ISSN 2531-2952

Volumen 3, Número 11 – Julio – Septiembre - 2019

Revista de Cómputo Aplicado

Revista de Cómputo Aplicado, Volumen 3, Número 11, de Julio a Septiembre - 2019, es una revista editada trimestralmente por ECORFAN-Spain. Calle Matacerquillas 38, CP: 28411. Moralzarzal -Madrid. WEB: www.ecorfan.org/spain, revista@ecorfan.org. Editor en Jefe: ALDIVIA - ALTAMIRANO, William Fernando. PhD. ISSN-2531-2952. Responsables de la última actualización de este número de la Unidad de Informática ECORFAN. ESCAMILLA-BOUCHÁN, Imelda, LUNA-SOTO, Vladimir, actualizado al 30 de Septiembre 2019.

Revista de Cómputo Aplicado

Definición del Research Journal

Objetivos Científicos

Apoyar a la Comunidad Científica Internacional en su producción escrita de Ciencia, Tecnología en Innovación en el Área de Ingeniería y Tecnología, en las Subdisciplinas Teoría de Sistemas, Redes, Interconectividad de Empresas, Gobierno Corporativo, Comunicación por satélite, Conectividad, Emisores de tv y transmisión, Enlaces de microondas, Radio comunicaciones y receptores de radio, Radiocomunicación, Receptores de radio, Receptores de TV, Telefonía, Transmisores de radio y TV.

ECORFAN-México S.C es una Empresa Científica y Tecnológica en aporte a la formación del Recurso Humano enfocado a la continuidad en el análisis crítico de Investigación Internacional y está adscrita al RENIECYT de CONACYT con número 1702902, su compromiso es difundir las investigaciones y aportaciones de la Comunidad Científica Internacional, de instituciones académicas, organismos y entidades de los sectores público y privado y contribuir a la vinculación de los investigadores que realizan actividades científicas, desarrollos tecnológicos y de formación de recursos humanos especializados con los gobiernos, empresas y organizaciones sociales.

Alentar la interlocución de la Comunidad Científica Internacional con otros centros de estudio de México y del exterior y promover una amplia incorporación de académicos, especialistas e investigadores a la publicación Seriada en Nichos de Ciencia de Universidades Autónomas - Universidades Públicas Estatales - IES Federales - Universidades Politécnicas - Universidades Tecnológicas - Institutos Tecnológicos Federales - Escuelas Normales - Institutos Tecnológicos Descentralizados - Universidades Interculturales - Consejos de CyT - Centros de Investigación CONACYT.

Alcances, Cobertura y Audiencia

Revista de Cómputo Aplicado es un Research Journal editado por ECORFAN-México S.C en su Holding con repositorio en Spain, es una publicación científica arbitrada e indizada con periodicidad trimestral. Admite una amplia gama de contenidos que son evaluados por pares académicos por el método de Doble-Ciego, en torno a temas relacionados con la teoría y práctica de la Teoría de Sistemas, Redes, Interconectividad de Empresas, Gobierno Corporativo, Comunicación por satélite, Conectividad, Emisores de tv y transmisión, Enlaces de microondas, Radio comunicaciones y receptores de radio, Radiocomunicación, Receptores de radio, Receptores de TV, Telefonía, Transmisores de radio y TV con enfoques y perspectivas diversos, que contribuyan a la difusión del desarrollo de la Ciencia la Tecnología e Innovación que permitan las argumentaciones relacionadas con la toma de decisiones e incidir en la formulación de las políticas internacionales en el Campo de las Ciencias de Ingeniería y Tecnología. El horizonte editorial de ECORFAN-México® se extiende más allá de la academia e integra otros segmentos de investigación y análisis ajenos a ese ámbito, siempre y cuando cumplan con los requisitos de rigor argumentativo y científico, además de abordar temas de interés general y actual de la Sociedad Científica Internacional.

Consejo Editorial

Comité Arbitral

Cesión de Derechos

El envío de un Artículo a Revista de Cómputo Aplicado emana el compromiso del autor de no someterlo de manera simultánea a la consideración de otras publicaciones seriadas para ello deberá complementar el Formato de Originalidad para su Artículo.

Los autores firman el Formato de Autorización para que su Artículo se difunda por los medios que ECORFAN-México, S.C. en su Holding Spain considere pertinentes para divulgación y difusión de su Artículo cediendo sus Derechos de Obra

Declaración de Autoría

Indicar el Nombre de 1 Autor y 3 Coautores como máximo en la participación del Articulo y señalar en extenso la Afiliación Institucional indicando la Dependencia.

Identificar el Nombre de 1 Autor y 3 Coautores como máximo con el Número de CVU Becario-PNPC o SNI-CONACYT- Indicando el Nivel de Investigador y su Perfil de Google Scholar para verificar su nivel de Citación e índice H.

Identificar el Nombre de 1 Autor y 3 Coautores como máximo en los Perfiles de Ciencia y Tecnología ampliamente aceptados por la Comunidad Científica Internacional ORC ID - Researcher ID Thomson - arXiv Author ID - PubMed Author ID - Open ID respectivamente

Indicar el contacto para correspondencia al Autor (Correo y Teléfono) e indicar al Investigador que contribuye como primer Autor del Artículo.

Detección de Plagio

Todos los Artículos serán testeados por el software de plagio PLAGSCAN si se detecta un nivel de plagio Positivo no se mandara a arbitraje y se rescindirá de la recepción del Articulo notificando a los Autores responsables, reivindicando que el plagio académico está tipificado como delito en el Código Penal.

Proceso de Arbitraje

Todos los Artículos se evaluarán por pares académicos por el método de Doble Ciego, el arbitraje Aprobatorio es un requisito para que el Consejo Editorial tome una decisión final que será inapelable en todos los casos. MARVID® es una Marca de derivada de ECORFAN® especializada en proveer a los expertos evaluadores todos ellos con grado de Doctorado y distinción de Investigadores Internacionales en los respectivos Consejos de Ciencia y Tecnología el homologo de CONACYT para los capítulos de America-Europa-Asia-Africa y Oceania. La identificación de la autoría deberá aparecer únicamente en una primera página eliminable, con el objeto de asegurar que el proceso de Arbitraje sea anónimo y cubra las siguientes etapas: Identificación del Research Journal con su tasa de ocupamiento autoral - Identificación del Autores y Coautores- Detección de Plagio PLAGSCAN - Revisión de Formatos de Autorización y Originalidad-Asignación al Consejo Editorial- Asignación del par de Árbitros Expertos- Notificación de Dictamen-Declaratoria de Observaciones al Autor-Cotejo de Artículo Modificado para Edición-Publicación.

Instrucciones para Publicación Científica, Tecnológica y de Innovación

Área del Conocimiento

Los trabajos deberán ser inéditos y referirse a temas de Teoría de Sistemas, Redes, Interconectividad de Empresas, Gobierno Corporativo, Comunicación por satélite, Conectividad, Emisores de tv y transmisión, Enlaces de microondas, Radio comunicaciones y receptores de radio, Radiocomunicación, Receptores de radio, Receptores de TV, Telefonía, Transmisores de radio y TV y a otros temas vinculados a las Ciencias de Ingeniería y Tecnología

Presentación del Contenido

Como primer artículo presentamos, *Control de brazo robótico clasificador mediante HMI y servidor Web*, por LUNA -PUENTE, Rafael, PERÉZ-CHIMAL, Rosa Janette, HERNÁNDEZ – MOSQUEDA, Carlos y MUÑOZ-MINJAREZ, Jorge Ulises, con adscripción en la Universidad Tecnológica de Salamanca, como segundo artículo presentamos, *Herramienta para la enseñanza de la lengua Mazateca basada en Realidad Aumentada*, por MOTA-CARRERA, Luis Cresencio, MÁRQUEZ-DOMÍNGUEZ, José Alberto, SABINO-MOXO, Beatriz Adriana y SÁNCHEZ-ACEVEDO, Miguel Ángel, con adscripción en la Universidad de la Cañada, como tercer artículo presnetamos, *Cómputo en la niebla aplicado a la manufactura inteligente bajo el contexto de la industria 4.0: Desafíos y oportunidades*, por ALONSO-CALPEÑO, Mariela Juana, SANTANDER-CASTILLO, Julieta, RAMÍREZ-CHOCOLATL, Yuridia y ALANIS-TEUTLE, Raúl, con adscripción en el Instituto Tecnológico Superior de Atlixco, como último artículo presentamos, *Criptografía basada en curvas elípticas*, por RAMÍREZ-HERNÁNDEZ, Héctor David, CONTRERAS-JUÁREZ, Roberto, ESPINOZA-HERNÁNDEZ, Nelva Betzabel y SÁNCHEZ-MENDOZA, Eduardo, cpon adscripción en la Benemérita Universidad Autónoma de Puebla.

Contenido

Artículo **Revista de Cómputo Aplicado**
Septiembre 2019 Vol.3 No.11 1-7

Control de brazo robótico clasificador mediante HMI y servidor Web

Control of robotic arm classifier using HMI and Web server

LUNA -PUENTE, Rafael†*, PERÉZ-CHIMAL, Rosa Janette, HERNÁNDEZ –MOSQUEDA, Carlosy MUÑOZ-MINJAREZ, Jorge Ulises

Universidad Tecnológica de Salamanca, Av. Universidad Tecnológica #200, Ciudad Bajío, Salamanca, Gto. C.P. 36766

ID 1er Autor: *Rafael, Luna -Puente* / **ORC ID**: 0000-0002-9909-2530, **Researcher ID Thomson**: V-6510-2018, **CVU CONACYT ID**: 507896

ID 1er Coautor: *Rosa Janette, Peréz-Chimal* / **ORC ID**: 0000-0002-9294-533X, **Researcher ID Thomson**: V-6530-2018, **CVU CONACYT ID**: 290119

ID 2do Coautor: *Carlos, Hernández –Mosqueda* / **ORC ID**: 0000-0001-6120-9308, **Researcher ID Thomson**: V-6533-2018, **CVU CONACYT ID**: 241514

ID 3er Coautor: *Jorge Ulises, Muñoz-Minjarez* / **ORC ID**: 0000-0001-8097-9551, **Researcher ID Thomson**: W-5465-2018, **CVU CONACYT ID**: 388890

DOI: 10.35429/JCA.2019.11.3.1.7 Recibido Junio 30, 2019; Aceptado Septiembre 30, 2019

Resumen

El uso de máquinas automatizadas y manipuladas con inteligencia artificial es cada vez más común para realizar tareas rutinarias dentro del ámbito industrial. El presente trabajo pretende mostrar la automatización de un brazo robótico, su monitoreo y control usando un servidor web y una pantalla Interface Hombre-Máquina (HMI). Para este trabajo se programó un brazo robótico MITSUBISHI para la clasificación de piezas basándose en su color Posteriormente, este sistema es monitoreado y controlado mediante el diseño de una página web y el diseño de una HMI creada usando el software TIA-Portal. Como resultado de esta metodología se obtendrá un sistema completo de la industria 4.0, el cual puede ser implementado para controlar y monitorear un brazo robótico mediante pantalla HMI y Servidor Web en la industria actual. Los sistemas empleados para la realización del control fue un PLC S300 (cpu313C 2 DP) con tarjeta de Red ASI CP 343 2 DP, con 5 esclavos, Botonera (Esclavo 1) Modulo 2DI (Esclavo 2), Sensor Optoreflexivo (Esclavo 3) Conjunto de válvulas FESTO (Esclavo 4) Módulos 2DI 2DO (Esclavo 5) 2DO un PLC S1200 (CPU 1214 C DC/DC/DC) una pantalla HMI (KTP600 Basic Mono DP) la cual se empleó como clasificados de color.

Brazo robótico, Servidor Web, HMI

Abstract

The use of automated machines and its manipulation using artificial intelligence is increasingly common to perform routine tasks within the industrial field. The present work aims to show the automation of a robotic arm, its monitoring and control using a web server and a Human Machine Interface (HMI) screen. For this work a robotic arm MITSUBISHI was programmed for the classification of pieces based on their color. Subsequently, this system is monitored and controlled employing the programming of a web page and the design of an HMI created using the TIA-Portal software. As a result of this methodology, a complete system of industry 4.0 will be obtained, which can be implemented to control and monitor a robotic arm using a HMI screen and Web Server in the current industry. The systems used to carry out the control were a PLC S300 (cpu313C 2 DP) with ASI CP 343 2 DP network card, with 5 slaves, Keypad (Slave 1) Module 2DI (Slave 2), Optoreflexive Sensor (Slave 3) Set of valves FESTO (Slave 4) Modules2DI 2DO (Slave 5) 2DO an S1200 PLC (CPU 1214 C DC / DC / DC) an HMI screen (KTP600 Basic Mono DP) as color sort.

Robotic arm, Web Server, HMI

Citación: LUNA -PUENTE, Rafael, PERÉZ-CHIMAL, Rosa Janette, HERNÁNDEZ –MOSQUEDA, Carlos y MUÑOZ-MINJAREZ, Jorge Ulises. Control de brazo robótico clasificador mediante HMI y servidor Web. Revista de Cómputo Aplicado. 2019, 3-11: 1-7

† Investigador contribuyendo como primer autor.

Introducción

La integración de tecnologías en el sector industrial juega un papel muy importante en la actualidad con la implementación de la industria 4.0. La industria moderna requiere de métodos eficientes que sean capaces de realizar tareas rutinarias con el mínimo error, ya que estos representan grandes pérdidas financieras.

A causa de esta nueva revolución industrial surge la necesidad de automatizar y monitorear continuamente los procesos de producción. Para lograr esto se utilizan nuevas metodologías de reconocimiento de patrones, robótica, inteligencia artificial, monitoreo remoto, etcétera.

Los robots han causado gran interés en el mundo, cambiando de manera significativa el área de producción. Los brazos robóticos son un ejemplo de esta nueva gama de herramientas inteligentes, los cuales se utilizan para incontables tareas rutinarias, siendo la clasificación de objetos una de las más novedosas.

Además de los grandes avances en la instrumentación de procesos, se requiere de instrumentos de control y monitoreo remoto. Es común que los procesos industriales sean monitoreados y controlados usando internet, debido a que su cobertura es cada vez mayor y su velocidad se incrementa de igual manera.

Hoy en día existen dispositivos electrónicos capaces de realizar tareas bajo un lenguaje de programación básico y que poseen propiedades de conectividad mediante un servidor web. Ejemplo de estos dispositivos son los controladores lógicos programables (PLC por sus siglas en inglés), los cuales son ampliamente usados en actividades industriales por su robustez y facilidad de uso.

La integración de las tecnologías descritas anteriormente genera sistemas eficientes y precisos para realizar tareas específicas. Por ello en este trabajo se describe el sistema que consta de una pantalla HMI, que envía las condiciones de operación al PLC para que el brazo robótico clasifique las piezas en función de su color, así como una página web que nos permite forzar las señales de control sin necesidad de emplear la pantalla HMI.

Primero se presenta la etapa de programación del brazo robótico, la página web y el PLC. Enseguida se muestran los parámetros de calibración y ajustes necesarios para el funcionamiento óptimo de los sensores de detección de color. Después se presenta el funcionamiento de la integración del brazo robótico, el PLC, el HMI y el monitoreo por servidor web. Finalmente se presentan los resultados y conclusiones

Programación

La programación de los componentes para el desarrollo de la metodología propuesta es fundamental para su acoplamiento. En la etapa de programación se pueden apreciar los códigos utilizados para cada uno de los sistemas en sus respectivos softwares: el brazo robótico, la página web, el PLC y la HMI.

Programación del Brazo MITSUBISHI

La programación del brazo MITSUBISHI se realizó mediante la programación Melfa Basic IV, que es un lenguaje estructurado basado en una lista de instrucciones y condiciones, tales como IF, GOTO, MVS y MOV.

La secuencia creada (mirar Tabla 1 del Anexo) se determina las condiciones del tipo de pieza que se desea clasificar. La clasificación se basa en cuatro casos fundamentales si las piezas son negras, rojas, azules. Para esto se implementa un módulo de entradas digitales que permite el condicionamiento de los movimientos del robot.

Programación de Pagina WEB

El desarrollo de la página web para monitorear de manera remota, el proceso de selección se realizó con la ayuda de Notepad++. La página web presenta 8 señalizaciones: sensor on, sensor off, negras on, negras off, roja on, roja off, desechar on y desechar off.

Estas señalizaciones arrojaran información del correcto arranque del sensor, y el color detectado por el mismo. En la Tabla 2 del anexo se describe detalladamente la parte principal del código para generar la página web, cabe resaltar que se pueden generalizar estas líneas de código para obtener los casos faltantes. La imagen de la Figura 1 muestra la interfaz de la página web programada.

ISSN-2531-2952

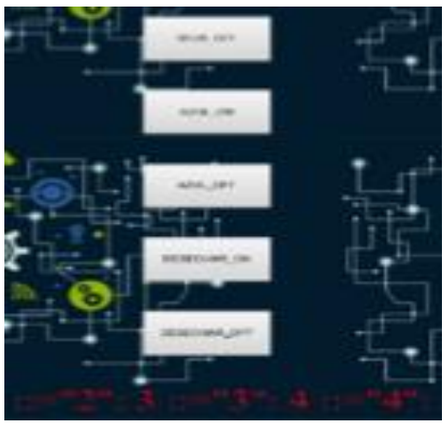
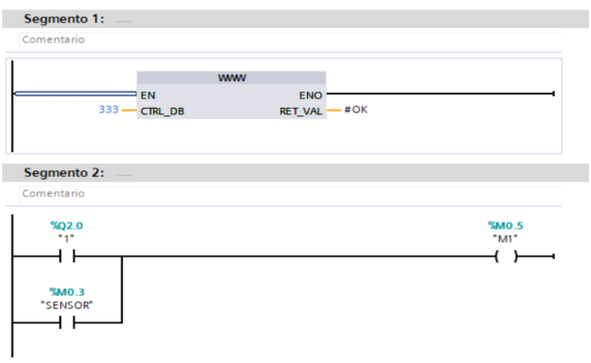


Figura 1 Pagina web para en monitoreo de arranque de la diferentes condiciones de color

Programación del PLC

Para lograr enviar la información hacia la página web se requiere de un dispositivo con las características adecuadas para realizar esta tarea. Por esta razón se optó por utilizar un PLC 1214C DC/DC/DC de siemens, el cual posee una herramienta capaz de enlazar un proceso a una página web.

Con la ayuda del TIA Portal V13 se realizó la programación y el llamado de la página web creada anteriormente. La Figura 2 muestra la programación en escalera en TIA Portal para el monitoreo de las variables del sensor mediante la página web. Para esto se requirió del bloque especial llamado "*www*" y un conjunto de interruptores y bobinas. Cabe señalar que las variables monitoreadas de manera remota son almacenadas en el PLC como variables de memoria %M0.0, %M0.1…%M0.7 para cada uno de los casos expuestos, que representan las rutinas de trabajo en función del color de la pieza que se desea clasificar.



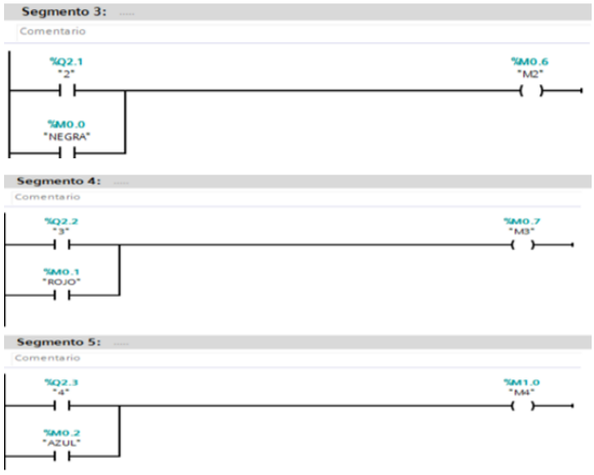


Figura 2 Programación en TIA Portal para el enlace de las variables de selección de colores mediante la página web

Programación de HMI

Además del monitoreo remoto usando un servidor web, se propuso utilizar un monitoreo local mediante una pantalla HMI. Esto con el objetivo de corroborar los datos mostrados por las dos interfaces y así localizar los errores generados por el sistema de manera rápida.

La pantalla de control fue programada desde la misma plataforma que el PLC, con el programa TIA Portal V13. Para el desarrollo de esta interfaz se crearon 5 indicadores, los cuales se activarían de acuerdo con el caso detectado por el sensor. En la Figura 3 se puede observar cada uno de los indicadores programados como animaciones según corresponda el caso para la pieza detectada: NEGRA, ROJA, AZUL O DESECHADA.

Figura 3 Pantalla HMI para el monitoreo de arranque del sensor y la variable detectada por el mismo

ISSN-2531-2952

Etapa II Calibración y Ajustes

La calibración se los sensores se realizó en campo, donde se encontraba el brazo robótico, el cual clasifica las piezas en función de su color.

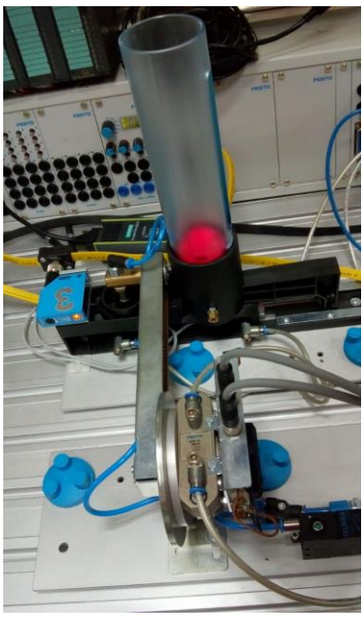


Figura 4. Ajuste de la válvula de vacío, para garantizar la sujeción de las piezas.

Como se puede apreciar en la figura 4 se muestra el sistema de Pick and Place de la Red ASI. Asi como el alimentador de piezas por gravedad empleado para el traslado de las fichas de trabajo hacia el Brazo robótico

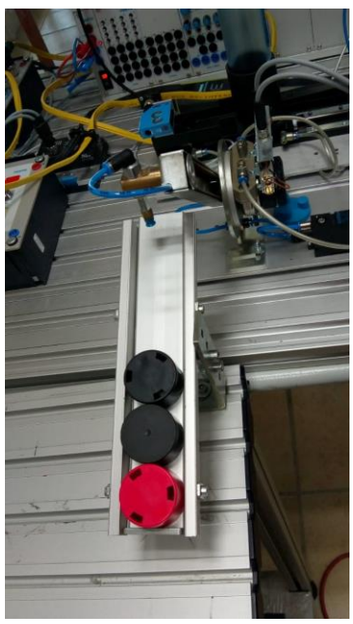
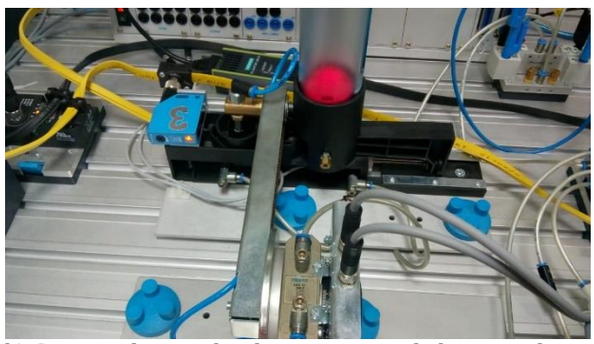


Figura 5 Alimentador de Red ASI, basado en un sistema de Pick And Place

La figura 5 se aprecia la rampa de alimentación, donde el sistema Pick And Place posiciona la pieza en el área de trabajo del Robot

a) Implementación de un PLC S300 con comunicación MPI y tarjeta de Red ASI



b) Sistema alimentador de piezas controlado por esclavos de en Red ASI, "Sistema Pick And Place"

Figura 6 Sistema de Red ASI a) y b)

Sistema de red ASI mediante un PLC S313C-2 DP y una tarjeta de Red CP 343 2 DP Fig. 6 (a), el cual controla 4 esclavos Fig. 6 (b)

Figura 7 Comunicación Pantalla HMI y PLC S1200, pruebas de forzado de variables de salida

Una vez relaizada la programación se procedioa realizar el forzado de las variables de salida del PLC S1214 C DC/DC/DC, así como la puesta en marcha mediante la Pantalla HMI KTP600 Basic Mono PN.

ISSN-2531-2952

Etapa III Puesta en Marcha

En esta etapa se logró realizar la puesta en marcha el sistema de control empleando los componentes de la RED ASI, La pantalla Monocromatica, el PLC S300 y el PLC S1200. Consiste en la integración de los dispositivos probados por separados, así como la sincronización de los elementos de trabajo y los elementos de control.

Figura 8 Selelección de piezas de trabajo, en relación a su color en base a la pantalla HMI

El Brazo selecciona las piezas de trabajo obtenida de la rampa de alimentación hacia el área de selección de color, la cual mediante la pantalla KTP600 Basic Mono PN se asigna el color de la pieza.

Figura 9 Clasificación de fichas, una vez que el Robot sabe el color de la pieza de trabajo se clasifica en los contenedores asignados

Una vez que el brazo robótico identifico la pieza a través de la pantalla se realiza la ubicación de la misma mediante los contenedores asignados por el usuario que realizo la programación.

Figura 10 Implementación de Pantalla HMI, para el forzado directo de señales digitales

Con la ayuda de la Pantalla KTP 600 se puede asignar el color de las piezas de trabajo, además cabe señalar que se realizó la misma prueba mediante la página web obteniendo los mismos resultados de operación del robot.

Figura 10 El sistema cuenta con sensores de presencia que permiten mantener en espera “stand by”

El esclavo 3 de pieza en posición (Sensor Optoreflexibo) señala que el alimentador se vació y en sistema entra en reposo esperando que llegaren más piezas para realizar de nueva cuenta el proceso.

Resultados

La programación del brazo robótico MITSUBISHI realizó los movimientos indicados y la clasificación correcta de cada una de las piezas proporcionadas. La pantalla HMI genero los mismos resultados que los de la página web, corroborando así su eficiente funcionamiento. Con respecto a la programación del PLC, el código escalera diseñado funcionó de manera correcta enlazando exitosamente las variables asignadas con las señalizaciones de ambas interfaces a distancia (Servidor WEB) y en piso (Mediante la pantalla HMI).

ISSN-2531-2952

Finalmente, el sistema completo se pudo integrar para manipular el brazo robótico MITSUBISHI mediante una página WEB realizando la secuencia requerida, corroborando los datos con una pantalla HMI.

Anexos

```
10 *INICIO
20 MOV P5
30 HOPEN 1
40 DLY 0.5
50 MOV P1, -100
60 MVS P1
70 HCLOSE 1
80 DLY 0.5
90 MVS P1, -100
100 MOV P5
110 IF M_IN (0) = 1 THEN *NEGRO
120 IF M_IN (1) = 1 THEN *ROJO
130 IF M_IN (2) = 1 THEN *AZUL
140 IF M_IN (3) =1 THEN *DESECHA
150 GOTO *INICIO
160 *NEGRO
170 MOV P2, -100
180 MVS P2
190 HOPEN 1
200 DLY 0.5
210 MVS P2, -100
220 GOTO *INICIO
230 *ROJO
240 MOV P3, -100
250 MVS P3
260 HOPEN 1
270 DLY 0.5
280 MVS P3, -100
290 GOTO *INICIO
300 *AZUL
310 MOV P4, -100
320 MVS P4
330 HOPEN 1
340 DLY 0.5
350 MVS P4, -100
360 GOTO *INICIO
370 *DESECHA
380 MOV P5, -100
390 MVS P5
400 HOPEN 1
410 DLY 0.5
420 MVS P5, -100
430 GOTO *INICIO
```

Tabla 1 Programación realizada en Melfa Basic IV para la programación del brazo robótico MITSUBISHI

```
<!DOCTYPE html>
<!-- AWP_In_Variable Name="'1"' -->
<!-- AWP_In_Variable Name="'2"' -->
<!-- AWP_In_Variable Name="'3"' -->
<!-- AWP_In_Variable Name="'4"' -->
<!-- AWP_In_Variable Name="'5"' -->
<html lang="esp"
<head>
<meta charset="gtf-8">
   <title>CONTROL DE CALIDAD</title>
</head>
<body>
<body
background="imagenes/muro.jpg"/>
 <img src="imagenes/logo raccoons.png" width="350"
height="250" align="left"/>
 <center> <font color="red"> <font
size=7><h1>Control Linea de Calidad</h1><center/>
  <center> <img src="imagenes/images.jpg"
width="600" height="350"/><center/>
   <form>
          <p>
            <input type="submit"
value="SENSOR_ON" style='width:150px;
height:75px'>
                  <input type="hidden" name="'1"'
value="1">
          </p>
   </form>
           <form>
          <p>
            <input type="submit"
value="SENSOR_OFF" style='width:150px;
height:75px'>
                  <input type="hidden" name="'1"'
value="0">
          </p>
   </form>
          <form>
          <p>
                  <input type="submit"
value="NEGRA_ON" style='width:150px;
height:75px'>
                  <input type="hidden" name="'2"'
value="1">
          <p>
          </form>
           <form>
          <p>
            <input type="submit"
value="NEGRA_OFF" style='width:150px;
height:75px'>
                  <input type="hidden" name="'2"'
value="0">
          </p>
   </form>
          <form>
```

Tabla 2 Programación de la página web para el monitoreo remoto del sensor detector de colores

ISSN-2531-2952

Conclusiones

Con la implementación de este sistema los alumnos de la carrera de Mecatrónica y Procesos Industriales podrán analizar y conocer el procedimiento en la automatización de procesos los cuales pueden ser implementados en diversas áreas. Además, los alumnos adquirieron los conocimientos básicos de la industria 4.0, siendo esta una tendencia actual que está generando nuevos retos en el área de automatización, monitoreo y control.

Referencias

Baturone, A. O. (2005). Robótica: manipuladores y robots móviles. Marcombo.

Creus, A. (2014). *Instrumentación Industrial 8° Editorial.* Alfaomega.

FESTO. (1993). *Fundamentos de Robótica.* Esslinger: H. Dahlhoff.

Fran Yañes. (2017). *INDUSTRIA 4.0 (E-Book) IS. Editorial* AUTOR-EDITOR. ISBN cdlap00008977

Jouaneh, M. (2017). *Fundamentos de Mecatrónica. Editorial.* CENGAGE.

JOYANES, Luis. (2017). *INDUSTRIA 4.0 - La cuarta revolución industrial. Editorial* Alfaomega.

Yuste, R. L. (2009). *Comunicaciones ndustriales. Editorial*. Alfaomega.

ISSN-2531-2952

Artículo **Revista de Cómputo Aplicado**
Septiembre 2019 Vol.3 No.10 8-15

Herramienta para la enseñanza de la lengua Mazateca basada en Realidad Aumentada

Tool for the teaching of the Mazatec language based on Augmented Reality

MOTA-CARRERA, Luis Cresencio†, MÁRQUEZ-DOMÍNGUEZ*, José Alberto, SABINO-MOXO, Beatriz Adriana y SÁNCHEZ-ACEVEDO, Miguel Ángel

Universidad de la Cañada (UNCA), Oaxaca, México

ID 1er Autor: *Luis Cresencio, Mota-Carrera* / **ORC ID:** 0000-0001-9427-5002, **CVU CONACYT ID:** 999991

ID 1er Coautor: *José Alberto, Márquez-Domínguez* / **ORC ID:** 0000-0003-2552-2289, **CVU CONACYT ID:** 210472

ID 2do Coautor: *Beatriz Adriana, Sabino-Moxo* / **ORC ID:** 0000-0002-8577-494X, **CVU CONACYT ID:** 210495

ID3er Coautor: *Miguel Ángel, Sánchez-Acevedo* / **ORC ID:** 0000-0002-0996-0038, **CVU CONACYT ID:** 205720

DOI: 10.35429/JCA.2019.11.3.8.15 Recibido Mayo 30, 2019; Aceptado Agosto 30, 2019

Resumen

En este trabajo se presenta una herramienta para la enseñanza de la lengua mazateca basado en la tecnología de Realidad Aumentada (RA), dirigido a los profesores del centro de educación preescolar indígena *Naxhó* Café, ubicada en la población de Huautla de Jiménez, Oaxaca. El proyecto fue desarrollado con la metodología de Desarrollo Centrado en el Usuario (DCU), esta metodología permitió llevar a cabo dos actividades de enseñanza con alumnos de primer, segundo y tercer año de preescolar obteniendo resultados considerables en la eficiencia, eficacia y satisfacción de dicha herramienta.

Mazateca, UCD, Realidad aumentada

Abstract

This paper presents a tool for teaching the Mazatec language based on Augmented Reality (RA) technology, aimed at teachers at the Naxhó Café indigenous preschool education center, located in the town of Huautla de Jiménez, Oaxaca. The project was developed using the methodology of User Center Desing (DCU), this methodology allowed to carry out two teaching activities with students of first, second and third year of preschool with which they could obtain considerable results in efficiency, efficiency and satisfaction of said tool.

Mazatec, UCD, Augmented Reality

Citación: MOTA-CARRERA, Luis Cresencio, MÁRQUEZ-DOMÍNGUEZ, José Alberto, SABINO-MOXO, Beatriz Adriana y SÁNCHEZ-ACEVEDO, Miguel Ángel. Herramienta para la enseñanza de la lengua Mazateca basada en Realidad Aumentada. Revista de Cómputo Aplicado. 2019, 3-11: 8-15

* Correspondencia al Autor (Correo electrónico: albertomarquez@unca.edu.mx)
† Investigador contribuyendo como primer Autor.

Introducción

Lengua materna, también conocida como primera lengua es el que una persona aprende y adquiere en primera instancia dentro del entorno inmediato en el cual crece y se desenvuelve (Galdames *et al*., 2006).

Datos del INALI (Instituto Nacional de Lenguas Indígenas) proporciona información del grado de desaparición de la lengua Mazateca, en el año 2010 había 20.3% de hablantes mazatecos y en el 2015 se redujo al 15.6%, es por ello la importancia de establecer herramientas educativas que apoyen en la conservación, difusión y promoción de las lenguas maternas.

De acuerdo a la Secretaria de Cultura de México, hasta el año 2018 se contemplaban registros de 7,000 idiomas alrededor del mundo, de los cuales, casi el 50 por ciento se encuentra en peligro de desaparecer. México ocupa un segundo lugar entre las primeras 10 naciones de América Latina con mayor riqueza y diversidad lingüística contando con 69 lenguas nacionales -68 indígenas y el español- (Secretaría de Cultura, 2018).

Tal como lo señala El Programa Especial de los Pueblos Indígenas (2014-2018), las comunidades hablantes de alguna lengua indígena se enfrentan a serios problemas tales como la discriminación, estigmatización, migración, globalización, poco o nulo involucramiento de las instituciones educativas para fomentar la conservación de las lenguas, entre otros, estos factores influyen en la pérdida directa o indirecta de las lenguas.

Ante este fenómeno, se vio una oportunidad para contribuir en el rescate de la lengua materna mazateca variante de Huautla de Jiménez, Oaxaca. En coordinación con profesores del centro indígena de educación preescolar bilingüe *Naxhó* Café se logró el desarrollo de materiales didácticos de enseñanza y una aplicación para dispositivos móviles que integra tecnología de realidad aumentada, con el objetivo de poner en sus manos una herramienta tecnológica para complementar el trabajo que realizan a través de la enseñanza del mazateco.

Desarrollo

A continuación, se describen los principales aspectos en el desarrollo de la herramienta para la enseñanza de la lengua materna mazateca.

Lengua materna mazateca de Huautla de Jiménez, Oaxaca

La lengua mazateca en el estado de Oaxaca se habla en municipios y localidades que se encuentran en las regiones de la montaña en la parte alta, región de la Cañada, y de la zona baja que corresponde a la región de la Cuenca del Papaloapan (Guzmán, 2011).

Los mazatecos se autodenominan *Ha shuta Enima*, que en su lengua quiere decir "los que trabajamos el monte, humildes, gente de costumbre". Según otros autores, el origen del nombre mazateco viene del náhuatl mazatecatl, o "gente del venado", nombre que les fue dado por los nonoalcas debido al gran respeto que tenían por el venado (INPI, 2017).

Las TIC en el rescate de las lenguas maternas

Tal como lo señala la UNESCO, las tecnologías de la información y comunicación se consideran factores estratégicos para ampliar la funcionalidad de las lenguas indígenas, ya que permiten potenciar su uso en diferentes entornos y su aprovechamiento puede ser dirigido al desarrollo social, académico, institucional y comunicacional (PROINALI, 2014).

Dentro de las TIC se encuentra la realidad aumentada, aquella tecnología que permite percibir, ver y conectarnos con el mundo mediante el uso de dispositivos tecnológicos interactuando con un entorno virtual, donde es posible añadir al mundo físico información virtual tales como, objetos tridimensionales, video, audio, texto el cual permite explotar una gran variedad de beneficios (UNESCO, 2016).

Gracias al software libre existe una multitud de herramientas que permiten integrar tecnología de realidad aumentada en aplicaciones móviles. Para el trabajo a desarrollar se eligieron las siguientes:

ISSN-2531-2952

Pixabay.com

Es un sitio web con una comunidad de creativos que comparten imágenes sin derechos de autor. Todos los contenidos se publican bajo la Licencia Pixabay, que los hace seguros para usar sin pedir permiso o dar crédito al artista, incluso con fines comerciales.

Poly de Google

Poly es una biblioteca en línea donde las personas pueden navegar, compartir y mezclar activos 3D. Un activo es un modelo 3D o una escena creada con Tilt Brush, Blocks o cualquier programa 3D que genere un archivo que se pueda cargar en Poly. Muchos activos están autorizados bajo la licencia CC BY, lo que significa que los desarrolladores pueden usarlos en sus aplicaciones de forma gratuita, siempre que el creador reciba crédito (Poly-Google, 2019).

Blender

Es el paquete de creación 3D de código abierto y gratuito. Admite la totalidad de la canalización 3D: modelado, *rigging*, animación, simulación, renderización, composición y seguimiento de movimiento, incluso edición de video y creación de juegos (Blender, 2019).

Vuforia Engine

Es la plataforma más utilizada para el desarrollo de RA, con soporte para teléfonos, tabletas y gafas. Cuenta con SDK (Kit de Desarrollo de Software) que permite construir aplicaciones basadas en realidad aumentada (Vuforia Engine, 2019).

Unity 3D

Es una de las plataformas más amplias para el desarrollo de videojuegos siendo uno de los líderes en el manejo de tecnología de RA para dispositivos móviles (Unity 3D, 2019).

A continuación, se propone el desarrollo de la herramienta.

Desarrollo de la Herramienta

Para el desarrollo del proyecto se siguió la metodología de Diseño Centrado en el Usuario (DCU).

Figura 1 Etapas del Diseño Centrado en el Usuario. Ciclo Iterativo
Fuente: Garreta y Mor (2019)

Como lo indican los autores Garreta y Mor (2019), el objetivo del DCU es la creación de productos que los usuarios encuentren útiles y usables; es decir, que satisfagan sus necesidades teniendo en cuenta sus características. Empleando la metodología (Figura 1) permitió conocer y comprender las necesidades, limitaciones, comportamientos y características que tienen los profesores y alumnos del preescolar, para llevar a cabo la herramienta acorde a las necesidades específicas, involucrándolos en todo el proceso del desarrollo descritos en los siguientes puntos.

Investigación

La primera etapa que comprende la metodología DCU se abarcó mediante un estudio contextual llevado a cabo en las instalaciones del preescolar *Naxhó* Café con el objetivo de conocer la situación actual de la lengua materna mazateca desde la opinión de los profesores bilingües.

Como lo señalan los profesores, los trabajos que se han hecho a través de diversas actividades escolares y culturales, padres de familia y la comunidad han contribuido en la conservación de la identidad de todo el pueblo para revalorar, revitalizar y fortalecer la lengua y cultura mazateca. Sin embargo, falta mucho por trabajar y llevar a cabo más acciones que permitan la conservación de identidad cultural y lingüística de la comunidad, sobre todo en el aspecto educativo.

ISSN-2531-2952

Análisis

Derivado del estudio contextual se identificó que no existe ningún trabajo previo que vincule el uso de las TIC en la enseñanza de la lengua mazateca variante de Huautla de Jiménez, esto permitió fortalecer más la idea de contribuir en la labor de enseñanza del mazateco empleando las TIC.

Diseño

Continuando con la siguiente etapa de DCU, y con apoyo de los profesores de *Naxhó* Café se propusieron dos actividades acordes a las necesidades educativas y al contexto cultural de la educación indígena:

Tarjetas con reconocimiento de marcadores: es un conjunto de 24 tarjetas con representaciones gráficas de animales característicos de la región Cañada, éstos son marcadores que proporcionan información adicional a través de un modelo tridimensional con animación, audio en español, audio en mazateco y su respectivo nombre. A través de prototipos de baja y alta fidelidad se concretó el diseño de las tarjetas, como se muestra en la Figura 2.

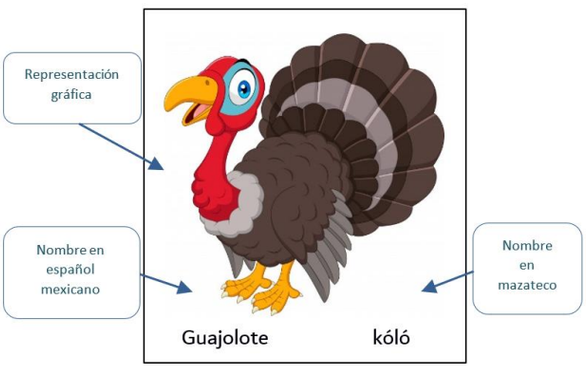


Figura 2 Tarjetas con reconocimiento de marcadores
Fuente: Elaboración Propia

Variante del juego de domino de formas empleando el alfabeto mazateco: similar a un juego de mesa de memorama, se diseñaron 53 marcadores que proporcionan el audio en español y audio en mazateco. Del mismo modo, a través de prototipos de baja y alta fidelidad se concretó el diseño de los marcadores de la Figura 3.

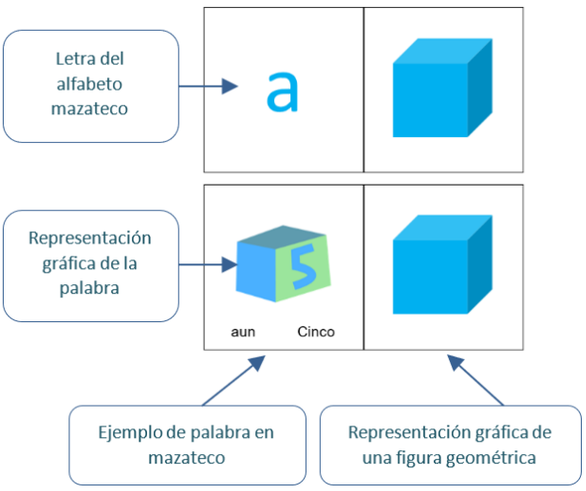


Figura 3 Variante del juego de domino de formas
Fuente: Elaboración Propia

Aplicación móvil: un aspecto inherente al desarrollo de cualquier producto o servicio debe ser la usabilidad, que se refiere a la capacidad de un producto en ser entendido, aprendido, usado y atractivo para el usuario, persiguiendo tres aspectos fundamentales:

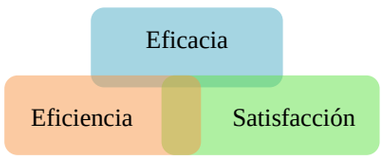


Figura 4 Aspectos de la usabilidad
Fuente: Elaboración Propia

Partiendo de los principios de la usabilidad, y con el análisis de la información recopilada se procedió al desarrollo de la aplicación para dispositivos móviles con sistema operativo Android.

A partir de un diseño de baja fidelidad hecho el papel, se realizó un bosquejo de la aplicación móvil (Figura 5) para ser evaluado y mejorado con la retroalimentación de los usuarios en las siguientes fases de la metodología DCU.

ISSN-2531-2952

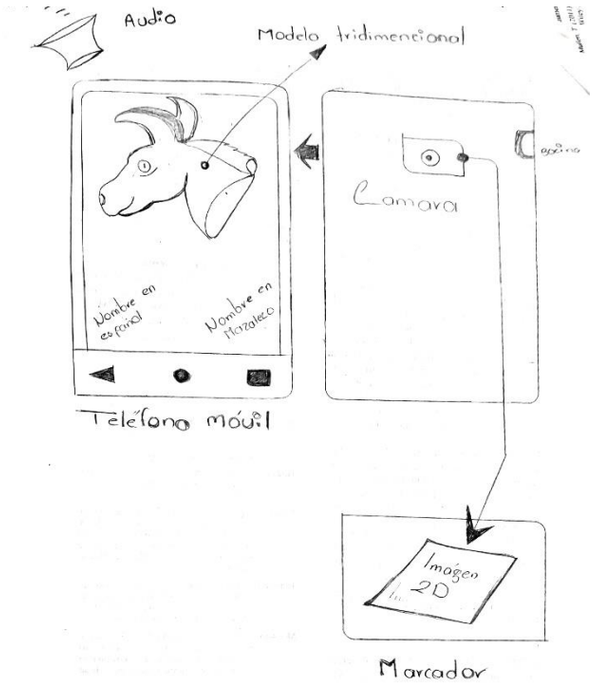


Figura 5 Bosquejo de la aplicación móvil

Evaluación

En la etapa de evaluación de la aplicación móvil se llevó acabo tres pruebas de usabilidad en las instalaciones de *Naxhó* Café, en diferentes sesiones con profesores y alumnos de primero, segundo y tercer grado.

Para cada dinámica se asignó diferentes tareas a los participantes, que deberían realizar con los estudiantes a su cargo.

Tarjetas con reconocimiento de marcadores:

- **Tarea 1:** enfocar la cámara trasera del dispositivo tecnológico hacia un activador de realidad aumentada.
- **Tarea 2:** escanear e identificar el objeto 3D mostrado en la aplicación móvil.
- **Tarea 3:** repetir el sonido emitido de la aplicación móvil.
- **Tarea 4:** pronunciar en voz alta la palabra en español mexicano y lengua materna mazateca respectivo al ejemplo proporcionado.

Tarjetas con reconocimiento de marcadores:

- **Tarea 1:** en un conjunto de 20 tarjetas sobrepuestas en una mesa, el usuario tiene que encontrar los pares iguales y ordenarlos.
- **Tarea 2:** enfocar la cámara trasera del dispositivo hacia un activador de realidad aumentada.
- **Tarea 3:** pronunciar en voz alta la palabra en español mexicano y lengua materna mazateca respectivo al ejemplo proporcionado.

El objetivo de cada sesión de prueba fue identificar los aspectos de usabilidad obteniendo resultados cualitativos y cuantitativos, además de determinar la satisfacción del participante. De esta manera, en cada iteración las herramientas fueron adaptándose acorde a las necesidades de los profesores.

Adaptación

Se hicieron tres pruebas de usabilidad, como se mencionó anteriormente. En la primera se proporcionó la herramienta usando una tableta para llevar a cabo la primera actividad (ver Figura 6 y Figura 7).

Figura 6 Primera pruebas de usabilidad, empleando las tarjetas con reconocimiento de marcadores

Figura 7 Primera pruebas de usabilidad, empleando las tarjetas con reconocimiento de marcadores

ISSN-2531-2952

Las observaciones de la primera prueba son los siguientes:

- La dificultad de manipular la tableta ya que se les hacía pesada a los niños al ir pasando por cada uno de los marcadores.
- Haber utilizado objetos tridimensionales demasiado grandes dificultaba la apreciación completa de cada una.
- Al enfocar la cámara a los marcadores y mostrar los modelos tridimensionales en el dispositivo, se confundía con los colores de fondo.
- El volumen de sonido de la tableta no era tan fuerte para ser escuchada correctamente los audios en un ambiente de ruido.
- Las mejoras que se realizaron en esta sesión fueron las siguientes:
- En lugar de una tableta, se propuso la utilización de un teléfono celular.
- Se colocó un fondo blanco a los objetos tridimensionales para una mejor visualización.
- Se redujeron de tamaño los objetos tridimensionales.
- La utilización de una bocina conectada al dispositivo tecnológico vía *bluetooth*, para contar con un nivel de volumen mayor (Figura 8).

Figura 8 Teléfono celular y bocina *bluetooth*

En una segunda sesión, realizando los cambios respectivos, la prueba de usabilidad se llevó a cabo mediante un teléfono celular (ver Figura 9 y Figura 10).

El tamaño del teléfono celular hacía mucho más fácil su manipulación, con la reducción de tamaño de los objetos tridimensionales y el fondo blanco se podían apreciar desde el ángulo de visión de los niños.

Figura 9 Segunda prueba de usabilidad, empleando las tarjetas con reconocimiento de marcadores

Figura 10 Segunda prueba de usabilidad, empleando las tarjetas con reconocimiento de marcadores

Las observaciones de la segunda prueba son los siguientes:

- La iluminación de los objetos tridimensionales era muy tenue.
- La forma de colocar las tarjetas con reconocimiento de imágenes influía en el aspecto visual de los usuarios para enfocar la cámara del teléfono celular.
- Los profesores sugirieron la posibilidad de ver el nombre del animal en la pantalla del dispositivo tecnológico dentro del espacio en blanco colocado.
- Las mejoras que se realizaron en esta sesión fueron las siguientes:
- Colocar mayor iluminación de los objetos tridimensionales.

ISSN-2531-2952

– Utilizar una base para colocar las tarjetas con reconocimiento de marcadores permitiendo mayor comodidad al momento de utilizar la herramienta.
– Y la colocación del nombre en texto tridimensional.
– En la última prueba de usabilidad, ya no se realizaron cambios en la herramienta para llevar a cabo ambas actividades.

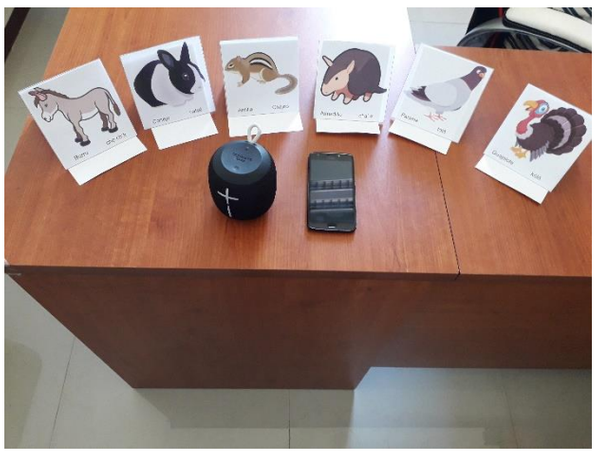


Figura 11 Tarjetas con reconocimiento de marcadores

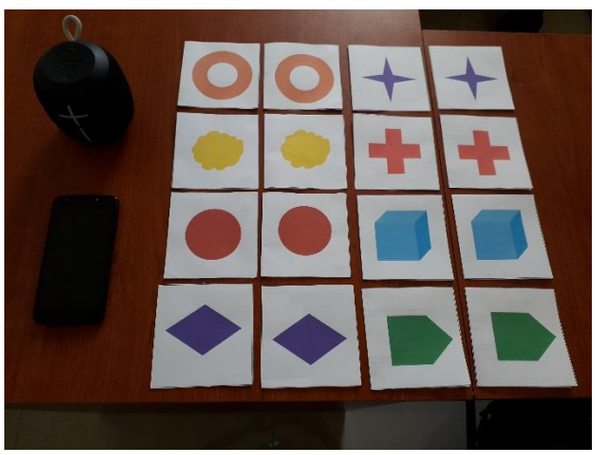


Figura 12 Variante del juego de domino de formas

Resultados

Recopilando los datos de las tres pruebas de usabilidad, llevada a cabo con profesores y alumnos de primer, segundo y tercer año de preescolar, en la Tabla 1 se muestran los resultados de aplicar la herramienta.

Pruebas de usabilidad	
Eficacia	Con el objetivo de saber si la herramienta cumple con el propósito para la cual fue diseñada, se midió el desempeño de las tareas mencionadas en la etapa de evaluación. Cumplimiento del 100% de las tareas asignadas a profesores y alumnos de la institución educativa empleando las herramientas.
Eficiencia	Para conocer el tiempo promedio para llevar a cabo las tareas mencionadas en la etapa de evaluación, se midieron en minutos las actividades a desempeñar por cada usuario. Un promedio de 5 minutos por cada 4 marcadores, utilizado las tarjetas con reconocimiento de marcadores. Un promedio de 5 minutos por cada 10 marcadores de la variante del juego de domino de formas.
Satisfacción	Al termino de cada actividad, a los usuarios profesores se les pidió asignar una calificación a la herramienta utilizada. En una escala del 1 al 10 se obtuvo una calificación promedio de 9.5 dada por los profesores del preescolar acorde a la utilización de la herramienta.

Tabla 1 Resultados de las tres pruebas de usabilidad
Fuente: Elaboración Propia

Referente a los aspectos de usabilidad con los resultados obtenidos en la Tabla 1, los profesores concluyeron que la herramienta es muy útil ya que abarca una nueva forma de enseñanza utilizando la tecnología de la RA y a los estudiantes se les hace atractivo y fácil de utilizar la herramienta.

Agradecimientos

A los profesores y alumnos del preescolar *Naxhó* Café por ser nuestros principales usuarios y colaboradores para llevar a cabo el presente trabajo.

A la licenciada Alejandrina Pedro Castañeda por la traducción de palabras del español al mazateco.

A la ciudadana Elvia Cerqueda Delgado, originaria de Huautla de Jiménez, por ayudarnos en la grabación de las palabras en mazateco y español.

A la Universidad de la Cañada por darme los medios y apoyo para acudir al preescolar y llevar a cabo las pruebas con las herramientas desarrolladas.

Conclusiones

A través del tratamiento informático de la lengua mazateca variante de Huautla de Jiménez para su almacenamiento, procesamiento y presentación con medios electrónicos como lo son los dispositivos móviles, se hace posible la documentación y conservación a través del tiempo.

ISSN-2531-2952

Como lo indican los profesores del preescolar, la herramienta que se les proporciono es de gran ayuda, ya que a los niños se les hace muy interesante y entretenido, a su vez, los diversos contenidos que se integraron coadyuvan en las dinámicas de enseñanza de la lengua Mazateca impartida por los educadores. Con lo anterior se puede deducir que un correcto enfoque y empleo de las TIC en el área educativa trae consigo grandes beneficios, más aún con el rescate de la lengua Mazateca.

Con el proyecto desarrollado se obtuvo una herramienta tecnológica que sirve para la enseñanza de la lengua materna mazateca y que es empleada en el centro de educación preescolar *Naxhó* Café, acercando a los niños al uso de la tecnología a través de la educación en el primer nivel de estudio escolar, a través de una educación supervisada y controlado por el docente.

Referencias

Blender (2019). Recuperado de: https://www.blender.org/about/

Carrera G. C. (2011). Acercamiento gramatical a la lengua mazateca de Mazatlán Villa de Flores, Oaxaca. México: Talleres Gráficos de México. Recuperado de: https://site.inali.gob.mx/pdf/libro_gramatica_mazateca.pdf

Galdames V., Walqui A. & Gustafson B. (2006). Enseñanza de lengua indígena como lengua materna. Bolivia: Editorial. Recuperado de: https://eib.sep.gob.mx/isbn/dl41105605.pdf

Garreta D, M & Mor P, E (2019). Diseño centrado en el usuario. PID_00176058. Recuperado de: https://www.exabyteinformatica.com/uoc/Informatica/Interaccion_persona_ordenador/Interaccion_persona_ordenador_(Modulo_3).pdf

Guzmán C, C. (2011). Acercamiento gramatical a la lengua mazateca de Mazatlán de Villa de Flores, Oaxaca. INALI. Recuperado de: https://site.inali.gob.mx/pdf/libro_gramatica_mazateca.pdf

INALI - Instituto Nacional de Lenguas Indígenas. (2015). Proyecto de indicadores sociolingüísticos de las lenguas indígenas nacionales. Recuperado de: https://site.inali.gob.mx/Micrositios/estadistica_basica/estadisticas2015/pdf/general/general7.pdf

INPI - Instituto Nacional de los Pueblos Indígenas (2017). Etnografía del pueblo mazateco de Oaxaca - Ha shuta Enima. https://www.gob.mx/inpi/articulos/etnografia-del-pueblo-mazateco-de-oaxaca-ha-shuta-enima
PROINALI - Programa Institucional del Instituto Nacional de Lenguas Indígenas (2014). Recuperado de: https://site.inali.gob.mx/publicaciones/Proinali_2014.pdf

Programa Especial de los Pueblos Indígenas (2014 - 2018). Recuperado de: https://www.gob.mx/cms/uploads/attachment/file/32305/cdi-programa-especial-pueblos-indigenas-2014-2018.pdf

Pixabay (2019). Recuperado de: https://pixabay.com/
Poly-Google (2019). Recuperado de: https://poly.google.com/

Rigueros B, C. (2017). La realidad aumentada: lo que debemos conocer. Tecnología Investigación y Academia, 5(2), 257-261. Recuperado de https://revistas.udistrital.edu.co/ojs/index.php/tia/article/view/11278

Secretaría de Cultura. (21 de febrero de 2018). ¿Sabías que en México hay 68 lenguas indígenas, además del español? [Mensaje en un blog]. Recuperado de: https://www.gob.mx/cultura/articulos/lenguas-indigenas?idiom=es

Unity 3D (2019). Recuperado de: https://unity.com/solutions/mobile-ar
Vuforia Engine (2019). Recuperado de: https://engine.vuforia.com/engine

Artículo **Revista de Cómputo Aplicado**
Septiembre 2019 Vol.3 No.11 16-27

Cómputo en la niebla aplicado a la manufactura inteligente bajo el contexto de la industria 4.0: Desafíos y oportunidades

Fog computing applied to intelligent manufacturing in the Industry 4.0 context: Challenges and opportunities

ALONSO-CALPEÑO, Mariela Juana†*, SANTANDER-CASTILLO, Julieta, RAMÍREZ-CHOCOLATL, Yuridia y ALANIS-TEUTLE, Raúl

Instituto Tecnológico Superior de Atlixco

ID 1er Autor: *Mariela Juana, Alonso-Calpeño* / **ORC ID:** 0000-0001-7276-1923

ID 1er Coautor: *Julieta, Santander-Castillo* / **ORC ID:** 0000-0002-6998-471X

ID 2do Coautor: *Yuridia, Ramírez-Chocolatl* / **ORC ID**: 0000-0002-7840-098

ID 3er Coautor: *Raúl, Alanis-Teutle* / **ORC ID**: 0000-0003-1852-1149

DOI: 10.35429/JCA.2019.11.3.16.27 Recibido Abril 20, 2019; Aceptado Junio 30, 2019

Resumen

El cómputo en la nube ofrece una alta capacidad de procesamiento de datos a nivel de servidor, mientras que el cómputo en la niebla funciona utilizando los nodos en el borde de la red, lo que habilita el procesamiento de datos en tiempo real con baja latencia y ubicuidad mejorada, por lo que puede contribuir en aplicaciones del Internet Industrial de las Cosas (IIoT). En este artículo se exponen los desafíos técnicos que han surgido al implementar el IIoT, y cómo es que el paradigma del cómputo en la niebla está ayudando a resolver algunos de ellos. Para ello, se ha realizado una revisión de artículos científicos en las bases de datos Google Scholar, y Web of Science utilizando palabras clave. Los resultados muestran que hay diversos desafíos en lo que respecta a interoperabilidad, criticidad mixta, latencia, tolerancia a fallas, escalabilidad, Integración horizontal y vertical, seguridad funcional, los sistemas industriales heredados y, la eficiencia energética. Se reportan las principales tendencias para afrontar estos desafíos. Este artículo propone una serie de áreas de oportunidad para fines de investigación y desarrollo de posibles soluciones.

Internet Industrial de las cosas, Cómputo en la niebla, Industria 4.0

Abstract

Cloud computing offers high server-level data processing capacity, while fog computing works using nodes at the edge of the network, enabling real-time data processing with low latency and improved ubiquity, so it can contribute on Industrial Internet of Things (IIoT) applications. This article discusses the technical challenges that have arisen in implementing the IIoT, and how the fog computing paradigm is helping to solve some of them. For this, a review of scientific articles in the Google Scholar and Web of Science databases has been carried out using keywords. The results show that there are various challenges related to interoperability, mixed criticality, latency, fault tolerance, scalability, horizontal and vertical integration, functional safety, legacy industrial systems, and energy efficiency. The main trends to face these challenges are reported. This article proposes a series of opportunity areas for research and development of possible solutions.

Industrial Internet of things, Fog computing, Industry 4.0

Citación: ALONSO-CALPEÑO, Mariela Juana, SANTANDER-CASTILLO, Julieta, RAMÍREZ-CHOCOLATL, Yuridia y ALANIS-TEUTLE, Raúl. Cómputo en la niebla aplicado a la manufactura inteligente bajo el contexto de la industria 4.0: Desafíos y oportunidades. Revista de Cómputo Aplicado. 2019, 3-11: 16-27

† Investigador contribuyendo como primer Autor.
* Correspondencia del Autor (mariela.alonso@itsatlixco.edu.mx)

Introducción

La implementación de tecnologías disruptivas en las organizaciones se deriva de la transformación en la visión de una industria y, por tanto, del diseño de estrategias corporativas para llegar a ella.

La industria manufacturera requiere de transformaciones constantes en sus procesos para lograr ventajas competitivas dentro de las cadenas globales de valor. Las necesidades emergentes en esta industria se refieren, entre otras, a disminuir el ciclo de vida de los productos y atender la creciente demanda de productos personalizados. Esto exige una mayor complejidad en los procesos de producción (Vaidya, Ambad, & Bhosle, 2018), ya que implica lograr una mayor rapidez, flexibilidad, granularidad, precisión y eficiencia en los mismos (Trejo, 2019).

La industria 4.0, tiene como uno de sus fines lograr que los sistemas de manufactura se conviertan en "inteligentes" para lograr procesos flexibles, autónomos y reconfigurables (Vaidya et al., 2018). Esto se logra debido a que las aplicaciones que implementa, permiten acceso a la información de manera transparente y oportuna desde cualquier ubicación, lo que ofrece una visión completa de la cadena de producción y permite mejorar la calidad del producto así como el nivel del servicio, al realizar ajustes instantáneos ante cualquier desviación (Riahi Sfar, Natalizio, Challal, & Chtourou, 2018).

Para hacer posibles estos beneficios, uno de los requisitos imperantes es la capacidad de obtención, procesamiento, y almacenaje de una gran cantidad de datos en tiempo real. Ello implica una creciente demanda de datos y la explosión en la cantidad de dispositivos de detección conectados y, también, restricciones en términos de comunicación, batería y potencia de cómputo (Peralta et al., 2017), que se pueden traducir en problemas de latencia, seguridad, conectividad y una conexión interrumpida (Chiang & Zhang, 2016).

Estos son algunos de los desafíos funcionales para la industria 4.0 que hacen necesario introducir una capa intermedia entre el borde y, la nube de datos, con el fin de reducir las transmisiones requeridas desde los dispositivos conectados hacia la nube.

Esta capa se denomina cómputo en la niebla (Aazam, Zeadally, & Harras, 2018; Bellavista et al., 2019; Casarrubio, 2017; Chiang & Zhang, 2016; Gazis et al., 2015; Peralta et al., 2017; Steiner & Poledna, 2016; Yin, Luo, & Luo, 2018; Yousefpour et al., 2019; Zuo, Shao, Wei, Xie, & Ji, 2018).

El objetivo de este artículo es identificar los desafíos que enfrenta la industria 4.0 en el pilar del Internet Industrial de las cosas (IIoT), y cómo los están resolviendo a través del uso del cómputo en la niebla, esto con el fin de identificar áreas de oportunidad para futuras investigaciones.

Para ello, el contenido del documento se ha dividido en tres secciones: la primera se refiere a una revisión de literatura que abarca los conceptos que permitan establecer el contexto de investigación, en la siguiente sección se describe la metodología utilizada, en la tercera sección se muestran los resultados de la investigación respecto a los desafíos en el IIoT, cómo es que se integra el cómputo en la niebla al IIoT, y cómo es que se están abordando algunos de los desafíos identificados. Finalmente se redactan las conclusiones obtenidas y se identifican las áreas de oportunidad para investigaciones futuras.

Contexto teórico

Internet Industrial de las cosas (IIoT)

El Internet de las cosas (IoT) es una red de información de objetos físicos interconectados a través de Internet, que permite la interacción y cooperación de estos objetos para alcanzar objetivos comunes (Jeschke, Brecher, Meisen, Özdemir, & Eschert, 2017). Dichos objetos, tienen la capacidad de medir, comunicarse, y actuar desde cualquier lugar (Díaz, Martín, & Rubio, 2016).

Cuando los datos se recopilan de la misma manera y con los mismos fines, pero dentro de un entorno industrial, ese escenario se denomina Internet Industrial de las Cosas (IIoT). Mientras que IoT proporciona acceso a cualquier "cosa" a través de Internet, el IIoT restringe las "cosas" al escenario de la industria (Aazam et al., 2018). La definición de IIoT incluye la conexión de sensores y actuadores de máquinas industriales al procesamiento local y, a internet (Boyes, Hallaq, Cunningham, & Watson, 2018).

ISSN-2531-2952

Las tecnologías en que se apoya el IIoT, son: IoT, big data, robótica avanzada o sistemas ciberfísicos, servicios de conectividad industrial, sensores de última generación, y el cómputo en la nube (Zhong, Xu, Klotz, & Newman, 2017).

Industria 4.0

Se refiere a la cuarta generación de la industria que se enfoca sólo en el escenario de la industria manufacturera, que es un subconjunto de IIoT (Aazam et al., 2018; Sisinni, Saifullah, Han, Jennehag, & Gidlund, 2018). Es una iniciativa estratégica alemana que tiene como objetivo crear fábricas inteligentes, donde las tecnologías de fabricación se actualicen y transformen mediante los sistemas cibernéticos, IoT, y el cómputo en la Nube, para transformar fundamentalmente las cadenas de valor de la industria (Zhong et al., 2017). El cambio de paradigma de esta cuarta generación de la industria se ilustra en la figura 1.

Figura 1 El cambio de paradigma hacia la industria 4.0
Fuente: (López Ramón y Cajal & Escudero Ceballos, 2016)

La Industria 4.0 se refiere a la estricta integración de personas en el proceso de fabricación, para lograr en ella una mejora continua y centrarse en actividades de valor agregado (Vaidya et al., 2018), esto es, las personas lograrán ventajas competitivas en la industria, con un impacto económico positivo asociado a través de su implementación (Jeschke et al., 2017).

Comprende la convergencia de diversas tecnologías disruptivas que están alcanzado conjuntamente su madurez: big data y análisis de datos, robots autónomos, simulación, sistemas integrados horizontales y verticales, el Internet Industrial de las cosas (IIoT), ciberseguridad, sistemas ciberfísicos, cómputo en la nube y, manufactura aditiva (Vaidya et al., 2018). Varias de estas tecnologías tienen ya individualmente un enorme potencial disruptivo, pero conjuntamente van a transformar empresas, sectores y mercados. Son tecnologías ahora accesibles para todo tipo de empresas, grandes y pequeñas, que se prevé permitan el diseño de soluciones a medida a un costo asequible (López Ramón y Cajal & Escudero Ceballos, 2016).

Cómputo en la nube

El cómputo en la nube se refiere a un modelo para permitir el acceso ubicuo a la red conveniente y bajo demanda, a un conjunto de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se puede aprovisionar y lanzar rápidamente con un mínimo esfuerzo de gestión o interacción del proveedor de servicios (Mell & Grance, 2011). Sus características se muestran en la figura 2.

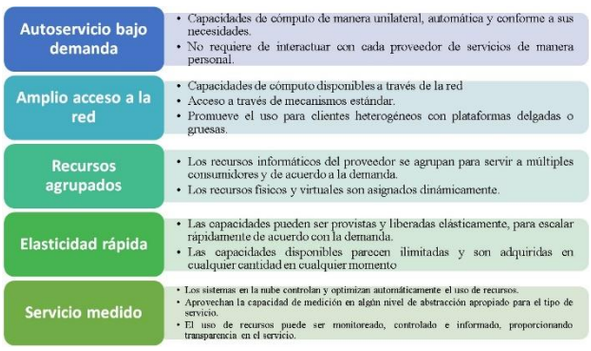


Figura 2 Características del cómputo en la nube
Fuente: (Mell & Grance, 2011)

El cómputo en la nube ha sido útil para las aplicaciones al expandir el alcance, capacidades de computación, almacenamiento, e infraestructura de red. El Instituto Nacional de Estándares y Tecnología (NIST) lo define también como un modelo que promueve la ubicuidad y el acceso a la red sobre demanda a recursos informáticos compartidos. El cómputo en la nube ofrece servicios de infraestructura, plataforma, o software como servicios (IaaS, PaaS, SaaS).

ISSN-2531-2952

El IaaS permite a los consumidores el acceso directo a infraestructura de Tecnologías de Información, para procesamiento, almacenamiento, y recursos de red. Por otra parte, el PaaS permite a los consumidores desarrollar software, además de ser totalmente compatible con el ciclo de vida del software - frecuentemente con la ayuda de un Middleware- para la gestión y configuración del software. El SaaS provee un ambiente para que el consumidor aloje centralmente sus aplicaciones y elimina la necesidad de que él instale el software manualmente (Yousefpour et al., 2019).

Limitaciones del cómputo en la nube

Cisco predice que para el año 2020 los dispositivos interconectados a través de la nube alcanzarán los 50 mil millones, y el tráfico IP anual del centro de datos alcanzará los 15.3 ZB. Derivado de esos datos, es que se prevén problemas en el uso del cómputo en la nube aplicado al IoT, tales como: que al crecer el número de dispositivos interconectados se transferirán enormes cantidades de datos a la nube para su procesamiento, lo que provocará un alto retraso y congestión en la red (Yin et al., 2018). Asimismo, (Chiang & Zhang 2016), agregan los desafíos de latencia, ancho de banda restringido, recursos limitados, seguridad, conectividad y, que no se asegura una conexión ininterrumpida.

Como solución a estos problemas, autores como (Aazam et al., 2018; Bellavista et al., 2019; Casarrubio, 2017; Chiang & Zhang, 2016; Mukherjee & Matam, 2017; Yousefpour et al., 2019), proponen utilizar una capa intermedia inteligente distribuida, para agregar funcionalidades adicionales al sistema, realizar un procesamiento de datos cuando los dispositivos los recopilan antes de enviarlos a la red y, finalmente, a la nube. Esta capa se denomina cómputo en la niebla.

Cómputo en la niebla

El concepto de cómputo en la niebla fue introducido por Cisco en el año 2012, y lo define como una extensión del paradigma del cómputo en la nube que provee cómputo, almacenamiento, y servicios de red, entre dispositivos finales y servidores de nube tradicionales.

No reemplaza el almacenamiento o procesamiento remoto de datos en la nube, pero si lo complementa (Ni, Zhang, Lin, & Shen, 2018). Las arquitecturas de niebla mueven de manera selectiva el cálculo, control, almacenamiento, comunicación, y toma de decisiones más cerca del borde de la red donde se están generando los datos, lo que permite resolver las limitaciones en la infraestructura actual para permitir su uso en casos de misión crítica y con gran densidad de datos. Y de acuerdo al Open Fog Consortium, al proporcionar un enlace continuo de la nube a "cosas", se considera una extensión del cómputo en la nube (Iorga et al., 2018).

Dastjerdi, et al. (2016) mencionan que el cómputo en la niebla soporta la movilidad, recursos de cómputo, interfaces heterogéneas, protocolos de comunicación, integración a la nube y análisis de datos distribuidos para satisfacer las necesidades de baja latencia en distribuciones geográficas amplias y densas.

Iorga, et al. (2018) consideran que el cómputo en la niebla es un modelo en capas que permite el acceso ubicuo a recursos escalables compartidos, el cual consta de nodos de niebla que residen entre los dispositivos inteligentes finales y los servicios centralizados en la nube.

El modelo de tres capas se ilustra en la figura 3. Entre la nube y la niebla se encuentra una red central para ofrecer servicios de red. Desde allí puede observarse que la nube se encuentra en el nivel superior del núcleo y está lejos de los dispositivos de borde. También puede notarse, que la niebla se encuentra en el nivel medio y está más cerca de los dispositivos de borde que la nube. Cada nodo de niebla está conectado a la nube. Cada dispositivo de borde está conectado a un nodo de niebla. Y finalmente, los nodos de niebla pueden conectarse entre sí y, las comunicaciones entre ellas son todas bidireccionales (Zhang, Zhou, & Fortino, 2018).

ISSN-2531-2952

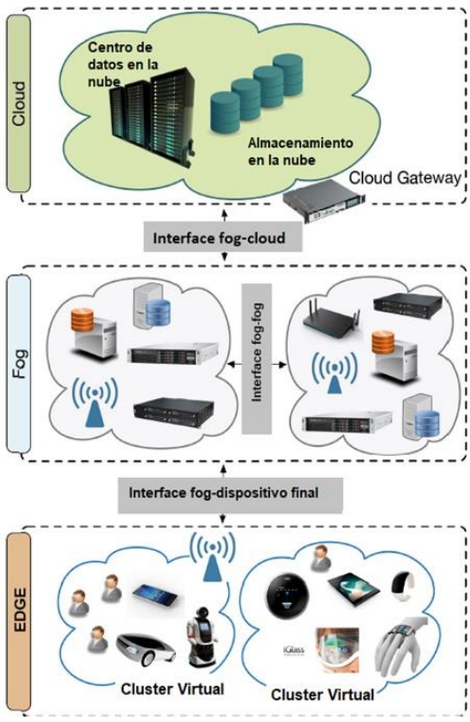


Figura 3 Arquitectura de 3 capas del IoT
Fuente: (Mukherjee & Matam, 2017)

Esta arquitectura minimiza el tiempo de solicitud-respuesta, de-hacia las aplicaciones compatibles y, proporciona para los dispositivos finales recursos de computación locales y, cuando sea necesario, conectividad de red a servicios centralizados (Mukherjee & Matam, 2017).

De acuerdo a lo publicado en el NIST.SP.500-325 por el National Institute of Standards and Technology, el cómputo en la niebla está formado por nodos de niebla. El nodo de niebla es el componente central de la arquitectura del cómputo en la niebla. Los nodos de niebla son componentes físicos (por ejemplo, puertas de enlace, conmutadores, enrutadores, servidores, etc.) o componentes virtuales (por ejemplo, conmutadores virtualizados, máquinas virtuales, cloudlets, entre otros) que están estrechamente acoplados a los dispositivos finales inteligentes o redes de acceso, y proporcionan recursos informáticos a estos dispositivos. Un nodo de niebla es consciente de su distribución geográfica y ubicación lógica dentro del contexto de su grupo (Iorga et al., 2018).

Metodología

La investigación se refiere a identificar los desafíos técnicos que enfrenta el IIoT, y cómo es que se están abordando a través de la integración del cómputo en la niebla. Para lograrlo, la búsqueda de información se realizó en las bases de datos de Google Scholar, y Web of Science.

Siguiendo a Boyes et al., (2018), la búsqueda de literatura se hizo a través de la combinación de palabras clave:

- (“Industrial Internet of Things” OR “Industrial Internet” OR “industry 4.0”) AND “fog computing”
- (“fog computing” AND (“industrial internet” OR “industry 4.0” OR “Industrial Internet of Things”) AND “challenges”)
- (industrial internet” OR “industry 4.0” OR “Industrial Internet of Things”) AND “challenges”
- (“Internet Industrial de las cosas” OR “industria 4.0” OR “IIoT”) AND desafíos

Aunque no es una lista exhaustiva, abarca los términos sobre los cuales se plantea la investigación. La restricción principal para la revisión de las propuestas fue el acceso libre a los artículos, por lo cual se aclara que la información presentada no incluye todos los trabajos realizados para abordar los desafíos que presenta el IIoT. Sin embargo, puede servir como una muestra respecto a cómo se están abordando a través de la implementación del cómputo en la niebla.

Los resultados se muestran a continuación. Primero se identifican los desafíos del IIoT, y posteriormente cómo es el que paradigma del cómputo en la niebla puede integrarse al IIoT, para resolverlos.

Resultados

Desafíos del IIoT

Después de la revisión realizada, se encontró que autores como Breivold & Sandstrom, (2015), Hegazy & Hefeeda, (2015), Trujillo, Crespo, & Alonso, (2013), (Virat, Bindu, Aishwarya, Dhanush, & Kounte, (2018), Sisinni et al., (2018), mencionan los siguientes desafíos en el IIoT:

ISSN-2531-2952

Interoperabilidad

La cantidad de dispositivos y componentes del sistema de diferentes proveedores y diferentes dominios plantea desafíos en términos de múltiples plataformas, numerosos protocolos y un gran número de Interfaz de Programación de Aplicaciones (API).

Criticidad mixta

La disponibilidad y la confiabilidad reciben cada vez más prioridad en muchos productos, sistemas y servicios, estas funciones de diferentes criticidades deben separarse para que las funciones de baja criticidad no interfieran con una función de alta criticidad. La disponibilidad de hardware de procesador multinúcleo debe proporcionar la independencia necesaria entre las aplicaciones de software. los principales indicadores de confiabilidad y disponibilidad incluyen *1) Tiempo medio entre fallas (MTBF), 2) Tiempo medio de reparación (MTTR y, 3) Probabilidad de falla en la demanda (PFD).*

Latencia

Los sistemas de control industrial son sistemas en tiempo real que tienen requisitos estrictos sobre el comportamiento temporal, la precisión y la respuesta del sistema. La latencia y las variaciones en el tiempo que toma una operación para realizar son una preocupación importante además del rendimiento promedio. El desafío es cómo implementar dinámicamente datos e inteligencia de servicio en diferentes niveles desde el borde de la red hasta la nube, para lograr un rendimiento óptimo.

Tolerancia a fallas

Esta es una consideración clave en IIoT donde muchos miles de dispositivos industriales heterogéneos están conectados e intercambian información. Es esencial diseñar e implementar soluciones de IIoT resistentes, con mecanismos de recuperación y tolerancia a fallos para poder tolerar y recuperarse rápidamente de fallas accidentales y malintencionadas que pueden conducir a una falta de disponibilidad del servicio.

Escalabilidad con respecto a los ciclos de actualización de datos

Muchas plantas industriales podrían tener decenas de miles de bucles de control y aplicaciones para mantener el rendimiento deseado en operación. Estas diferentes aplicaciones de control industrial tienen diferentes requisitos de tiempo de ciclo. Estos conjuntos de datos de alta frecuencia son útiles para estudiar el análisis del comportamiento dinámico a fin de crear modelos dinámicos para la optimización y el monitoreo. Esto implica una gran cantidad de datos que deben gestionarse, por ejemplo, mediante el filtrado, el pre procesamiento en, o cerca de dispositivos de borde antes de enviarlos a la nube.

Colaboración escalable

Un desafío aquí es permitir que los sistemas, plataformas y dispositivos horizontales y verticales puedan comunicarse y colaborar.

Seguridad funcional

La función de seguridad y, la integridad de seguridad, son dos tipos de requisitos para lograr la seguridad funcional. La seguridad funcional pone requisitos muy específicos tanto en cómo se desarrollan los sistemas, como en la tecnología en sí. La necesidad de cumplir con las normas de seguridad para garantizar servicios de seguridad funcional adecuados es primordial.

Desafío de seguridad específico de la industria

La arquitectura de software de una solución de IoT debe proteger a los dispositivos interconectados de intrusiones e interferencias provenientes de los canales de comunicación para que no ingresen al sistema a fin de garantizar operaciones seguras. Debe garantizar también una operación continua. Un desafío de seguridad de una solución de IIoT es cómo permitir actualizaciones de seguridad sin interrupciones y sin perjudicar la seguridad funcional o la interferencia a los servicios proporcionados en un proceso de control.

ISSN-2531-2952

Sistemas industriales heredados

Existe un desafío implícito para adaptar sistemas heredados (con los que se ha trabajado hace mucho ya en la industria) con soluciones de IoT de extremo a extremo que se implementan para servicios de operación adicionales.

Eficiencia de energía

La recolección de energía debe ser un enfoque prometedor para el emergente IIoT.

Cómo se está integrando el cómputo en la niebla al IIoT para resolver algunos desafíos

El modelo de Referencia Purdue, es un modelo muy reconocido en la industria manufacturera, que segmenta dispositivos y equipos en funciones jerárquicas. Este modelo ha sido utilizado por organizaciones con estándares internacionales (Boyes et al., 2018). Los niveles más bajos de la pirámide se centran en el control de procesos, y los niveles superiores se ocupan de la gestión de la producción (Figura 4).

Esto implica inicialmente que la arquitectura para IIoT pueda basarse en dos capas interconectadas: una de dispositivos IoT, y otra en Cómputo en la nube, como se muestra en la Figura 5. Esto puede imponer severas restricciones en el flujo de información entre los diferentes niveles, dado que las tecnologías de comunicación y computación utilizadas difieren mucho entre las diferentes capas (Steiner & Poledna, 2016).

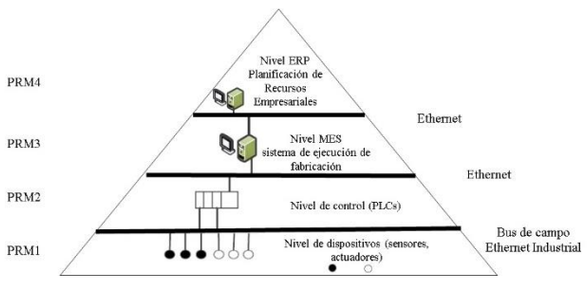


Figura 4 Pirámide de comunicación simplificada en automatización según el modelo de referencia de Purdue (PRM). Fuente: (Steiner & Poledna, 2016)

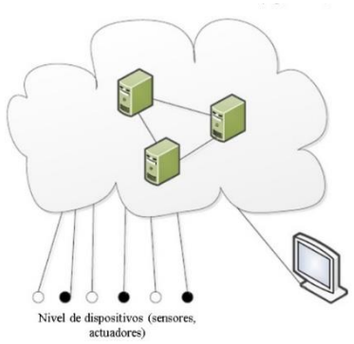


Figura 5 Arquitectura basada en dos capas para IIoT
Fuente: (Steiner & Poledna, 2016)

En aras de detonar el IIoT, y tratar de resolver algunos de los desafíos mencionados en el apartado anterior, autores como (Aazam et al., 2018; Breivold & Sandstrom, 2015; Chiang & Zhang, 2016; Gazis et al., 2015; O'Donovan, Gallagher, Bruton, & O'Sullivan, 2018; Peralta et al., 2017; Steiner & Poledna, 2016; Tao, Qi, Liu, & Kusiak, 2018; Wu et al., 2017; Yin et al., 2018; Zuo et al., 2018), proponen introducir una capa intermedia, utilizando el cómputo en la niebla, de tal manera que puedan lograr una arquitectura de 3 capas, como se muestra en la figura 6.

En esta arquitectura, el despliegue estratégico de niebla asegura una retroalimentación rápida basada en los datos entrantes. En general, la niebla será responsable de las siguientes tareas (Aazam et al., 2018):

- Minería de big data industrial en tiempo real para alto rendimiento.
- Recolección concurrente de datos de múltiples tipos de sensores, robots y máquinas.
- Procesamiento rápido de los datos detectados para generar instrucciones para los actuadores y robots dentro de una latencia aceptable.
- Conectar sensores y máquinas incompatibles a través de la traducción y mapeo de protocolos necesarios.
- Gestión de la energía del sistema.
- Estructuración y filtrado de datos para evitar el envío de datos innecesarios al núcleo y la nube.

ISSN-2531-2952

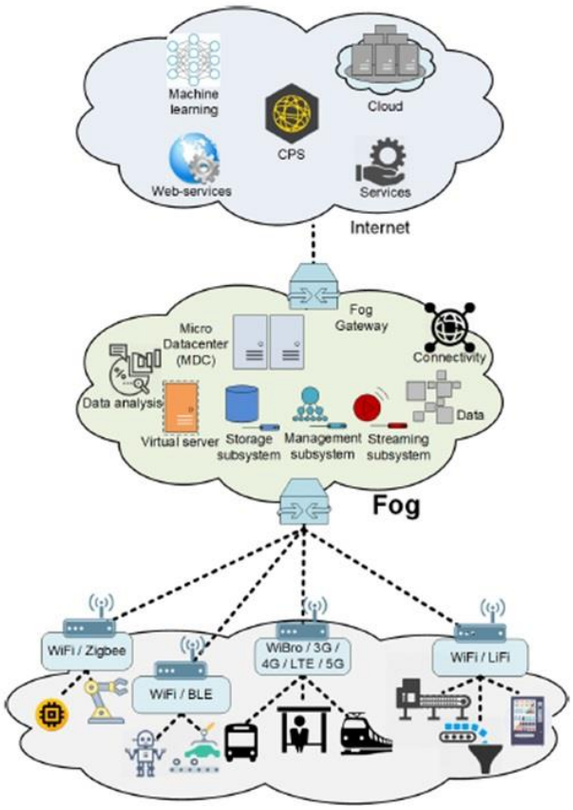


Figura 6 Cómputo en la niebla en el IIoT
Fuente: (Aazam et al., 2018)

Para implementar una capacidad determinada de cómputo en la niebla, los nodos de niebla funcionan de manera centralizada o descentralizada y pueden configurarse como nodos de niebla independientes que se comunican entre ellos para brindar el servicio o pueden ser federados para formar agrupaciones que brindan escalabilidad horizontal sobre geolocalizaciones dispersas, a través de mecanismos de espejo o extensión.

Asimismo, para facilitar el despliegue de una capacidad de cómputo en la niebla que muestre las características descritas anteriormente, los nodos de niebla deben admitir uno o más de los siguientes atributos: autonomía, heterogeneidad, agrupación jerárquica, manejabilidad, y que sean programables (Iorga et al., 2018). Cada uno es descrito en la figura 7.

Figura 7 Atributos de los nodos de niebla
Fuente: (Iorga, et al., 2018)

Diferentes escenarios de casos de uso pueden tener diferentes arquitecturas basadas en el enfoque óptimo para soportar la funcionalidad de dispositivos finales. Pero, la elección de esta representación se basa en la intención de capturar una arquitectura compleja que incorpora sus servicios (Iorga et al., 2018).

Desafíos del IIoT que han sido abordados integrando el cómputo en la niebla.

En las siguientes tablas se muestra cómo diversos autores consideran que la implementación del cómputo en la niebla, sirve para abordar diversos desafíos del IIoT (Tabla 1 a Tabla 5).

Desafío: comunicación y colaboración	
Solución propuesta	Autores
Arquitectura HFC para interconectar dominios de nube y niebla distribuidos geográficamente.	(Moreno-Vozmediano et al. 2017), citado en Mouradian et al. (2018)

Tabla 1 Solución propuesta al desafío de comunicación y colaboración

Desafíos: actualización de datos	
Solución propuesta	Autores
Agregado de datos mediante técnicas jerárquicas. Mantener una especificación uniforme. Normalización de los datos intercambiados. Hacer uso de técnicas de homogeneización de datos.	(Bellavista, et al., 2018)
El análisis de datos debe ser en tiempo real y requiere ser realizado en la niebla, en la nube e incluso en ambos. La toma de decisiones se realiza en la niebla, cerca de la frontera.	(Bellavista, et al., 2018)

Tabla 2 Solución propuesta al desafío de la actualización de datos

ISSN-2531-2952

Desafío: latencia	
Solución propuesta	Autores
Proponen recortar y refinar el Big data industrial localmente antes de enviarlo a la nube con el fin de disminuir retrasos	(Aazam et al., 2018)

Tabla 3 Solución propuesta al desafío de latencia

Desafío: seguridad	
Solución propuesta	Autores
Proponen el modelo de seguridad CCA de OD-ABE, y luego presentan el primer esquema C-OD-ABE seguro.	(Zuo et al., 2018)
Los dispositivos con recursos más limitados se unen a la plataforma de computación de niebla, y la actualización de atributos hace que el cambio de roles de usuario sea más flexible.	(P. Zhang, Chen, Liu, Liang, & Liu, 2018)

Tabla 4 Soluciones propuestas para el desafío de seguridad

Desafío: criticidad mixta	
Solución propuesta	Autores
Arquitectura basada en capas que soporte virtualización para la migración entre nodos de niebla.	(Bittencourt et al., 2015), citado en Mouradian et al. (2018)
Arquitectura para asignación de recursos que incluya un algoritmo de distribución de cargas de trabajo entre la nube y la niebla.	(Agarwal et al., 2016), citado en Mouradian et al. (2018)
Arquitectura para administración de recursos y balanceo de cargas entre la nube y la niebla.	Kapsalis et al. (2017), citado en Mouradian et al. (2018)
Introducción de una Plataforma de Operaciones Adaptativa (AOP) para proporcionar la capacidad de administración de extremo a extremo de la infraestructura de computación de niebla habilitada de acuerdo con los requisitos operacionales del proceso industrial.	(Gazis, et al., 2015)
Consideran un thin client y la movilidad. Los cómputos simples y constantes se dejan para las terminales de usuario, de modo que los dispositivos con recursos más limitados se unen a la plataforma de computación de niebla.	(P. Zhang, Chen, Liu, Liang, & Liu, 2018)
Proponen un nuevo algoritmo de programación de tareas y diseñan el esquema de reasignación de recursos para mejorar la utilización de recursos de los nodos de niebla y reducir los retrasos en las tareas.	(Yin et al., 2018)
Desafío: criticidad mixta	
Solución propuesta	**Autores**
Considera el uso de la computación en niebla para entregar aplicaciones de aprendizaje automático en tiempo real para las operaciones de la Industria 4.0. Los hallazgos iniciales resaltan la capacidad de la niebla para proporcionar interacciones ciberfísicas consistentes y confiables para escenarios de ingeniería en tiempo real	(O'Donovan et al., 2018)

Tabla 5 Soluciones propuestas al desafío de criticidad mixta

A forma de resumen, los principales desafíos que se están abordando a través de la implementación del cómputo en la niebla son: comunicación y colaboración, actualización de datos, latencia, seguridad funcional, y criticidad mixta. Sin embargo, debido a la restricción mencionada en la metodología, respecto al acceso a los artículos académicos, no se puede afirmar como una verdad absoluta.

Conclusiones

En esta revisión se han mostrado dos de las tecnologías que impulsan la industria 4.0: el IIoT y en cómputo en la nube. Se ha planteado la implementación del cómputo en la niebla como respuesta a las restricciones funcionales que presenta la integración del cómputo en la nube al IIoT.

Por otro lado, se plantearon los desafíos principales del IIoT: interoperabilidad, criticidad mixta, latencia, tolerancia a fallas, escalabilidad, colaboración escalable (Integración horizontal, y vertical), seguridad funcional, desafío de seguridad específico de la industria, los sistemas industriales heredados y la eficiencia en el manejo de energía.

Como puede observarse en la revisión presentada, no todos los desafíos han sido abordados utilizando el paradigma del cómputo en la niebla. Aun así, a pesar de que el cómputo en la niebla es una tecnología disruptiva que presenta sus propios desafíos, ha empezado a ser implementada porque realmente está siendo considerada una tecnología que puede ayudar a resolver los desafíos enfrenta el IIoT en el marco de la industria 4.0

Los autores mencionan como áreas de oportunidad importantes, las de interoperabilidad, seguridad y privacidad, la eficiencia energética que mantenga todos los dispositivos interconectados, la tolerancia a fallos y, desempeño en tiempo real.

Esta no ha sido una revisión exhaustiva, ya que tiene la restricción del acceso libre a las bases de datos, sin embargo permite dilucidar que la investigación seguirá enfocándose en los desafíos que presenta cada uno de los pilares en que se apoya la industria 4.0, por lo que se considera que aporta áreas de oportunidad para el desarrollo de tecnología.

ISSN-2531-2952

Referencias

Aazam, M., Zeadally, S., & Harras, K. A. (2018). Deploying Fog Computing in Industrial Internet of. En *IEEE Transactions on Industrial Informatics* (Vol. 14, pp. 4674–4682). IEEE. https://doi.org/10.1109/TII.2018.2855198

Bellavista, P., Berrocal, J., Corradi, A., Das, S. K., Foschini, L., & Zanni, A. (2019). A survey on fog computing for the Internet of Things. *Pervasive and Mobile Computing*, *52*, 71–99. https://doi.org/10.1016/j.pmcj.2018.12.007

Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in Industry*, *101*(April), 1–12. https://doi.org/10.1016/j.compind.2018.04.015

Breivold, H. P., & Sandstrom, K. (2015). Internet of Things for Industrial Automation-Challenges and Technical Solutions. *Proceedings - 2015 IEEE International Conference on Data Science and Data Intensive Systems; 8th IEEE International Conference Cyber, Physical and Social Computing; 11th IEEE International Conference on Green Computing and Communications and 8th IEEE Inte*, 532–539. https://doi.org/10.1109/DSDIS.2015.11

Casarrubio, B. P. (2017). *Tratamiento de los activos intangibles*. Recuperado de https://repositori.upf.edu/bitstream/handle/10230/33175/BorjaPascualTFG.pdf?sequence=1&isAllowed=y

Chiang, M., & Zhang, T. (2016). Fog and IoT : An Overview of Research Opportunities. *IEEE Internet of Things Journal*, *3*(6), 854–864. https://doi.org/10.1109/JIOT.2016.2584538

Díaz, M., Martín, C., & Rubio, B. (2016). State-of-the-art , challenges , and open issues in the integration of Internet of things and cloud computing. *Journal of Network and Computer Applications*, *67*, 99–117. https://doi.org/10.1016/j.jnca.2016.01.010

Gazis, V., Leonardi, A., Mathioudakis, K., Sasloglou, K., Kikiras, P., & Sudhaakar, R. (2015). Components of fog computing in an industrial internet of things context. En *2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking - Workshops, SECON Workshops 2015* (pp. 37–42). https://doi.org/10.1109/SECONW.2015.7328144

Hegazy, T., & Hefeeda, M. (2015). Industrial Automation as a Cloud Service. *IEEE Transactions on Parallel and Distributed Systems*, *26*(10), 2750–2763. https://doi.org/10.1109/TPDS.2014.2359894

Iorga, M., Feldman, L., Barton, R., Martin, M., Goren, N., & Mahmoudi, C. (2018). Fog Computing Conceptual Model, Recommendations of the National Institute of Standards and Technology. En *NIST Special Publication* (pp. 500–325).

Jeschke, S., Brecher, C., Meisen, T., Özdemir, D., & Eschert, T. (2017). Industrial Internet of Things and Cyber Manufacturing Systems. En *Industrial Internet of Things. Springer Series in Wireless Technology*. (pp. 3–19). Springer, Cham. https://doi.org/10.1007/978-3-319-42559-7

López Ramón y Cajal, J., & Escudero Ceballos, V. (2016). Industria 4.0, la gran oportunidad. *Economía Aragonesa*, *59*, 109–122. Recuperado dehttp://gorilaa.com/resources/o6loOSw1mk/6a204800660741ecb9de0cb060c8a024.pdf#page=111

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology*.

Mukherjee, M., & Matam, R. (2017). Security and Privacy in Fog Computing: Challenges. *IEEE Access*, *5*, 19293–19304. Recuperado de http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8026115&isnumber=7859429

Ni, J., Zhang, K., Lin, X., & Shen, X. S. (2018). Securing Fog Computing for Internet of Things Applications: Challenges and Solutions. *IEEE Communications Surveys and Tutorials*, *20*(1), 601–628. https://doi.org/10.1109/COMST.2017.2762345

ISSN-2531-2952

O'Donovan, P., Gallagher, C., Bruton, K., & O'Sullivan, D. T. J. (2018). A fog computing industrial cyber-physical system for embedded low-latency machine learning Industry 4.0 applications. *Manufacturing Letters*, *15*, 139–142. https://doi.org/10.1016/j.mfglet.2018.01.005

Peralta, G., Iglesias-Urkia, M., Barcelo, M., Gomez, R., Moran, A., & Bilbao, J. (2017). Fog computing based efficient IoT scheme for the Industry 4.0. En *Proceedings of the 2017 IEEE International Workshop of Electronics, Control, Measurement, Signals and their Application to Mechatronics, ECMSM 2017* (pp. 1–6). https://doi.org/10.1109/ECMSM.2017.7945879

Riahi Sfar, A., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. *Digital Communications and Networks*, *4*(2), 118–137. https://doi.org/10.1016/j.dcan.2017.04.003

Sisinni, E., Saifullah, A., Han, S., Jennehag, U., & Gidlund, M. (2018). Industrial internet of things: Challenges, opportunities, and directions. *IEEE Transactions on Industrial Informatics*, *14*(11), 4724–4734. https://doi.org/10.1109/TII.2018.2852491

Steiner, W., & Poledna, S. (2016). Fog Computing as enabler for de Industrial Internet of Things. *Elektrotechnik und Informationstechnik*, *133*(7), 310–314. https://doi.org/10.1007/s00502-016-0438-2

Tao, F., Qi, Q., Liu, A., & Kusiak, A. (2018). Data-driven smart manufacturing. *Journal of Manufacturing Systems*, *48*, 157–169. https://doi.org/10.1016/j.jmsy.2018.01.006

Trejo, T. Á. (2019). *Programa para la productividad y competitividad industrial: implementación para el desarrollo de las regiones y el impulso de la manufactura 4.0*. INFOTEC. Recuperado de https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/337/1/PROPUESTA DE INTERVENCIÓN_PPCI_ IMPLEMENTACIÓN PARA EL DESARROLLO DE LAS REGIONES Y EL IMPULSO A LA MANUFACTURA 4.0 %281%29.pdf

Trujillo, S., Crespo, A., & Alonso, A. (2013). MultiPARTES: Multicore virtualization for mixed-criticality systems. *Proceedings - 16th Euromicro Conference on Digital System Design, DSD 2013*, *8*, 260–265. https://doi.org/10.1109/DSD.2013.37

Vaidya, S., Ambad, P., & Bhosle, S. (2018). Industry 4.0 - A Glimpse. *Procedia Manufacturing*, *20*, 233–238. https://doi.org/10.1016/j.promfg.2018.02.034

Virat, M. S., Bindu, S. M., Aishwarya, B., Dhanush, B. N., & Kounte, M. R. (2018). Security and Privacy Challenges in Internet of Things. *Proceedings of the 2nd International Conference on Trends in Electronics and Informatics, ICOEI 2018*, 454–460. https://doi.org/10.1109/ICOEI.2018.8553919

Wu, D., Liu, S., Zhang, L., Terpenny, J., Gao, R. X., Kurfess, T., & Guzzo, J. A. (2017). A fog computing-based framework for process monitoring and prognosis in cyber-manufacturing. *Journal of Manufacturing Systems*, *43*(2017), 25–34. https://doi.org/10.1016/j.jmsy.2017.02.011

Yin, L., Luo, J., & Luo, H. (2018). Tasks Scheduling and Resource Allocation in Fog Computing Based on Containers for Smart Manufacturing. *IEEE Transactions on Industrial Informatics*, *14*(10), 4712–4721. https://doi.org/10.1109/TII.2018.2851241

Yousefpour, A., Fung, C., Tech, G., Kadiyala, K., Charlotte, U. N. C., & Jue, J. P. (2019). All One Needs to Know about Fog Computing and Related Edge Computing Paradigms. *Journal of Systems Architecture*, *7*(18). Recuperado de http://10.0.3.248/j.sysarc.2019.02.009%0Ahttp://ezproxy.unal.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edselp&AN=S1383762118306349&lang=es&site=eds-live

Zhang, P. Y., Zhou, M. C., & Fortino, G. (2018). Security and trust issues in Fog computing: A survey. *Future Generation Computer Systems*, *88*, 16–27. https://doi.org/10.1016/j.future.2018.05.008

ISSN-2531-2952

Zhong, R. Y., Xu, X., Klotz, E., & Newman, S. T. (2017). Intelligent Manufacturing in the Context of Industry 4 . 0 : A Review. *Engineering*, *3*(5), 616–630. https://doi.org/10.1016/J.ENG.2017.05.015

Zuo, C., Shao, J., Wei, G., Xie, M., & Ji, M. (2018). CCA-secure ABE with outsourced decryption for fog computing. *Future Generation Computer Systems*, *78*, 730–738. https://doi.org/10.1016/j.future.2016.10.028

ISSN-2531-2952

Artículo **Revista de Cómputo Aplicado**
Septiembre 2019 Vol.3 No.11 28-35

Criptografía basada en curvas elípticas

Cryptography based on elliptic curves

RAMÍREZ-HERNÁNDEZ, Héctor David†*, CONTRERAS-JUÁREZ, Roberto, ESPINOZA-HERNÁNDEZ, Nelva Betzabel y SÁNCHEZ-MENDOZA, Eduardo

Benemérita Universidad Autónoma de Puebla, Facultad de Ciencias de la Computación.

ID 1er Autor: *Héctor David, Ramírez-Hernández* / **ORC ID**: 0000-0003-3741-4285

ID 1er Coautor: *Roberto, Contreras-Juárez* / **ORC ID**: 0000-0001-3271-6754

ID 2do Coautor: *Nelva Betzabel, Espinoza-Hernández* / **ORC ID**: 0000-0002-5620-2336

ID 3er Coautor: *Eduardo, Sánchez-Mendoza* / **ORC ID**: 0000-0003-2690-6217

DOI: 10.35429/JCA.2019.11.3.28.35 Recibido Abril 30, 2019; Aceptado Junio 30, 2019

Resumen

La criptografía incorpora las técnicas con las que se busca garantizar protección de la información, frente a personas no autorizadas. Esta manera de resguardar información ha existido desde tiempos remotos, en donde existían elementos que sólo ciertas personas eran capaces de entender e interpretar. En un principio la criptografía fue utilizada para efectos de guerra y poder, pero gracias a los grandes avances tecnológicos desarrollados a finales del siglo pasado, se ha visto la necesidad de resguardar la información que cada individuo maneja y comparte por medio del internet. Es por lo que la criptografía toma una mayor importancia. La criptografía actual se basa en dos tipos de protocolos, uno el de la criptografía simétrica y el otro que corresponde a la criptografía asimétrica. En este trabajo se analizó un protocolo del tipo asimétrico basado en curvas elípticas sobre el campo finito GF(p), proponiendo una librería desarrollada en PHP que permite cifrar y descifrar información, la cual pretende brindar los servicios de seguridad, autenticación, integridad y confidencialidad de la información.

Criptografía, Protocolo, Curvas elípticas

Abstract

Cryptography incorporates the techniques with which it seeks to guarantee protection of information, in front of unauthorized persons. This way of protecting information has existed since ancient times, where there were elements that only certain people were able to understand and interpret. In the beginning, cryptography was used for the purposes of war and power, but thanks to the great technological advances developed at the end of the last century, we have seen the need to safeguard the information that everyone manages and shares through the internet. That is why cryptography takes on greater importance. Current cryptography is based on two types of protocols, one of symmetric cryptography and the other corresponding to asymmetric cryptography. In this paper, an asymmetric type protocol based on elliptic curves on the finite field GF(p) was analyzed, proposing a library developed in PHP that allows to encrypt and decrypt information, which aims to provide security services, authentication, integrity and confidentiality of the information.

Cryptography, Protocol, Elliptic curves

Citación: RAMÍREZ-HERNÁNDEZ, Héctor David, CONTRERAS-JUÁREZ, Roberto, ESPINOZA-HERNÁNDEZ, Nelva Betzabel y SÁNCHEZ-MENDOZA, Eduardo. Criptografía basada en curvas elípticas. Revista de Cómputo Aplicado. 2019, 3-11: 28-35

* Correspondencia al Autor (Correo electrónico: hector.ramirezhe@correo.buap.mx)
† Investigador contribuyendo como primer Autor.

Introducción

La criptografía se puede definir como el arte o la ciencia de cifrar y descifrar información, utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que solo puedan ser leídos por las personas a quienes van dirigidos (Granados, 2006). La finalidad de la criptografía es garantizar que el contenido del mensaje enviado no haya sido modificado en su tránsito, o que si se resguarda esta no pueda ser extraída (Granados, 2006). Los criptosistemas utilizados son los denominados simétricos y los asimétricos. Los criptosistemas simétricos son aquellos que usan un método matemático para cifrar y descifrar un mensaje (Gómez, 2002).

Este tipo de criptografía utiliza únicamente una llave para realizar el proceso, así el mensaje únicamente se descifra con la única llave existente. Este tipo de criptografía garantiza confidencialidad, pero al querer compartir el mensaje con otro usuario deberá crearse una nueva llave y el número de llaves aumenta conforme aumenten los usuarios con quienes se comparta el mensaje (Amalraj y Raybin, 2016). En 1976, Whitfield Diffie y Martin Hellman (Diffie y Hellman, 1976) revolucionan la criptografía al introducir el concepto de criptosistema asimétrico, que surge como una solución al problema de intercambiar claves privadas por canales inseguros.

Los sistemas asimétricos son aquellos en los cuales tanto el emisor como el receptor poseen un par de claves: una de tipo pública y la otra de tipo privada y para enviar mensajes el emisor tiene que cifrar el mensaje con la clave pública del receptor para que así este sea el único que pueda descifrar el mensaje usando su clave privada (Hankerson et al. 2004). Este novedoso sistema de encriptación fundamenta su seguridad en problemas matemáticos cuya solución computacional resulta difícil de resolver, ya que, aun conociendo los algoritmos para resolverlos, no es factible su ejecución en un tiempo razonable. Ejemplos de este tipo de criptografía son RSA y criptografía basado en curvas elípticas (ECC) (Amalraj y Raybin, 2016). La teoría de curvas elípticas conforma una herramienta matemática que brinda a la criptografía la oportunidad de optimizar los algoritmos de cifrado, tal es el caso de El Gamal, mejorando la eficiencia y robustez sin utilizar más recursos computacionales.

La criptografía de curva elíptica (ECC), planteada por Koblitz y Miller (Koblitz, 1987), es una variante de la criptografía asimétrica la cual se basa en las propiedades de las curvas elípticas que resulta ser más eficiente que los métodos como el Rivest, Shamir y Adleman (RSA), además de proporcionar un nivel de seguridad equivalente (Gupta et al., 2004).

En la sección de curva elíptica se da un panorama general de las curvas elípticas, en los que se definen los tipos de curvas elípticas utilizadas, así como las operaciones que hacen que conformen un grupo abeliano.

En la sección del protocolo criptográfico, se consideran los parámetros necesarios para implementar la criptografía de curvas elípticas, se menciona un método para calcular la cantidad de puntos que contiene una curva elíptica usando el símbolo de Legendre para el cálculo de los residuos cuadráticos. En la última sección de cifrado de datos, se explica la implementación del algoritmo El Gamal para el cifrado y descifrado de datos, en la que se muestra la aplicación de la librería desarrollada en PHP.

Criptografía de curvas elípticas (ECC)

Como se mencionó anteriormente, la criptografía de curvas elípticas (ECC) pertenece a la criptografía asimétrica, debido a que se utilizan dos tipos de llaves distintas, una pública y una privada, en la que el conocimiento de la llave pública no permite determinar el conocimiento de la clave privada. La criptografía de curvas elípticas fue propuesta en 1985 por Neal Koblitz (Koblitz, 1987) y Víctor Miller (Miller, 1986). Desde entonces una gran cantidad de investigaciones se han realizado para tener implementaciones eficientes y seguras de estos esquemas criptográficos. La Criptografía de Curvas Elípticas ha permitido explorar nuevos criptosistemas, tal como la técnica de emparejamientos bilineales (Kawahara et al., 2006).

Curva Elíptica

Definimos de manera general a las curvas elípticas de la siguiente forma. Sea K un campo. Una curva elíptica sobre K, es la curva plana sobre K definida por la ecuación de Weierstrass:

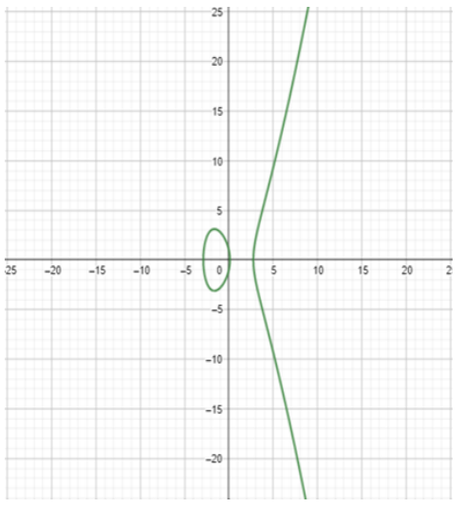
$$y^2 = x^3 + ax + b \quad (1)$$

ISSN-2531-2952

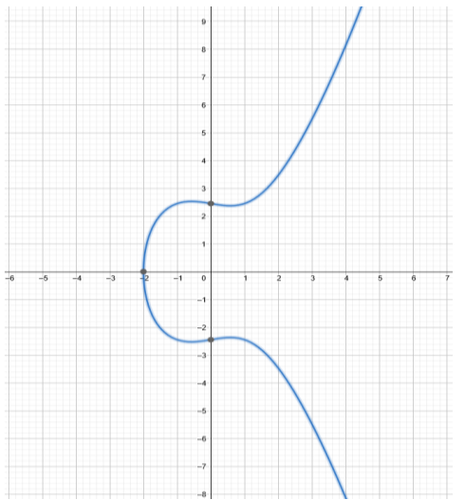
donde $x, y, a, b \in K$.

Para poder definir una estructura algebraica de grupo abeliano es necesario incluir un punto, denotado por ∞ y llamado punto en el infinito, que no se encuentra en la curva. Este punto se encuentra situado por encima del eje de las abscisas a una distancia infinita, y que por lo tanto no tiene un valor en concreto. Si $x^3 + ax + b$ no tiene raíces múltiples, entonces la curva correspondiente, aunado con el punto ∞, más la operación suma definida más adelante, es lo que se denomina grupo de la curva elíptica sobre K, denotado por $E(K)$. Esto es, el conjunto: $E(K) = \{(x, y): x, y \in K, y^2 = x^3 + ax + b\} \cup \{\infty\}$ forma un grupo abeliano, en donde, ∞ es el elemento identidad del grupo de curva elíptica.

Las siguientes gráficas son ejemplos de curvas elípticas definidas sobre $\mathbb{R}$.

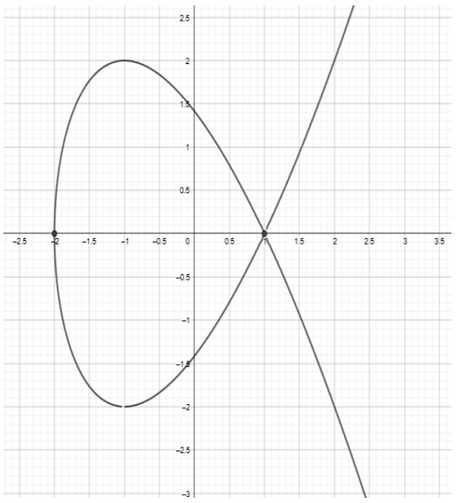


Gráfica 1 *Curva elíptica* $y^2 = x^3 - 8x + 1$

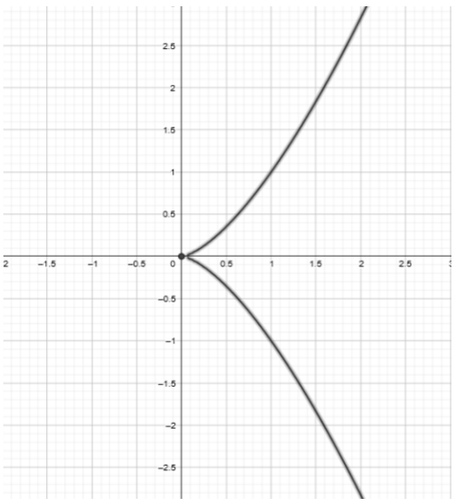


Gráfica 2 *Curva Elíptica* $y^2 = x^3 - x + 6$

A la expresión $\Delta = 4a^3 + 27b^2$ se le conoce como el discriminante de la curva elíptica. Se verifica que para que la curva elíptica no tenga raíces múltiples es necesario que $\Delta \neq 0$. Esta condición permite excluir las curvas elípticas que tengan un punto doble o un pico como lo muestran las Gráficas 3 y 4.



Gráfica 3 Curva Elíptica $y^2 = x^3 - 3x + 2$ sobre $\mathbb{R}$



Gráfica 4 Curva Elíptica $y^2 = x^3$ sobre $\mathbb{R}$

Trabajar criptografía con curvas elípticas sobre los números reales se puede volver lento e inexacto, debido a los errores de redondeo que puedan existir. En la práctica, el trabajo de criptografía se lleva a cabo con curvas elípticas sobre el campo finito $GF(p)$ pertenecientes a los campos primos y $GF(2^m)$ pertenecientes a los campos de binarios. En este trabajo nos centramos en las curvas elípticas sobre el campo finito $GF(p)$, con p un número primo.

Recordando que el campo de $GF(p)$ usa los números del 0 al p-1 y en cómputo final se obtiene el módulo de p.

ISSN-2531-2952

Una curva elíptica definida sobre el campo de $GF(p)$, denotada por $E(GF(p))$, esta formada por las variables a y b dentro del campo de $GF(p)$. Las curvas elípticas incluyen todos los puntos de (x, y) que satisface la ecuación de una curva elíptica módulo p. Esto es, una curva elíptica sobre $GF(p)$ tiene por ecuación:

$$y^2 \ mod \ p = (x^3 + ax + b) \ mod \ p, \qquad (2)$$

donde $a, b, x, y \in GF(p)$.

De manera análoga, si $x^3 + ax + b$ contiene factores no repetidos, o equivalentemente si

$$4a^3 + 27b^2 \neq 0 \ mod \ p \qquad (3)$$

entonces la curva elíptica se puede utilizar para la criptografía. Una curva elíptica sobre el campo de $GF(p)$ tiene los puntos correspondientes en la curva elíptica, junto con un punto especial ∞, el cual se le llama punto en infinito o punto cero. La cantidad de puntos de una curva elíptica sobre un campo finito es finita. La cardinalidad de puntos de una curva elíptica se denota por $\#E(GF(p))$. El número de puntos de una curva elíptica es llamado el orden de la curva.

Ejemplo: Consideremos la curva elíptica sobre $GF(11)$. Con $a = 6$ y $b = 10$, la ecuación de la curva elíptica es $y^2 = x^3 + 6x + 10$. Los puntos que pertenecen a esta curva son: (0,3), (0,5), (6,3), (6,8), (8,3), (8,8), (9,1), (9,10), (10,5), (10,6) incluyendo a ∞. Esto es, $\#E(GF(p)) = 11$.

Figura 1 Número de puntos de la curva

Desde el punto de vista algebraico la ley de grupo para una Curva Elíptica representada por la ecuación de *Weierstrass* (1), se define de acuerdo con las siguientes propiedades:

1. $P_1 + \infty = P_1$
2. Si $P_1 = (x_1, y_1)$, entonces $-P_1 = (x_1, -y_1)$.
3. Sean $P_1 = (x_1, y_1)$ y $P_2 = (x_2, y_2)$ puntos de la curva elíptica con $P_1, P_2 \neq \infty$. Entonces si $x_1 = x_2$ pero $y_1 \neq y_2$ o $P_1 = P_2$ y $y_1 = 0$ entonces $P_1 + P_2 = \infty$. En otro caso $P_1 + P_2 = P_3 = (x_3, y_3)$ con

$$x_3 = m^2 - x_1 - x_2,$$
$$y_3 = m(x_1 - x_3) - y_1$$
$$m = \begin{cases} \dfrac{3x_1^2 + a}{2y_1} & x_1 = x_2 \\ \dfrac{y_2 - y_1}{x_2 - x_1} & x_1 \neq x_2 \end{cases}$$

La curva elíptica $E(GF(p))$ dotada de la operación suma definida anteriormente forma un grupo abeliano. Sea P un punto de la curva elíptica $E(GF(p))$. Entonces, kP significa la suma del punto P consigo mismo k-veces, con la suma definida anteriormente.

Es conocido el hecho (Katz y Lindell, 2015) de que si $\#E(GF(p))$ es un número primo entonces el grupo $E(GF(p))$ es un grupo cíclico. Este proceso facilita el hecho de que, si una curva elíptica cumple con esta condición, entonces cualquiera de sus puntos diferente del ∞ será un punto generador del grupo.

Protocolo criptográfico

Hoy en día se vive en un ambiente donde la interacción con las nuevas tecnologías es tan cotidiana como tener que ir al colegio. No hay cosa que no manejemos a través de un ordenador, ya sea para mandar un mensaje a un ser querido, hacer un trabajo escolar o hasta nuestro mismo trabajo necesita de un ordenador, es claro que la mayoría de las veces es a través de diferentes páginas web.

Estas tecnologías han permitido un sin fin de cosas, como las aplicaciones móviles y aplicaciones web. Es más que un hecho que cualquier documento importante, transferencia bancaria, correos confidenciales hasta la documentación de un caso penal no sea enviada por internet, es por ello por lo que es importante proteger esa información que en términos computacionales llamamos encriptar y la herramienta que nos permite trabajar en el lado del servidor para proteger este tipo de datos es PHP.

ISSN-2531-2952

Para llevar a cabo la encriptación y desencriptación usando curvas elípticas, es necesario realizar múltiples operaciones que nos permiten establecer los mecanismos de seguridad que se necesitan en el resguardo de la información. Para ello detallamos las operaciones utilizadas para llevar a cabo el objetivo de este trabajo. El desarrollo de este sistema fue utilizando PHP.

El primer paso consiste en proporcionar un número primo p y los coeficientes a y b, para formar la curva elíptica de la forma **¡Error! No se encuentra el origen de la referencia.** cumpliendo la condición **¡Error! No se encuentra el origen de la referencia.**. Para mostrar este paso, consideremos los coeficientes a = 9, b = 13 y el número primo p = 19. Con estos parámetros se obtiene la curva $y^2 = (x^3 + 9x + 13)\ mod\ 19$, cumpliendo con la condición *(3)*.
Para el siguiente paso se necesita determinar el número de puntos con los que cuenta la curva elíptica, $\#E(GF(p))$. Para calcularlo se puede implementar el algoritmo de Schoff que es de un tiempo polinómico.

Sin embargo, su teoría e implementación queda fuera del alcance de este artículo, para obtener detalles de este algoritmo se puede consultar (Schoff, 1995). Para nuestro propósito, utilizamos el cálculo de los residuos cuadráticos para determinar $\#E(GF(p))$. Para ello, el número de Legendre nos apoya para determinar los puntos que contienen residuos cuadráticos. Dados un número primo p y un entero cualquiera x, el símbolo de Legendre está definido de la siguiente manera:

$$\left(\frac{x}{p}\right) = \begin{cases} 1\ si\ x\ es\ un\ residuo\ cuadrático \\ -1\ si\ x\ no\ es\ residuo\ cuadrático \\ 0\ si\ x\ es\ múltiplo\ de\ p \end{cases} \quad (4)$$

Una alternativa para el cálculo del símbolo de Legendre es mediante el criterio de Euler utilizando la siguiente fórmula:

$$\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}} mod\ p, \quad (5)$$

En el que, al resolver **¡Error! No se encuentra el origen de la referencia.** se obtienen los valores 1, -1 y 0, y para determinar si es o no un residuo cuadrático se utiliza **¡Error! No se encuentra el origen de la referencia.**. A continuación, se muestra el algoritmo, del número de Legendre. Tomando a x como un número entero positivo cualquiera menor a p, z representa el resultado de evaluar en la ecuación $y^2 = (x^3 + 9x + 13)\ mod\ 19$ y r es el residuo cuadrático aplicando el símbolo de Legendre, se obtiene la tabla 1.

Una vez calculado el número de Legendre, se conoce la cantidad de puntos que tiene la curva, que en nuestro caso es #E(GF(p)) = 21. Ahora para calcular todos los puntos de la curva se toman los valores mostrados en la tabla 1 y se utiliza la formula $H = (x - p)^2$ dando como resultado la tabla 2.

x	z	residuo
0	13	-1
1	4	1
2	1	1
3	10	-1
4	18	-1
5	12	-1
6	17	1
7	1	1
8	8	-1
9	6	1
10	1	1
11	18	-1
12	6	1
13	9	1
14	14	-1
15	8	-1
16	16	1
17	6	1
18	3	-1

Tabla 1 Residuos Cuadráticos

y	H
0	0
1	1
2	4
3	9
4	16
5	6
6	17
7	11
8	7
9	5
10	5
11	7
12	11
13	17
14	6
15	16
16	9
17	4
18	1

Tabla 2 coordenadas y

Cuando obtenemos los valores de $x, z,$ y H en las tablas (1) y (2) respectivamente, se aplica el algoritmo de la Figura 2 para encontrar todos los puntos que pertenecen a la curva $E(GF(p))$. Para esto, se reciben dos arreglos donde tenemos almacenados los datos de las tablas anteriores, primeramente, se toma el primer valor de la tabla 1, es decir, el valor z**,** y si algún valor de z coincide con un valor de H en la tabla 2**,** entonces el punto está formado por el valor de x de la tabla 1 y el valor de y de la tabla 2.

Entrada: $arrayXZ$, $arrayYH$
Salida: Puntos de la curva E(GF(p))
1: $count \leftarrow 0$
2: **for** ($i = 0$ to length arrayXZ) **do**
3: $z \leftarrow arrayXZ[i] -> getZ()$ //función para obtener el valor de z
4: **for** ($j = 1$ to length arrayYH) **do**
5: **if** ($z = \boldsymbol{arrayYH[j] -> getH()}$) **then**
6: $arrayPoint[count] \leftarrow (arrayXZ[i] -> getX(), arrayYH[j] -> getY())$
7: $count \leftarrow +1$
8: **if** (isGen($arrayPoint[count]$)) **then**
9: return $arrayPoint[count]$

```
10:                    EndIf
11:          Endif
12:             Endfor
13: Endfor
```

Figura 2 Algoritmo para encontrar los puntos de la curva elíptica

Al hacer una modificación al algoritmo anterior se puede calcular el orden de todos los puntos de la curva. Para fines de ilustración en nuestro ejemplo se calcularon los órdenes de todos los puntos de la curva obteniendo la tabla 3. En la práctica esto no es necesario, puesto que sería demasiado costoso, ya que al ser un método que necesita calcular el símbolo de Legendre desde 0 hasta $p-1$ este se vuelve inviable a medida que el p crece.

x	y	Orden
1	2	21
1	17	21
2	1	7
2	18	7
6	6	21
6	13	21
7	1	21
7	18	21
9	5	21
9	14	21
10	1	3
10	18	3
12	5	7
12	14	7
13	3	21
13	16	21
16	4	7
16	15	7
17	5	21
17	14	21

Tabla 3 Orden de cada punto de la curva elíptica

Cifrado de datos

Para realizar el cifrado de los datos, se debe contar con los siguientes parámetros: el número primo p, los coeficientes a y b, la cardinalidad de puntos de la curva elíptica $\#E(GF(p))$, un punto generador G de la curva, valores M y h con $Mh < p$, $llaveSA$ (llave secreta del usuario A), $llaveSB$ (llave secreta del usuario B) en donde $mcd(llaveSA, llaveSB) = 1$**.** Estos parámetros son utilizados por el cifrado de El Gamal. Mostramos con un ejemplo el uso de la librería desarrollada en PHP. Para ello consideremos:

$p = 500009$
$a = 15567$
$b = 7896$
$\#E(GF(p)) = 499879$
$G = (241479, 71146)$
$M = 456$
$h = 123$
$LlaveSA = 24528$
$LlaveSB = 11923$
$y^2 = (x^3 + 15567x + 7896) \ mod\ 500009.$

Supongamos que tenemos un usuario que se va a registrar en una plataforma y lo que interesa cifrar es la contraseña. Para nuestro caso la contraseña es carlos123 e ingresa sus datos en un formulario, Figura 3.

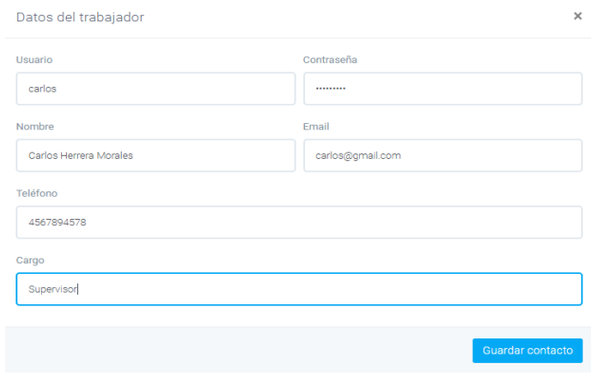


Figura 3 Formulario de contacto

Procedemos a cifrar la contraseña del usuario de la siguiente manera:

Paso 1. Codificar el mensaje, para ello usamos el código ascii que comprende del 0 al 255.

Inicializamos con $j = 1$. Sabiendo que el ascii de la letra c es 99 se realizan los siguientes pasos:

Paso 1. 1 Calculamos $x = ascii(c)(h) + j = 99\,(123) + 1 = 12178$, y se sustituye este resultado en la ecuación de la curva elíptica, esto es, $y^2 = (x^3 + 15567x + 7896) = 12178^3 + 15567(12178) + 7896 = 334992$**,** dado que no existe valor de y que cumpla con esta ecuación, se aumenta a $j = 2$ y se reinicia el proceso.

Paso 1.2 $x = ascii(c)\,h + j = 99\,(123) + 2 = 12179$**,** y se sustituye este resultado en la ecuación de la curva elíptica, esto es, $y^2 = (x^3 + 15567x + 7896) = 12179^3 + 15567(12179) + 7896 = 290136$ este número si tiene raíz cuadrada que es igual a 161435. Por tanto, la codificación de la letra c es $(12179, 161435)$. Repetimos este proceso para cada una de las letras y números obtenemos:

$c = (12179, 161435)$
$a = (11936, 218659)$
$r = (14023, 101746)$
$l = (13285, 115296)$

$o = (13656,29398)$
$s = (14147,176240)$
$1 = (6031,183341)$
$2 = (6152,153375)$
$3 = (6277,52620)$

Paso 2. Se calcula la llave pública de A: $llavePA = LlaveSA * G$ 0 24528 (241479 , 71146) (253513 , 78497), entonces la pareja es igual $A = (24528, (253513, 78497))$.

Paso 3. Se calcula la llave pública de B: $llavePB = LlaveSB * G =$ 11923 (241479 , 71146) = (339894 , 358573), entonces la pareja es igual $B = (4562, (339894,358573))$.

Paso 4. Ciframos la letra c eligiendo un entero aleatorio $k = 205887$ y multiplicamos ese número por el punto G, esto es, $kG = 205887(241479,71146) = (45235,155942)$.

Paso 5. Sumando la codificación de la letra c $+ k(llavePB)$ se obtiene:
$(12179,161435) + 205887(339894,358573)$
$= (12179,161435) + (237547,189319)$
$= (493092,311065)$.

Paso 6. Se unen los resultados obtenidos en los pasos 4 y 5 para que la pareja de coordenadas quede como: $((45235,155942), (493092,311065))$.
Repetimos estos pasos para cada uno de los caracteres restantes, se obtuvieron los siguientes resultados:

	Coordenadas Asignadas	k
c	(45235,155942,493092,311065)	205887
a	(464947,454208,261541,436656)	425387
r	(1424,194779,211919,45374)	294652
l	(91384,133847,124363,495034)	258306
o	(22940,216821,391383,182458)	99447
s	(30055,298941,323275,69773)	340580
1	(220188,341581,147194,45165)	162281
2	(254288,121557,358833,451256)	470133
3	(310143,142529,222099,59930)	92723

Al tener todos los puntos cifrados solo bastará con mandarlos a una base de datos, como se muestra en la Figura 4.

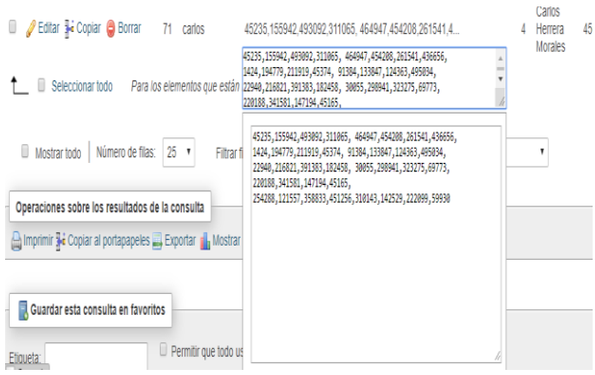


Figura 4 Puntos almacenados en una base de datos

El usuario al ser registrado puede ingresar a su información mediante su usuario y contraseña.

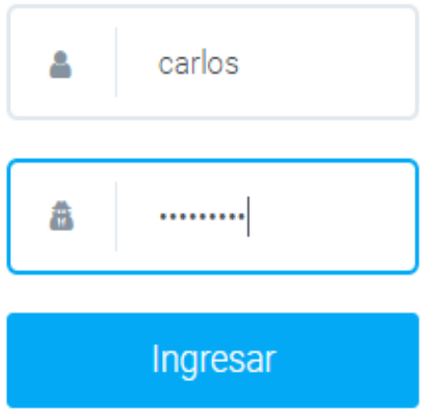


Figura 5 Datos del usuario

Ahora debemos verificar que el usuario ingreso la contraseña correcta para ello debemos descifrar esa información.

Paso 1. Descifraremos el primer punto que son $(45235,155942,493092,311065)$, tomando la primera pareja y multiplicándola por la llave secreta de B, esto es, $11923(45235,155942) = (237547,189319)$.

Paso 2. Se resta el resultado del paso 1 con la segunda pareja, recordando que $(x1, y1) - (x2, y2) = (x1, y1) + (x2, -y2)$. Por lo que se obtiene: $(493092,311065) + (237547, -189319) = (12179,161435)$.

Paso 3. Se realiza la decodificación usando la fórmula $\frac{x-1}{h}$. Sustituyendo los valores tenemos: $\frac{12179-1}{123} = 99.00813$. Redondeando el resultado para que este quede solo en 99, y como sabemos el número 99 en el código ascii corresponde a la letra c, se obtiene el primer descifrado. Procedemos así para cada uno de los puntos.

Conclusiones

Se muestran los conceptos matemáticos para la realización de los algoritmos de cifrado y descifrado usando criptografía en curvas elípticas.

Dado que actualmente las plataformas móviles o web recaban mucha información confidencial, se observó la necesidad de aportar un método de cifrado de esta información para que no pueda ser utilizada de manera incorrecta. Al hacer uso de una programación en PHP, se propone una librería que puede ser implementada para estos propósitos.

La dificultad que se presenta es la de calcular el número de puntos que contiene una curva elíptica, para ello será necesario establecer la programación adecuada para que logremos contar con este dato de una manera eficiente y poder trabajar con valores de números primos aún más grandes. Es por ello que, como trabajo a futuro se pueda realizar la implementación del algoritmo de Schoff para este propósito.

Referencias

Amalraj, J., Raybin, J. (2016). A survey paper on cryptography techniques. IJCSMC, Vol. 5, Issue 8, 55 – 59.

Diffie, W. & Hellman, M. (1976). New directions in cryptography. IEEE transactions on Information Theory, 22(6), 644-654.

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE transactions on information Theory, 31, 469-472

Gómez, J. (2002). Criptografía y curvas elípticas. La Gaceta de la RSME, Vol. 5, 737-777.

Granados, G. (2006). Introducción a la criptografía. Revista Digital Universitaria, Vol. 7, No. 7, 1-17.

Gupta, V., Stebila, D. y Chang, S. (2004). Integrating Elliptic Curve Cryptography into the Web's Security Infrastructure. Sun Microsystems, Inc., 402-403.

Hankerson, D., Menezes, A. and Vanstone, S. (2004). Guide to Elliptic Curve Cryptography. Springer-Verlag New York, Inc.

Koblitz, N. (1987). Elliptic curve in cryptography. American Mathematical Society J. Comput. Math., 207–209.

Miller, V. S. (1986). Use of elliptic curves in cryptography. In Lecture notes in computer sciences; 218 on Advances in cryptology. CRYPTO 85, USA. Springer-Verlag New York, Inc., 417– 426,

Kawahara, Y. Takagi, T. and Okamoto E. (2006). Efficient Implementation of Tate Pairing on a Mobile Phone Using Java. In Computational Intelligence and Security, vol. 2, 1247 - 1252, Berlin.

Katz, J., Lindell, Y. (2015) Introduction to Modern Cryptography. NY: Chapmann & Hall Book/CRC.

Schoff, N. (1995). Counting points on elliptic curves over _finite _fields, Journal de Théorie des Nombres de Bordeaux 7, 219-254.

ISSN-2531-2952

[Título en Times New Roman y Negritas No. 14 en Español e Inglés]

Apellidos (EN MAYUSCULAS), Nombre del 1er Autor†*, Apellidos (EN MAYUSCULAS), Nombre del 1er Coautor, Apellidos (EN MAYUSCULAS), Nombre del 2do Coautor y Apellidos (EN MAYUSCULAS), Nombre del 3er Coautor

Institución de Afiliación del Autor incluyendo dependencia (en Times New Roman No.10 y Cursiva)

International Identification of Science - Technology and Innovation

ID 1er Autor: (ORC ID - Researcher ID Thomson, arXiv Author ID - PubMed Autor ID - Open ID) y CVU 1er Autor: (Becario-PNPC o SNI-CONACYT) (No.10 Times New Roman)

ID 1er Coautor: (ORC ID - Researcher ID Thomson, arXiv Author ID - PubMed Autor ID - Open ID) y CVU 1er Coautor: (Becario-PNPC o SNI-CONACYT) (No.10 Times New Roman)

ID 2do Coautor: (ORC ID - Researcher ID Thomson, arXiv Author ID - PubMed Autor ID - Open ID) y CVU 2do Coautor: (Becario-PNPC o SNI-CONACYT) (No.10 Times New Roman)

ID 3er Coautor: (ORC ID - Researcher ID Thomson, arXiv Author ID - PubMed Autor ID - Open ID) y CVU 3er Coautor: (Becario-PNPC o SNI-CONACYT) (No.10 Times New Roman)

(Indicar Fecha de Envío: Mes, Día, Año); Aceptado (Indicar Fecha de Aceptación: Uso Exclusivo de ECORFAN

Resumen (En Español, 150-200 palabras)

Objetivos
Metodología
Contribución

Indicar 3 palabras clave en Times New Roman y Negritas No. 10 (En Español)

Resumen (En Inglés, 150-200 palabras)

Objetivos
Metodología
Contribución

Indicar 3 palabras clave en Times New Roman y Negritas No. 10 (En Inglés)

Citación: Apellidos (EN MAYUSCULAS), Nombre del 1er Autor†*, Apellidos (EN MAYUSCULAS), Nombre del 1er Coautor, Apellidos (EN MAYUSCULAS), Nombre del 2do Coautor y Apellidos (EN MAYUSCULAS), Nombre del 3er Coautor. Título del Artículo Revista de Cómputo Aplicado. Año 1-1: 1-11 (Times New Roman No. 10)

* Correspondencia del Autor (ejemplo@ejemplo.org)
† Investigador contribuyendo como primer autor.

Texto redactado en Times New Roman No.12, espacio sencillo.

Explicación del tema en general y explicar porque es importante.

¿Cuál es su valor agregado respecto de las demás técnicas?

Enfocar claramente cada una de sus características

Explicar con claridad el problema a solucionar y la hipótesis central.

Explicación de las secciones del Artículo

Desarrollo de Secciones y Apartados del Artículo con numeración subsecuente

[Título en Times New Roman No.12, espacio sencillo y Negrita]

Desarrollo de Artículos en Times New Roman No.12, espacio sencillo.

Inclusión de Gráficos, Figuras y Tablas-Editables

En el *contenido del Artículo* todo gráfico, tabla y figura debe ser editable en formatos que permitan modificar tamaño, tipo y número de letra, a efectos de edición, estas deberán estar en alta calidad, no pixeladas y deben ser notables aun reduciendo la imagen a escala.

[Indicando el título en la parte inferior con Times New Roman No. 10 y Negrita]

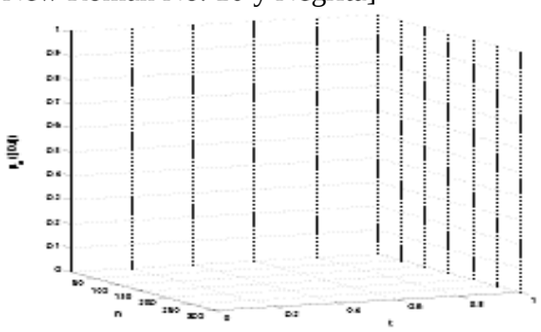


Gráfico 1 Titulo y *Fuente (en cursiva)*

No deberán ser imágenes, todo debe ser editable.

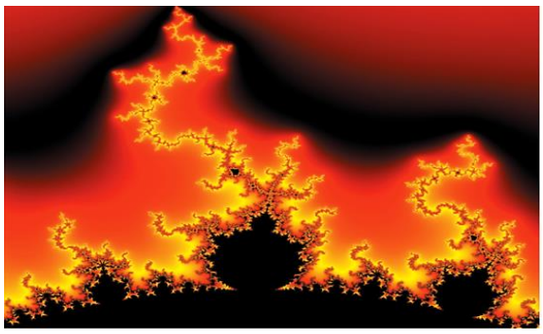


Figura 1 Titulo y *Fuente (en cursiva)*

No deberán ser imágenes, todo debe ser editable.

Tabla 1 Titulo y *Fuente (en cursiva)*

No deberán ser imágenes, todo debe ser editable.

Cada Artículo deberá presentar de manera separada en **3 Carpetas**: a) Figuras, b) Gráficos y c) Tablas en formato .JPG, indicando el número en Negrita y el Titulo secuencial.

Para el uso de Ecuaciones, señalar de la siguiente forma:

$$Y_{ij} = \alpha + \sum_{h=1}^{r} \beta_h X_{hij} + u_j + e_{ij} \qquad (1)$$

Deberán ser editables y con numeración alineada en el extremo derecho.

Metodología a desarrollar

Dar el significado de las variables en redacción lineal y es importante la comparación de los criterios usados

Resultados

Los resultados deberán ser por sección del Artículo.

Anexos

Tablas y fuentes adecuadas.

Agradecimiento

Indicar si fueron financiados por alguna Institución, Universidad o Empresa.

ISSN: 2531-2952

Conclusiones

Explicar con claridad los resultados obtenidos y las posibilidades de mejora.

Referencias

Utilizar sistema APA. No deben estar numerados, tampoco con viñetas, sin embargo en caso necesario de numerar será porque se hace referencia o mención en alguna parte del Artículo.

Utilizar Alfabeto Romano, todas las referencias que ha utilizado deben estar en el Alfabeto romano, incluso si usted ha citado un Artículo, libro en cualquiera de los idiomas oficiales de la Organización de las Naciones Unidas (Inglés, Francés, Alemán, Chino, Ruso, Portugués, Italiano, Español, Árabe), debe escribir la referencia en escritura romana y no en cualquiera de los idiomas oficiales.

Ficha Técnica

Cada Artículo deberá presentar un documento Word (.docx):

Nombre de la Revista
Título del Artículo
Abstract
Keywords
Secciones del Artículo, por ejemplo:

1. *Introducción*
2. *Descripción del método*
3. *Análisis a partir de la regresión por curva de demanda*
4. *Resultados*
5. *Agradecimiento*
6. *Conclusiones*
7. *Referencias*

Nombre de Autor (es)
Correo Electrónico de Correspondencia al Autor
Referencias

Requerimientos de Propiedad Intelectual para su edición:

-Firma Autógrafa en Color Azul del Formato de Originalidad del Autor y Coautores

-Firma Autógrafa en Color Azul del Formato de Aceptación del Autor y Coautores

ISSN: 2531-2952

Reserva a la Política Editorial

Revista de Cómputo Aplicado se reserva el derecho de hacer los cambios editoriales requeridos para adecuar los Artículos a la Política Editorial del Research Journal. Una vez aceptado el Artículo en su versión final, el Research Journal enviará al autor las pruebas para su revisión. ECORFAN® únicamente aceptará la corrección de erratas y errores u omisiones provenientes del proceso de edición de la revista reservándose en su totalidad los derechos de autor y difusión de contenido. No se aceptarán supresiones, sustituciones o añadidos que alteren la formación del Artículo.

Código de Ética – Buenas Prácticas y Declaratoria de Solución a Conflictos Editoriales

Declaración de Originalidad y carácter inédito del Artículo, de Autoría, sobre la obtención de datos e interpretación de resultados, Agradecimientos, Conflicto de intereses, Cesión de derechos y distribución

La Dirección de ECORFAN-México, S.C reivindica a los Autores de Artículos que su contenido debe ser original, inédito y de contenido Científico, Tecnológico y de Innovación para someterlo a evaluación.

Los Autores firmantes del Artículo deben ser los mismos que han contribuido a su concepción, realización y desarrollo, así como a la obtención de los datos, la interpretación de los resultados, su redacción y revisión. El Autor de correspondencia del Artículo propuesto requisitara el formulario que sigue a continuación.

Título del Artículo:

- El envío de un Artículo a Revista de Cómputo Aplicado emana el compromiso del autor de no someterlo de manera simultánea a la consideración de otras publicaciones seriadas para ello deberá complementar el Formato de Originalidad para su Artículo, salvo que sea rechazado por el Comité de Arbitraje, podrá ser retirado.

- Ninguno de los datos presentados en este Articulo ha sido plagiado ó inventado. Los datos originales se distinguen claramente de los ya publicados. Y se tiene conocimiento del testeo en PLAGSCAN si se detecta un nivel de plagio Positivo no se procederá a arbitrar.

- Se citan las referencias en las que se basa la información contenida en el Artículo, así como las teorías y los datos procedentes de otros Artículos previamente publicados.

- Los autores firman el Formato de Autorización para que su Artículo se difunda por los medios que ECORFAN-México, S.C. en su Holding Spain considere pertinentes para divulgación y difusión de su Artículo cediendo sus Derechos de Obra.

- Se ha obtenido el consentimiento de quienes han aportado datos no publicados obtenidos mediante comunicación verbal o escrita, y se identifican adecuadamente dicha comunicación y autoría.

- El Autor y Co-Autores que firman este trabajo han participado en su planificación, diseño y ejecución, así como en la interpretación de los resultados. Asimismo, revisaron críticamente el trabajo, aprobaron su versión final y están de acuerdo con su publicación.

- No se ha omitido ninguna firma responsable del trabajo y se satisfacen los criterios de Autoría Científica.

- Los resultados de este Artículo se han interpretado objetivamente. Cualquier resultado contrario al punto de vista de quienes firman se expone y discute en el Artículo.

Copyright y Accesso

La publicación de este Artículo supone la cesión del copyright a ECORFAN-México, S.C en su Holding Spain para su Revista de Cómputo Aplicado, que se reserva el derecho a distribuir en la Web la versión publicada del Artículo y la puesta a disposición del Artículo en este formato supone para sus Autores el cumplimiento de lo establecido en la Ley de Ciencia y Tecnología de los Estados Unidos Mexicanos, en lo relativo a la obligatoriedad de permitir el acceso a los resultados de Investigaciones Científicas.

Título del Artículo:

Nombre y apellidos del Autor de contacto y de los Coautores	Firma
1.	
2.	
3.	
4.	

Principios de Ética y Declaratoria de Solución a Conflictos Editoriales

Responsabilidades del Editor

El Editor se compromete a garantizar la confidencialidad del proceso de evaluación, no podrá revelar a los Árbitros la identidad de los Autores, tampoco podrá revelar la identidad de los Árbitros en ningún momento.

El Editor asume la responsabilidad de informar debidamente al Autor la fase del proceso editorial en que se encuentra el texto enviado, así como de las resoluciones del arbitraje a Doble Ciego.

El Editor debe evaluar los manuscritos y su contenido intelectual sin distinción de raza, género, orientación sexual, creencias religiosas, origen étnico, nacionalidad, o la filosofía política de los Autores.

El Editor y su equipo de edición de los Holdings de ECORFAN® no divulgarán ninguna información sobre Artículos enviado a cualquier persona que no sea el Autor correspondiente.

El Editor debe tomar decisiones justas e imparciales y garantizar un proceso de arbitraje por pares justa.

Responsabilidades del Consejo Editorial

La descripción de los procesos de revisión por pares es dado a conocer por el Consejo Editorial con el fin de que los Autores conozcan cuáles son los criterios de evaluación y estará siempre dispuesto a justificar cualquier controversia en el proceso de evaluación. En caso de Detección de Plagio al Artículo el Comité notifica a los Autores por Violación al Derecho de Autoría Científica, Tecnológica y de Innovación.

Responsabilidades del Comité Arbitral

Los Árbitros se comprometen a notificar sobre cualquier conducta no ética por parte de los Autores y señalar toda la información que pueda ser motivo para rechazar la publicación de los Artículos. Además, deben comprometerse a mantener de manera confidencial la información relacionada con los Artículos que evalúan.

Cualquier manuscrito recibido para su arbitraje debe ser tratado como documento confidencial, no se debe mostrar o discutir con otros expertos, excepto con autorización del Editor.

Los Árbitros se deben conducir de manera objetiva, toda crítica personal al Autor es inapropiada.

Los Árbitros deben expresar sus puntos de vista con claridad y con argumentos válidos que contribuyan al que hacer Científico, Tecnológica y de Innovación del Autor.

Los Árbitros no deben evaluar los manuscritos en los que tienen conflictos de intereses y que se hayan notificado al Editor antes de someter el Artículo a evaluación.

Responsabilidades de los Autores

Los Autores deben garantizar que sus Artículos son producto de su trabajo original y que los datos han sido obtenidos de manera ética.

Los Autores deben garantizar no han sido previamente publicados o que no estén siendo considerados en otra publicación seriada.

Los Autores deben seguir estrictamente las normas para la publicación de Artículos definidas por el Consejo Editorial.

Los Autores deben considerar que el plagio en todas sus formas constituye una conducta no ética editorial y es inaceptable, en consecuencia, cualquier manuscrito que incurra en plagio será eliminado y no considerado para su publicación.

Los Autores deben citar las publicaciones que han sido influyentes en la naturaleza del Artículo presentado a arbitraje.

Servicios de Información

Indización - Bases y Repositorios

RESEARCH GATE (Alemania)
GOOGLE SCHOLAR (Índices de citaciones-Google)
MENDELEY (Gestor de Referencias bibliográficas)
REDIB (Red Iberoamericana de Innovación y Conocimiento Científico- CSIC)
HISPANA (Información y Orientación Bibliográfica-España)

Servicios Editoriales:

Identificación de Citación e Índice H.
Administración del Formato de Originalidad y Autorización.
Testeo de Artículo con PLAGSCAN.
Evaluación de Artículo.
Emisión de Certificado de Arbitraje.
Edición de Artículo.
Maquetación Web.
Indización y Repositorio
Traducción.
Publicación de Obra.
Certificado de Obra.
Facturación por Servicio de Edición.

Política Editorial y Administración

38 Matacerquillas, CP-28411. Moralzarzal –Madrid-España. Tel: +52 1 55 6159 2296, +52 1 55 1260 0355, +52 1 55 6034 9181; Correo electrónico: contact@ecorfan.org www.ecorfan.org

Licencias del Sitio

03-2010-032610094200-01-Para material impreso, 03-2010-031613323600-01-Para material electrónico, 03-2010-032610105200-01-Para material fotográfico, 03-2010-032610115700-14-Para Compilación de Datos, 04 -2010-031613323600-01-Para su página Web, 19502-Para la Indización Iberoamericana y del Caribe, 20-281 HB9-Para la Indización en América Latina en Ciencias Sociales y Humanidades, 671-Para la Indización en Revistas Científicas Electrónicas España y América Latina, 7045008-Para su divulgación y edición en el Ministerio de Educación y Cultura-España, 25409-Para su repositorio en la Biblioteca Universitaria-Madrid, 16258-Para su indexación en Dialnet, 20589-Para Indización en el Directorio en los países de Iberoamérica y el Caribe, 15048-Para el registro internacional de Congresos y Coloquios. financingprograms@ecorfan.org

Oficinas de Gestión

38 Matacerquillas, CP-28411. Moralzarzal –Madrid-España.

Revista de Cómputo Aplicado

2531 2952
ISSN 2531 - 2952