfoque constructivista con la premisa que el conocimiento emerge en contextos que le son significativos al estudiante (Ertmer y Newby, 1993). La descomposición de textos e identificación de componentes gramaticales para generación de contenidos personalizados son la base del diseño de instrucción. Las aplicaciones para el aprendizaje de idiomas más señaladas en la web como Duolingo, Bussu y Babbel, no consideran directamente elementos que personalicen el material didáctico.

Bajo este panorama, la aplicación móvil plantea un desarrollo conjunto de las competencias lingüísticas[ii], sociolingüísticas y pragmáticas, para el aprendizaje de idioma inglés, a través de tres mecanismos (véase Figura 2):

1) **Categorías** (o partes de la oración) **como ejes temáticos:** conformada por la lingüísticas de las categorías léxicas (sustantivo, verbo, adjetivo, adverbio, preposición y pronombre) y funcionales o gramaticales (determinador, auxiliar, conjunciones) propias del idioma inglés (van Gelderen, 2010).

2) **Información del contexto:** conformada por textos en inglés referentes a los intereses del usuario.

3) **Diccionario de términos:** conjunto de definiciones de un contexto, como elemento de apoyo para la comprensión del texto provisto por el usuario.

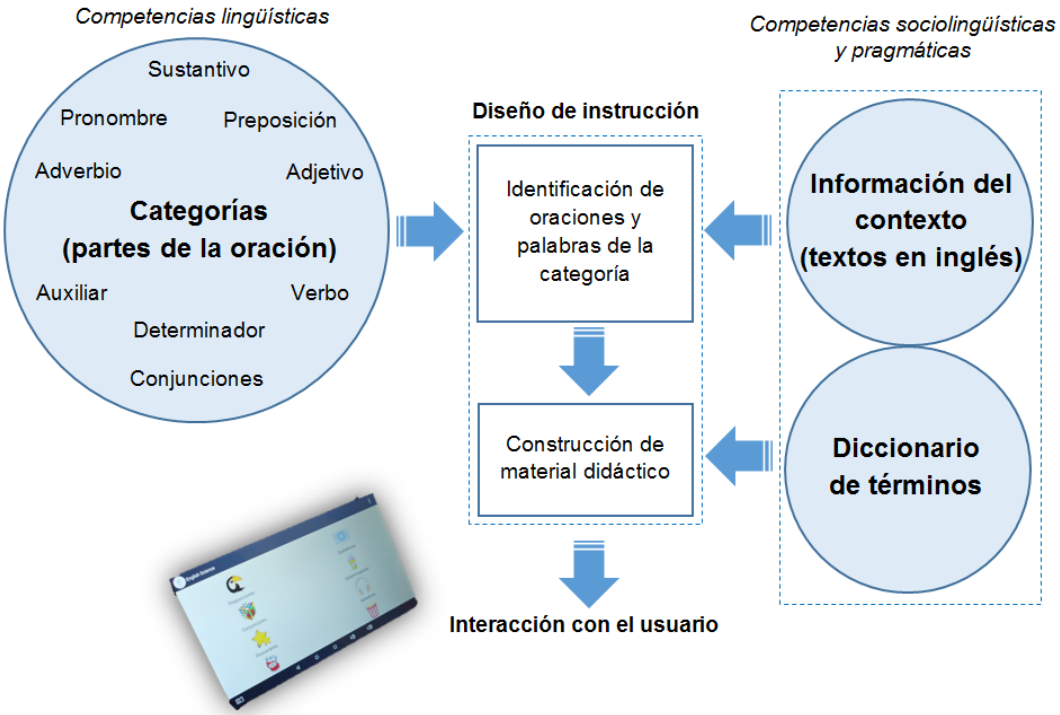

***Figura 2**. Diseño conceptual del contenido educativo de la aplicación.*

Los materiales didácticos llamados lecciones, que se definen a través de los mecanismos listados, se componen de cuatro secciones. La lectura con el texto en inglés, el glosario con la definición de términos/palabras en el texto, la gramática con información sobre la categoría seleccionada y los ejercicios. La lectura, el glosario y la gramática forman la base de conocimiento que el usuario requiere para su aprendizaje. Los ejercicios son el medio regulador del autoaprendizaje en el usuario.

En la Figura 3, se muestra un ejemplo de un material didáctico, bajo la categoría de adverbios como eje temático, en el que puede apreciarse la integración de los conceptos descritos anteriormente. En este caso, la lectura de interés que el usuario proporciona, corresponde a un texto sobre generalidades de la programación. Ya dentro de la aplicación, una vez cargada una lectura es posible desarrollar ejercicios para diferentes categorías.

PROGRAMACIÓN

In use today are more than a billion general-purpose computers and billions more cell phones, smartphones and handheld devices (such as tablet computers). According to a study by eMarketer, the number of mobile Internet users will reach approximately 134 million by 2013. Other studies have projected smartphone sales to surpass personal computer sales in 2011 and tablet sales to account for over 20% of all personal computer sales by 2015. By 2014, the smartphone applications market is expected to exceed $40 billion, which is creating significant opportunities for programming mobile applications.

(Deitel y Deitel, 2012)

Glosario

cell phones	Teléfono portátil sin hilos conectado a una red celular y que permite al usuario su empleo en cualquier lugar cubierto por la red (Fernández, 2011).
Internet	Red de telecomunicaciones nacida en 1969 en los EE.UU. a la cual están conectadas centenares de millones de personas, organismos y empresas en todo el mundo (Fernández, 2011).
personal computer	Una computadora diseñada para ser utilizado por una sola persona a la vez. (Microsoft, 2002).
application	Un programa informático que lleva a cabo una función con el objeto de ayudar a un usuario a realizar una determinada actividad (Fernández, 2011).
programming	El arte y ciencia de la creación de programas de computadora (Microsoft, 2002).
tablet computers	Un tipo de computadora portátil que tiene una pantalla LCD en la que se puede escribir con un lápiz o un bolígrafo digital. La pantalla se puede plegar fácilmente o girar (Remacha, 2008).

Gramática: Adverbios

Los adverbios son palabras que dicen más sobre los verbos, adjetivos y otros adverbios. Muchos adverbios son construidos agregando la terminación mente (**ly**) a los adjetivos. Algunas palabras que terminan en mente no son adverbios. Algunos adjetivos terminan también en **ly** (ej *Sam was feeling very lonely*.)

Adverbios de tiempo: describen cuando algo sucede, responden a la pregunta "Cuándo?" (often, always, sometimes, early, late, again, yesterday, today, tomorrow,...).

Adverbios de modo: describen la forma en que se hace algo, responden a la pregunta "Cómo?" (clearly, correctly, carefully, smartly,...).

Adverbios de lugar: indican dónde pasa algo, responden a la pregunta "Dónde?" (outside, upstairs, here, there, anywhere, away...)

Ejemplos:

He often swims in the evening.
He was driving carefully.
Come here!

Algunos otros adverbios: here, however, more, once, quickly, there,

---

Ejercicios

Llene el espacio en blanco con la palabra correcta

1. In use _____ are _____ than a billion general-purpose computers and billions _____ cell phones, smartphones and handheld devices (_____ tablet computers).
2. According to a study ____ eMarketer, the number of mobile Internet users will reach _____ 134 million ___ 2013.
3. Other studies have projected smartphone sales to surpass personal computer sales in 2011 and tablet sales to account for over 20% of all personal computer sales ___ 2015.
4. ____ 2014, the smartphone applications market is expected to exceed $40 billion, which is creating significant opportunities for programming mobile applications.

Figura 3. *Ejemplo de material didáctico.*

4. Diseño Funcional de la Aplicación

En una aplicación, la arquitectura de la información permite organizar el contenido y funciones de la misma, así como estudiar su complejidad, además, nos permite analizar los diferentes niveles de profundidad, visualizar y entender la relación entre contenidos de una manera organizada (Cuello y Vittone, 2013). En la Figura 4 se presenta la arquitectura para la aplicación propuesta en función de la organización del contenido educativo.

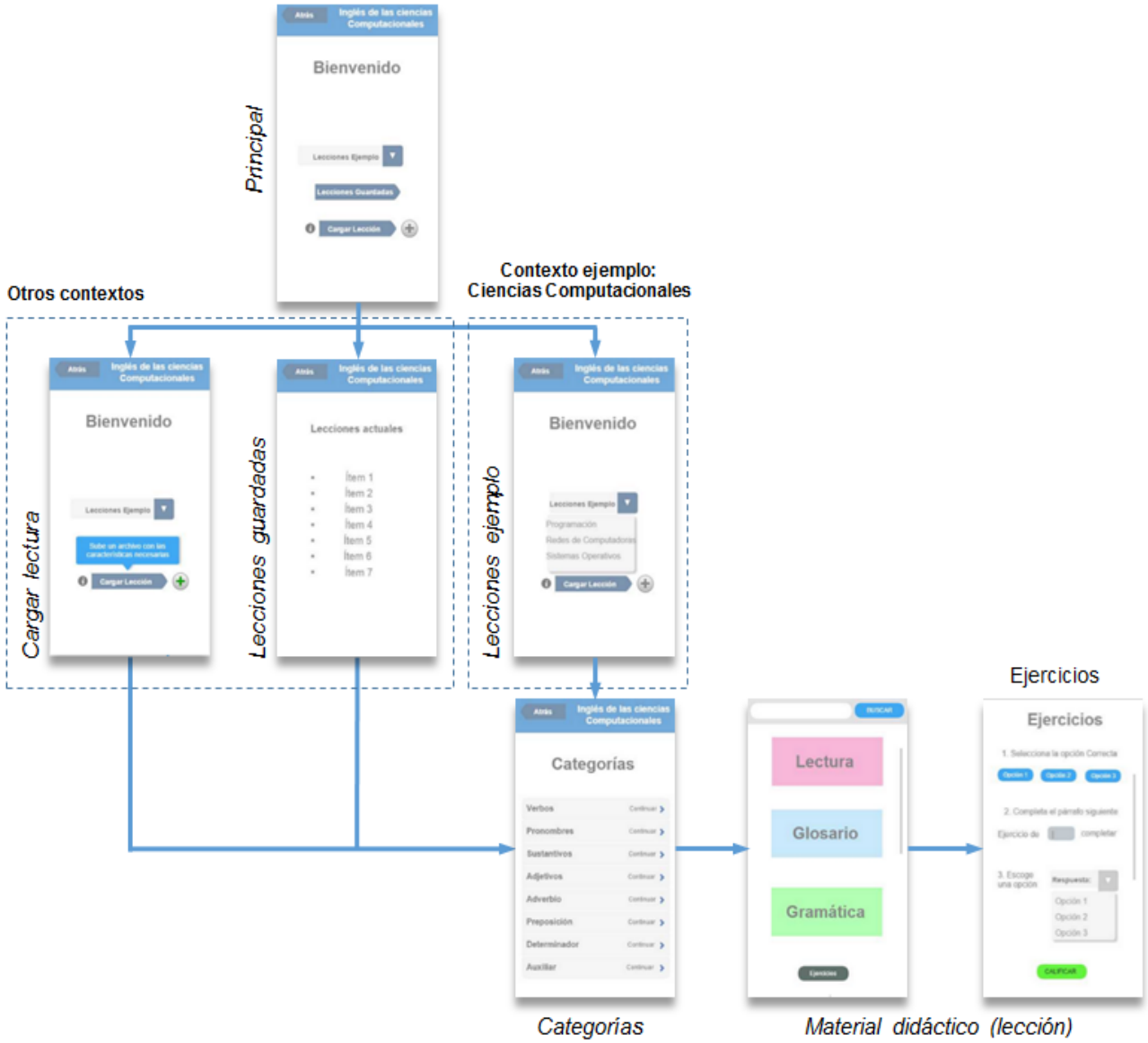

***Figura 4**. Arquitectura de información para la aplicación.*

La pantalla *Cargar lectura* permitirá al usuario ingresar nueva información proveniente de temas de su interés. La pantalla *Lecciones guardadas* facilita el uso de información ya incorporada a través de la pantalla *Cargar lectura*. La

pantalla *Lecciones ejemplo* muestra un menú de temáticas alrededor del ámbito de las ciencias computacionales, y que representan el caso de estudio desglosado en la sección 6. De manera puntual, las pantallas en este nivel permiten ingresar nueva información de interés del usuario (*Cargar lectura*), recuperar textos ya utilizados (*Lecciones guardadas*) y hacer uso de información precargada en la aplicación (*Lecciones ejemplo*). Partiendo de cualquiera de las pantallas mencionadas, se observará un listado de las categorías a seleccionar. Realizada la elección se desplegará el material didáctico generado a partir de la información proporcionada y la categoría elegida las cuales se han descrito en la sección 3.1. La lección es mostrada a través de dos pantallas, la primera con la lectura, el glosario y la gramática y una segunda con ejercicios de opción múltiple donde un registro de aciertos y errores permiten al usuario la regulación de su autoaprendizaje. Para generar material didáctico de otra categoría, basta con regresar a la pantalla *Categorías* y realizar una nueva selección.

Para adherir información de interés del usuario, a través de la pantalla *Cargar lección,* el usuario deberá seleccionar un archivo de texto (con un máximo de 1700 caracteres/ una cuartilla) almacenado en su dispositivo móvil, para lo cual deberá contar con un explorador de archivos. La aplicación almacena la información incorporada en archivos de texto no visibles al usuario. En caso de no contar con una aplicación de este género, existen diversas alternativas tales como: *ES Explorador de Archivos, File Explorer, File Wrangler, Root Browser, Root Explorer, ASTRO Administrador de Archivo y AntTek Explorer Ex*. Todas estas aplicaciones de distribución gratuita pueden ser descargadas a través de la plataforma *Google Play Store*.

5. Desarrollo de la Aplicación

Las tareas de programación se desarrollaron bajo una plataforma Android, empleando el kit de desarrollo de Java (JDK, *Java Development Kit*), el entorno Android Studio 1.3 y el kit de desarrollo de software de Android (*Android SDK tools*). Se empleó un *smartphone* modelo BLU Dash JR, con pantalla de 3.5'' y sistema operativo Android v4.4 KitKat, durante las pruebas funcionales de la aplicación.

En la Figura 5 se muestra el flujo de información a través de los diferentes niveles marcados por la arquitectura de la aplicación. Para generar el glosario y los ejercicios del material didáctico (lección) se realizaron tres búsquedas secuenciales de texto empleando algoritmos de fuerza bruta (Stephens, 2013). La primera corresponde a la búsqueda sobre el texto en inglés del carácter patrón ".", que permite separar las oraciones. Una vez identificadas las oraciones se realiza una segunda búsqueda donde los patrones corresponderán a las palabras disponibles en la base de datos de categorías (de acuerdo a aquella seleccionada). Esta búsqueda dará como resultado la información que compone

los ejercicios, donde cada uno de ellos será una oración que contiene algún elemento de la categoría seleccionada. Finalmente utilizando las palabras encontradas se ejecuta una tercera búsqueda ahora sobre la base de datos de términos, lo cual permitirá definir el glosario de las palabras encontradas en el texto.

La base de datos asociada al diccionario de términos se encuentra limitada al contexto del caso de estudio tratado en la sección 6. La información en esta base de datos de términos contempla un pequeño universo de palabras usadas habitualmente en las áreas de las ciencias computacionales, cuya información fue obtenida de fuentes especializadas. Lo anterior no condiciona al usuario a proporcionar textos del ámbito de las ciencias computacionales (caso de estudio) para que la aplicación sea funcional, ya que de no encontrar elementos en la base de datos de términos simplemente el glosario en el material didáctico estará vacío.

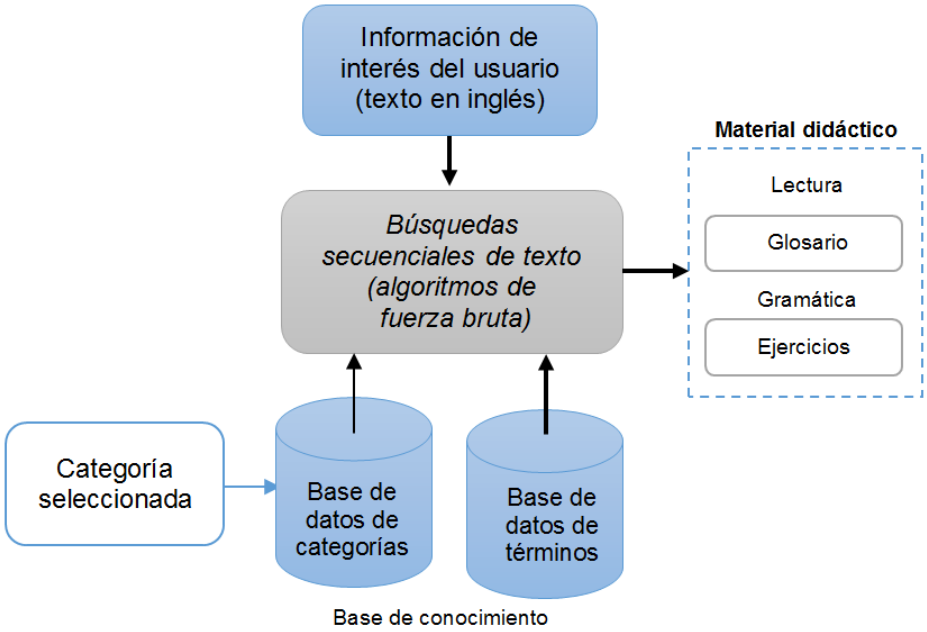

***Figura 5**. Diagrama de flujo de información en la aplicación.*

6. Resultados

A manera de ejemplificar su desarrollo y prueba, la aplicación incluye una serie de lecciones ejemplo bajo el ámbito de las ciencias computacionales, tomando como referencia algunos tópicos comunes de la computación presentes en los programas de estudio de diferentes instituciones educativas de nivel superior en México (véase Tabla 1). Los tópicos seleccionados fueron: Programación, Redes de Computadoras, Sistemas Operativos, Base de Datos, Ingeniería de Software e Inteligencia Artificial.

Institución	Plan de Estudios	Programación	Redes de Computadoras	Sistemas Operativos	Base de Datos	Ingeniería de Software	Inteligencia Artificial	Compiladores	Lenguaje Ensamblador	Graficación
Benemérita Universidad Autónoma de Puebla	Ingeniería en Computación	X	X	X	X	X			X	X
Benemérita Universidad Autónoma de Puebla	Ciencias de la Computación	X	X	X	X	X	X	X	X	X
Instituto Politécnico Nacional	Ingeniería en Computación	X	X	X	X	X	X	X		
Universidad Autónoma Benito Juárez de Oaxaca	Ingeniería en Computación	X	X	X	X	X	X	X		X
Universidad del Istmo, *Campus Tehuantepec*	Ingeniería en Computación	X	X	X	X	X	X	X	X	X
Universidad del Valle de México	Ingeniería en Sistemas Computacionales	X	X	X	X		X		X	X
Universidad Nacional Autónoma de México	Ciencias de la Computación	X	X	X	X	X	X	X		
Universidad Nacional Autónoma de México	Ingeniería en Computación	X	X	X	X	X	X	X		X
	Total:	**8**	**8**	**8**	**8**	**7**	**7**	6	4	6

***Tabla 1**. Áreas de las ciencias computacionales en planes de estudio de diferentes instituciones en 2015.*

Para su evaluación, se aplicaron pruebas considerando métodos de indagación con la finalidad de identificar información y opiniones relevantes en términos del uso, contenido y utilidad de la aplicación por parte de los usuarios. Según Hurtado y Forero (2014), los métodos de indagación son estrategias útiles y sencillas para obtener una primera aproximación de las impresiones del sistema antes de proceder con estrategias más formales concernientes a pruebas de usabilidad. Por lo tanto, se definieron dos estrategias dentro de este marco, una interna en el cual mediante Focus Group con los integrantes de trabajo se consideraron objeto de discusión los aspectos técnicos, pedagógicos y funcionales (véase Figura 6). De esta evaluación interna se definieron mejoras para la provisión de estímulos visuales, la visibilidad, y un diseño *responsive*.

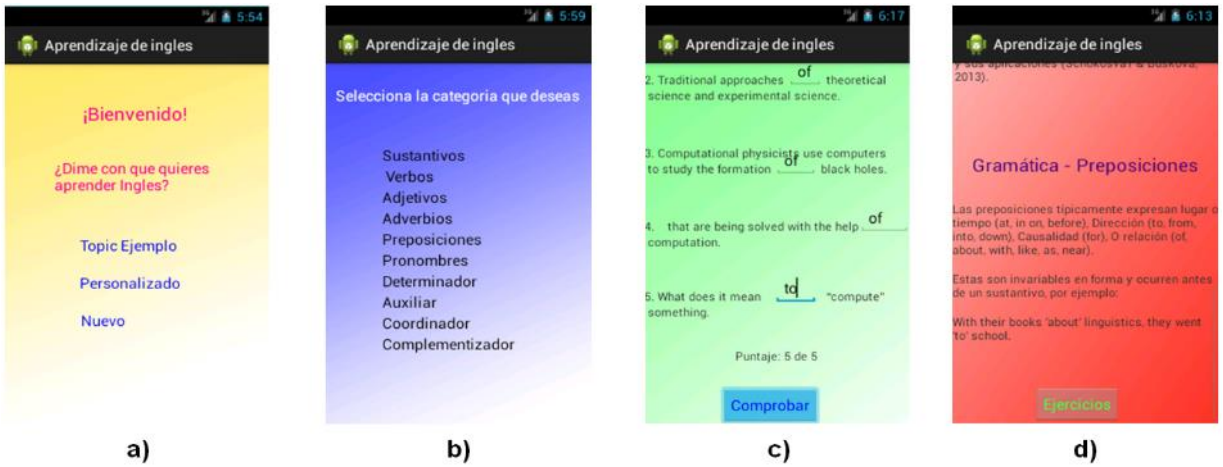

***Figura 6**. Pantallas en evaluación Focus Group. **a)** Principal, **b)** Categorías, **c)** Ejercicios, **b)** Lectura-Glosario-Gramática.*

En la Figura 7 se muestran tres pantallas de la aplicación, resultado del proceso de mejora señalado por la evaluación interna. Las Figuras 7a, 7b y 7c corresponde a la aplicación en un *smartphone* con pantalla de 480x800 pixeles. La Figura 7d pertenece a la aplicación en una *tablet* con resolución de 1024x600 pixeles.

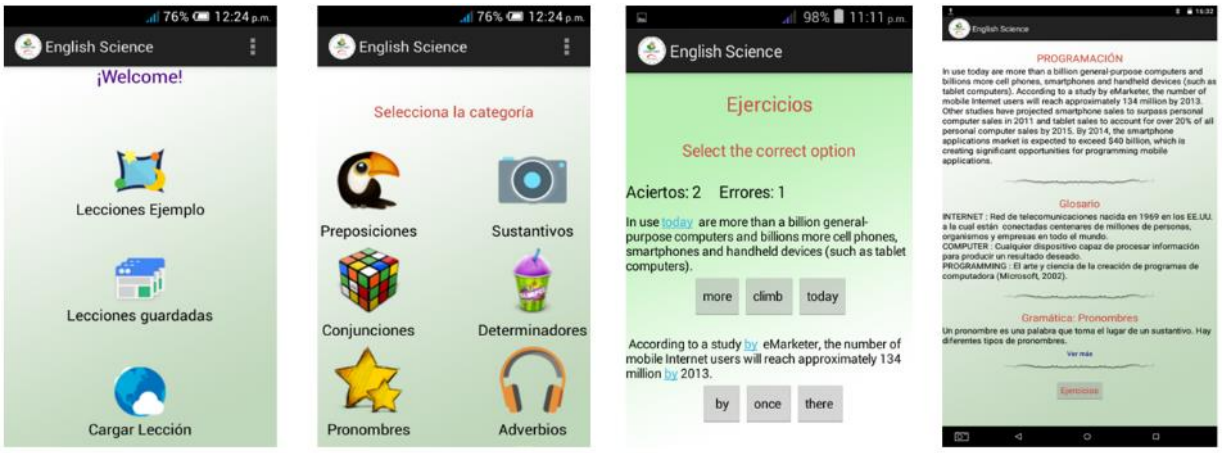

***Figura 7**. Pantallas. **a)** Principal, **b)** Categorías, **c)** Ejercicios, **b)** Lectura-Glosario-Gramática. Fuente: Elaboración propia.*

La evaluación externa se realizó mediante una muestra de 14 alumnos de la carrera de Ingeniería de Computación a los cuales se les proporcionó la aplicación y a través de una encuesta de satisfacción diseñada (véase Figura 8) se captaron una serie de puntos relevantes en términos de uso, contenido y utilidad que se describen a continuación:

- El 86% de los encuestados aseguran tener un nivel regular o bueno de inglés. De esta forma, se confirma que la población tiene conocimientos básicos del idioma, por lo que podrán observar a la aplicación como una herramienta de apoyo.
- El 93% considera que la aplicación es fácil de utilizar, el 7% la cataloga como muy fácil, no hay registro que indique una dificultad para el manejo de la aplicación (véase Figura 9a).
- El 79% piensa que los contenidos relacionados con las ciencias computacionales son buenos o muy buenos. El 21% los califica de regulares. Los contenidos no son catalogados como malos, a sabiendas que la población (estudiantes de computación) deberá presentar un mínimo interés (véase Figura 9b).
- El 71% califica como útil o muy útil la aplicación. No hay registros que indiquen la que aplicación no presente utilidad alguna (véase Figura 9c).
- El 43% de los encuestados dijeron no estar dispuesto a comprar la aplicación, pero sin embargo algunos comentaron que la usarían si esta fuera gratis. El 57% consideraría comprar la aplicación.

Encuesta de satisfacción

1. ¿Cuál considera que es su nivel de inglés?
   ☐ Muy bueno ☐ Bueno ☐ Regular ☐ Malo
2. El uso de la aplicación le resultó
   ☐ Muy fácil ☐ Fácil ☐ Regular ☐ Difícil
3. ¿Cómo calificaría los contenidos de la aplicación?
   ☐ Muy buenos ☐ Buenos ☐ Regulares ☐ Malos
4. ¿Qué grado de utilidad le otorgaría a la aplicación?
   ☐ Muy útil ☐ Útil ☐ Mediana ☐ Inútil
5. ¿Usted compraría esta aplicación?
   ☐ Si ☐ Tal vez ☐ No ☐

Incluya al reverso sus comentarios.

***Figura 8**. Encuesta de satisfacción.*

***Figura 9**. Evaluación de la aplicación. **a)** Uso, **b)** Contenido, **c)** Utilidad.*

7. Conclusiones

Los cambios en el entorno representan una característica inherente del cómputo móvil, lo cual hace adecuados a los dispositivos móviles para el desarrollo de sistemas basados en el contexto. La aplicación presentada evidencia el uso de la lectura de interés como elemento del perfil de usuario y por tanto de su contexto para fomentar el autoaprendizaje. Así, a un médico le podrá resultar más atractiva una lección de inglés que le hablará de enfermedades, y a un joven aquella que le hable de la serie de televisión del momento. La aplicación permite la adaptación de los materiales didácticos mediante la incorporación de información presente en un archivo de texto.

El trabajo presentado busca situar el interés del usuario por un tipo de lectura en particular, como una herramienta para romper la barrera que representa el inglés, debido a los frecuentes escenarios en el que los estudiantes que cursan sus estudios universitarios tras al menos seis años de cursos de inglés, aún muestren fuertes carencias en conceptos básicos del idioma.

En el aspecto funcional, el uso de una metodología común para la enseñanza del idioma inglés como lo son las “categorías” o “partes de la oración”, facilitó la generación de material didáctico. No obstante la enorme complejidad que presentan los sistemas lingüísticos.

El caso de estudio considerado (ciencias computacionales), verificó la factibilidad del uso textos de interés del usuario como base para el desarrollo de aplicaciones relacionadas con la enseñanza. Conforme a la evaluación preliminar la aplicación muestra ser útil e intuitiva, no obstante resulta adecuado en un trabajo futuro realizar pruebas de usabilidad para estimar la aceptación del producto.

Referencias

Abowd, G. D., Dey, A. K., Brown, P. J., Davies, N., Smith, M., & Steggles, P. (1999). Towards a better understanding of context and context-awareness. In Proceedings of the 1st International Symposium on Handheld and Ubiquitous Computing (pp. 304–307). London, UK: Springer-Verlag. doi: 10.1007/3-540-48157-5_29

Calderón, D. (2015). Introducción al reporte Sorry y al aprendizaje del inglés en México. México: Mexicanos Primero. Recuperado de http://www.mexicanosprimero.org/images/stories/sorry/discurso-david-calderon-sorry.pdf

Consejo de Europa (2002). Marco Común Europeo de Referencia para las Lenguas: Aprendizaje, Enseñanza, Evaluación. Madrid, España: Instituto Cervantes. Recuperado de http://cvc.cervantes.es/ensenanza/biblioteca_ele/marco/cvc_mer.pdf

Cuello, J., & Vittone, J. (2013). Diseñando apps para móviles. Catalina Duque Giraldo. Recuperado de http://appdesignbook.com/es/contenidos/

Ertmer, P., & Newby, T. (1993). Conductismo, cognitivismo y constructivismo: una comparación de los aspectos críticos desde la perspectiva del diseño de instrucción. Performance improvement quarterly, 6 (4), 50-72.

Fernández, R. (2001). Glosario básico inglés-español para usuarios de Internet (4a ed.). Barcelona, España: Asociación de Técnicos de Informática. Recuperado de http://www2.ati.es/novatica/glosario/glointv4.pdf

Gómez, J. E., Hernández, V. L., & Morales, M. A. (2015). Arquitectura interactiva como soporte al aprendizaje situado en la enseñanza de la ingeniería. Educación en Ingeniería, 10 (20), 88–97.

Hurtado, L. L., & Forero, J. A. (2014). Metodología de evaluación de usabilidad de interfaces humano-máquina. Tecnura, Edición especial 2014, 103-113. doi: http://dx.doi.org/10.14483/udistrital.jour.tecnura.2014.SE1.a08

Jardines, F. J. (2010). Comparación de la educación a distancia con la educación presencial: modelos de educación, diseños instruccionales y rendimiento académico de los alumnos. InnOvaciOnes de NegOciOs, 7 (2). 293-314.

Kolangade, O. (2013). A Context-based framework for mobile applications (Master's thesis). Retrieved from http://scholarworks.rit.edu/theses/5530/

Lemus, M. E., Duran, K., & Martínez, M. (2008). El nivel de inglés y su problemática en tres universidades de México geográficamente distantes. En Memorias del IV Foro Nacional de Estudios en Lenguas (pp. 243-251). Quintana Roo, México: Departamento de Lengua y Educación.

Microsoft (2002). Computer Dictionary (5th ed.). Redmond, Washington: Microsoft Press.

Peña, A. (ed.). (2016). Mobile, Ubiquitous, and Pervasive Learning: Fundaments, Applications, and Trends. Switzerland: Springer.

Remacha, S. (2008). Infotech, English for computer users, Student's Book (4th ed.). Cambridge, UK: Cambridge University Press.

UNESCO (2013). Directrices de la UNESCO para las políticas de aprendizaje móvil. Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. Recuperado de http://unesdoc.unesco.org/images/0021/002196/219662S.pdf

UNESCO (s.f.). El aprendizaje móvil. Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. Recuperado de http://www.unesco.org/new/es/unesco/themes/icts/m4ed/

Stephens, R. (2013). Essential Algorithms: A Practical Approach to Computer Algorithms. Indianapolis, IN: Wiley.

Sun, L., Hou, J., Hu, X., & Al-mekhlafi, K. (2015). A Context-based Support System of Mobile Chinese Learning for Foreigners in China. Procedia Computer Science, 60, 1396–1405. doi: 10.1016/j.procs.2015.08.215

Van Gelderen, E. (2010). An Introduction to the Grammar of English (Revised ed.). Amsterdam, The Netherlands: John Benjamins Publishing Company.

Wanumen, L. F., Cavanzo, G.A., & Guevara, J.C. (2015). Plataforma de enseñanza aprendizaje de conceptos básicos de astronomía basada en un modelo de adaptación sensible al contexto y al perfil del usuario de Facebook. Horizontes Pedagógicos, 17 (2), 76–87.

Zheng, M., Cheng, S.H., & Xu, Q. (2016). Context-Based Mobile User Interface. Journal of Computer and Communications, 4, 1–9. doi: 10.4236/jcc.2016.49001

Notas Biográficas:

Osiris Montero Ríos es estudiante de Ingeniería en Computación en la Universidad del Istmo. Participó en la Feria Nacional de Ciencia e Ingenierías fase nacional en 2015. Sus áreas de interés incluyen: el cómputo móvil, las bases de datos, y la programación en diferentes lenguajes y entornos.

Francisco Aguilar Acevedo es Ingeniero en Electrónica por la Universidad Tecnológica de la Mixteca y Maestro en Ciencias en Ingeniería Mecatrónica por el Centro Nacional de Investigación y Desarrollo Tecnológico. Actualmente es Profesor-Investigador de tiempo completo adscrito a la carrera de Ingeniería en Computación en la Universidad del Istmo, y miembro activo del cuerpo académico de Cómputo Aplicación. Sus áreas de interés incluyen: la inteligencia artificial, la robótica, los sistemas embebidos y la instrumentación electrónica.

Guadalupe Toledo Toledo es Ingeniera en Sistemas Computacionales por el Instituto Tecnológico de Tuxtepec, y Maestra en Computación Aplicada por parte del Laboratorio Nacional de Informática Avanzada. Actualmente es Profesor-Investigador de tiempo completo adscrito a la carrera de Ingeniería en Computación en la Universidad del Istmo. Sus áreas de interés se centran en el desarrollo de software y prototipos didácticos con aplicación en ingeniería y computación, aplicación de evaluaciones de usabilidad a productos de software centrados en el usuario y la integración del cómputo aplicado en la solución de problemas multidisciplinares.

Silvia Reyes Jiménez es Licenciada en Administración y Maestra en Administración y Gestión de Negocios por el Instituto Tecnológico de Oaxaca. Actualmente es Profesor-Investigador de tiempo completo adscrito a la carrera de Ingeniería en Computación en la Universidad del Istmo. Su principal área de investigación es la gestión del conocimiento.

Daniel Pacheco Bautista es ingeniero en electrónica por el Instituto Tecnológico de Oaxaca, Maestro en Ciencias con especialidad en diseño de circuitos integrados por el Instituto Nacional de Astrofísica, Óptica y Electrónica, y Doctor en ingeniería biomédica por la Universidad Popular Autónoma del Estado de Puebla, Actualmente es Profesor-Investigador adscrito a la carrera de Ingeniería en Computación en la Universidad del Istmo. Sus líneas de investigación incluyen: Arquitectura de computadoras y Lógica reconfigurable, Osciladores controlados por voltaje y Circuito de amarre de fase en VLSI, y plataformas alternativas para el ensamble de secuencias cortas de ADN.

[i] Teléfono móvil, teléfono básico o *feature phone* es un término aplicado a teléfonos móviles con características limitadas respecto a los *smartphone*.

[ii] De las competencias lingüísticas, la aplicación se centra en el desarrollo de las competencias léxicas; las cuales comprenden el conocimiento del vocabulario de una lengua y la capacidad para utilizarlo (Consejo de Europa, 2002).

Recibido 25 Oct 2017 *ReCIBE, Año 6 No. 2, Noviembre 2017*
Aceptado 30 Oct 2017

Analysis of Agile Practices Adoption on CMMI Organizations through a Systematic Literature Review

Análisis de la adopción de prácticas ágiles en organizaciones CMMI a través de una Revisión Sistemática de Literatura

Marco Palomino[1]
palomino.marco@pucp.edu.pe

Abraham Dávila[2]
abraham.davila@pucp.edu.pe

Karin Melendez[2]
kmelendez@pucp.edu.pe

Marcelo Pessoa[3]
mpessoa@usp.br

[1] Escuela de Posgrado, Pontificia Universidad Católica del Perú, Lima, Perú
[2] Departamento de Ingeniería, Pontificia Universidad Católica del Perú, Lima, Perú
[3] Polytechnic School, University of Sao Paulo, Brazil

Abstract: In the recent years, the adoption of agile frameworks and methodologies in Software Development Organizations (SDO) has grown up considerably. Unfortunately, the level required of formal documentation in bigger or longer software development projects is not full covered by agile practices alone; likewise, this kind of situations happen frequently in a context of CMMI organizations. The aim of this study is identify, review and analyze the most used agile practices that are being used in combination with CMMI within SDO. To accomplish this, a systematic literature review has been performed according to relevant guidelines. This study has identified multiple practices such as Daily Meeting and Product Backlog management that are being used constantly in combination with CMMI. In addition, we could identify that there are specific benefits of implementing practices from both approaches.

Keywords: Agile Practice, Agile Software Development, CMMI

Resumen: En los años recientes, la adopción de marcos de trabajo y metodologías ágiles en las Organizaciones de Desarrollo de Software (ODS) ha crecido considerablemente, Desafortunadamente, el nivel requerido de documentación formal en proyectos de software más grandes y extensos no es totalmente cubierto por las prácticas ágiles únicamente; de igual manera, este tipo de situaciones ocurren frecuentemente en contextos de organizaciones CMMI. El objetivo de este estudio es identificar, revisar y analizar las prácticas ágiles más usadas que están siendo usadas en combinación con CMMI dentro de una ODS. Para cumplir con el objetivo, una revisión sistemática de literatura ha sido ejecutada de acuerdo a las directivas relevantes. Este estudio ha identificado múltiples prácticas ágiles como Daily Meeting y gestión de Product Backlog que son usadas constantemente en combinación con CMMI. Adicionalmente, se identificaron beneficios específicos al implementar prácticas de ambos enfoques en conjunto.

Palabras Clave: Práctica Ágil, Desarrollo Ágil de Software, CMMI

1. Introduction

The methodologies or process models that have being used on the Software Development Organizations (SDO) have evolved over time; as a consequence of this evolution, in the last years these organizations have considered (with more interest) the adoption of agile practices in software development (Dahlem, Diebold, & Marc, 2014), (Dingsøyr, 2012). This agile approach promotes an easy and fast way of software development where short iterations are scheduled for satisfying customers with product's partial deliveries (Dahlem et al., 2014), (Cockburn, 2002) and (Boehm & Turner, 2003).

On the other side, CMMI (Capability Maturity Model Integration), which is a model that groups best practices in development and maintenance activities (Salinas, Escalona, & Mejías, 2012), (Team, 2010); is a process model that has been adopted by many SDO (Marcal, de Freitas, Furtado Soares, & Belchior, 2007), (Łukasiewicz & Miler, 2012). According to (Omran, 2008), the practices and process adoption from a certain level is relatively a challenge in small companies, that is why the importance of identifying agile practices which in concordance with CMMI could help in software development improvement's process.

The analysis concluded that this study was performed in order to identify agile practices commonly used in contexts of organizations which have already adopted CMMI. In fact, identifying most used agile practices in these kinds of organizations will allow recognizing activities and processes that could get higher benefits when implementing agile and CMMI together. To sum up, the aim of this research is to identify the practices from frameworks and agile methodologies commonly used in CMMI organizations.

To accomplish the goal of this research, a Systematic Literature Review (SLR) (Kitchenham & Charters, 2007) was performed in the relevant digital databases. This study also pretends to identify mappings between agile practices and CMMI processes, primary studies about application of agile practices in CMMI contexts and, finally, researches about adoption of recent agile practices and CMMI.

The remainder of this paper is structured as follows: section 2 presents the background and related work; section 3, the methodology of the SLR; section 4, the identified agile practices and results; and finally, in section 5, it is presented the final discussion and future work.

2. Background and Related Work

On the other hand, there are several studies related with agile practices and CMMI and how these different approaches work together First of all, there are researches of how agile practices could contribute to get CMMI maturity levels (Salinas et al., 2012), (Kähkönen & Abrahamsson, P, 2004). Second of all, there are case studies (Omran, 2008), (Dybå & Dingsøyr, 2008) that describe the consequences of implementing agile practices within an organization with CMMI culture.

On the other hand, in the Silva study (Silva et al., 2015) the authors analyzed the combined use of agile and CMMI through a SLR. This previous research (Silva et al., 2015) only considered studies published up to 2011 and the research questions were mainly focused on benefits and limitations of implementing both approaches. We could identify differences between their and our research. The newest in our research are: (i) verify if team's size affects the combined use of agile and CMMI, (ii) analyze studies and researches published up to 2016, which extends the scope of the previous research (iii) analyze if any agile methodology can be used in contexts of CMMI organizations. Due to these differences mentioned, we consider that this work is needed because it will include new primary studies and also, it will consider all recent agile practices incorporated in CMMI contexts.

This study is a complement to a previous research (Palomino, M., Dávila, A., Melendez, K., & Pessoa, 2016) that was focused also on the agile practices adoption in context of CMMI organizations. This recent research includes a deep analysis on the bibliometric results and it considers one additional research question to the analysis. Also, this research adds more conclusions and discussions on the previous four research questions in order to improve the first approach provided in the previous study.

3. Systematic Literature Review

This section presents the SLR fundamentals taken into account and the application of the review according to the defined review.

3.1 Systematic Review Fundamentals

The research method used is a SLR based on the guidelines and lessons learned proposed by Brereton and Kitchenham (P. Brereton, B. A. Kitchenham, D. Budgen, 2007) (Kitchenham & Charters, 2007). In the figure 1, we can show the three phases described on the guidelines.

As part of Phase 1, Plan Review, it was specified the research questions, which were separated into three bibliometric questions and five research questions.

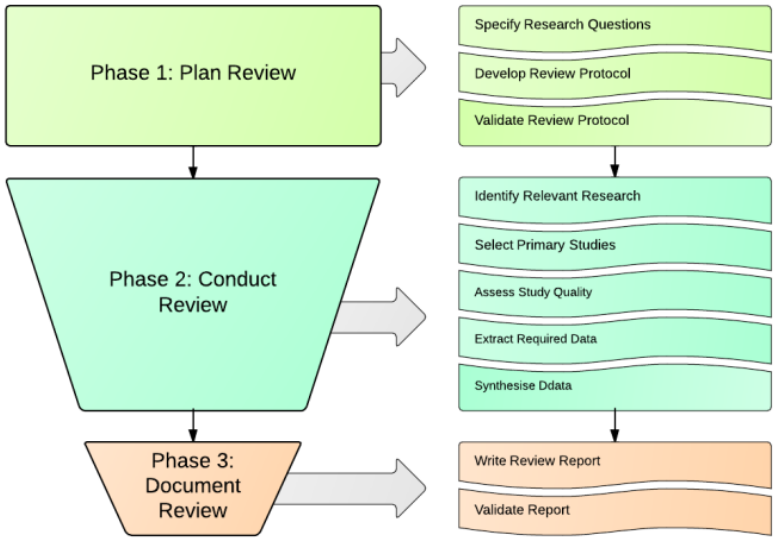

Figure 1. *The SLR Process by Brereton (P. Brereton, B. A. Kitchenham, D. Budgen, 2007)*

The bibliometric questions (BQ) are:

BQ-1: How was the evolution of number of published articles related with the topic of this research?
BQ-2: What kinds of researches are presented related with the topic of this research?
BQ-3: Which are the Conferences, Journals, Digital Libraries with more publications related to the topic of this research?

The research questions (RQ) are:

RQ-1: Why are agile practices implemented in organizations with CMMI culture?
RQ-2: Could any agile practice be used in combination with CMMI?
RQ-3: Is there any influence from the team's size in the agile practices use with CMMI culture?
RQ-4: Are there primary studies related with the combined use of agile practices and CMMI?
RQ-5: Are there advantages or disadvantages in the agile practices use with CMMI culture?

In order to frame the research questions and define the search string, it was used the PICOC (Population, Intervention, Comparison, Outcome, Context) criteria applied to software engineering. The Table 1 shows the main keywords used on

PICOC criteria and Table 2 shows the different Search Strings elaborated regarding all Data Sources used.

Table 1. *Principal Keywords used based on PICOC Criteria.*

Population:	Organizations with CMMI and Agile Methodologies
Intervention:	Agile Practice, Activity
Comparison:	None
Outcome:	Analysis, Researches
Context:	Software Engineering

Data Source	Search String
Scopus	("CMMI" or "Capability Maturity Model Integration") AND ABS("Agil*" or "Agile Method" or "Agil* Software" or "Light*" or "Scrum" or XP or "Extreme Programming" or "Scrumban" or "Kanban" or "software development") AND("Practic*" or "Activit*" or "Software Development Practice" or "System Development" or "Application") AND("Research*" or "Mappin*" or "Evaluation*" or "Experience*")
IEEE Xplore	((("Abstract":(agile OR "Agile Methodology" OR scrum OR xp OR light* OR kanban)) AND "Abstract":cmmi OR "capability maturity model") AND "Abstract":software)
Elsevier ScienceDirect	ALL((cmmi or maturity)) and TITLE-ABSTR-KEY(("Agil*" OR "scrum" OR "xp" OR "light" OR "kanban"))[Journals(Computer Science)]
ACM Digital Library	content.ftsec:(cmmi "capability maturity model integration") AND (agile "software development" "Agil* Method*" scrum xp "extreme programming" kanban "light*")

Table 2. *Search Strings*

On the other hand, the automatic search of primary studies was complemented by a manual search in the main repositories and conferences related with Agile and CMMI. The reason of this additional search was that there are several studies and researches of the combined use of Agile and CMMI that have not been published yet in scientific databases, but most of them add a significant value to this research.

3.2 RSL Protocol

A RSL protocol was defined and adjusted later to reduce the possibility of researcher bias. This protocol was structured by six steps that included a first studies selection regarding the execution of Search String in scientific databases plus the original results obtained from the manual search. Then, the articles were analyzed, considering the article Title and Abstract and then the article Introduction and Conclusion. At the end, the final articles were verified by peer review in order to evaluate their exclusion or inclusion in our research.

The exclusion and inclusion criteria considered were:

Inclusion criteria: Academic articles with methodological basis (mainly experiment, case study, Systematic Reviews, Systematic Mappings). In addition, only papers from sources mentioned in the research were considered. Also, we saw convenient to consider papers in Spanish and English language due to in recent years the agile approach in software development is widely adopted in Latin American companies. Finally, only papers that show the combined use of agile and CMMI approaches were considered. Even if the paper mentions agile practices, we do not use it unless the adoption of those practices is performed within an organization implementing CMMI.

In order to include articles that add significant value to our research, we also considered the reference list from all primary studies.

Exclusion criteria: Duplicated papers were excluded and the search scope was limited to the following publication types: Journals, Conferences, Magazines, Technical Reports and Books. In addition, we excluded the papers that only show the results of adopting agile practices without considering CMMI contexts.

3.3 Quality Assessment

Quality Assessment of this SLR followed 11 criteria defined by (Dybå & Dingsøyr, 2008) based on (Shea et al., 2007). The following are the criteria used in the Quality Assessment:

- Is this study based on research?
- Is there a clear statement of the aims of the research?
- Is there an adequate description of the context?
- Was the study design appropriate to address the aims of the research?
- Was the selection strategy appropriate to the aims of the research?
- Was there a control group for comparing treatments?
- Was the data collected in a way that addressed the research aims?
- Was the data analysis rigorous enough?
- Has the relationship between researcher and participants been considered as an adequate degree?
- Is there a clear statement of results?
- Is the study relevant for practice or research?

According to (Shea et al., 2007), these mentioned criteria include three important issues related to quality, which were considered in the Quality Assessment:

- Rigor: a complete and adequate approach was applied to key research methods in the study?

- Credibility: are the results in a meaningful and well-presented way?
- Relevance: how useful are the results to the software industry and the scientific community?

For the assessment, each one of the primary studies obtained after inclusion and exclusion criteria of the RSL protocol was analyzed using the 11 questions defined. The scale used in the assessment had two values ("yes" or "no"). When the answer was affirmative, the criteria had a value of "1"; otherwise, the value was "0". As a result, the minimum result could be "0" and "11" as maximum value.

3.4 Data Extraction and Data Synthesis Strategies

The Petersen Guides (K. Petersen S. Mujtaba, 2008) suggest the exploration of some papers sections in case the abstract is not well-structured or vague. For this study and with the aim of answer all of the research questions, all the primary studies selected after last step of the RSL protocol were fully read.
A spreadsheet editor was used in order to elaborate a template for getting the relevant information of all primary studies. This information was helpful for summarizing the data in order to make the data synthesis easier.

The following data were extracted from the primary studies:

- bibliographic References
- type of study (Presentation, Conference, Journal, Technical Report, Magazine, Book chapter)
- editor
- year
- aim of the study
- research question that makes reference
- point of view regarding the research question

Then, the primary studies were grouped in order to associate it in a high level. The aim of this grouping is to identify the main concepts that will allow the answer of the five research questions. In order to conduct the analysis, a narrative synthesis was defined (Popay J Sowden A, Petticrew M, Arai L, Rodgers M, Britten N, 2006); especially the "Grouping and Clustering" as main method.

3.5 Studies Selection

The studies selection process started with the automatic search in November 2015 with the first tests. Then, in January 2016 the last execution was performed. Using a spreadsheet editor, the titles, abstracts and references were selected from all studies obtained after executing the search strings in the digital sources. After this step, a total of 2,265 potential studies were identified. On the other hand, the Manual Search was conducted in December 2015 and January 2016 in order to get relevant studies from journals and conferences specialized in agile approaches. At the end, 110 studies were defined by Manual Search. The initial results are displayed in Table 3.
Then, the duplicated studies were excluded using the list of all 2,375 studies. After that, the titles were revised in order to exclude irrelevant studies. After this step, 299 studies were selected.

Type	Name of Database	Initial Results	Search Date
Automatic Search	IEEE Xplore	736	January, 2016
	ACM Digital Library	236	January, 2016
	Science Direct	215	January, 2016
	Scopus	1,078	January, 2016
Manual Search	Agile Journal, Agile Conferences and SEI Digital Library	110	January, 2016

Table 3. *Data Sources of the Systematic Review*

Then, the abstracts of all 299 potential studies were reviewed in order to exclude the studies that do not consider agile practices and CMMI approaches. After abstract's review, a total of 75 studies were defined. Finally, the introduction and conclusion of all 75 studies were analyzed in order to get all the studies that considers agile and CMMI approaches. At this moment, 47 studies were identified. Finally, the references of the 47 studies were analyzed in order to get additional studies. At the end, 5 more studies were added and a total of 52 studies were identified. The Table 4 shows the 52 studies along with the identifier we used on the research.

ID	Ref
D1	(Clark, 2011)
D2	(Abdel-Hamid & Hamouda, A. E. D, 2015)
D3	(Weller, 2013)
D4	(Potter & Sakry, M., 2009)
D5	(McMahon, 2012)
D6	(Alegria & Bastarrica, M. C, 2006)
D7	(Jakobsen & Sutherland, J, 2009)
D8	(Maller Ochoa, C., & Silva, J, 2005)
D9	(Paulk, 2001)
D10	(Baker, 2006)
D11	(Kovacheva, 2011)
D12	(Sutherland Jakobsen, C. R., & Johnson, K, 2007)
D13	(Aggarwal Deep, V., & Singh, R, 2014)
D14	(Anderson, 2005)
D15	(Bos & Vriens, C, 2004)
D16	(Garzás & Paulk, M. C, 2013)
D17	(de Souza Carvalho, 2011)
D18	(Selleri Silva Santana Furtado Soares, F., 2014)
D19	(Omran, 2008)
D20	(Torrecilla-Salinas Sedeño, J., Escalona, M. J., & Mejías, M., 2016)
D21	(Cohan & Glazer, 2009)
D22	(Santana Furtado Soares & Romero de Lemos Meira, 2015)
D23	(Pikkarainen & Mantyniemi, A, 2006)
D24	(Trujillo Oktaba, H., Pino, F. J., & Orozco, M. J., 2011)
D25	(Miller & Haddad, H. M., 2012)
D26	(Gandomani, 2013)
D27	(Łukasiewicz & Miler, 2012)
D28	(Diaz Garbajosa, J., & Calvo-Manzano, J. A., 2009)
D29	(Marcal et al., 2007)

ID	Ref
D30	(Jakobsen & Johnson, 2008)
D31	(López-Lira Hinojo, 2014)
D32	(Lina & Dan, 2012)
D33	(Morris, 2012)
D34	(Bougroun Zeaaraoui, A., & Bouchentouf, T., 2014)
D35	(Pikkarainen, 2009)
D36	(El Deen Hamouda, 2014)
D37	(Kähkönen & Abrahamsson, P, 2004)
D38	(Gazzan Shaikh, A., 2014)
D39	(Torrecilla-Salinas Sedeño, J., Escalona, M. J., & Mejías, M, 2014)
D40	(Tuan & Thang, H. Q., 2013)
D41	(Marcal de Freitas, B. C. C., Soares, F. S. F., Furtado, M. E. S., Maciel, T. M., & Belchior, A. D., 2008)
D42	(Leithiser & Hamilton, D., 2008)
D43	(Salinas et al., 2012)
D44	(Konrad & McGraw, 2008)
D45	(Boehm Turner's, R., & Network, P. I., 2010)
D46	(Irrazabal Vásquez, F., Díaz, R., & Garzás, J., 2011)
D47	(Turgeon., 2011)
D48	(Glazer Dalton, J., Anderson, D., Konrad, M. D., & Shrum, S., 2008)
D49	(Turner & Jain, A., 2002)
D50	(Santana Gusmão, C., Soares, L., Pinheiro, C., Maciel, T., Vasconcelos, A., & Rouiller, A., 2009)
D51	(Vriens, 2003)
D52	(Mahnic & Zabkar, N., 2007)

Table 4. *Identified Studie*

4. Results

In addition to Research Questions, it was also performed a review of the 52 studies selected in order to analyze the publication years, publication channels and research types of all studies identified at the end of selection process. The following section will display the answer of the Bibliometric and Research Questions defined in previous section.

4.1 BQ-1. How was the evolution of number of published articles related with the topic of this research?

In Figure 2 are the studies that were identified grouped by the publish year. As we can see, the studies were obtained in a 2001-2016 period. It is important to mention that the first three years (2001-2003) were the years with the less number of studies, while 2014 is the year with more studies. In addition, at the end of the 90's, the first versions of XP and Scrum appeared and it is necessary to highlight the importance of these agile methodologies due to the years where the first versions appeared, also appeared studies of the integration of CMMI and agile approaches.

Also, from 2008 to 2014 is the period with most papers. In fact, during this time around 69% of the total studies were obtained. This pattern is caused by the recent interest in agile approaches for the software industry and also the scientific community. It is important to point that the year 2010 has only one study. This result does not represent a trend in the scientific community due to the previous and next years there are numerous articles.

After reviewing all the studies obtained from the first step in the selection process, we could see that several studies were excluded due to the aim of the research. These studies did not display combinations of CMMI and agile approaches and, as a result, were discarded from this research.
Finally, regarding the last two years, from 2015 to 2016 there was not obtained many studies related to the combined use of agile and CMMI approaches. In case of 2016, it is necessary to point that the automatic and manual searches were performed only up to January. Regarding to 2015, it should be noted that in the early stages of selection, numerous articles were obtained, but most of these were not explicitly focused on the combined use of agile and CMMI practices; as a result, those studies were discarded in the following stages of the selection procedure.

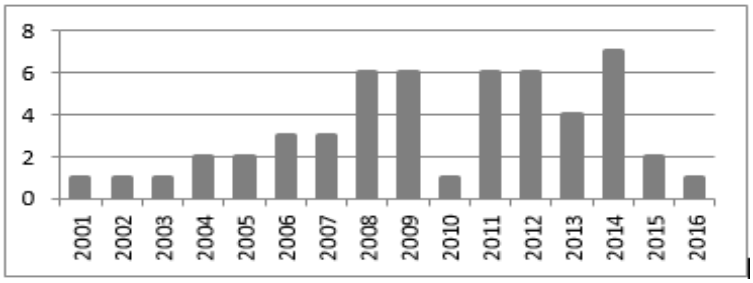

Figure 2. *Number of publications by year*

4.2 BQ-2. What kinds of researches are presented related with the topic of this research?

In Table 5, there is a list with the number of studies grouped by the Research Type. As we can see, the highest number of occurrences is found in Conferences and Journals with a 73% of the total approximately. This high number of occurrences is caused by the execution of search string in recognized scientific databases due to these data sources collect academic researches which are published mainly in specialized conferences or journals.
It is important also to point the studies obtained from book chapters because all of them represents a 15% approximately. This percentage makes this research type an important source to consider in future researches related with CMMI and agile approaches. Finally, the research types with less presence are Magazines and Technical Reports with only 1 study each one.

4.3 BQ-3. Which are the Conferences, Journals, Digital Libraries with more publications related to the topic of this research?

There are various conferences and journals specialized in CMMI and agile approaches (e.g. Agile Conference and Agile Journals). These sources represent 22% of the total of primary studies with 11 elements. Moreover, the rest of the primary studies were published uniformly in the other publication channels.

Research Type	# Occurrences
Conference Paper	26
Journal Paper	12
Book Chapter	8
Presentation	4
Technical Report	1
Magazine	1

Table 5. *Number of studies regarding research type*

The majority of the publication channels had only one primary study. In fact, there are 21 distributed in Conferences, Journals and Workshops; each of these with

only one primary study. This variety between these 21 publication channels proves a real interest in the scientific community regarding the adoption of agile approaches and CMMI.

Finally, in Table 6, there is a list of all publication channels where the 52 primary studies were collected.

4.4 RQ-1. Why are agile practices implemented in organizations with CMMI culture?

First of all, we want to define if both approaches are compatible or not. From the analysis of the 52 primary studies, we could identify that both agile and CMMI approaches are not opposed to each other. In fact, both cultures share similar criteria and practices. From the previous premise, we can affirm that there is a compatibility level between agile and CMMI approaches which is corroborated in the studies [D1], [D3], [D4], [D5], [D6], [D7], [D9], [D12], [D14], [D16], [D17], [D20], [D23], [D28], [D30], [D32], [D34], [D35], [D37], [D44], [D45], [D48], [D49] and [D52] where we could identify that practices from different cultures, such as agile or CMMI, can be complemented each other in order to improve the current processes. Additionally, it proposes that the compatibility level is defined by the organizations. In conclusion, we can affirm that both approaches can coexist but there are some inconveniences mentioned in [D3], [D7], [D24], [D25], [D45] and [D27] that should be considered:

- Keep the agile principles while the agile practices and processes are extended.
- Identify the organization needs for a successful implantation of both approaches.
- Keep the premise that both approaches are complemented each other and there are no practices substituted by others.
- Make sure to combine successfully the maturity approach in the organization and agile approach in the practices.

Due to both agile and CMMI approaches can coexist in a same organization, there is a recent interest from the organizations that even with the CMMI culture decide to get familiar with agile approaches in order to continue improving their processes.

On the other hand, we can see that the adoption of agile practices in organizations with the CMMI approach is not influenced by the CMMI maturity level of the companies. In fact, the studies [D4], [D6], [D28], [D29], [D30], [D37], [D41] and [D43] shows scenarios where the organizations have or try to get levels 2 and 3 from CMMI; whereas in studies [D7], [D12], [D14], [D21] and [D24] there are references to higher maturity levels such as 4 and 5. This indicates that there is

an interest in agile practices regardless the maturity level of the organizations. Also, it is important to point that the organizations with CMMI culture looks to continue to improve not only by using one single agile methodology; in fact, the adoption of agile practices can be done by using a mix of agile approaches in order to get the best of these practices. The studies [D14], [D24], [D34], [D20], [D39], [D43] and [D51] show the multiple agile practices that were used in contexts of CMMI organizations.

Additionally, there are scenarios where the use of agile practices in combination with CMMI is appropriate; for instance, in the studies [D13], [D27] and [D29] there are situations where is recommendable getting certain level of flexibility and agility, which is achieved with agile practices adoption. In fact, in software projects where changes are constant and rapid responses are required as noted in studies [D36], [D28] and [D47], it is recommendable the requirement management proposed by Scrum; furthermore, in web development projects, where the "time to market" is one of the main features, it is necessary to have partial deliveries, which are proposed by agile approaches as we could find from [D20], [D39] and [D43] studies.

Publication Channel	Total
Agile Conference	8
Lecture Notes in Computer Science	4
Agile Journal	3
Crosstalk	3
IEEE	3
Agile Development Conference	2
Communications in Computer and Information Science	2
CLEI Electronic Journal	2
Lecture Notes in Business Information Processing	2
SEI	2
ACM SIGSOFT	1
CISTI	1
Fourth Symposium on Information and Communication Technology	1
ICACCI	1
ICCSEE	1
ICTTA	1
Indian Journal of Science and Technology	1
Information and Software Technology Journal	1
Information Science and Technology	1
Innovations in Systems and Software Engineering Journal	1
Institution of Engineering and Technology	1
International Journal of Mathematics and Computers In Simulation	1
ISD	1
ITNG	1
Journal of Software: Evolution and Process	1
Proceedings of the 46th Annual Southeast Regional Conference on XX	1
QUATIC	1
SCCC	1
Software Engineering Workshop	1
SPICE	1
14th International Conference on Information Integration and Web-based Applications & Services	1

Table 6. *Studies by publication channel*

Finally, we can conclude from the analysis of all 52 primary studies that agile practices are implemented in CMMI contexts because that combination allows the organizations to:

- Reduce the "waste time" inside the team
- Reduce the delivery time of the products
- Increase the team productivity
- Improve the competitiveness of organizations and product's quality
- Include flexibility and agility in the processes of CMMI organizations
- Improve communication with stakeholders using agile practices

4.5 RQ-2. Could any agile practice be used in combination with CMMI?

From the analysis of 52 primary studies we could identify that agile methodologies and practices are characterized mainly because they obey entirely to the agile principles and as long as this principles are respected, as we can see in the studies [D2], [D22] and [D33], any kind of agile practice could be adapted to any context, even those where the organization culture is more traditional.

In the previous Research Question (RQ-1) it was defined that both agile and CMMI approaches can coexist. Using this statement, we could see in the primary studies that there are various agile practices from different methodologies that were implemented in CMMI contexts; in fact, there is also mentioned in [D37], [D39], [D6], [D21] and [D25] that it is possible to get a CMMI certification using agile practices as a starting point.

Regarding agile practices using in CMMI contexts, we identify that in the studies [D3], [D4], [D5], [D6], [D7], [D8], [D9], [D10], [D12], [D16], [D17], [D19], [D20], [D22], [D23], [D24], [D25], [D26], [D27], [D28], [D29], [D30], [D32], [D33], [D34], [D35], [D36], [D37], [D39], [D41], [D43], [D44], [D45], [D47], [D48], [D50], [D51] and [D52], there are some agile practices mentioned. In addition, we could found that in the majority of the studies, Scrum and XP are mentioned. In fact, regarding [D8], [D20], [D39], [D43] and [D52] studies, both methodologies can be complemented each other; whereas Scrum focus in the organization and management, XP focus in the technical area proposing agile development practices. This features makes easier the adoption of agile practices in organizations with CMMI due to in case an improvement at organization or management level is required, using Scrum practices is the best option; whereas if it is required an improvement in development practices, using XP approach would be recommendable.

Due to agile methodologies do not consider formal classifications or levels, the adoption of any agile practice is possible, but it is necessary in some cases, adapting the practice to the organization context.

In addition, there are also scenarios where the use of agile practices are not recommended; for instance, those scenarios where the kind of project requires an in-depth documentation and those where it is necessary to record all changes periodically. In addition, there are similar cases where contractual conditions prevent communication and intense customer involvement. This point was evident in [D17], [D28] and [D52], which using agile practices that demand approach to customers is only possible according to the facilities that customers can give.

It is worth mentioning that the aim of a combined adoption of agile and CMMI approaches is to get adequate synergy for getting the benefits of both. This aim is mentioned in the studies [D28], [D30], [D31], [D32], [D44] and [D48] which states that the success of a combined application will depend on the convergence degree between both approaches.

Finally, from the analysis of 52 studies, we could find that the agile practices applicability is defined by the organization's needs, when the needs are defined correctly and agile principles are considered, there are no restrictions on the use and adaptation of certain agile practices unless the application of some of them are conditioned by the project or organization context. Next, in Table 7, there are all agile practices which are mentioned or referred in the primary studies.

4.6 RQ-3. Is there any influence from the team's size in the agile practices use with CMMI culture?

The agile approach is distinguished due to, among others, it proposes intensely the interaction of team members; in fact, the success of the applicability of these practices is based on trust and compromise reached within teams [D47]. This feature negatively influences in the correct functioning of agile practices in scenarios where teams are larger, since as the team grows, it requires more robust and stable channels to allow free flow of communication. That's why in [D17], [D36], [D29] and [D32] are mentioned, for example, that small teams are ideal for implementing agile practices.

Agile practice	Primary Studies
Daily Meeting	[D1], [D4], [D5], [D7], [D8] [D33], [D34], [D52]
Burndown Charts	[D2], [D4], [D13], [D14], [D24] [D28], [D52]
Story Points	[D13], [D21], [D28], [D36]
Sprint Meetings	[D4], [D17], [D24], [D28] [D30] [D43], [D45], [D52]
Retrospectives	[D13], [D21], [D24], [D35] [D43], [D45]
Backlog Management	[D7], [D8], [D12], [D13], [D17] [D21], [D24], [D28], [D34] [D43], [D45]
Continue Integration	[D8], [D34], [D39], [D50]

Table 7. *Agile practices mentioned in primary studies*

Usually, small and medium-sized organizations face more challenges in adopting complex models such as CMMI, so in [D19], [D37], [D41] referred to the benefits that small organizations obtain by implementing agile practices based on the practices defined in CMMI. The processes definition and practices based on CMMI, but adapted to the context of a small organization, enables organizations to consider a CMMI certification in the future.

Additionally, [D48] and [D44] studies mention an important factor besides the team size, this factor is the location of the team members, and it is recommended that teams that implement agile practices should be in the same location because it requires intense communication and interaction among members. In contrast, CMMI provides an organizational infrastructure that allows successful projects with distributed teams, these types of teams can negatively influence in the adoption of agile practices in CMMI contexts.

4.7 RQ-4. Are there primary studies related with the combined use of agile practices and CMMI?

With this RQ we pretend to analyze the interest of the scientific community on the combined use of agile and CMMI practices. To answer this question the results obtained in the selection step were analyzed. As shown in Appendix A, they were 52 primary studies obtained after the selection process. This is a great sign that there is a widespread interest from industry, since it is a large number of studies to analyze in a SRL. Additionally, if we refer to the BQ-1, BQ-2 and BQ-3, we can see that the interest is not only recent; in fact, there is a constant interest over the last 10 years.

As evidenced in the RQ-1, it is possible to combine both agility and maturity approaches since it is beneficial for an organization either it has traditional schemes such as CMMI or being an organization based on agile methodologies. Both types of organizations, as shown in several studies from 52 obtained, are constantly adapting in order to generate competitiveness; allowing them to be

sustainable over time. Along with the previous reason, the scientific community is in the research and development of empirical studies in order to demonstrate the benefits of using both approaches.
Moreover, the interest of the scientific community can also be seen in the numerous studies that refer to mappings between agile and CMMI practices in different maturity levels. These mappings between some practices are carried out with the aim of facilitating the adoption of them in organizations that require it. In Table 8 there is a list of all studies that we could find mappings between CMMI and agile practices according to CMMI level that is referred.

CMMI Maturity Level	Primary Studies
CMMI Level 2	[D4], [D6], [D9], [D27], [D28], [D29] [D32], [D41], [D47], [D50]
CMMI Level 3	[D8], [D14], [D27], [D29], [D34], [D39] [D47], [D50]
CMMI Level 4	[D21], [D29]
CMMI Level 5	[D21]

Table 8. *Primary studies with agile and CMMI mappings*

4.8 RQ-5. Are there advantages or disadvantages in the agile practices use with CMMI culture?

From the analysis of 52 primary studies, it has been fully identified that both approaches working together significantly contribute to improving productivity of the organizations that implement them. In addition, it is noted that in the way agile practices are adapted using different methodologies in the context of CMMI, the benefit is even greater because recognized engineering practices by CMMI are used with additional flexibility and speed that agile practices provide.

In studies [D28], [D32], [D43], [D47], [D24] and [D22] we found that not having established a flexible structure that allows response immediately to the constant changes is a main drawback in organizations with CMMI. Getting the ability to respond to changes in a fast way increases the competitiveness of SDO.

On the other hand, in studies [D12], [D19] and [D51], there are scenarios where organizations with agile practices require some formality in organizational infrastructure to meet the guidelines that customers may require. This formality, as can be analyzed in the studies, is possible to get by the combined use of agile practices and CMMI. From the previous statement, we can affirm that using both approaches together not only benefits organizations with CMMI, but also organizations whose processes and practices are based entirely in agile methodologies.

Furthermore, from studies [D24], [D25], [D27], [D32], [D33], [D35] and [D39] we can identify the following benefits of using a mix of agile and CMMI approaches:

- Reduce delivery times
- Improve quality of delivered product
- Improve stability of agile teams in organizational processes
- Include flexibility and agility in the processes of CMMI organizations
- Efficient implementations of CMMI when using agile principles
- Improve communication with stakeholders using agile practices
- Reduce defects

Finally, regarding the disadvantages of a combined adoption of agile practices and CMMI, it can be analyzed from the primary studies [D43] and [D48] that by combining both approaches with different principles, there is a risk of affecting the current defined processes. Additionally, it was observed from studies that in some situations the teams modify the agile practices regardless the agile principles; as a consequence, the practices are not well-defined and it ends up generating discomfort on team members due to additional work.

5. Conclusion and Future Work

It can be concluded that there is an interest from industry and scientific community regarding the integration of agile and CMMI approaches. Both were considered by the software industry as guidelines with opposite principles and, in some circumstances, incompatible; however, we have found in recent researches that both share the same goals and that may converge to contribute beneficially to the organizations.

This compatibility between agile and CMMI approaches can take the best of both cultures because it is recognized that agile guidelines provide flexibility that enables organizations to respond to the constant changes, particularly in the management of requirements; on the other hand, organizations with agile guidelines are benefit from CMMI because they incorporate good practices that add formality in organizational infrastructure. On the other hand, we could verify that there are studies that indicate it is possible to get certification in the first CMMI maturity levels through the use of agile practices. In addition, using various practices from different agile methodologies allows organizations to apply for even higher maturity levels of CMMI.

During the SLR, there were validations in the planning and the methodology used. These validations were performed by other members of the project but despite peer review and assurance of the methodological framework, we have considered situations that can influence on the results and conclusions obtained. The main identified threat was the selection bias, because research results are conditioned by the proper selection of primary studies. The omission of any of the studies that

can contribute to research is one of the most important threats to take into consideration.

Finally, in this study, a SLR was conducted in order to analyze studies about combined agile and CMMI approaches. From the research of RSL, we could find that there could be a further work related to the empirical validation of what is stated in the analysis of 52 primary studies. In addition, there could be future works about the verification of advantages and disadvantages in the use of both agile and CMMI approaches; as well as, the review of more successful cases of organization that mixes both guidelines.

Acknowledgements:

This work is framed within the ProCal-ProSer project funded by Innóvate Perú under contract 210-FINCYT-IA-2013 and partially supported by the Department of Engineering and the Grupo de Investigación y Desarrollo de Ingeniería de Software (GIDIS) from the Pontificia Universidad Católica del Perú.

References

Abdel-Hamid & Hamouda, A. E. D, A. N. (2015). Lean CMMI: An Iterative and Incremental Approach to CMMI-Based Process Improvement. In Agile Conference (AGILE) (pp. 65–70). IEEE.

Aggarwal Deep, V., & Singh, R, S. K. (2014). Speculation of CMMI in Agile Methodology. In Advances in Computing, Communications and Informatics (ICACCI) (pp. 226–230). IEEE.

Alegría & Bastarrica, M. C, J. A. H. (2006). Implementing CMMI using a combination of agile methods. CLEI Electronic Journal, 1–15.

Anderson, D. J. (2005). Stretching Agile to fit Cmmi level 3 the story of creating msf for Cmmi process improvement. In Agile Development Conference. IEEE.

Baker, S. W. (2006). Formalizing agility, part 2: How an agile organization embraced the CMMI. In Agile Conference (p. 8). IEEE.

Boehm, B. W., & Turner, R. (2003). Balancing agility and discipline: a guide for the perplexed. Addison-Wesley.

Boehm Turner's, R., & Network, P. I., B. (2010). Love and Marriage: CMMI and Agile Need Each Other. SEI Digital Library.

Bos & Vriens, C, E. (2004). An agile CMM. In Extreme Programming and Agile

Methods - XP/Agile Universe 2004 (pp. 129–138). Springer Berlin Heidelberg.

Bougroun Zeaaraoui, A., & Bouchentouf, T., Z. (2014). The projection of the specific practices of the third level of CMMI model in agile methods: Scrum, XP and Kanban. In Information Science and Technology (CIST) (pp. 174–179). IEEE.

Clark, C. (2011). Get to CMMI ML3 Using Agile Development Processes for Large Projects. In Agile Conference.

Cockburn, A. (2002). Agile Software Development. Reading, Massachusetts: Addison–Wesley.

Cohan, S., & Glazer, H. (2009). An Agile Development Team's Quest for CMMI® Maturity Level 5. In Agile Conference (pp. 201–206). IEEE.

Dahlem, Diebold, P., & Marc. (2014). Agile Practices in practice: a mapping study. In 18th International Conference on Evaluation and Assessment in Software Engineering. New York: ACM.

de Souza Carvalho, W. C. (2011). A Comparative Analysis of the Agile and Traditional Software Development Processes Productivity. In Computer Science Society (SCCC) (pp. 74–82). IEEE.

Diaz Garbajosa, J., & Calvo-Manzano, J. A., J. (2009). Mapping CMMI level 2 to scrum practices: An experience report. In Software process improvement (pp. 93–104). Springer Berlin Heidelberg.

Dingsøyr, T. (2012). A decade of agile methodologies: Towards explaining agile software development. Journal of Systems and Software, 85(6), 1213–1221.

Dybå, T., & Dingsøyr, T. (2008). Empirical studies of agile software development: A systematic review. Information and Software Technology, 833–859.

El Deen Hamouda, A. (2014). Using Agile Story Points as an Estimation Technique in CMMI Organizations. In Agile Conference (pp. 16–23). IEEE.

Gandomani, T. J. (2013). Compatibility of agile software development methods and CMMI. Indian Journal of Science and Technology, 5089–5094.

Garzás & Paulk, M. C, J. (2013). A case study of software process improvement with CMMI-DEV and Scrum in Spanish companies. Journal of Software: Evolution and Process, 1325–1333.

Gazzan Shaikh, A., M. (2014). Towards bridging the gap between CMMI and agile development methodologies. In CAINE (pp. 299–304). ISCA.

Glazer Dalton, J., Anderson, D., Konrad, M. D., & Shrum, S., H. (2008). CMMI or agile: why not embrace both! SEI.

Irrazabal Vásquez, F., Díaz, R., & Garzás, J., E. (2011). Applying ISO/IEC 12207:2008 with SCRUM and Agile Methods. In Software Process Improvement and Capability Determination (pp. 169–180). Springer Berlin Heidelberg.

Jakobsen, C. R., & Johnson, K. A. (2008). Mature Agile with a twist of CMMI. In Agile Conference (pp. 212–217). IEEE.

Jakobsen & Sutherland, J, C. R. (2009). Scrum and CMMI going from good to great. In Agile Conference (pp. 333–337). IEEE.

K. Petersen S. Mujtaba, R. F. (2008). Systematic mapping studies in software engineering. In 12th International Conference on Evaluation and Assessment in Software Engineering (pp. 1–10).

Kähkönen & Abrahamsson, P, T. (2004). Achieving CMMI level 2 with enhanced extreme programming approach. In Product Focused Software Process Improvement (pp. 378–392). Springer Berlin Heidelberg.

Kitchenham, B., & Charters, S. (2007). Guidelines for performing Systematic Literature Reviews in Software Engineering. Staffordshire: Elsevier.

Konrad, M., & McGraw, S. (2008). CMMI & Agile. SEI Webinar. SEI Digital Library.

Kovacheva, T. (2011). Optimizing Software Development Process. In EUROCON - International Conference on Computer as a Tool (EUROCON) (pp. 1–2). IEEE.

Leithiser & Hamilton, D., R. (2008). Agile versus CMMI-process template selection and integration with microsoft team foundation server. In 46th Annual Southeast Regional Conference on XX (pp. 186–191). ACM.

Lina, Z., & Dan, S. (2012). Research on Combining Scrum with CMMI in Small and Medium Organizations. In Computer Science and Electronics Engineering (ICCSEE) (pp. 554–557). IEEE.

López-Lira Hinojo, F. J. (2014). Agile, CMMI®, RUP®, ISO/IEC 12207...: is there a method in this madness? In SIGSOFT Software Engineering Notes (pp. 1–5).

Łukasiewicz, K., & Miler, J. (2012). Improving agility and discipline of software development with the Scrum and CMMI. Institution of Engineering and Technology, 6, 416–422.

Mahnic & Zabkar, N., V. (2007). Introducing CMMI Measurement and Analysis Practices into Scrum-based Software Development Process. International Journal of Mathematics and Computers In Simulation, 65–72.

Maller Ochoa, C., & Silva, J, P. (2005). Agilizando el Proceso de Producción de Software en un Entorno CMM de nivel 5. Revistas Del IEEE América Latina.

Marcal, A. S. C., de Freitas, B. C. C., Furtado Soares, F. S., & Belchior, A. D. (2007). Mapping CMMI Project Management Process Areas to SCRUM Practices. Software Engineering Workshop, 13–22.

Marcal de Freitas, B. C. C., Soares, F. S. F., Furtado, M. E. S., Maciel, T. M., & Belchior, A. D., A. S. C. (2008). Blending Scrum practices and CMMI project management process areas. Innovations in Systems and Software Engineering , 17–29.

McMahon, P. E. (2012). Taking an agile organization to higher CMMI maturity. Agile Journal, 19–23.

Miller & Haddad, H. M., J. R. (2012). Challenges Faced While Simultaneously Implementing CMMI and Scrum: A Case Study in the Tax Preparation Software Industry. In Information Technology: New Generations (ITNG) (pp. 314–318). IEEE.

Morris, P. D. (2012). The Perfect Process Storm: Integration of CMMI, Agile, and Lean Six Sigma. Crosstalk, 39–45.

Omran, A. (2008). AGILE CMMI from SMEs perspective. In 3rd International Conference (pp. 1–8). ICTTA.

P. Brereton, B. A. Kitchenham, D. Budgen, M. T. y M. & K. (2007). Lessons from applying the systematic literature review process within the software engineering domain. Journal of Systems and Software, 571–583.

Palomino, M., Dávila, A., Melendez, K., & Pessoa, M. (2016). Agile Practices Adoption in CMMI Organizations: A Systematic Literature Review. In S. I. Publishing. (Ed.), International Conference on Software Process Improvement (pp. 57–67).

Paulk, M. C. (2001). Extreme programming from a CMM perspective (pp. 19–26). IEEE.

Pikkarainen, M. (2009). Towards a Better Understanding of CMMI and Agile Integration - Multiple Case Study of Four Companies. In Product-Focused Software Process Improvement (pp. 401–415). Springer Berlin Heidelberg.

Pikkarainen & Mantyniemi, A, M. (2006). An approach for using CMMI in agile software development assessments: experiences from three case studies. In SPICE.

Popay J Sowden A, Petticrew M, Arai L, Rodgers M, Britten N, R. H. (2006). Guidance on the conduct of narrative synthesis in systematic reviews: A product from the ESRC Methods Programme. Lancaster: Lancaster University.

Potter & Sakry, M., N. (2009). Implementing SCRUM (agile) and CMMI together. Agile Journal, 1–6.

Salinas, C. J. T., Escalona, M. J., & Mejías, M. (2012). A scrum-based approach to CMMI maturity level 2 in web development environments. In Proceedings of the 14th International Conference on Information Integration and Web-based Applications & Services (IIWAS) (pp. 282–285). New York: ACM.

Santana Gusmão, C., Soares, L., Pinheiro, C., Maciel, T., Vasconcelos, A., & Rouiller, A., C. (2009). Agile Software Development and CMMI: What We Do Not Know about Dancing with Elephants. In Agile Processes in Software Engineering and Extreme Programming (pp. 124–129). Springer Berlin Heidelberg.

Santana Furtado Soares, F., & Romero de Lemos Meira, S. (2015). An Agile Strategy for Implementing CMMI Project Management Practices in Software Organizations. In Information Systems and Technologies (CISTI) (pp. 1–4). IEEE.

Selleri Silva Santana Furtado Soares, F., F. (2014). A Reference Model for Agile Quality Assurance: Combining Agile Methodologies and Maturity Models. In Quality of Information and Communications Technology (QUATIC) (pp. 139–144). IEEE.

Shea, B. J., Grimshaw, J. M., Wells, G. A., Boers, M., Andersson, N., & Hamel, C. (2007). Development of AMSTAR: A measurement tool to assess the methodological quality of systematic reviews. BMC Medical Research Methodology.

Silva, F. S., Soares, F. S. F., Peres, A. L., Azevedo, I. M. de, Vasconcelos, A. P. L. F., Kamei, F. K., & Meira, S. R. de L. (2015). Using CMMI together with agile software development: A systematic review. Information and Software Technology, 20–43.

Sutherland Jakobsen, C. R., & Johnson, K, J. (2007). Scrum and CMMI Level 5: The Magic Potion for Code Warriors. In Agile Conference (pp. 272–278). IEEE.
Team, C. P. (2010). CMMI for Development, Version 1.3 (CMU/SEI-2010-TR-033).

Torrecilla-Salinas Sedeño, J., Escalona, M. J., & Mejías, M, C. J. (2014). Mapping Agile Practices to CMMI-DEV Level 3 in Web Development Environments. In International Conference on Information Systems Development (ISD).

Trujillo Oktaba, H., Pino, F. J., & Orozco, M. J., M. M. (2011). Applying Agile and Lean Practices in a Software Development Project into a CMMI Organization. In Product-Focused Software Process Improvement (pp. 17–29). Springer Berlin Heidelberg.

Tuan & Thang, H. Q., N. N. (2013). Combining maturity with agility: lessons learnt from a case study. In Fourth Symposium on Information and Communication Technology (pp. 267–274). ACM.

Turgeon., J. (2011). SCRUMP (Scrum + RUP) and CMMI:The Story of a Harmonious Process and Product Deployment.

Turner & Jain, A., R. (2002). Agile Meets CMMI: Culture Clash or Common Cause? In Extreme Programming and Agile Methods — XP/Agile Universe 2002 (pp. 153–165). Springer Berlin Heidelberg.

Vriens, C. (2003). Certifying for CMM Level 2 and IS0 9001 with XP@ Scrum. In Agile Development Conference (pp. 120–124). IEEE.
Weller, E. (2013). "Agile and CMMI: Friend or Foe? A Lead Appraiser's View." Agile Journal.

Notas biográficas:

Marco A. Palomino es Ingeniero Informático y Magister en Ingeniería Informática con mención en Ingeniería de Software por la Pontificia Universidad Católica del Perú (PUCP). Actualmente es Senior Software Developer en TranSolutions System con más de 7 años de experiencia en análisis, diseño e implementación de software para compañías norteamericanas. Adicionalmente, es integrante del Grupo de Investigación y Desarrollo de Ingeniería de Software (GIDIS-PUCP). El interés en áreas de investigación gira en torno a buenas prácticas en Ingeniería de Software, Desarrollo de Software y Calidad de Producto Software.

Abraham Dávila es investigador y profesor principal de la Pontificia Universidad Católica del Perú (PUCP) desde el 2000. Dirige y es investigador principal del proyecto ProCalProSer (2013-2016 Fase I y 2017-2018 Fase II) y miembro fundador de GIDIS-PUCP. Posee el grado de bachiller en ciencias con mención en Ingeniería Mecánica y magister en Informática por la PUCP. Miembro del grupo de trabajo de la ISO/IEC que elabora la norma ISO/IEC 29110. Sus principales áreas de interés son calidad en informática (a nivel de proceso software, productos y gestión de servicios) y educación en ingeniería de software.

Karin Meléndez es profesora en la Pontificia Universidad Católica del Perú (PUCP) e investigadora del proyecto ProCal-ProSer (2013-2016), consultor en calidad de software y miembro del comité técnico de normalización en ingeniería de software y sistemas de información en el Perú. Magíster en Administración Estratégica de Empresas en Centrum Católica, escuela de negocios de la PUCP (2013), e ingeniera informática de la PUCP (2003). Sus áreas de investigación son la gestión de procesos para desarrollo de software y servicios de tecnologías de información.

Marcelo Pessoa es Ingeniero Electrónico, tiene una maestría, doctorado y libre docencia por la Universidad Politécnica de San Pablo – Brasil. Profesor del Dpto. de Ingeniería de la Producción desde 1987. Tiene experiencia e investigaciones en las áreas de sistemas de operaciones, computación, electrónica, telecomunicaciones y automatización. Miembro de la Comisión del Estudio de Procesos del Ciclo de Vida de Software de la ABNT en el área de Ingeniería de Software para la elaboración de normas nacionales e internacionales en la ISO. Coordinador del CEGPTI Curso de Especialización en Gestión de la TI desde 2008. Coordinador del curso Análisis de Negocio basado en BABOK. Fue Director-Presidente de la Fundación Carlos Alberto Vanzolini en el periodo 2002-2005 y después miembro del Consejo Curador de las misma Fundación. Actualmente es vice-Jefe del Dpto. de Ingeniería de la Producción 2015/2017. Trabaja como investigador en los laboratorios eLabSoft donde realiza

investigación sobre Fábrica de Software y Proceso Software. También es investigador de LADOS (Laboratorio de Análisis, Desarrollo y Operaciones de Sistemas donde desarrolla investigación sobre sistemas tecnológicos avanzados, combinando software y servicios tecnológicos para la generación de innovaciones, desarrollo de nuevos productos y servicios tecnológicos para la re-estructuración de los procesos productivos.

Recibido 14 Sep 2017 *ReCIBE, Año 6 No. 1, Noviembre 2017*
Aceptado 5 Oct 2017

New S-box calculation approach for Rijndael-AES based on an artificial neural network

Nuevo enfoque para el calculo de la Caja-S para Rijndael-AES basado en una red neuronal artificial

Jaime David Rios Arrañaga[1]
jaime.rios.1xyz@gmail.com

Janneth Alejandra Salamanca Chavarin[1],
salecita_ale@hotmail.com

Juan José Raygoza Panduro[1]
juan.raygoza@cucei.udg.mx

Edwin Christian Becerra Alvarez[1]
edwincbecerra@gmail.com

[1]Centro Universitario de Ciencias Exactas e Ingenierías, Universidad de Guadalajara, Jalisco, México.

Abstract: The S-box is a basic important component in symmetric key encryption, used in block ciphers to confuse or hide the relationship between the plaintext and the ciphertext. In this paper a way to develop the transformation of an input of the S-box specified in AES encryption system through an artificial neural network and the multiplicative inverse in Galois Field is presented. With this implementation more security is achieved since the values of the S-box remain hidden and the inverse table serves as a distractor since it would appear to be the complete S-box. This is implemented on MATLAB and HSPICE using a network of perceptron neurons with a hidden layer and null error.

Keywords: Artificial Neural Network, Cryptography, Circuits, SPICE.

Resumen: La Caja-S es un componente básico en el cifrado de clave simétrica, usado en los cifradores por bloques para confundir o esconder la relación entre el texto plano y el texto cifrado. Este trabajo presenta una manera de desarrollar la transformación de los valores de entrada de la Caja-S especificada en el sistema de cifrado AES por medio de una red neuronal y los valores del inverso multiplicativo en el campo de Galois. Con esta implementación se logra mayor seguridad debido a que los valores de la Caja-S permanecen ocultos mientras que la tabla de los valores inversos en el dominio de Galois sirve de distractor pareciendo ser la verdadera Caja-s. Este trabajo fue implementado en MATLAB y HSPICE utilizando una red con neuronas del tipo Perceptron con una capa oculta, obteniendo los valores esperados por la Caja-S original sin error.

Palabras clave: Circuitos, Criptografia, Red Neuronal Artificial, SPICE

1. Introduction

In cryptography, an S-box consists of a look up table with the corresponding 8-bit word for each possible input in a non-linear transformation, in which the input byte is considered the address of the table (Rodriguez-Henriquez, Saqib, Díaz & Koc 2007). The S-box represents a bricklayer non-linear function that can be decomposed in several boolean functions operating independently on a subset of bits from the input vector (Daemen & Rijmen, 2002). If the functions are linear they are called D-boxes.

The operation of an S-box is as follows: when a transformation is required for a certain input, this input enters the S-box and points, or directs to the previously calculated output of its transformation and then the input is replaced, as shown in fig.1, where the value $a_{i,j}$ is substituted for the value $b_{i,j}$ as it passes through the S-box.

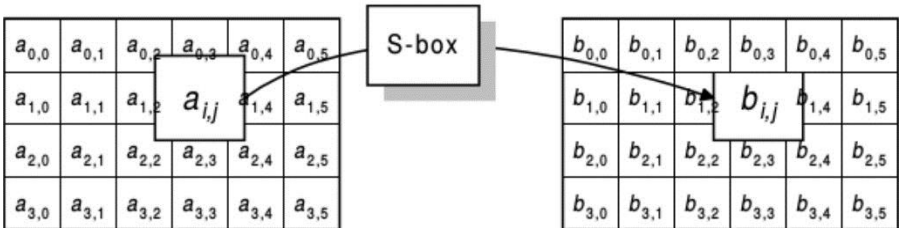

Figure 1. *Graphic representation of the use of an S-box*

Due to their importance, S-boxes are chosen and designed to be resistant to cryptanalysis, in literature several proposals with different characteristics are found, some of them based on neural networks, like the framework for the design of S-boxes used in ciphers based on neural networks by Noughabi (Noughabi & Sadeghiyan, 2010) and “a new scheme for implementing s-box based on neural network” by X. Zhang (Zhang, Chen, Chen, & Cao, 2015), others that optimize existing boxes such as the high speed implementation of S. Oukili for the AES S-box (Oukili, Bri & Kumar, 2016) and low-area S-box implementation of Thomson (Thomson, Siva, & Priya, 2014); even new proposals such as the evolutionary design of S-Box of M. Yang (Yang, Wang, Meng & Han, 2011) and the based on chaotics maps of C. I. Rîncu (Rîncu & Iana, 2014).

This article presents a substitution of the S-box for another module that calculates the AES S-box outputs with the use of a neural network and the multiplicative inverse on Galois field 2^8 (GF (2^8)) of the input value to transform, or S-box input value.

Section 2 introduces the AES algorithm giving a brief introduction to history and a complete description of the Rijndael-AES algorithm, in this section under the subsection “The Round Transformation” highlights the sub-Bytes function that

describe how the values of the S-box are calculated. Section 3 describes the proposed method, this includes the neural network topology and the approach for hardware implementation. The simulations are presented in section 4, this section is an explanation of the implementation, behavior and results in MATLAB and HSPICE. Finally conclusions are given in section 5.

2. AES, Advance Encryption Standard

Developed by Joan Daemen and Vincent Rijimen, Rijndael was finally chosen on October 2000 by the National Institute of Standards and Technology (NIST) among other encryption algorithms in an open process organized by the same institute on January 1997 to become the new *Advanced Encryption Standard* (AES) to replace *Data Encryption Standard* (DES) and triple-DES as encryption standard (Daemen & Rijmen, 2002). Following NIST specifications, AES is a symmetric block cipher algorithm with variable length of 128 bits, 192 bits and 256 bits, with a variable length key of 128 bits, 192 bits y 256 bits and easy on hardware and software implementation (Daemen & Rijmen, 2002).

Although it is common to talk about AES and Rijndael indistinctly, being Rijndael the selected algorithm for AES, there is a difference among them in the range of values supported by the block length and key length to use. In Rijndael, the block length and key length can be independently specified to any multiple of 32 bits, with a minimum of 128 bits and a maximum of 256 bits. AES fixes the length block and the length key to 128, 192 o 256 bits only (Daemen & Rijmen, 1999).

Independently of technical differences in the length of block and key permitted, when talking about Rijndael or AES, we are talking about the same iterative block cipher algorithm. Inputs and outputs of Rijndael-AES are considered to be one-dimensional arrays of 8-bits. For encryption the input is a Plaintext block and a cipher key, and the output is a ciphertext block. For decryption the inputs is a ciphertext block and a cipher key, and the output is a Plaintext block (Daemen & Rijmen, 2002).

The cipher can be divided in two parts with different functionality: the transformation or encoding of the message, function called “The Round transformation” and denoted as “Round” and “FinalRound”, this encryption function is described in fig. 2 along with the functions that make it up, called steps; and the transformation of the key called “Key schedule” given by the function “KeyExpansion”.

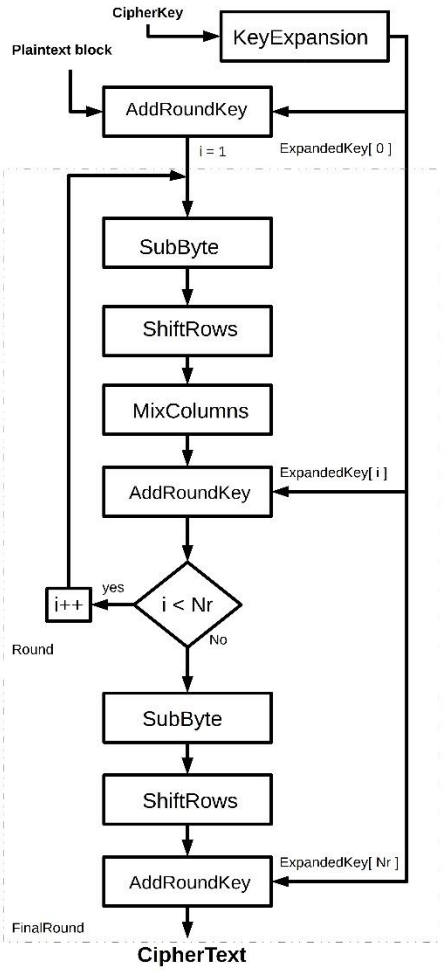

Figure 2. *Flowchart of the AES encryption algorithm*

The different transformation operates on an intermediate result called State which is represented as a rectangular array of bytes, with four rows and N_b number of columns.

$$N_b = \frac{blocklength}{32} \quad (1)$$

Similarly, the cipher key is represented as a rectangular array with four rows and N_k number of columns (Daemen & Rijmen, 1999), (Rodriguez-Henriquez et al., 2007), (Daemen & Rijmen, 2002), (Katz & Lindell, 2008), where

$$N_k = \frac{keylength}{32} \quad (2)$$

The number of rounds N_r depends on the values of N_b and N_k as presented in the table 1.

N_k	Nb				
	4	5	6	7	8
4	10	11	12	13	14
5	11	11	12	13	14
6	12	12	12	13	14
7	13	13	13	13	14
8	14	14	14	14	14

Table 1. *Number Of Rounds N_r As Function Of N_b And N_k*

2.1. The Round Transformation

As shown in the fig. 2, the round transformation is divided in Round and FinalRound. Round is formed by a sequence of four different and invertible mathematical transformations on GF(2^8) which are called steps: *1) SubBytes, 2) ShiftRows, 3) MixColumn, 4) AddRoundKey* (Daemen & Rijmen, 1999), (Rodriguez-Henriquez et al., 2007), (Daemen & Rijmen, 2002). The FinalRound is similar to round but without the MixColumns function.

2.1.1. subBytes.

It is a non-linear transformation where each input byte of the state matrix is replaced by another byte produced by the transformation. This Transformation is defined in two steps (Daemen & Rijmen, 1999):

- Multiplicative inverse:
  The input byte a is replaced by its multiplicative inverse $x = a^{-1}$, with x = 0 for a = 0.
- Affine transformation:
  Defined by $y = M \times x \oplus b$, where M is a constant matrix of 8 × 8 bits, x represents the value to transform while b is a constant byte equal to 63_{16} (01100011_2) (Daemen & Rijmen, 2002).

The matrix representation of the transformation is shown in (3), where M is replaced by the constant matrix of 8×8 bits, x is expanded to the polynomial representation of a byte, starting with the most significant bit; and b the binary constant.

$$\begin{bmatrix} y_7 \\ y_6 \\ y_5 \\ y_4 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} x_7 \\ x_6 \\ x_5 \\ x_4 \\ x_3 \\ x_2 \\ x_1 \\ x_0 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} \quad (3)$$

Another way to implement this transformation is to use the corresponding S-Box shown in fig. 3 replacing the input value (row, column) by the value that crosses them.

		Y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
X	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	a	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	b	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	c	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	d	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	e	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	f	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Figure 3. *AES S-box*

The inverse operation, called InvSubBytes, consists of the use of the inverse S-Box of fig. 4 for each byte of the state.

		Y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
X	0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
	1	7C	E3	39	82	9B	2F	FF	87	34	83	43	44	C4	DE	E9	CB
	2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
	3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
	4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
	5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
	6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
	7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
	8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
	9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
	a	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
	b	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
	c	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
	d	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
	e	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
	f	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

Figure 4. *AES Inverse S-box*

The inverse S-box is obtained by the applying the inverse of the affine transformation, shown in ec. 3 followed by taking the multiplicative inverse in GF(2^8). The inverse of (3) is represented in (4) (Daemen & Rijmen, 2002).

$$\begin{bmatrix} y_7 \\ y_6 \\ y_5 \\ y_4 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} x_7 \\ x_6 \\ x_5 \\ x_4 \\ x_3 \\ x_2 \\ x_1 \\ x_0 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} \quad (4)$$

2.1.2. ShiftRows

In ShiftRows, the rows of the state are shifted cyclically to the left in different proportions. Row 0 does not changes, but the remaining rows follow an offset of C_1 , C_2 and C_3 bytes respectively, this proportion depends only of the block length N_b (Daemen & Rijmen, 2002). The inverse operation, called InvShiftRows, consists in a cyclic shift of the three bottom rows over $N_b - C_1$, $N_b - C_2$ *y* $N_b - C_3$ bytes respectively. The table 2 shows the value of C_n per each possible N_b.

N_b	C_0	C_1	C_2	C_3
4	0	1	2	3
5	0	1	2	3
6	0	1	2	3
7	0	1	2	3
8	0	1	2	3

Table 2. *Shifted Bytes In Shiftrows Per Block Lenght*

2.1.3. MixColumns

The MixColumns step is a bricklayer permutation operating on the state column by column. In Mixcolumns the state columns are considered as polynomials in GF (2^8) and multiplied modulo $x_4 + 1$ with the fixed polynomial c(x) given by *c(x) = (03_{16})x_3 + (01_{16})x_2 + (01_{16})x + 02_{16}* . This operation can be written as a matrix multiplication, let *b(x) = c(x) a(x) mod x^4 +1 as is show in (5).*

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02_{16} & 03_{16} & 01_{16} & 01_{16} \\ 01_{16} & 02_{16} & 03_{16} & 01_{16} \\ 01_{16} & 01_{16} & 02_{16} & 03_{16} \\ 03_{16} & 01_{16} & 01_{16} & 02_{16} \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} \quad (5)$$

The inverse of MixColumns is called InvMixColumns. It is similar to MixColumns.

The transformation is performed by multiplying each column by the polynomial $d(x) = (0B_{16})x_3 + (0D_{16})x_2 + (09_{16})x + 0E_{16}$, represented in (6) as a matrix multiplication (Daemen & Rijmen, 1999), (Daemen & Rijmen, 2002), (Parikh & Narkhede, 2016).

$$\begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} 0E_{16} & 0B_{16} & 0D_{16} & 09_{16} \\ 09_{16} & 0E_{16} & 0B_{16} & 0D_{16} \\ 0D_{16} & 09_{16} & 0E_{16} & 0B_{16} \\ 0B_{16} & 0D_{16} & 09_{16} & 0E_{16} \end{bmatrix} \times \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} \quad (6)$$

2.1.4. AddRoundKey

In this transformation the state is modified with the bitwise XOR operation with the round key derived from the cipher key and the function Key Schedule. The length of round key is equal to the block length N_b (Daemen & Rijmen, 1999). The inverse of AddRoundKey is called InvAddRoundKey, and is applied in the same way as AddRoundKey applying the keys in reverse order (Rodriguez-Henriquez et al., 2007).

2.2. Key Schedule

Consists in the expansion of the key and in the key selection round (Daemen & Rijmen, 2002). The key expansion specifies how the expanded key is calculated from the cipher key. The number of bits in the expanded key is equal to the block length multiplied by the number of rounds N_r plus one, generating a total of $N_b \times (N_r + 1)$ words, or $N_r + 1$ subkeys, one per each round (Bonadero, Liberatori, Bria & Villagarcía, 2005).

The cipher key is expanded inside of the Expanded key. Round keys are taken from Expanded key as follows: the first round key consists on the initial N_b words, the second on the subsequent N_b words, and so on (Daemen & Rijmen, 1999).

2.2.1 KeyExpansion.

Expanded Key is a four byte linear array denoted by W $[N_b \times (N_r + 1)]$. The first N_k words contain the cipher key, while all other words are defined recursively. KeyExpansion depends of the N_k value and is calculated as in fig. 5, employing the functions subBytes, Rotbyte and Rcon (Daemen & Rijmen, 1999), (Daemen & Rijmen, 2002).

RotByte returns a word that results from a cyclical permutation from the input word, e.g., for an input {a,b,c,d} the output is {b,c,d,a}.

The constant Rcon is independent of N k and is defined in (7) as:

$$Rcon[i]=(RC[i],00_{16},00_{16},00_{16}) \quad (7)$$

where RC[i] represents an element in GF (2^8) with value $x^{(i-1)}$ such that:

$$RC[1]=x^0=01_{16} \quad (8)$$

$$RC[2]=x^1=02_{16} \quad (9)$$

$$RC[j]=x\times RC[j-1]=X^{j-1},\ j>2 \quad (10)$$

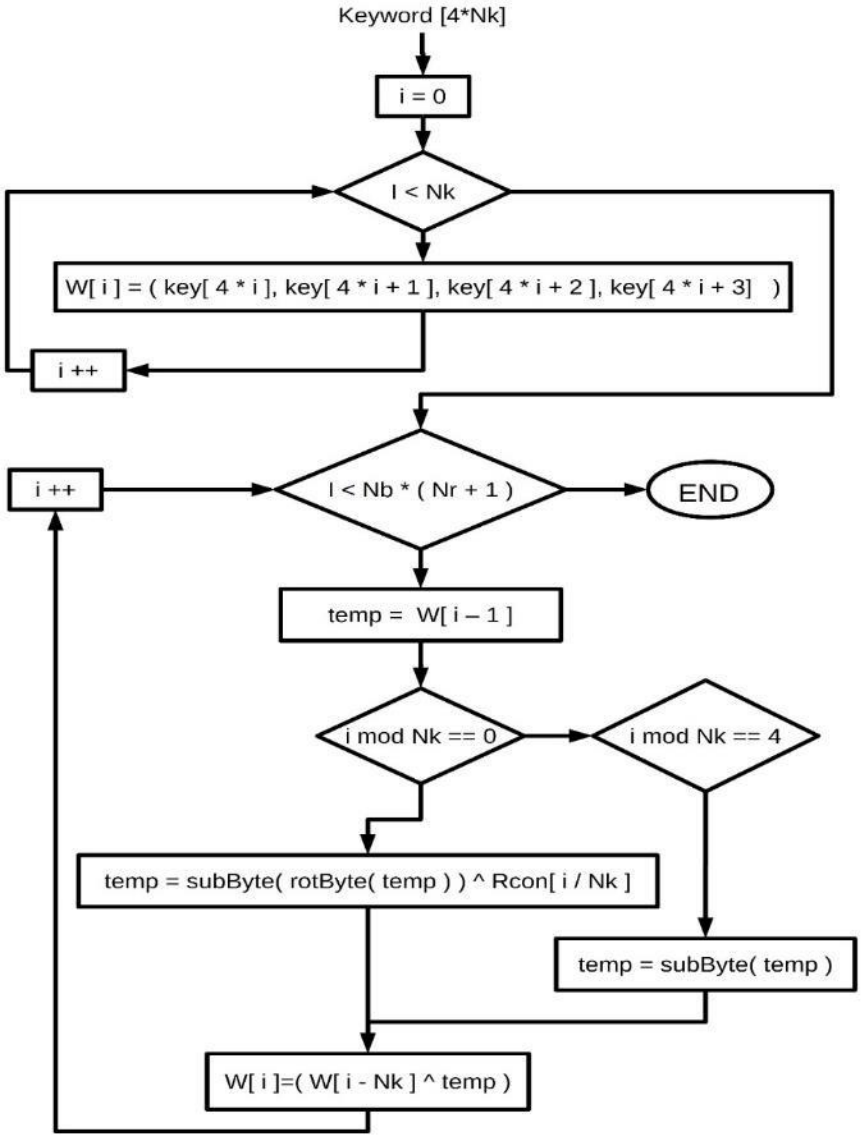

Figure 5. *Flowchart diagram for KeyExpansion function*

3. Proposed Method

The modification consists in substituting the AES S-box for an Artificial Neural Network (ANN) that solves the transformation using as input the corresponding multiplicative inverse value GF (2^8) of the original S-box input value. To obtain the corresponding inverse a lookup table is used. The S-box is substituted for a module formed by a table with the inverse values obtained from (Pelzl & Paar, 2010), (Srebrny, Kościelny & Kurkowski, 2013) and a neural network as is shown in fig. 6. With this method two advantages are obtained, the first one is that the values of the S-box are hidden, and the second one is that it's possible to change the values of the S-box just by a simply changing the weights.

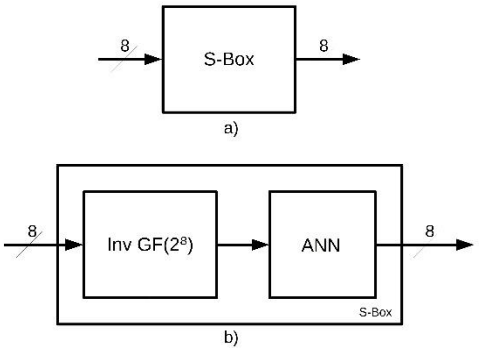

Figure 6. *a) S-box representation. b) Representation of the S-box proposed*

The neural network topology was proposed by means of observation. The transformation is performed bitwise, nevertheless another arrangement is also acceptable. The neural network consists of eight subnetworks, one per bit, each one as illustrated in fig. 7 is composed by seven perceptron neurons in three layers: input layer, hidden layer and output layer. Based on neural networks that perform AND and XOR behaviors each neuron has two inputs and a pulse activation function given by (11).

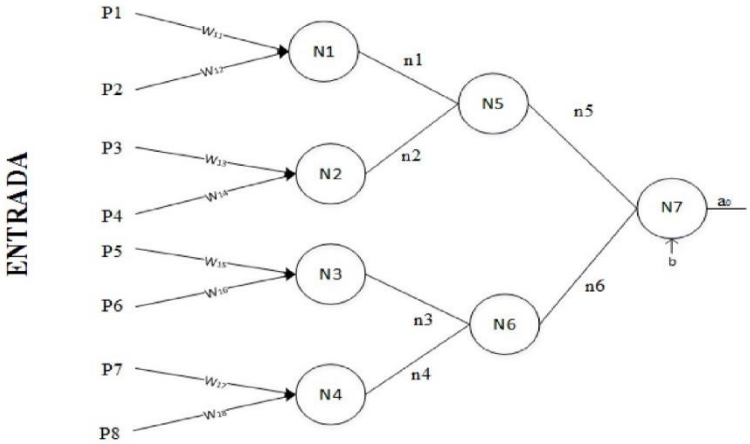

Figure 7. *Neural network with one bit output*

$$f(x)=\begin{cases} if & x=1, \quad 1 \\ if & x\neq 1, \quad 0 \end{cases} \tag{11}$$

The circuit implementation was developed in HSPICE which is an electric circuit simulator (synopsys, 2003), (Piuri, 1991). In hardware implementation, Operational Transconductance Amplifiers (OTA) are used as proposed in (Kawaguchi, Umeno & Ishii, 2014), (Ghosh, LaCour & Jackson, 1994) in order to manage current signals and simplify the sum of the synaptic weights.

The OTA is a voltage controlled current source (VCCS). Its main characteristics are high input impedance and high output impedance (Barclay & Wood, 1994), (Qing-Lin, Jian-You & Mei-Lun, 1991). The OTA macromodel is shown in fig. 8, where V_{in1} and V_{in2} are the voltage inputs, the voltage difference of these sources is reflected in nodes a and b.

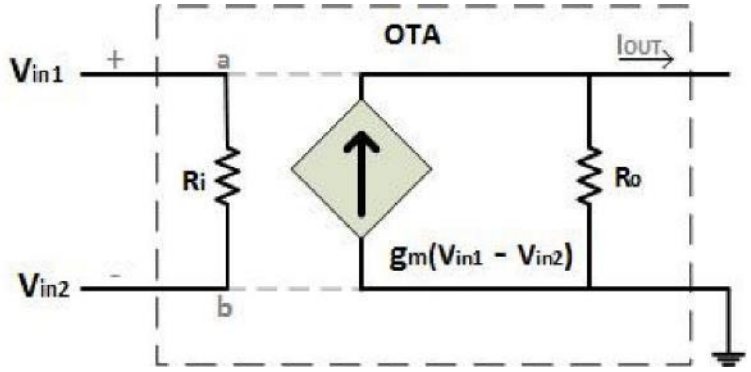

Figure 8. *Macromodel for the Operational Transconductance Amplifier*

The output current I_{out} is proportional to the difference between these voltages as in eqn. 12.

$$I_{out}=g_m\left(V_{positive}-V_{negative}\right) \tag{12}$$

where g_m is the transconductance gain, V_{in1} the positive input voltage, V_{in2} the negative input voltage and I_{out} the output current.

The OTA is used to represent the neuron inputs, converting (in the input layer) or keeping (in the remaining layers) the input signal into a current signal and using the amplifiers gain (g_m) as the corresponding synaptic weight. The signals are summed by simply connecting the OTAs outputs to a wire line which is then the input to the activation function.

4. Simulations

The proposed network was simulated in Matlab, where it was tested and the expected operation for the S-box specified for AES was verified. An implementation using OTAs in HSPICE was performed, where the gain is equivalent to the corresponding weights. Simulating the electric behavior of the system. In the next subsections details of its implementation and results are given.

4.1. Simulation and Results in MATLAB

In the simulation the inverse value in GF(2^8) was used as input of the system and the results were compared and verified with its corresponding S-box values. For a better visualization of the results, the binary values were converted to decimal and are presented in fig. 9 highlighting that the values obtained correspond to those expected with an error of 0%.

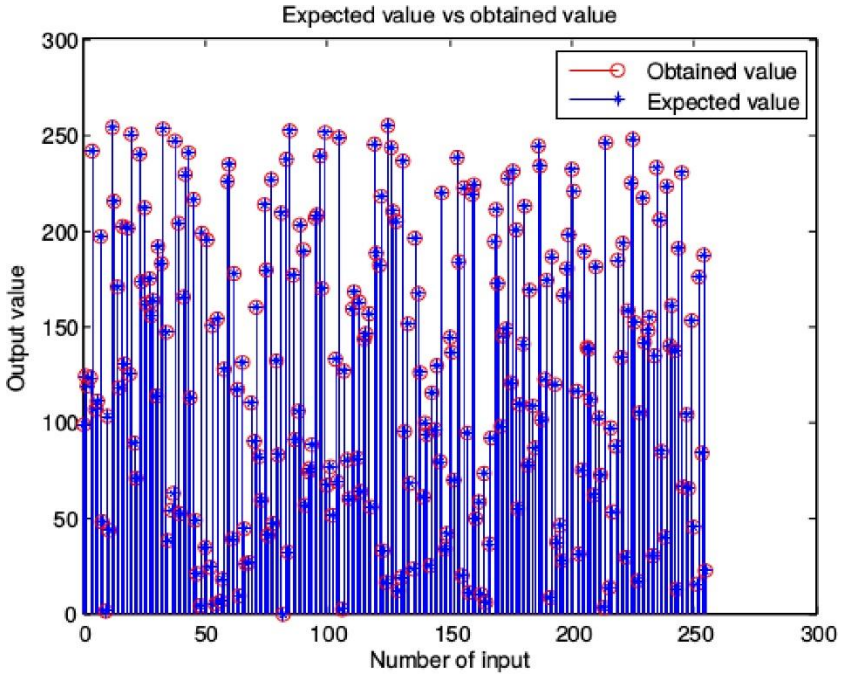

Figure 9. *Expected vs. obtained values. Inputs from 0 to 255*

The synaptic weights used are shown in table 3, these values were obtained from neural networks with AND and XOR behaviors, hence there was no previous training of the network.

Network no.	Synaptic weights	
Bit 0	Input layer	$n_{1,1} = 1, n_{1,2} = 0, n_{2,1} = 0, n_{2,2} = 0, n_{3,1} = 1, n_{3,2} = 1, n_{4,1} = 1, n_{4,2} = 1$
	Hidden layer	$n_{5,1} = 1, n_{5,2} = 1, n_{6,1}=1, n_{6,2}=1$
	Output layer	$n_{7,1} = 1, n_{7,2} = 1$
	Bias	$n_1 = 0, n_2 = 0, n_3 = 0, n_4 = 0, n_5 = 0, n_6 = 0, n_7 = 0$
Bit 1	Input layer	$n_{1,1} = 1, n_{1,2} = 1, n_{2,1}=0, n_{2,2}=0, n_{3,1} = 0, n_{3,2} = 1, n_{4,1}=1, n_{4,2}=1$
	Hidden layer	$n_{5,1} = 1, n_{5,2} = 1, n_{6,1}=1, n_{6,2}=1$
	Output layer	$n_{7,1} = 1, n_{7,2} = 1$
	Bias	$n_1 = 0, n_2 = 0, n_3 = 0, n_4 = 0, n_5 = 0, n_6 = 0, n_7 = 0$
Bit 2	Input layer	$n_{1,1} = 1, n_{1,2} = 1, n_{2,1}=1, n_{2,2}=0, n_{3,1} = 0, n_{3,2} = 0, n_{4,1}=1, n_{4,2}=1$
	Hidden layer	$n_{5,1} = 1, n_{5,2} = 1, n_{6,1}=1, n_{6,2}=1$
	Output layer	$n_{7,1} = 1, n_{7,2} = 1$
	Bias	$n_1 = 0, n_2 = 0, n_3 = 0, n_4 = 0, n_5 = 0, n_6 = 0, n_7 = 0$
Bit 3	Input layer	$n_{1,1} = 1, n_{1,2} = 1, n_{2,1}=1, n_{2,2}=1, n_{3,1} = 0, n_{3,2} = 0, n_{4,1}=0, n_{4,2}=1$
	Hidden layer	$n_{5,1} = 1, n_{5,2} = 1, n_{6,1}=1, n_{6,2}=1$
	Output layer	$n_{7,1} = 1, n_{7,2} = 1$
	Bias	$n_1 = 0, n_2 = 0, n_3 = 0, n_4 = 0, n_5 = 0, n_6 = 0, n_7 = 0$
Bit 4	Input layer	$n_{1,1} = 1, n_{1,2} = 1, n_{2,1}=1, n_{2,2}=1, n_{3,1} = 1, n_{3,2} = 0, n_{4,1}=0, n_{4,2}=0$
	Hidden layer	$n_{5,1} = 1, n_{5,2} = 1, n_{6,1}=1, n_{6,2}=1$
	Output layer	$n_{7,1} = 1, n_{7,2} = 1$
	Bias	$n_1 = 0, n_2 = 0, n_3 = 0, n_4 = 0, n_5 = 0, n_6 = 0, n_7 = 0$
Bit 5	Input layer	$n_{1,1} = 0, n_{1,2} = 1, n_{2,1}=1, n_{2,2}=1, n_{3,1} = 1, n_{3,2} = 1, n_{4,1}=1, n_{4,2}=0$
	Hidden layer	$n_{5,1} = 1, n_{5,2} = 1, n_{6,1}=1, n_{6,2}=1$
	Output layer	$n_{7,1} = 1, n_{7,2} = 1$
	Bias	$n_1 = 0, n_2 = 0, n_3 = 0, n_4 = 0, n_5 = 0, n_6 = 0, n_7 = 0$
Bit 6	Input layer	$n_{1,1} = 0, n_{1,2} = 0, n_{2,1}=1, n_{2,2}=1, n_{3,1} = 1, n_{3,2} = 1, n_{4,1}=1, n_{4,2}=0$
	Hidden layer	$n_{5,1} = 1, n_{5,2} = 1, n_{6,1}=1, n_{6,2}=1$
	Output layer	$n_{7,1} = 1, n_{7,2} = 1$
	Bias	$n_1 = 0, n_2 = 0, n_3 = 0, n_4 = 0, n_5 = 0, n_6 = 0, n_7 = 0$
Bit 7	Input layer	$n_{1,1} = 0, n_{1,2} = 0, n_{2,1}=0, n_{2,2}=1, n_{3,1} = 1, n_{3,2} = 1, n_{4,1}=1, n_{4,2}=1$
	Hidden layer	$n_{5,1} = 1, n_{5,2} = 1, n_{6,1}=1, n_{6,2}=1$
	Output layer	$n_{7,1} = 1, n_{7,2} = 1$
	Bias	$n_1 = 0, n_2 = 0, n_3 = 0, n_4 = 0, n_5 = 0, n_6 = 0, n_7 = 0$

Table 3 *Synaptic Weight Values*

4.2. HSPICE Implementation and Results

According to the structure proposed in fig. 7 the architecture shown in fig. 10 is implemented in HSPICE, where V1 through V8 represent the input signals, the weight, W, are represented by the transconductance of the OTAs, the sums are represented by linking the OTAs outputs, and finally the activation function described in (11) is applied.

The structure in fig. 10 has one bit output, hence it's necessary to replicate the structure in order to have an eight bit output. It should be noted that it is not necessary to replicate the voltage sources and their resistance, i.e. the inputs, only the current source, their resistance and the activation functions.

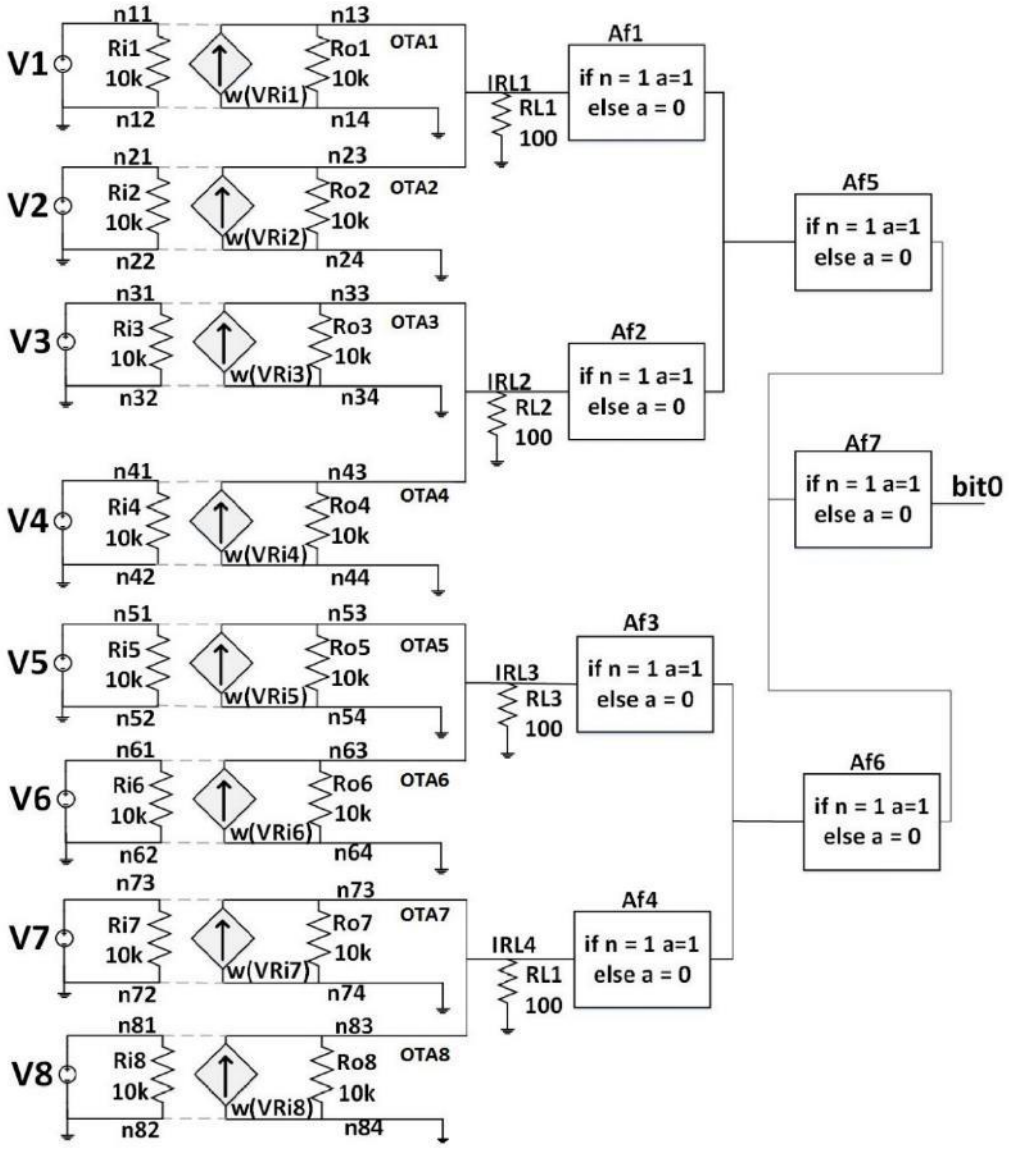

Figure 10. *S-box structure with 1 bit output*

Circuit operation steps

1. The input value is placed in the voltage sources V1 through V8 for the S-box value that wants to be obtained.
2. The voltage difference between nodes n11 and n12 is the voltage in source V1. This difference is multiplied by the gain (weight). This is repeated in voltage source V2 to V8.
3. Since the outputs from the OTAs are given in current, they can be summed by joining them as follows:
   OTA1 output and OTA2 output are linked in Irl1
   OTA3 output and OTA4 output are linked in Irl2
   OTA5 output and OTA6 output are linked in Irl3
   OTA7 output and OTA8 output are linked in Irl4
4. Activation function (11) is applied in Af1 through Af4.
5. Af1 output is linked with Af2, and Af3 with Af4
6. Activation function is applied in Af5 and Af6
7. Af5 and Af6 outputs are linked
8. 8) Activation function is applied in Af7
9. 9) Af7 output corresponds to bit0

As mentioned previously, the structure is replicated to obtain the eight output bits, therefore the same steps are repeated to obtain bit1 to bit7.

To verify the circuit operation, tests were performed with the input values shown in table IV, the table displays some of the values found in the S-box and the result to those inputs, the next two columns show the input value for the proposed network which corresponds to the multiplicative inverse in GF(2^8) and the result obtained from that input. The results obtained from the network are identical, thus the operation of the network is validated.

In figs. 11 and 12 the results obtained from the circuit for four inputs of the table are shown.

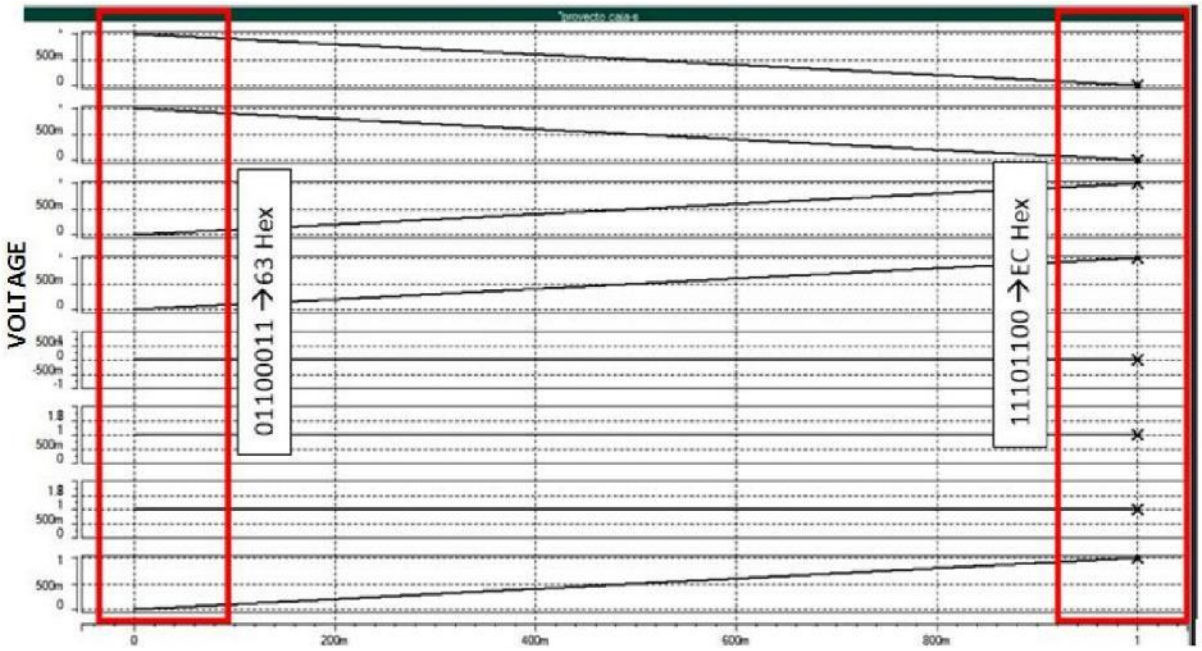

Figure 11. *Obtained result for input 00 16 and 80 16 in GF (2^8)*

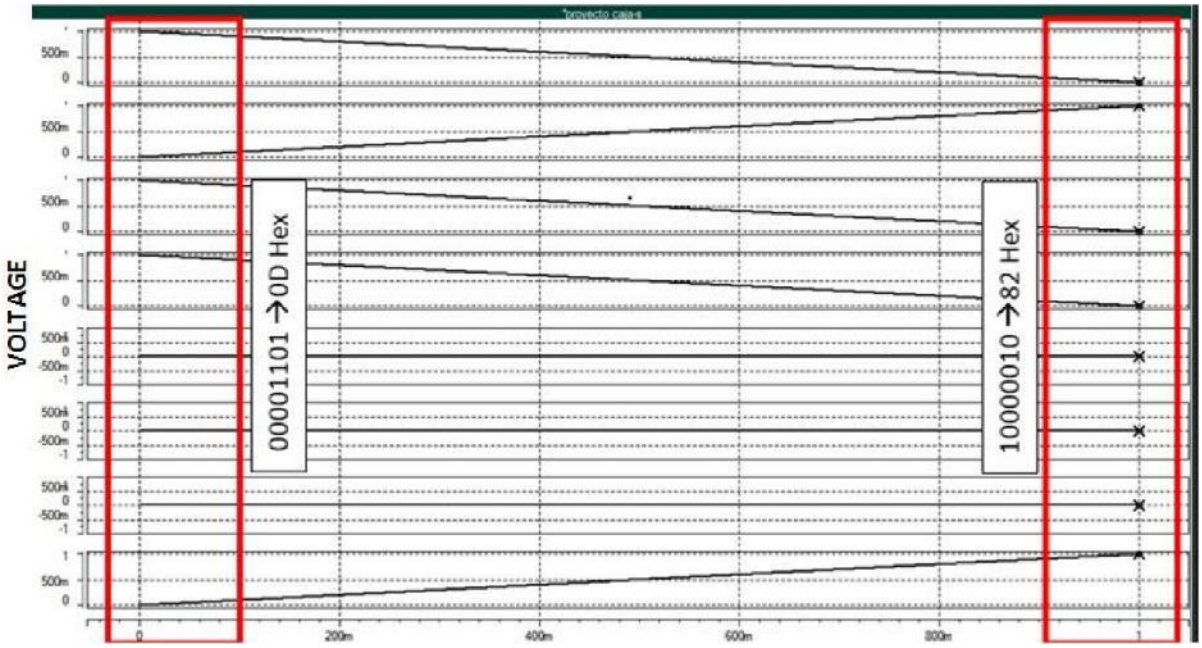

Figure 12. *Obtained result for input 34 16 and 11 16 in GF (2^8)*

e.g. On the left side in fig. 11 the obtained result from the circuit to input 00 16 in GF(2^8) is 63_{16} , the result is verified in table 4. Similarly on the left side the result EC_{16} is obtained for an input 80_{16} in GF(2^8).

S-Box input(Hex)	Result(Hex)	GF(2^8) input(Hex)	Result(Hex)
0	63	0	63
11	82	B4	82
22	93	5A	93
33	C3	6C	C3
44	IB	2D	1B
55	FC	24	FC
66	33	36	33
77	F5	3C	F5
88	C4	9B	C4
83	EC	80	EC
F3	0D	34	0D
C4	1C	DA	1C
5D	4C	EC	4C
E7	94	AD	94
8F	73	A4	73
78	BC	B6	BC
BD	7A	BC	7A
CC	4B	1B	4B

Table 4. *Test Values For The Circuit Implemented In HSPICE*

5. Conclusion

An implementation of an S-box using a neural network in MATLAB and HSPICE is presented, this neural network is based on the operations used to obtain the values of the S-box through 8 perceptron subnetworks and a lookup table with the inverse in GF(2^8). Even if this method of calculating S-box values for AES does not present an advantage reducing resources, since storing the inverse values for each possible input represent hundred percent of the necessary resources to store the original S-box, the values computed by a neural network offers greater security by maintaining the transformation values hidden and using a distractor or an apparently S-box that contains the inverse values in GF(2^8). The simulation results show that the implementation presents a null error, thereafter if the neural network were applied, it will not show changes in the results expected within the encryption algorithm because it simulates without error the operation of the S-box.

References

Barclay M. & Wood J., (1994) A SPICE macromodel for operational transconductance amplifiers. *IEE Colloquium on Analogue Signal Processing*, London, 1994, pp. 1/1-1/4.

Bonadero J., Liberatori M., Bria O. & Villagarcía-Wanza H. (2005) Expanción de la clave en rijndael: diseño y optimización en vhdl. In XI Workshop IBERSHIP.

Daemen J. & Rijmen V. (1999) AES proposal: Rijndael.

Daemen J. & Rijmen V. (2002) The design of Rijndael: AES - the Advanced Encryption Standard. Springer-Verlag.

Ghosh J., LaCour P. & Jackson S. (1994) Ota based neural network architectures with on-chip tuning of synapses. In Proceedings of 7th International Conference on VLSI Design, pages 71–76.

Katz J. & Lindell Y. (2008) Introduction to Modern Cryptography. Chapman & Hall/CRC cryptography and Network Security.

Kawaguchi M., Umeno M. & Ishii N. (2014) The two-stage analog neural network model and hardware implementation. In 2014 IIAI 3rd International Conference on Advanced Applied Informatics, pages 936–941.

Noughabi M. N. A. & Sadeghiyan B. (2010) Design of s-boxes based on neural networks. In 2010 International Conference on Electronics and Information Engineering, volume 2, pages V2–172–V2–178.

Oukili S., Bri S., & Kumar A. V. S. (2016) High speed efficient fpga implementation of pipelined aes s-box. In 2016 4th IEEE International Colloquium on Information Science and Technology (CiSt), pages 901–905.

Parikh P. & Narkhede S. (2016) High performance implementation of mixing of column and inv mixing of column for aes on fpga. In 2016 International Conference on Computation of Power, Energy Information and Commuincation (ICCPEIC), pages 174–179.

Pelzl J. & Paar C.. (2010) Understanding Cryptography - A Textbook for Students and Practitioners. Springer-Verlag Berlin Heidelberg, 1 edition.

Piuri V. (1991) The use of the electrical simulator spice for behavioral simulation of artificial neural networks. In 1991 Proceedings of the 24th Annual Simulation

Symposium, pages 18–29.

Qing-Lin Sun, Jian-You Liu & Mei-Lun Liu, (1991) An improved nonlinear macromodel of OTA, *1991 International Conference on Circuits and Systems*, Shenzhen, *China.* pp. 906-908 vol.2.

Rîncu C. & Iana V. (2014) S-box design based on chaotic maps combination. In 2014 10th International Conference on Communications (COMM), pages 1–4.

Rodriguez-Henriquez F., Saqib N.A., Díaz A., & Koc CK. (2007) Cryptographic Algorithms on Reconfigurable Hardware. US: Springer.

Srebrny M., Kościelny C. & Kurkowski M. (2013) Modern Cryptography Primer, Theoretical Foundations and Practical Applications. Springer-Verlag Berlin Heidelberg, 1 edition.

synopsys. (2003) HSPICE Simulation and Analysis User Guide.

Thomson K, Siva. N, & Priya S. (2014) Implementation of low-area s-box based on normal basis. In 2014 International Conference on Electronics and Communication Systems (ICECS), pages 1–4.

Yang M., Wang Z., Meng Q., & Han L. (2011) Evolutionary design of s-box with cryptographic properties. In 2011 IEEE Ninth International Symposium on Parallel and Distributed Processing with Applications Workshops, pages 12–15.

Zhang X., Chen F., Chen B., & Cao Z. (2015) A new scheme for implementing s-box based on neural network. In 2015 International Conference on Computational Science and Computational Intelligence (CSCI), pages 571–576.

Notas biográficas:

Jaime David Rios Arrañaga received the B. degree in Eng. in communications and electronics in 2014, currently pursuing a M.Sc. degree in electronics and computer science engineering at the University of Guadalajara. His current research is on cryptographic systems in reconfigurable hardware.

Janneth Alejandra Salamanca Chavarin received the B. degree in Eng. In communications and electronics in 2014, currently pursuing a M.Sc. degree in electronics and computer science engineering at the University of Guadalajara. Her current research interest is biological neural networks.

Juan José Raygoza Panduro Ph.D. in Computer Science and Telecommunications from Autonomous University of Madrid, Spain. He specializes in the design of digital architecture based on FPGAs, Microprocessors, VLSI, embedded system and bioelectronics, Neuroengineering. Research Professor at University of Guadalajara.

Edwin C. Becerra Alvarez Ph.D. degree in Microelectronics from University of Seville, Spain. His current research interests are on integrated CMOS design, transceiver design and embedded systems. Research Professor at CUCEI; University of Guadalajara