Modelo arquitectónico para soluciones basadas en BlockChain

ANEXOS

PROYECTO DE GRADO

Juan David Muñoz Garzón
Astrid Carolina Ordoñez Guerrero

Director: PhD. Julio Ariel Hurtado Alegría

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones Departamento de Sistemas
Grupo de Investigación y Desarrollo en Ingeniería de Software (IDIS) Línea de Investigación en Ingeniería de Software
Popayán, diciembre de 2021

Tabla de contenido

ANEXO A. Descripción General del Proyecto Traslado de Pacientes

Gestión de información relacionada con el traslado de pacientes entre hospitales: Una solución basada en BlockChain

Juan David Muñoz, Astrid Carolina Ordóñez, Edgar Dulce, Julio A. Hurtado

Gestión de información relacionada con el traslado de pacientes entre hospitales: Una solución basada en BlockChain

Problemática General

La información en la mayoría de los sistemas de salud en Colombia trabaja en forma aislada lo cual limita la eficiencia y flexibilidad siendo estas dos características un factor vital para cada paciente. Y más que las razones técnicas, es la confianza entre las dependencias para compartir información sensible de sus pacientes, debido a que es muy apetecida por delincuentes y ciberdelincuentes que quieren lucrarse financieramente causando diferentes delitos como lo son sobornos, venta de información a otros proveedores de salud, violaciones a la intimidad entre otros. Con ese antecedente, se requiere del planteamiento de una solución que permita la gestión de información de forma digital, automatizada y segura entre diferentes organizaciones de salud, de diferente naturaleza jurídica (eps, ips, hospitales, etc..), las cuales requieren

frecuentemente interactuar entre sí para llevar un control de las recepciones y remisiones de los pacientes.

El traslado de pacientes entre hospitales

Particularmente se quiere construir una solución para la gestión de la información que soporta los traslados de pacientes, en los cuales se maneja información sensible como el motivo del traslado, su historia clínica, exámenes médicos y pruebas realizadas. Esta información se debe manejar de forma confidencial de acuerdo a los datos, según personas y organizaciones autorizadas para su lectura y actualización. En casos de urgencias durante el tiempo que dure el traslado (viaje) el paciente puede ser intervenido para su estabilización, esta información es importante para la organización que procede a recibirlo. Cada organización puede adicionar exámenes, pruebas o datos a la historia clínica de un paciente según los procedimientos que se le realicen, por lo tanto, la confiabilidad, trazabilidad, integridad y persistencia de la información es un factor vital. Cabe aclarar que cada anexo o actualización a los datos del paciente debe guardar constancia de quién lo hizo y el motivo por el cual se realizó, esto para llevar un mejor control de las actividades que se han realizado y se deban realizar.

Evaluando BlockChain y Hyperledger Fabric

Para resolver lo anterior, se ha pensado en abordar la solución basada en la tecnología BlockChain, y se ha establecido que la plataforma candidata para el desarrollo es Hyperledger Fabric. Sin embargo, se necesita evaluar de forma objetiva si la tecnología BlockChain y la arquitectura de Hyperledger Fabric soportará las necesidades actuales y futuras para la construcción de la solución de traslado de pacientes. Para ello, se propone hacer la evaluación de la arquitectura en este contexto haciendo uso del método de evaluación de arquitecturas ATAM Architecture Trade-off Analysis Method, el cual centra su actividad de evaluación en la interacción entre los diferentes atributos de calidad arquitectónica y basa sus evaluaciones sobre los escenarios desarrollados por los involucrados y un equipo de evaluación. En este caso el responsable de la construcción del sistema es el Ingeniero Edgar Dulce y el evaluador de la Arquitectura es el Tesista Juan David Muñoz.

Aspectos metodológicos y técnicos

1. El Método ATAM

El método se enfoca en la identificación de las *estrategias arquitectónicas (estilos arquitectónicos)*, ya que estos elementos representan los medios empleados por la arquitectura para alcanzar *los atributos de calidad*, así como también permiten describir la forma en la que el sistema puede escalar, facilitar los cambios, inter-operar con otros sistemas, responder a las demandas de solicitudes de servicio, tolerar fallos, entre otros. ATAM inicia con una arquitectura de sistema y las perspectivas de los actores involucrados con ese sistema y está basado en la generación de *escenarios de atributos de calidad* para

evaluar la arquitectura [1]. Después de que se identifica y describe los escenarios por las partes interesadas, la evaluación se realiza aplicándolos a la arquitectura con el fin de lograr una comprensión de los mecanismos arquitectónicos que se utilizan para lograr o no determinados atributos de calidad y las consecuencias que esos mecanismos tendrán sobre la solución. En un escenario, un atributo de calidad se describe considerando los estímulos externos relevantes (incluyendo la fuente del estímulo), la respuesta esperada del sistema al estímulo bajo unas condiciones de operación, los mecanismos que se utilizan dentro de la arquitectura para controlar la respuesta, así como una medida de la respuesta a estos estímulos. Finalmente se hace una Identificación de Riesgos / Sensibilidad / Concesiones de compromiso como resultado de la asignación de escenarios y el análisis subsiguiente, los grupos de riesgos, los puntos de sensibilidad, y las concesiones quedan documentados.

2. BlockChain y Hyperledger

El BlockChain es una estructura de datos en la que la información contenida se agrupa en conjuntos (bloques) a los que se les añade meta-información relativa a otro bloque de la cadena anterior en una línea temporal, de manera que, gracias a técnicas criptográficas, la información contenida en un bloque solo puede ser repudiada o editada modificando todos los bloques posteriores. Esta propiedad permite su aplicación en un entorno distribuido de manera que la estructura de datos BlockChain puede ejercer de
base de datos pública no relacional que contenga un histórico irrefutable de información. Hyperledger es una es una plataforma BlockChain, de código abierto que inició en diciembre de 2015 por la Fundación Linux, para apoyar a los ledgers (libros) distribuidos basados en BlockChain. Está centrado en ledgers diseñados para apoyar transacciones empresariales globales, incluyendo importantes gigantes tecnológicos, financieros y compañías de retail, con el objetivo de mejorar muchos aspectos de desempeño y fiabilidad. Entre los objetivos de su arquitectura están el de aunar esfuerzos independientes para desarrollar estándares y protocolos abiertos, proporcionar un marco modular que soporte diferentes componentes con propósitos específicos. Esto incluye una variedad de BlockChain con su consenso propio y modelos de almacenamiento, servicios para identidad, control de acceso, y contratos.

ANEXO B. Descripción del método de evaluación ATAM

Descripción del método de evaluación ATAM

1. Introducción
   ATAM es una metodología de evaluación que permite observar el grado de satisfacción de la arquitectura del sistema hacia los atributos de calidad, los cuales son definidos por los interesados del proyecto. Brinda un análisis iterativo y ayuda a detectar posibles falencias en una etapa temprana donde es relativamente económico corregir problemas. El enfoque de la metodología se basa en varios aspectos, el primero se obtiene de las pautas del negocio donde se realiza

una recolección de escenarios que describen el comportamiento del sistema ante diferentes estímulos o circunstancias, los cuales se clasifican según al atributo de calidad al cual pertenezca; el segundo es la presentación de la arquitectura del sistema, la cual muestra la forma en la que está construido y cómo interactúan sus componentes, de este aspecto se derivan las propuestas arquitectónicas y las decisiones de diseño; por último se encuentra el análisis, donde se recopila la información del primer y segundo aspecto para evaluar el grado de satisfacción uno a uno de las propuestas arquitectónicas hacia los atributos de calidad, como resultado de este análisis tenemos, puntos de sensibilidad, riesgos, no riesgos y compensaciones [1]. En la Fig. 1 podemos observar la manera en cómo interactúan los 3 aspectos mencionados

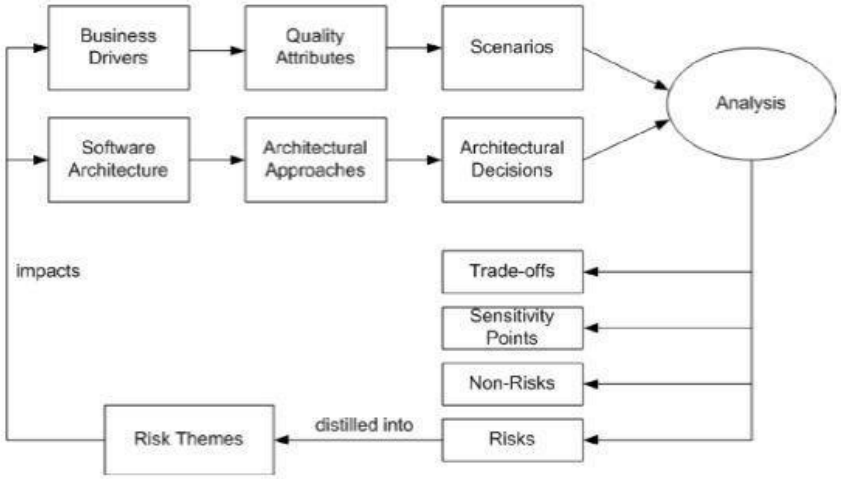


Fig. 1 Aspectos relevantes ATAM

2. Elementos del Método

La ejecución de ATAM consta de 9 pasos que se reparten en 4 fases y se conforma por un equipo de evaluación, donde cada integrante ocupa un rol a desempeñar; esta metodología cuenta con una serie de artefactos que ayudan a llevar una documentación y trazabilidad de la ejecución.

Fases:

- Fase 0: se establecen tiempo, fechas, costos, esfuerzo y se conforma el equipo de evaluación.
- Fase 1 y 2: se realiza la evaluación con ATAM siguiendo los 9 pasos (Fig. 2).
- Fase 3: se realiza el informe final de la evaluación realizada.

Roles:

Cada integrante del equipo tiene un rol específico para desempeñar las tareas asociadas. Para esta evaluación se tendrán 3 roles:

Ing. Julio Ariel Hurtado - Evaluador de la arquitectura, se encargará de llevar a cabo la ejecución de la evaluación en contraste con los atributos de calidad propuesto

Edgar Dulce Villareal – Cliente, el cual se encargará de explicar la finalidad y comportamiento que debería tener el sistema a implementar en este caso la gestión de información en el traslado de pacientes además de las expectativas de la evaluación

Juan David Muñoz – Arquitecto de la plataforma Hyperledger Fabric el cual expondrá cómo está construida junto con algunas decisiones de diseño y la forma en que interactúa en ejecución

Astrid Carolina Ordoñez - Arquitecta de software, expondrá sus puntos de vista acerca de las decisiones detrás de la plataforma Hyperledger Fabric, en el contexto del caso

Giovanna - Desarrolladora e investigadora en tecnologías BlockChain. Expondrá sus puntos de vista desde la perspectiva del desarrollo

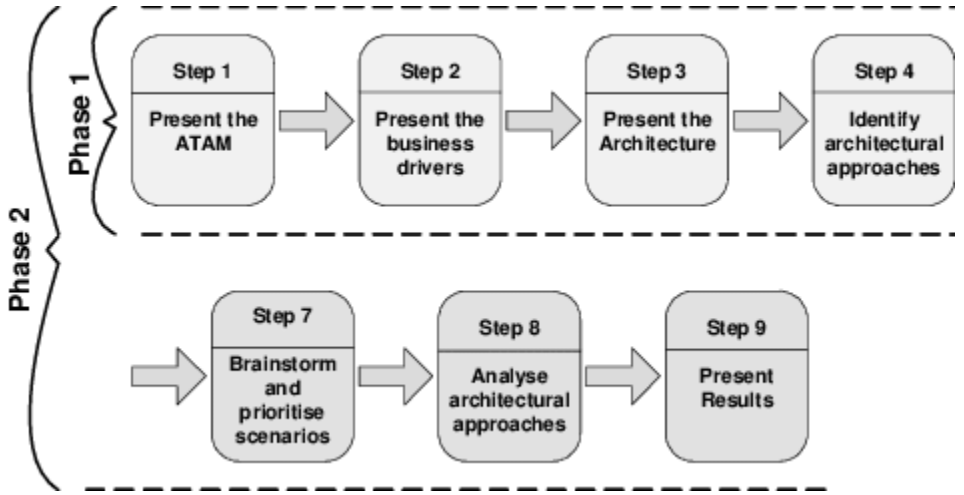


Fig. 2 Pasos de la metodología ATAM en la Fase 1 y 2

Artefactos:

- Árbol de utilidad: para la generación de este artefacto es importante la participación del equipo de arquitectura y de los clientes representativos, se deben identificar las metas de calidad y priorizarlas de tal manera que se obtengan las más importantes para los interesados Fig. 3.

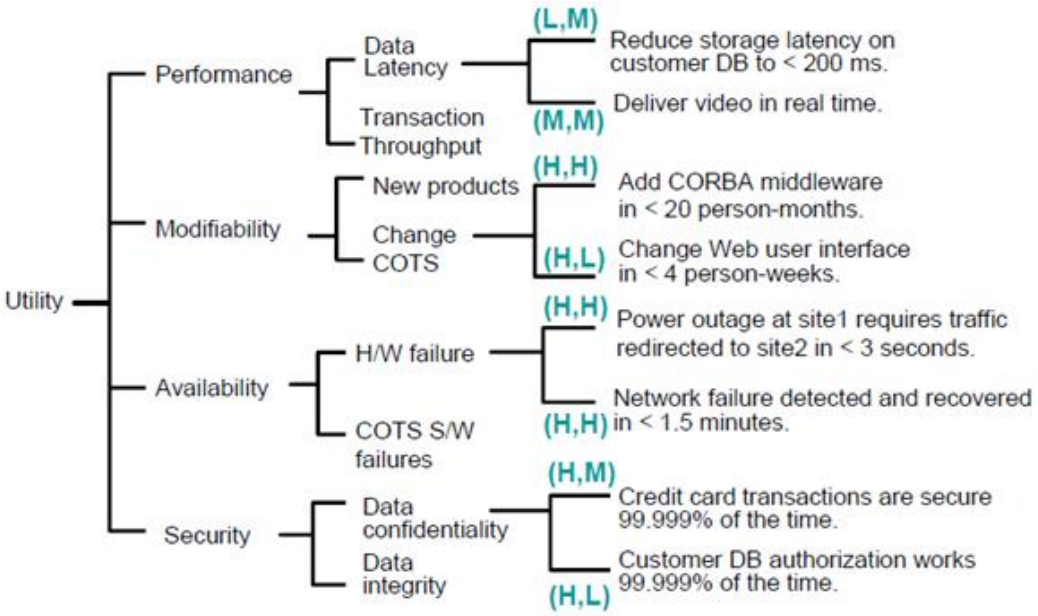


Fig. 3 Ejemplo de árbol de utilidad

- Análisis de una propuesta arquitectónica: para le generación de este artefacto se tienen en cuenta dos ámbitos, el primero es el escenario el cual describe de una forma corta la interacción de un interesado con el sistema y se analiza en 3 partes, la primera es el estímulo que explica lo que hace un interesado para interactuar con el sistema; la segunda el entorno, describe lo que pasa cuando se ejecuta el estímulo; y por último la respuesta, dice la forma en la que el sistema debería responder a través de la arquitectura al estímulo. El segundo ámbito es la propuesta arquitectónica que debería responder a ese escenario Fig. 4.

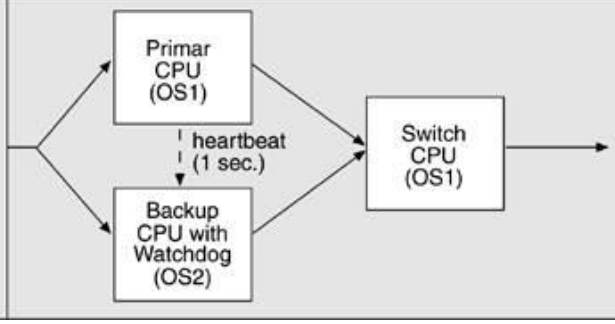
Scenario #: A12	Scenario: Detect and recover from HW failure of main switch.			
Attribute(s)	Availability			
Environment	Normal operations			
Stimulus	One of the CPUs fails			
Response	0.999999 availability of switch			
Architectural decisions	Sensitivity	Tradeoff	Risk	Nonrisk
Backup CPU(s)	S2		R8	
No backup data channel	S3	T3	R9	
Watchdog	S4			N12
Heartbeat	S5			N13
Failover routing	S6			N14
Reasoning	Ensures no common mode failure by using different hardware and operating system (see Risk 8) Worst-case rollover is accomplished in 4 seconds as computing state takes that long at worst Guaranteed to detect failure within 2 seconds based on rates of heartbeat and watchdog Watchdog is simple and has proved reliable Availability requirement might be at risk due to lack of backup data channel ... (see Risk 9)			
Architecture diagram				

Fig. 4 Ejemplo de análisis de una propuesta arquitectónica

ANEXO C. Riesgos Evaluación Arquitectura Hyperledger Fabric con ATAM

Riesgo	**Control ISO 27001**		
	Sección	**Controles de Seguridad de la Información**	**Preguntas**

Configuración maliciosa del proveedor	A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	¿Existen políticas, procesos, prácticas y registros relacionados con la gestión de relaciones con proveedores que involucran servicios de TI? ¿Incluyen servicios de nube, logística, servicios públicos, recursos humanos, médicos, financieros, legales y otros servicios subcontratados de alto riesgo? ¿Los contratos y acuerdos abordan lo siguiente? • Arreglos de gestión de relaciones, incluyendo el riesgo de la información y los aspectos de seguridad, la métrica, el rendimiento, problemas, rutas de escalada **• Información / propiedad intelectual, y obligaciones / limitaciones derivadas** **• Rendición de cuentas y responsabilidades relacionadas con el riesgo y la seguridad de la información** • Requisitos legales y normativos, como el cumplimiento certificado de ISO 27001 • Identificación de controles físicos y lógicos **• Gestión de eventos, incidentes y desastres incluyendo evaluación, clasificación, priorización, notificación, escalado, gestión de respuesta y aspectos de continuidad del negocio** • Habilitación de seguridad de los empleados y concienciación **• Derecho de auditoría de seguridad por parte de la organización** **¿Existe una obligación contractual de cumplimento?** **¿Los proveedores de servicios externos son monitoreados rutinariamente y auditados para cumplir con los requisitos de seguridad?**

	A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Más allá de A.15.1.1 y A.15.1.2 **¿Cómo se validan los requisitos de seguridad de los productos o servicios adquiridos?** ¿Cómo se logra una capacidad de recuperación cuando productos o servicios críticos son suministrados por terceros? **¿Se puede rastrear el origen del producto o servicio?**
Permisos de clientes a los usuarios	A9.1.1	Política de control de acceso	**¿Existe una política de control de acceso?** ¿Es consistente con la política de clasificación? **¿Hay una segregación de deberes apropiada?** ¿Existe un proceso documentado de aprobación de acceso? ¿El proceso de aprobación requiere que se involucre el propietario del sistema o la información en cuestión?
	A9.1.2	Acceso a las redes y a los servicios de red	¿Se utiliza autenticación de múltiples-factor para acceso a redes, sistemas y aplicaciones críticas, especialmente para los usuarios privilegiados? ¿Cómo monitoriza la red para detectar acceso no autorizado? ¿Los controles de seguridad de la red son evaluados y probados regularmente (Pentesting)? ¿La organización mide la identificación y los tiempos de respuesta ante incidentes?
Asignación de permisos a participantes	A9.1.1	Política de control de acceso	**¿Existe una política de control de acceso?** ¿Es consistente con la política de clasificación? **¿Hay una segregación de deberes apropiada?** ¿Existe un proceso documentado de aprobación de acceso? ¿El proceso de aprobación requiere que se involucre el propietario del sistema o la información en cuestión?
	A9.1.2	Acceso a las redes y a los servicios de red	¿Se utiliza autenticación de múltiples-factor para acceso a redes, sistemas y aplicaciones críticas, especialmente para los usuarios privilegiados? ¿Cómo monitoriza la red para

			detectar acceso no autorizado? ¿Los controles de seguridad de la red son evaluados y probados regularmente (Pentesting)? ¿La organización mide la identificación y los tiempos de respuesta ante incidentes?
En caso de fallo, la transacción no se lleva acabo	A12.1.4	Separación de los recursos de desarrollo, prueba y operación	¿Se segregan entornos de TIC de desarrollo, prueba y operacionales? ¿Cómo se logra la separación a un nivel de seguridad adecuado? ¿Existen controles adecuados para aislar cada entorno (ej. redes de producción, redes utilizadas para el desarrollo, redes de pruebas, la gestión)? ¿Se tienen acceso a través de perfiles de usuario debidamente diferenciados para cada uno de estos entornos? ¿Cómo se promueve y se lanza el software? ¿Se aplica la gestión de cambios a la autorización y migración de software, datos, metadatos y configuraciones entre entornos en cualquier dirección? ¿Se tiene en cuenta el riesgo de la información y los aspectos de seguridad que incluye el cumplimiento de privacidad si los datos personales se mueven a entornos menos seguros? ¿Se identifica un responsable de garantizar que el software nuevo / modificado no interrumpa las operaciones de otros sistemas o redes?
	A12.2.1	Controles contra el código malicioso	¿Existen políticas y procedimientos asociados a controles antimalware? ¿Se utilizan listas blancas o negras para controlar el uso de software autorizado y no autorizado? ¿Cómo se compila, gestiona y mantiene la lista y por quién? ¿Hay controles de antivirus de “escaneado en acceso” y “escaneo programático” en todos los dispositivos relevantes, incluidos servidores, portátiles, ordenadores de sobremesa y dispositivos integrados /

			IoT? ¿Se actualiza el software antivirus de forma automática? ¿Se general alertas accionables tras una detección? ¿Se toma acción de forma rápida y apropiada para minimizar sus efectos? ¿Cómo se gestionan las vulnerabilidades técnicas? ¿Existe una capacitación y una concienciación apropiada que cubra la detección, el informe y la resolución de malware para usuarios, gerentes y especialistas de soporte? ¿Existe un mecanismo de escalación para incidentes graves?
	A12.4.1	Registro de eventos	¿Existen políticas y procedimientos para el registro de eventos? ¿Se monitorean y registran de manera consistente y segura todos los sistemas clave incluido el registro de eventos en sí? ¿Se registra lo siguiente? • cambios en los ID de usuario • permisos y controles de acceso • actividades privilegiadas del sistema • intentos de acceso exitosos y fallidos • inicio de sesión y cierre de sesión • identidades y ubicaciones de dispositivos • direcciones de red, puertos y protocolos • instalación de software • cambios a las configuraciones del sistema • uso de utilidades y aplicaciones del sistema • archivos accedidos y el tipo de acceso • filtros de acceso web ¿Quién es responsable de revisar y hacer un seguimiento de los eventos informados? ¿Cuál es el periodo de retención de eventos? ¿Existe un proceso para revisar y responder adecuadamente a las alertas de seguridad?

ANEXO D. Videos Sesiones de Evaluación de la Arquitectura Hyperledger

Primera sesión
https://drive.google.com/file/d/1Y2NfKYp9DvL9YFCIGsuqtCMCsTAhi6Fv/view?usp=sharing

Segunda sesión
https://drive.google.com/file/d/1e2NnelViTNZ1Z5CYxRe2NkS-t9MHowYH/view?usp=sharing

ANEXO E. Link Guía Arquitectonica Usable

https://sites.google.com/view/guia-arquitectonica-blockchain/inicio

[1] R. Kazman, M. Klein, and P. Clements, “ATAM : Method for Architecture Evaluation,” *Cmusei*, vol. 4, no. August, p. 83, 2000, doi: (CMU/SEI-2000-TR-004, ADA382629).