Arquitectura de Computadoras en Sistemas IoT, Computación Móvil, Wearable Computing, MIPS aplicado a criptografía

Revisión de artículos científicos

Bryan Aguilar Yaguana.
Carrera de Sistemas
Universidad de Cuenca
Cuenca, Ecuador
bryan.aguilar@ucuenca.edu.ec

Christian Collaguazo Malla.
Carrera de Sistemas
Universidad de Cuenca
Cuenca, Ecuador
christian.collaguaz@ucuenca.edu.ec

Freddy Abad León.
Carrera de Sistemas
Universidad de Cuenca
Cuenca, Ecuador
freddy.abad@ucuenca.edu

I. Introducción

El presente informe detalla el proceso de investigación de 60 artículos académicos para obtener un tema central para el proyecto final de la Asignatura "Organización y Arquitectura de Computadoras". En el entorno actual la computación a visto un rápido crecimiento en términos de potencia llegando a tener hoy en dia Supercomputadoras las cuales poseen un gran poder de procesamiento, en contraparte se encuentran los pequeños dispositivos los cuales hace algunas décadas contaban con una capacidad limitada de procesamiento y de condiciones de hardware las cuales se veían limitados por potencia y fuente de energía limitada contando con un microcontrolador con órdenes previamente grabadas en memoria esto limitaba la cantidad de instrucciones con las cuales estas órdenes podrán ser grabadas. Arquitecturas como ARM están enfocados a funcionar sobre estos pequeños dispositivos, pero con la llegada de internet y la creciente demanda de dispositivos móviles, el IoT así como Wearable Computing se han visto un gran aumento en el uso de esta arquitectura llegando poco a poco a superar el poder de procesamiento de Supercomputadoras de hace algunas décadas, esto hace plantearse si la misma arquitectura funciona de mejor forma en términos de optimización de recursos en todos los dispositivos móviles, IoT o wearable computing. Así mismo, la seguridad en los entornos actuales donde se tiene dispositivos con procesadores (IoT) en donde no se pensaba tener antes, hace prever una revolución en cuanto a las arquitecturas de los procesadores, donde se exige un mayor procesamiento a coste de una mejor y mayor seguridad. Esto plantea distintas líneas de investigación, las cuales a continuación se toca algunos temas, y se elige articulos a desarrollar.

II. Estado del Arte

Desde la creación la creación del transistor la computación a visto un rápido crecimiento en términos de potencia llegando a tener hoy en dia Supercomputadoras las cuales poseen un gran poder de procesamiento, en contra parte se encuentran los pequeños dispositivos los cuales hace algunas décadas contaban con una capacidad limitada de procesamiento y de condiciones de hardware las cuales se veían limitados por potencia y fuente de energía limitada contando con un microcontrolador con órdenes previamente grabadas en memoria esto limitaba la cantidad de instrucciones con las cuales estas órdenes podrán ser grabadas.

Arquitecturas como ARM están enfocados a funcionar sobre estos pequeños dispositivos, pero con la llegada de internet y la creciente demanda de dispositivos móviles, el IoT así como Wearable Computing se han visto un gran aumento en el uso de esta arquitectura llegando poco a poco a superar el poder de procesamiento de Supercomputadoras de hace algunas décadas, esto hace plantearse si la misma arquitectura funciona de mejor forma en términos de optimización de recursos en todos los dispositivos móviles, IoT o wearable computing, todo esto depende del sistema que forman estos dispositivos por ejemplo los dispositivos móviles pueden funcionar sin necesidad de estar conectados a internet donde tanto Memoria, CPU, E/S se encuentran integrados en un mismo hardware y con la potencia que es mayor a supercomputadoras de decadas atras. Mientras que sistemas como el Wearable Computing pueden tener todo el hardware integrado pero se ven mucho más limitados en poder de procesamiento que otros dispositivos móviles, con un sistema que integra de igual forma un CPU, Memoria, E/S la cual en este caso puede verse de gran forma limitada y el

comportamiento interno se vuelve diferente al de un sistema normal.

Mientras tanto el IoT el cual puede estar formado por una red de nodos los cuales pueden formar un gran cluster el cual le da a estos un gran poder de procesamiento en conjunto mediante la computación distribuida, estos al ser sistemas altamente escalables pueden formar sistemas complejos los cuales pueden superar a la computadoras personales de hoy en día, por lo cual resulta interesante conocer el cómo se mueven los datos dentro de estos sistemas, ya que tanto CPU, Memoria, E/S pueden estar distribuidos en distintos nodos de la red que conforman estos.

Hoy en dia hay mas dispositivos conectados a internet que personas los cuales cada día aumentan en capacidad de almacenamiento, procesamiento, con nuevas formas para interactuar con ellos provocando cambios en los dispositivos de entrada y salida. Con esto se deja en claro que debe haber mejoras la arquitectura actual de estos dispositivos ya que cada dia que pasa, dicha arquitectura debe usar de mejor manera los recursos del sistema donde se ejecutan y al haber tantas alternativas puede que varien de un sistema a otro.
Por otro lado, la seguridad en una epoca donde todos los dispoitivos están conectados entre sí, es primordial. Sin embargo, es un tema que se suele pasar por alto, por la "confianza" que tienen los usuarios en las plataformas que utilizan, y el poco valor que otorgan a sus propios datos.
Dado esto, la Criptología "es la disciplina que se dedica al estudio de la escritura secreta, es decir, estudia los mensajes que, procesados de cierta manera, se convierten en difíciles o imposibles de leer por entidades no autorizadas".
El análisis de la Criptología y todos los subtemas que conllevan en la actualidad es imperante, gran parte de los algoritmos criptográficos permiten mantener seguridad en los datos transmitidos en la red, sin embargo, para que estos algoritmos funcionan correctamente y sean potentes, es necesaria una potencia computacional de cálculo cada vez más grande. Es por esto que la optimización de las operaciones que realiza cada algoritmo criptográfico disminuye el número de filtraciones de información secreta, y a la vez disminuye costes a los usuarios que optan por mantener sus datos seguros.

III. Análisis clúster

A. Análisis: 1er grupo de artículos - Clusterización 1

k = 2
Distancia media centroide cluster: 0.400
Cluster menores : 1
Distancia de Bouldin: 0.006

k = 3
Distancia media centroide cluster: 0.415
Cluster menores : 2
Distancia de Bouldin: 0.005

k = 4
Distancia media centroide cluster: 0.427
Cluster menores : 2
Distancia de Bouldin: 0.005

k = 5
Distancia media centroide cluster: 0.457
Cluster menores : 2
Distancia de Bouldin: 0.005

k = 6
Distancia media centroide cluster: 0.457
Cluster menores : 3
Distancia de Bouldin: 0.004

k = 7
Distancia media centroide cluster: 0.460
Cluster menores : 1
Distancia de Bouldin: 0.004

B. Análisis: 2er grupo de artículos - Clusterización 2

k = 2
Distancia media centroide cluster: 0.226
Cluster menores : 1
Distancia de Bouldin: 0.005

k = 3
Distancia media centroide cluster: 0.206
Cluster menores : 2
Distancia de Bouldin: 0.004

k = 4
Distancia media centroide cluster: 0.188
Cluster menores : 1
Distancia de Bouldin: 0.004

k = 5
Distancia media centroide cluster: 0.174
Cluster menores : 4
Distancia de Bouldin: 0.003

k = 6
Distancia media centroide cluster: 0.154
Cluster menores : 3
Distancia de Bouldin: 0.003

k = 7
Distancia media centroide cluster: 0.145
Cluster menores : 5
Distancia de Bouldin: 0.002

k = 8

Distancia media centroide cluster: 0.126
Cluster menores : 4
Distancia de Bouldin: 0.002

C. Análisis: 3er grupo de artículos - Clusterización 3

Para el análisis del 3er grupo de artículos, se utilizaron investigaciones referentes a la optimizaciones de operaciones en MIPS, Assembly y Web Assembly para aplicaciones criptográficas.

k = 2
Distancia media centroide cluster: 0.237
Cluster menores : 1
Distancia de Bouldin: 0.005

k = 3
Distancia media centroide cluster: 0.216
Cluster menores : 2
Distancia de Bouldin: 0.004

k = 4
Distancia media centroide cluster: 0.196
Cluster menores : 2
Distancia de Bouldin: 0.004

k = 5
Distancia media centroide cluster: 0.165
Cluster menores : 2
Distancia de Bouldin: 0.003

k = 6
Distancia media centroide cluster: 0.165
Cluster menores : 3
Distancia de Bouldin: 0.003

k = 7
Distancia media centroide cluster: 0.145
Cluster menores : 1
Distancia de Bouldin: 0.003

IV. RESULTADOS

Row No.	cluster	TITULO	ENLACE
2	cluster_0	The Case for VM-Based Cloudlets in Mobile Computing	https://ieeexpl...
3	cluster_0	VCMIA: A Novel Architecture for Integrating Vehicular Cyber-Physical Sy...	https://link.sp...
4	cluster_0	A QoS-aware system for mobile cloud computing	https://ieeexpl...
8	cluster_0	A survey of mobile cloud computing: architecture, applications, and app...	https://onlinel...
5	cluster_1	Wireless sensor network operating systems: a survey	https://dl.acm...
6	cluster_1	Xen on ARM: System Virtualization Using Xen Hypervisor for ARM-Base...	https://ieeexpl...
7	cluster_1	The low power architecture approach towards exascale computing	https://www.s...
15	cluster_1	Hermes: A Real Time Hypervisor for Mobile and IoT Systems	https://dl.acm...
18	cluster_1	Design of 32 bit (MIPS) RISC PROCESSOR using FPGA	https://dl.acm...
10	cluster_2	An IoT-Based Computational Framework for Healthcare Monitoring in ...	https://www....
16	cluster_2	A Software Defined Fog Node Based Distributed Blockchain Cloud Arc...	https://ieeexpl...
17	cluster_2	DIAT: A Scalable Distributed Architecture for IoT	https://ieeexpl...
19	cluster_2	An IoT Gateway Centric Architecture to Provide Novel M2M Services	https://ieeexpl...
9	cluster_3	Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the S...	https://ieeexpl...
11	cluster_3	Study of Various Internet of Things Platforms	https://www.r...
20	cluster_3	IOT Gateway: Bridging Wireless Sensor Networks into Internet of Things	https://ieeexpl...
1	cluster_4	Serving at the Edge: A Scalable IoT Architecture Based on Transparent ...	https://ieeexpl...
12	cluster_4	Edge Computing: Vision and Challenges	https://ieeexpl...
13	cluster_4	A Novel Meta OS Approach for Streaming Programs in Ubiquitous Com...	https://ieeexpl...
14	cluster_4	Introducing the new paradigm of Social Dispersed Computing: Applicat...	https://www.s...

Fig. 2. Agrupamiento de documentos con k = 5

A. Resultados de la primera Clusterización

Los datos arrojados por la herramienta y luego del análisis hecho de la distancia media interclusters nos da como resultado que el mejor agrupamiento está entre 5 y 7 agrupamientos ya que el número de clusters con centroides menores a la media, son relativamente pocos comparados con los que sobrepasan esta medida, además la distancia de Bouldin es relativamente baja lo cual reafirma esta elección.

El primer agrupamiento (Cluster_0) obtenido contiene los siguientes papers:

- The Case for VM-Based Cloudlets in Mobile Computing
- VCMIA: A Novel Architecture for Integrating Vehicular Cyber-Physical Systems and Mobile Cloud Computing
- A QoS-aware system for mobile cloud computing
- A survey of mobile cloud computing: architecture, applications, and approaches

Este cluster se descarta ya que no se realiza ninguna simulación si no se centra más en explicar las aplicaciones de la computación móvil con ambientes distribuidos, que integran servicios en la nube.

El segundo agrupamiento (Cluster_1) contiene los siguientes papers.

- Wireless sensor network operating systems: a survey
- Xen on ARM: System Virtualization Using Xen Hypervisor for ARM-Based Secure Mobile Phones
- Hermes: A Real Time Hypervisor for Mobile and IoT Systems.
- The low power architecture approach towards exascale computing
- Design of 32 bit (MIPS) RISC PROCESSOR using FPGA

En este caso se ha elegido el paper “Xen on ARM: System Virtualization Using Xen Hypervisor for ARM-Based Secure Mobile Phones” En el cual proponen un diseño de virtualización de un sistema para la arquitectura de CPU ARM.

Otro de los papers que se tomarán en cuenta para la siguiente etapa es el de “The low power architecture approach towards exascale computing” el busca una alternativa a la supercomputación, mediante el uso de procesadores de móviles de baja potencia basados en ARM.

El tercer agrupamiento (Cluster_2) contiene los siguientes papers.

- An IoT-Based Computational Framework for Healthcare Monitoring in Mobile Environments
- A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT
- DIAT: A Scalable Distributed Architecture for IoT
- An IoT Gateway Centric Architecture to Provide Novel M2M Services

De Forma general este grupo habla sobre aplicaciones IoT en ambientes distribuidos, como en el caso del primer paper el cual propone aplicar IoT en un ambiente distribuido orientado al monitoreo, este se descarta ya que nos es importante para el caso de estudio.
El tercer paper “DIAT: A Scalable Distributed Architecture for IoT” es el más interesante ya que trata sobre una nueva arquitectura distribuida nombrada DIAT. Trata específicamente la heterogeneidad de los dispositivos de IoT y permite la adición perfecta de nuevos dispositivos en todas las aplicaciones.

El cuarto agrupamiento (Cluster_3) contiene los siguientes papers.

- Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges
- Study of Various Internet of Things Platforms
- IOT Gateway: Bridging Wireless Sensor Networks into Internet of Things

El paper a tomar en cuenta es el de “Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges” el cual habla un poco del estado del arte actual integración de internet de las cosas en sistemas industriales y como puede ser la integración de nuevas arquitecturas más complejas sobre este sistema.

Los demás papers se centran más en las arquitecturas de redes de computadoras como la infraestructura de red que se puede aplicar sobre el IoT y su futuro.

El quinto agrupamiento (Cluster_4) contiene los siguientes papers

- Serving at the Edge: A Scalable IoT Architecture Based on Transparent Computing
- Edge Computing: Vision and Challenges
- A Novel Meta OS Approach for Streaming Programs in Ubiquitous Computing
- Introducing the new paradigm of Social Dispersed Computing: Applications, Technologies and Challenges

De este cluster se va descartar los tres últimos, ya que en ellos se habla más sobre la computación ubicua y se enfocan en dar una solución más orientadas al software y el SO de estas.

El paper titulado “Serving at the Edge: A Scalable IoT Architecture Based on Transparent Computing” da además de los enfoques de los posteriores papers una idea de la arquitectura de computadores que plantean como solución para mejorar tiempos de respuesta y consumo energético en sistemas IoT.

Una vez ya analizados los diferentes cluster los siguientes papers fueron tomados en cuenta para el siguiente análisis del caso de estudio.

1. **Primer Agrupamiento**

Se descartaron porque se centran más en la cloud computing aplicado a la computación móvil.

2. **Segundo Agrupamiento**

- **Xen on ARM: System Virtualization Using Xen Hypervisor for ARM-Based Secure Mobile Phones.**

Resultados de “Xen on ARM: System Virtualization Using Xen Hypervisor for ARM-Based Secure Mobile Phones”

Mediante el uso sistema de virtualización Xen los autores del paper realizan las siguiente prueba ellos modifican Xen 3.0.2 para que se ejecute en una plataforma de desarrollo de teléfonos inteligentes que está equipada con un núcleo ARM926-EJS de 266MHz, DRAM de 64MB y flash NOR de 32MB. Linux 2.6 está paravirtualizado para ejecutarse bajo Xen en ARM. Dos máquinas virtuales (dom0 y domU) de Linux 2.6.11 para virtualizadas se ejecutan en el VMM.

- **The low power architecture approach towards exascale computing.**

Resultados de "The low power architecture approach towards exascale computing" el cual realiza un prototipo el cual consta de un microprocesador de tipo SOC y de una red interconectada a través de una red de computadoras. Como resultado obtienen lo siguiente el experimento se hizo con el uso de procesadores ARM Cortex-A9 contra un procesador Intel Core I7 donde el procesador intel proporciona veces mayor rendimiento, pero ARM presenta una mayor eficiencia energética. La cual permite integrar varios nodos con un procesador ARM y así lograr competir con la potencia de procesadores más poderosos sin sacrificar la eficiencia energética.

- **Design of 32 bit (MIPS) RISC PROCESSOR using FPGA**

Resultados de "Design of 32 bit (MIPS) RISC PROCESSOR using FPGA"

- Los resultados son descritos de la siguiente manera por los autores "El resultado del diseño tiende a la siguiente conclusión El diseño descrito en HDL puede dirigirse fácilmente a diferentes tecnologías y también puede reconfigurarse fácilmente para diferentes requisitos de aplicación. También con la ayuda de una nueva metodología de diseño y herramientas EDA, el tiempo de diseño se puede reducir considerablemente. Todo el rendimiento del sistema se puede mejorar con la ayuda del mejor algoritmo disponible con estas herramientas EDA". []

3. Tercer Agrupamiento

- **DIAT: A Scalable Distributed Architecture for IoT**

Resultados de "DIAT: A Scalable Distributed Architecture for IoT".

- En este documento en la conclusión recalca que se describen los fundamentos de una arquitectura genérica de IoT, en esta arquitectura de IoT se propone también aspectos de seguridad y privacidad utilizando políticas de control de uso. Este paper se descarta ya que no se centra en la arquitectura interna del sistema.

4. Cuarto Agrupamiento

- **Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges.**

Resultados de "Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges."
De igual forma este paper solo brinda conclusiones sobre la asistencia de los servicios en la nube sobre sistemas IoT.

5. Quito Agrupamiento

- **Serving at the Edge: A Scalable IoT Architecture Based on Transparent Computing.**

Resultados de "Serving at the Edge: A Scalable IoT Architecture Based on Transparent Computing."
En este paper no se hace una demo o una simulación de la arquitectura que se propone lograr, si no se da una serie de conclusiones en la cual se remarca que el artículo es una introducción a esta arquitectura.

Casos Finales de Estudio
Después de un análisis más profundo de los se decidió tomar como punto de referencia los siguiente dos papers.

- Design of 32 bit (MIPS) RISC PROCESSOR using FPGA
- Xen on ARM: System Virtualization Using Xen Hypervisor for ARM-Based Secure Mobile Phones

Estos papers ya han sido revisados con lo cual se propone la creación de un simulador de un procesador RISC en el cual se pueda además simular y mostrar el tratamiento de los datos y la arquitectura interna en sistema moviles proponiendo una solución como en el paper "Xen on ARM".

B. Resultados de la segunda Clusterización

Los datos arrojados por la herramienta y luego del análisis hecho de la distancia media interclusters nos da como resultado que el mejor agrupamiento está en 4 grupos ya que el número de clusters con centroides menores a la media, son relativamente pocos comparados con los que sobrepasan esta medida, además la distancia de Bouldin es relativamente baja lo cual reafirma esta elección.

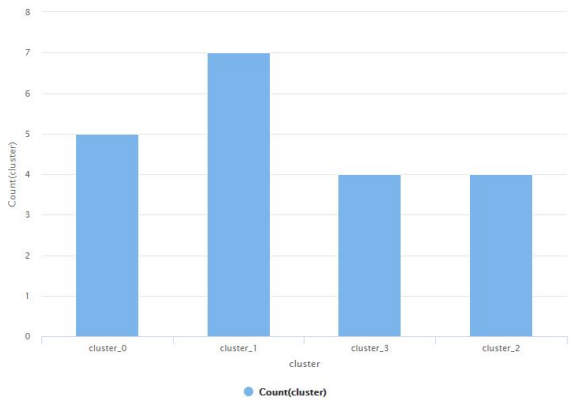

Fig. 2. Agrupamiento de documentos con k = 4

El primer agrupamiento (Cluster_0) obtenido contiene los siguientes papers:

- IOT Gateway: Bridging Wireless Sensor Networks into Internet of Things
- Internet of Things: Architectures, Protocols, and Applications
- An IoT Gateway Centric Architecture to Provide Novel M2M Services
- An IoT-Aware Architecture for Smart Healthcare Systems
- IOT Gateway: Bridging Wireless Sensor Networks into Internet of Things

De manera general, este primer grupo de artículos habla sobre el desarrollo de sensores, comunicaciones móviles inalámbricas y otras tecnologías de internet de las cosas que han sido empleadas para mejorar las condiciones de vida de las personas. Además, se analizan los métodos, protocolos y aplicaciones de vanguardia en esta nueva área emergente. Incluso se plantean arquitecturas de sistemas que permitan la interacción entre clientes móviles y dispositivos inteligentes.

El segundo agrupamiento (Cluster_1) contiene los siguientes papers:

- IoT Architectural Framework: Connection and Integration Framework for IoT Systems
- DIAT: A Scalable Distributed Architecture for IoT
- Challenges in IoT Networking via TCP/IP Architecture
- Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges
- Reliability and Security Issues for IoT-Based Smart Business Center: Architecture and Markov Model
- Semantic Gateway as a Service architecture for IoT Interoperability
- Study and Application on the Architecture and Key Technologies for IOT

De manera general, este segundo grupo de artículos se refieren a las arquitecturas implementadas y por implementar en IOT. Los principales inconvenientes de cada una de ellas, como por ejemplo la escalabilidad, heterogeneidad, seguridad e interoperabilidad. Y se presentan propuestas de arquitecturas de IOT para solventar dichos inconvenientes.

El tercer agrupamiento (Cluster_2) contiene los siguientes papers:

- An Integrated IoT Architecture for Smart Metering
- Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges
- Internet of Things(IoT): Security Challenges, Business Opportunities & Reference Architecture for E-commerce
- Internet of Things (IoT) System Architecture and Technologies

De manera general este tercer grupo de artículos se refieren a soluciones creadas con tecnología que involucra IOT que permitan recopilar y analizar la distribución de datos en diversos dispositivos. Con el objetivo de obtener información valiosa sobre los datos generados.

El cuarto agrupamiento (Cluster_3) contiene los siguientes papers:

- A Software Defined Fog Node based Distributed Blockchain Cloud Architecture for IoT
- Software-Defined Fog Network Architecture for IoT
- Responsive Data Architecture for the Internet of Things
- Serving at the Edge: A Scalable IoT Architecture Based on Transparent Computing

De manera general, el cuarto grupo de artículos se refiere a la expansión de IOT y al gran volumen de datos que generan los dispositivos inteligentes y las soluciones propuestas a estos problemas. Además habla sobre los desafíos que deben abordar las distintas arquitecturas frente a dichos problemas. Se plantean modelos de soluciones que contraataquen estos inconvenientes en las arquitecturas IOT tradicionales.

Una vez leídos los resúmenes de todos los documentos antes mencionados, se han elegido cinco papers que acotan de mejor manera el tema de investigación. De cada uno de ellos, se ha realizado la lectura tanto del abstract, resultados y conclusiones. Con esto se ha obtenido una mejor visión del tema de investigación; a continuación se muestra una breve descripción de cada unos de los papers elegidos. Los papers son:

- ***IOT Gateway: Bridging Wireless Sensor Networks into Internet of Things***

Con el desarrollo de sensores, comunicaciones móviles inalámbricas, sistemas integrados y computación en la nube, las tecnologías de IOT varios gobiernos de todo el mundo han prestado mucha atención a Internet of Things. Se propone un sistema IOT Gateway basado en los protocolos Zigbee y GPRS de acuerdo con los escenarios y requisitos típicos de las aplicaciones IOT, se presenta la transmisión de datos entre redes de sensores inalámbricos y redes de comunicaciones móviles, conversión de protocolos de diferentes protocolos de

redes de sensores, y funciones de control para redes de sensores, y finalmente dio una implementación del sistema de prototipos y la validación del sistema. Esta propuesta de sistema puede ser utilizado en hogares inteligentes, monitoreo industrial, redes inteligentes, monitoreo de entornos, etc. En trabajos futuros, se consideran funciones avanzadas de IOT Gateway, incluyendo manejo de fallas y administración de seguridad.

- ***A Software Defined Fog Node based Distributed Blockchain Cloud Architecture for IoT***

La expansión de IOT y la consiguiente explosión en el volumen de datos producidos por dispositivos inteligentes han llevado a la externalización de datos. Hay muchos desafíos que deben abordarse en la arquitectura de red tradicional debido al rápido crecimiento en la diversidad y la cantidad de dispositivos conectados a Internet. Se propone una arquitectura de nube distribuida basada en una cadena de bloques con un Software Defined Networking (SDN). El modelo propuesto es una arquitectura de nube distribuida basada en tecnología de cadena de bloques, que proporciona un acceso seguro, bajo demanda y de bajo costo a las infraestructuras informáticas más competitivas en una red IoT. Los resultados de la evaluación muestran que el rendimiento se mejora al reducir el retraso inducido, al reducir el tiempo de respuesta, al aumentar el rendimiento y la capacidad de detectar ataques en tiempo real en la red IoT con una sobrecarga de bajo rendimiento.

- ***An IoT-Aware Architecture for Smart Healthcare Systems***

En los últimos años, los avances convincentes en el desarrollo de Internet-of-Things (IoT) han permitido generar aplicaciones novedosas y fascinantes. Se propone una arquitectura novedosa, IoTaware, inteligente para el seguimiento y automático de pacientes, personal y dispositivos biomédicos en hospitales e institutos de enfermería. Se puede recopilar, en tiempo real, tanto las condiciones ambientales como los parámetros fisiológicos de los pacientes a través de una Red de detección híbrida (HSN). Los datos detectados se envían a un centro de control donde una aplicación de monitoreo avanzado los hace fácilmente accesibles para los usuarios locales y remotos a través de un servicio web REST.

- ***DIAT: A Scalable Distributed Architecture for IoT***

Uno de los principales desafíos en la realización de aplicaciones de IoT es la interoperabilidad entre varios dispositivos e implementaciones de IoT. La necesidad de una nueva arquitectura, que comprenda control inteligente y actuación, ha sido identificada por muchos investigadores. Se propone una arquitectura distribuida similar a Internet para las cosas (DIAT), que superará la mayoría de los obstáculos en el proceso de expansión a gran escala de IoT. Trata la heterogeneidad de los dispositivos de IoT y permite la adición perfecta de nuevos dispositivos en todas las aplicaciones. La arquitectura propuesta se combina con capacidades cognitivas que ayudan en la toma de decisiones inteligentes y permiten la creación automatizada de servicios.

- ***Software-Defined Fog Network Architecture for IoT***

Para abordar problemas como escalabilidad, entrega de datos en tiempo real y movilidad, se presenta un modelo de arquitectura que combina los beneficios de dos tecnologías emergentes: redes definidas por software y computación de niebla. La arquitectura propuesta está diseñada para soportar un alto nivel de escalabilidad, entrega de datos en tiempo real y movilidad. Los beneficios de usar esta arquitectura se han ilustrado con varios casos de uso que van desde visiones teóricas hasta servicios existentes.

Finalizada la lectura y análisis de los cinco papers anteriores, se procede a elegir dos que acoten aún más el tema de investigación. Los papers seleccionados son:

- IOT Gateway: Bridging Wireless Sensor Networks into Internet of Things
- An IoT-Aware Architecture for Smart Healthcare Systems

Dichos artículos ya han sido analizados, de manera que se puede presentar un tema contextualizado en torno a estos dos últimos artículos. La temática principal de dichos artículos se centra en la creación de arquitecturas para microcontroladores de IOT que permita la transmisión de datos en la red, dichos datos detectados se envían a un centro de control donde una aplicación de monitoreo los hace fácilmente accesibles para los usuarios locales y remotos a través de una especie de servicio web como por ejemplo REST.
En IoT, la filosofía es construir productos interconectados. El hardware de IoT siempre debe ser de bajo costo, de modo que estos dispositivos inunden el planeta. Los sistemas de IoT no son complicados, pero diseñarlos y construirlos puede ser una tarea compleja. Debido a factores como la elección de la tecnología, transferencia de datos, etc. Hay que tener en cuenta el consumo eléctrico, de modo que pueden funcionar con batería o incluso utilizar tecnologías como la recolección de energía. Los dispositivos integrados se basan en microcontroladores y ejecutan software con una pequeña cantidad de memoria. Estos sistemas operativos de uso general generalmente requieren un procesador de aplicaciones y tienen capacidades adicionales.

Con lo dicho anteriormente, se pretende generar una especificación arquitectónica que permita conocer las características adecuadas para el diseño de un microcontrolador de IOT. Teniendo en cuenta los conceptos revisados en la asignatura de Organización y arquitectura de computadores. Como por ejemplo: atributos arquitectónicos y organizacionales, estructura y funciones básicas (procesamiento, almacenamiento, transferencia y control de datos), principales componentes estructurales, memoria, arquitectura del procesador, enfoques de hardware y software e interconexiones para transferencias de datos (buses).

Determinado ya el **caso de estudio 2**, se tomaron nuevos datos, en este caso, las investigaciones que refieren a la **seguridad de los datos**, mediante la optimización de operaciones en algoritmos criptográficos.

C. Resultados de la segunda Clusterización

Los datos arrojados por la herramienta y luego del análisis hecho de la distancia media interclusters nos da como resultado que el mejor agrupamiento está en 4 grupos ya que el número de clusters con centroides menores a la media, son relativamente pocos comparados con los que sobrepasan esta medida, además la distancia de Bouldin es relativamente baja lo cual reafirma esta elección.

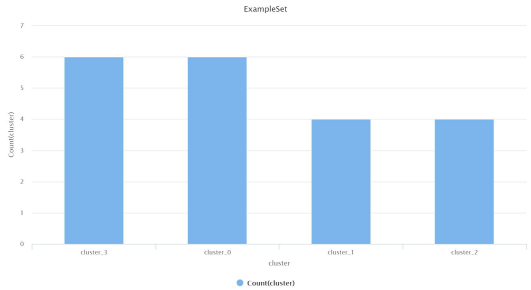

Fig. 2. Agrupamiento de documentos con k = 4

V. RESULTADOS

Row No.	cluster ↑	TITULO	ENLACE
3	cluster_0	Biometric ba...	https://www.r...
8	cluster_0	Secure Com...	https://link.sp...
13	cluster_0	GarbledCPU:...	https://ieeexpl...
14	cluster_0	Efficient Impl...	chrome-exten...
16	cluster_0	Implementati...	chrome-exten...
19	cluster_0	Elliptic curve ...	chrome-exten...
7	cluster_1	A Vector Appr...	https://link.sp...
9	cluster_1	Combining Al...	https://ieeexpl...
12	cluster_1	Implementin...	https://link.sp...
18	cluster_1	A Vectorial Ap...	chrome-exten...
11	cluster_2	Fast Implem...	https://link.sp...
15	cluster_2	Architectural ...	chrome-exten...
17	cluster_2	Optimizing M...	chrome-exten...
20	cluster_2	Algorithm Exp...	chrome-exten...
1	cluster_3	Design of Hig...	chrome-exten...

Fig. 2. Resultados clusterización con k=4

D. Resultados de la primera Clusterización

Los datos arrojados por la herramienta y luego del análisis hecho de la distancia media interclusters nos da como resultado que el mejor agrupamiento está entre 2 y 4 agrupamientos ya que el número de clusters con centroides menores a la media, son relativamente pocos comparados con los que sobrepasan esta medida, además la distancia de Bouldin es relativamente baja lo cual reafirma esta elección.

El primer agrupamiento (Cluster_0) obtenido contiene los siguientes papers:

- Biometric based Network Security using MIPS Cryptography Processor
- Secure Computation of MIPS Machine Code
- GarbledCPU: A MIPS processor for secure computation in hardware
- Efficient Implementation of Elliptic Curve Cryptography for Wireless Sensor Networks.
- Implementation of Secured MIPS Pipeline Processorusing RC6 Algorithm with Vhdl
- Elliptic curve cryptography on smart cards

Este cluster toma en cuenta la eficiencia representada hasta la actualidad de los algoritmos desarrollado y el uso de MIPS en el cálculo de curvas elípticas en tarjetas inteligentes. Sin embargo, el tema central de este algoritmo refiere al procesamiento de las instrucciones de cálculo de cualquier tipo de algoritmo criptográfico, optimizando operaciones, todo esto implementado en ambientes MIPS.

El artículo escogido de este cluster es "Implementation of Secured MIPS Pipeline Processorusing RC6 Algorithm with Vhdl" , la elección de esta investigación debido a que presenta el diseño y la implementación de un procesador de cifrado basado en algoritmos RC6 que contiene procesos de cifrado y

descifrado en el mismo diseño. La arquitectura del procesador criptográfico está dividida en diferentes módulos y cada módulo se implementa individualmente. Las partes principales del módulo ALU y del módulo de permutación en las descripciones de HDL están relacionadas con las transformaciones del algoritmo de cifrado Rivest Cipher-6, se compilan en hardware utilizando la herramienta Xilinx y HDL EASE. Además los resultados de las pruebas muestran que el procesador criptográfico MIPS funciona correctamente.
Este artículo recomienda el uso del método de algoritmo RC6 para la Criptografía de Arquitectura MIPS. Inicialmente, se toma la arquitectura MIPS básica y se implementan los núcleos criptográficos en base al algoritmo RC6. De esta manera, los datos dentro del procesador se volvieron más seguros y a prueba de amenazas. El sistema se volvió más robusto a medida que la transacción de datos se volvió más confiable. Por lo tanto, cuando se requieren los datos en forma criptográfica, este algoritmo es el más adecuado. El diseño se ha modelado en VHDL y se adoptan políticas de verificación funcional para ello. La optimización y síntesis del diseño se lleva a cabo en el último y más rápido dispositivo FPGA Virtex-6 que mejora el rendimiento. Todas las instrucciones están probadas con algunos de los vectores proporcionados por MIPS. Llegamos a la conclusión de que el rendimiento en base de la velocidad y el rendimiento del procesador criptográfico MIPS que utiliza RC6 es alto y confiable. Velocidad de 218 MHz (frecuencia de reloj) Rendimiento de 664 Mbits / s (Ancho de banda de datos) Tecla Configuración 188 ciclos de reloj en 4305 nss.) Ciclos de reloj Latency 21 (tanto para cifrar como para descifrar) Consumo de energía 1.746W (inactivo-1.303 y dinámico-0.444).
El segundo agrupamiento (Cluster_1) contiene los siguientes papers.

- A Vector Approach to Cryptography Implementation
- Combining Algorithm Exploration with Instruction Set Design: A Case Study in Elliptic Curve Cryptography
- Implementing Cryptography on TFT Technology for Secure Display Applications
- A Vectorial Approach to Cryptography Implementation

En este caso se ha elegido el paper "Combining Algorithm Exploration with Instruction Set Design: A Case Study in Elliptic Curve Cryptography" En el cual proponen a las extensiones de conjuntos de instrucciones aplicadas en los cálculos de curvas elípticas. Recordando que el uso de curvas elípticas en el cálculo de claves privadas y públicas, conllevan gran poder de procesamiento.
Las conclusiones de este artículo refiere a la demostración que la extensión automática del conjunto de instrucciones no es solo una herramienta para mejorar el rendimiento de la ejecución de aplicaciones integradas o para lograr una exploración rápida de soluciones de arquitectura personalizadas. Una motivación adicional para automatizar el proceso de selección de ISE es la exploración del algoritmo de ayuda. A través de un estudio basado en la criptografía EC, hemos demostrado que la disponibilidad de ISE puede tener un impacto dramático en el rendimiento relativo de diferentes opciones algorítmicas. Primero se selecciona manualmente los ISE para diferentes implementaciones de EC, y se mide la aceleración mediante la simulación, utilizando un modelo detallado de los ISE elegidos. Nuestro estudio muestra por primera vez que la disponibilidad de ISE puede revertir el interés relativo de las diferentes opciones de algoritmos. Además, se ha ejecutado una herramienta automática ISE y hemos demostrado que, incluso sin predecir aceleraciones tan precisamente como puede la simulación detallada, puede mostrar con exactitud y en cuestión de segundos las tendencias correctas que debe seguir el diseñador del sistema.

El tercer agrupamiento (Cluster_2) contiene los siguientes papers.

- Fast Implementation of Public-Key Cryptography on a DSP TMS320C6201
- Architectural Enhancements to Support Digital Signal Processing and Public-Key Cryptography
- Optimizing Multiprecision Multiplication for Public Key Cryptography
- Algorithm Exploration for Long Integer Modular Arithmetic on a SPARC V8 Processor with Cryptography Extensions

De Forma general este grupo habla sobre el desarrollo de arquitecturas de microprocesadores extendidas mediante una serie de instrucciones especiales para acelerar el procesamiento de DSP o las cargas de trabajo multimedia. Dado estos precedentes, se escoge el artículo "Architectural Enhancements to Support Digital Signal Processing and Public-Key Cryptography" debido a su estudio de idoneidad de las mejoras arquitectónicas para acelerar las operaciones aritméticas utilizadas en la criptografía de clave pública, sobre todo la multiplicación modular de precisión múltiple. En este se analiza diferentes algoritmos para aritmética modular y cómo estos algoritmos pueden aprovechar las unidades rápidas de MAC que están presentes en varios núcleos RISC basados en la arquitectura MIPS32 y ARMv5TE, respectivamente. Además, se compara mejoras arquitectónicas y extensiones de conjuntos de instrucciones específicamente diseñadas para acelerar un entero largo aritmética. Nuestro análisis muestra que la arquitectura MIPS32 se puede extender fácilmente para un procesamiento de criptografía eficiente y ofrece algunas ventajas en comparación con la arquitectura ARMv5TE.1.
Las conclusiones del artículo elegido refieren a la idoneidad

de las mejoras arquitectónicas orientadas a DSP para la implementación eficiente de aritmética modular de enteros largos. Analizamos la operación de bucle interno tanto del FIOS como del método FIPS para la multiplicación de Montgomery y se discuten los aspectos de implementación de estos algoritmos en el procesador MIPS 32 y el procesador ARM946E-S, respectivamente. Además, se muestra que la instrucción "clásica" de acumulación múltiple que agrega el producto de dos valores de 32 bits a un valor de 64 bits es de uso limitado para aritmética modular de precisión múltiple. El método FIPS requiere una unidad de MAC con un amplio acumulador, mientras que el método FIOS puede beneficiarse enormemente de una instrucción especial que ejecuta una operación de la forma x b + c + d. Este análisis y comparación de mejoras orientadas a la criptografía para MIPS32 y ARMv5TE permite dibujar las conclusiones: la arquitectura MIPS32 es más fácil de optimizar para el método FIPS, mientras que los procesadores ARM extendidos permiten alcanzar los mejores resultados con el método FIOS. Sin embargo, las extensiones para ambos algoritmos solo requieren cambios menores en la microarquitectura, son fáciles de integrar y casi no requieren hardware adicional. Un núcleo MIPS32 extendido necesita solo 9 ciclos de reloj para el bucle interno, mientras que el ARM946E-S extendido toma (al menos) 11 ciclos de reloj. Esta diferencia se debe principalmente al hecho de que los procesadores MIPS 32 permiten emitir instrucciones en paralelo a la operación de acumulación múltiple, que no es el caso para los núcleos ARM9E.142

El cuarto agrupamiento (Cluster_3) contiene los siguientes papers.

- Design of High Performance MIPS Cryptography Processor Based on TDES Algorithm
- Design of High Performance MIPS Cryptography Processor
- Performance Evaluation of Low Power MIPS Crypto Processor based on Cryptography Algorithms
- Extended instructions for the AES cryptography and their efficient implementation
- Reduced stall MIPS architecture using pre-fetching accelerator
- LOW POWER ENCRYPTED MIPS PROCESSOR BASED ON AES ALGORITHM

El paper a tomar en cuenta es el de "Reduced stall MIPS architecture using pre-fetching accelerator" ya que describe el diseño de una arquitectura MIPS con un pequeño número de paradas. El bloqueo ocurre frecuentemente en la arquitectura de tuberías, lo que resulta en ciclos de reloj más grandes. El bloqueo ocurre frecuentemente en la arquitectura de tuberías, lo que resulta en ciclos de reloj más grandes. En este documento, reducen significativamente el bloqueo al introducir una unidad de búsqueda previa. Esta unidad reduce el bloqueo al leer simultáneamente tres instrucciones y verificar su posibilidad de bloqueo. Si se detecta un bloqueo, esta unidad cambia la secuencia de instrucciones ejecutadas. Además, también empleamos unidades de detección de peligros de reenvío y memoria para reducir aún más el bloqueo. Para aumentar la funcionalidad y el rendimiento del procesador, especialmente para la aplicación de seguridad RSA, incluimos dos nuevas instrucciones de 32 bits mult y mod.

Este artículo presenta el diseño de arquitectura de hardware eficiente en el consumo de energía del procesador MIPS cifrado de 32 bits que ejecuta las instrucciones cifradas. Inicialmente, se leen los datos cifrados de la memoria de instrucciones, descifra los mismos datos y los envía a las siguientes etapas de la canalización. El procesador utiliza el bloque simétrico AES simple / cifrado que puede procesar datos de 128 bits. El bloque criptográfico en el procesador MIPS realiza el cifrado de datos. El diseño se ha modelado en VHDL y las políticas de verificación funcional se adoptan para ello. La optimización y síntesis del diseño se lleva a cabo en el último y más rápido dispositivo FPGA Virtex-6 que mejora el rendimiento. Las instrucciones de cada programa se prueban con algunos de los vectores proporcionados por MIPS. Llegamos a la conclusión de que el rendimiento del procesador criptográfico MIPS que utiliza AES es de 560 Mbits / s. El consumo de energía del procesador MIPS Crypto es 1.313W. El alto rendimiento y la alta flexibilidad del diseño del procesador criptográfico lo hacen aplicable a varias aplicaciones de seguridad.

Referencias

[1] Catarinucci, L., de Donno, D., Mainetti, L., Palano, L., Patrono, L. and Stefanizzi, M. (2015). An IoT-Aware Architecture for Smart Healthcare Systems. 1st ed. [ebook] Available at: https://ieeexplore.ieee.org/abstract/document/7070665 [Accessed 1 Jul. 2019].

[2] Zhu, Q., Wang, R. and Chen, Q. (2010). IOT Gateway: BridgingWireless Sensor Networks into Internet of Things. 1st ed. [ebook] Hong Kong. Available at: https://ieeexplore.ieee.org/abstract/document/5703542 [Accessed 1 Jul. 2019].

[3]]"Xen on ARM: System Virtualization Using Xen Hypervisor for ARM-Based Secure Mobile Phones - IEEE Conference Publication", Ieeexplore.ieee.org, 2019. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4446362. [Accessed: 03- Jul- 2019].

[4] "Design of 32 bit (MIPS) RISC PROCESSOR using FPGA", ACM DL, 2010. [Online]. Available: https://dl.acm.org/citation.cfm?id=1742123. [Accessed: 03- Jul- 2019].

[5] "Architectural Enhancements to Support DigitalSignal Processing and Public-Key Cryptography", Johann Großsch ¨adl1, Karl C. Posch1and Stefan Tillich, Graz University of Technology, 2010. [Online]. Available: chrome-extension://oemmndcbldboiebfnladdacbdfmadadm/https://pdfs.semanticscholar.org/1707/95e49c0051355b7fddff34a6185de58277ea.pdf. [Accessed: 03- Jul- 2019].

[6] “Combining Algorithm Exploration with Instruction Set Design:A Case Study in Elliptic Curve Cryptography”, JKirat Pal Singh*1, Shivani Parmar, Centre for Development of Advanced Computing (C-DAC) , 2010. [Online]. Available: chrome-extension://oemmndcbldboiebfnladdacbdfmadadm/https://pdfs.semanticscholar.org/4d71/79a483b11cc1b5b9c1fc064457582b8c8d26.pdf5f44f97cf [Accessed: 03- Jul- 2019].

[7] “Implementation of SecuredMIPS Pipeline Processorusing RC6 Algorithm with Vhdl”, Vishaka Ambardar, Dr.Munish Rattan, Graz University of Technology, 2010. [Online]. Available: chrome-extension://oemmndcbldboiebfnladdacbdfmadadm/https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.695.7766&rep=rep1&type=pdf. [Accessed: 03- Jul- 2019].

[8] “Combining Algorithm Exploration with Instruction Set Design:A Case Study in Elliptic Curve Cryptographyy”, Johann Großsch ¨adl1, Paolo Ienne2, Laura Pozzi2, Stefan Tillich1, and Ajay K. Verma2, Graz University of Technology, 2010. [Online]. Available: chrome-extension://oemmndcbldboiebfnladdacbdfmadadm/http://delivery.acm.org/10.1145/1140000/1131543/p218-groszschaedl.pdf?ip=191.100.91.27&id=1131543&acc=ACTIVE%20SERVICE&key=4D4702B0C3E38B35%2E4D4702B0C3E38B35%2E85C8CE441CB20768%2E4D4702B0C3E38B35&__acm__=1562234540_7f6d449466b452d0e8924e85f44f97cf [Accessed: 03- Jul- 2019].