BLOCKCHAIN® IN HEALTHCARE TODAY
PLATFORM APPROACHES IN HEALTHCARE

INVESTIGACIÓN ORIGINAL

Arquitectura segura y fiable habilitada para Fog usando Blockchain con curva elíptica sesgada funcional Algoritmo criptográfico para servicios sanitarios

Charu Awasthi, estudiante de doctorado[1] ; Satya Prakash Awasthi, PhD[2]; y Prashant Kumar Mishra, PhD[3]

[1]Becario de investigación del Departamento de Ingeniería Informática de la Universidad de Poornima, Jaipur, India; [2]Profesor asociado del Departamento de Ingeniería Informática de la Universidad de Poornima, Jaipur, India; [3]Profesor asociado del Departamento de Ciencias e Ingeniería Informática del Instituto de Tecnología Pranveer Singh, Kanpur, India.

Autor correspondiente: Charu Awasthi, Correo electrónico:

charuawasthi@gmail.com DOI: https://doi.org/10.30953/bhty.v7.347

Palabras clave: blockchain, FB-ECC, computación de niebla, algoritmo de criptografía de curva elíptica sesgada funcional, algoritmo de optimización de colonias de abejas galácticas, GBCOA, servicios sanitarios

Resumen

La computación en la niebla (FC) es una tecnología emergente que amplía la capacidad y eficiencia de las redes de computación en la nube actuando como puente entre la nube y el dispositivo. Los dispositivos de niebla pueden procesar localmente un enorme volumen de información, son transportables y pueden desplegarse en diversos sistemas. Por su procesamiento en tiempo real y sus reacciones ante eventos, son ideales para la asistencia sanitaria. Con una gama tan amplia de características, surgen nuevos problemas de seguridad y privacidad. Debido a la transmisión, llegada y acceso seguros, así como a la disponibilidad de dispositivos médicos, la seguridad crea nuevos problemas en el ámbito de la asistencia sanitaria. Como resultado, la FC necesita un enfoque único de las métricas de seguridad y privacidad, a diferencia de los métodos estándar de computación en nube. De ahí que este artículo sugiera una blockchain eficaz en función de los servicios sanitarios seguros en la CF. Aquí, los nodos de niebla recopilan la información del dispositivo sensor médico y los datos se validan mediante contratos inteligentes en la red blockchain. Proponemos un algoritmo de criptografía de curva elíptica con sesgo funcional para cifrar los datos. La optimización se realiza utilizando el algoritmo de optimización de colonias de abejas galácticas para mejorar el procedimiento de cifrado. Se evalúa el rendimiento de la metodología sugerida y se contrasta con las técnicas tradicionales. Se demuestra que la combinación de FC con blockchain ha aumentado la seguridad de la transmisión de datos en los servicios sanitarios.

Enviado: 7 de agosto de 2024; Aceptado: 4 de octubre de 2024; Publicado: 31 de diciembre de 2024

Ros recientes avances en comunicación electrónica han alterado el Internet de las Cosas (IoT) con la creación de pequeños aparatos que utilizan y controlan la recopilación y el intercambio de información. Esto permite la creación de sistemas de detección multifuncionales diminutos, rentables y menos potentes, capaces de observar y transmitir diferentes datos en numerosos ámbitos, como el transporte, la sanidad y la industria.(1)

El IoT sanitario ofrece varias ventajas, como la transferencia de datos en tiempo real y la capacidad de controlar el estado fisiológico de los pacientes durante distintos periodos. Equipos, incluidos medidores de glucosa, electroencefalografía, dispositivos wearables de electromiografía, etc., permite a los proveedores sanitarios recopilar localmente los datos sanitarios de un paciente y tomar una decisión en función de la información sobre su salud.

Las clínicas llevan varios años implantando el IoT, y ahora disponen de aparatos IoT sanitarios en las salas de atención al paciente y sus sistemas. Sin embargo, los organismos clínicos, las clínicas y las empresas no abordan la amenaza pro-tección del IoT sanitario que está vinculado a una red de área local o a una red de área amplia. Los dispositivos IoT son fácilmente secuestrados, lo que puede dar lugar a diversos problemas debido a la debilidad de las técnicas de validación y codificación.

Por lo tanto, se lanza blockchain para una transferencia segura y digna de confianza en el IoT sanitario. La figura 1 muestra el marco de la informática de niebla (FC).

El desarrollo de los sistemas IoT, especialmente en el sector sanitario, está generando cantidades ingentes de información, que se transporta y guarda en la nube. Debido a la necesidad de procesar y almacenar la información en tiempo real, el manejo de cantidades tan grandes de información en la nube crea un cuello de botella.

La protección de la información en la nube es también un problema importante[2].La idea de la FC fue un intento de resolver el problema. La computación en la niebla es una extensión del sistema de computación en la nube. Acompañar el funcionamiento de la nube es el papel principal de la niebla. Por ejemplo, la niebla proporciona recursos informáticos a los dispositivos que están más cerca del borde de la red. El marco típico de la nube IoT tiene problemas de escalabilidad y fiabilidad, pero la FC los soluciona.

Dado que los nodos de niebla operan en el borde de la red y están más dispersos geográficamente, como se muestra en la Figura 1, mejoran la protección y la precisión de la información, además de minimizar el retardo, lo que resulta crítico para aplicaciones como la información médica. También se minimiza el ancho de banda total a la nube, lo que mejora la calidad del servicio. La detección, validación y verificación de dispositivos IoT sanitarios en un contexto descentralizado puede resolverse integrando FC con blockchain[3].Para ello, presentamos una arquitectura habilitada para niebla que utiliza blockchain con un algoritmo de criptografía de curva elíptica sesgada funcional (FB-ECC) de FC para servicios sanitarios.

Trabajo relacionado

Este artículo propone un algoritmo FB-ECC para el cifrado de datos, cuya optimización se realiza mediante el algoritmo de optimización de colonias de abejas galácticas (GBCOA). Este algoritmo

Este algoritmo se compara con varios algoritmos propuestos en diferentes artículos para analizar su rendimiento.

La tabla 1 presenta las principales observaciones de los investigadores sobre la arquitectura basada en la niebla. Los resúmenes de la literatura relacionada sugieren que la integración de la arquitectura de niebla con las capacidades de utilización de blockchain de los dispositivos IoT es un campo interesante si podemos incorporar un algoritmo adecuado para un funcionamiento correcto.

Ngabo et al.[4]afirmaron que el objetivo principal de su trabajo es desarrollar mecanismos de protección contra los ataques de minería de datos médicos creados por la capa de detección y el almacenamiento de información en la base de datos en la nube del IoT. Un proceso de protección de blockchain de autorización pública que utiliza firmas digitales ECC para ayudar a una base de datos de libro mayor dispersa (servidor) a dar protección inmutable y claridad de transferencia, así como para proteger la manipulación de la información del paciente en la capa de niebla del IoT.

Baniata y Kertesz[5]presentaron un exhaustivo análisis bibliográfico y una categorización de la combinación FC-cadena de bloques (FC-BC): el estado actual de la técnica de l a combinación FC-BC. Los autores analizan y organizan los trabajos relevantes basándose en el año y el área de publicación, así como en los algoritmos empleados, las funciones de la FC y la posición de la FC en el diseño arquitectónico de la FC. El autor presenta en detalle las investigaciones, evaluaciones y dificultades futuras de la combinación BC-FC.

Tariq et al.[6]intentaron abordar los problemas de la futura protección de la infraestructura digital en un momento en que aún está en desarrollo. El marco de la niebla dependiente de la funcionalidad se establece con la llegada de la arquitec-tura que genera grandes cantidades de información.

También se discute la necesidad de protección adicional de los dispositivos IoT habilitados para la niebla, así como los retos de protección de la FC y la confidencialidad de la gran cantidad de información relacionada con la IoT habilitada para la niebla. A continuación, se examinan las

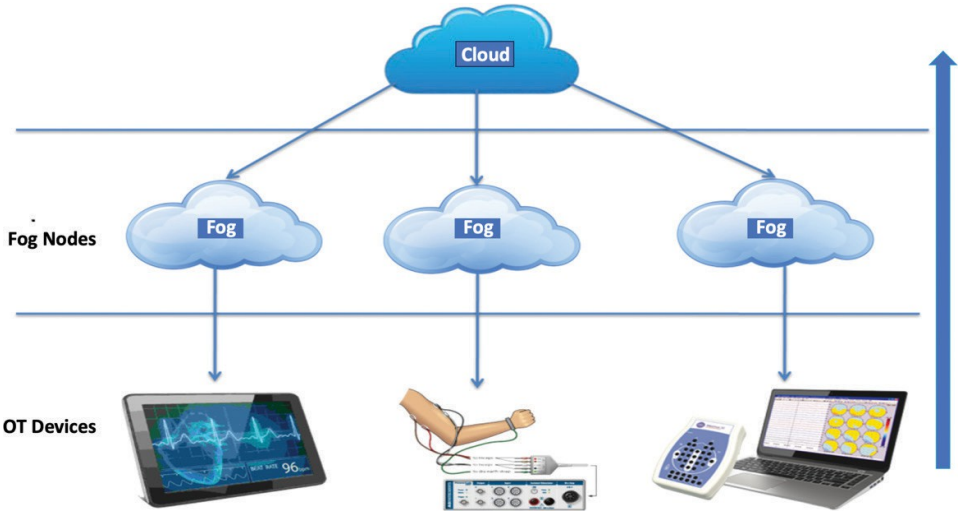

Fig. 1. Arquitectura de la computación en la niebla.

Citación: Blockchain en la sanidad hoy 2024, **7**: 347 - https://doi.org/10.30953/bhty.v7.347

Tabla 1. Observaciones de investigadores en el campo de la arquitectura habilitada para niebla

Fuente	Observación de la línea superior
Ngabo et al.[4]	El objetivo principal es desarrollar mecanismos de protección contra los ataques de minería de datos médicos creados por la capa de detección y el almacenamiento de información en la base de datos en la nube del IoT.
Tariq y colegas[6]	Abordan cuestiones relacionadas con la futura protección de infraestructuras digitales.
Banerjee y otros[7]	Mejora de la experiencia del usuario y de la resistencia del servicio en caso de emergencia.
Fernández et al.[8]	Implementaron un sistema que añade capacidades de IoT al MCG comercial para permitir la vigilancia remota de los pacientes.
Muthanna et al.[9]	Proponen un marco de SDN para regular y gestionar una capa de computación de borde de nodos de niebla.
Srivastava et al.[10]	Discutieron la FC, blockchain y el IoT en la asistencia sanitaria.
Yánez et al.[11]	Sugirieron un nuevo enfoque consciente del contexto para la asignación de información en la cadena en redes IoT-blockchain.
Kumari et al.[12]	Proporcionaron un examen de las funciones de la computación en la niebla y en la nube y de la IO en la prestación de servicios continuos conscientes del contexto a los usuarios finales.
Pareek et al.[13]	Observaron que la IO conecta muchos aparatos a nivel mundial.
Hanumantharaju et al.[14]	Afirman que la IO podría ayudar a pacientes y profesionales sanitarios a mantenerse en contacto y ofrecer a su comunidad una atención clara y de valor añadido.
Mayer et al.[15]	Proponen un paradigma arquitectónico de FC que integra blockchain, fog computing e IoT para el ámbito sanitario.

FC: computación en la niebla; CGM: monitorización continua de la glucosa; IoT: Internet de las cosas; SDN: redes definidas por software.

Se analizan las interdependencias entre blockchain y FC, así como su papel a la hora de abordar una amplia gama de preocupaciones de protección en IoT. Como consecuencia, este estudio ofrece una taxonomía de los tipos de ataques a los sistemas IoT basados en la niebla, compara las contribuciones más recientes al área en términos de su servicio de protección y formula recomendaciones para futuras investigaciones.

Banerjee et al.[7]mejoraron la experiencia del usuario y la resistencia del servicio en caso de emergencia; se han utilizado técnicas de FC para vincular la IO con la computación en tiempo real en las redes periféricas. La computación en el borde de la niebla, con su diseño disperso y su proximidad a los usuarios finales, puede ofrecer tiempos de reacción más rápidos y servicios de mayor calidad para el uso de IoT. La FC, la IoT y el aprendizaje automático se incluyen en cada parte del paradigma proporcionado por los investigadores para mejorar la calidad de la asistencia sanitaria. La tecnología Blockchain se utiliza para garantizar la protección de la arquitectura.

Fernández et al.[8]implementaron un sistema que añade capacidades de IoT al monitor continuo de glucosa (MCG) comercial para permitir la vigilancia remota de los pacientes y, por tanto, notificarles circunstancias potencialmente peligrosas. Para recoger las mediciones de glucosa en sangre del CGM, se utilizan teléfonos móviles para enviar las mediciones a una nube distante o a nodos dispersos en la niebla. También se incluye un sistema de almacenamiento descentralizado que recoge, procesa y guarda la información adquirida para compartir información precisa, fiable y cibersegura con científicos médicos, clínicos y cuidadores.

GlucoCoin se creó como un sistema de incentivos para que las personas proporcionen información nueva al sistema, así como dinero digital. Mediante una cadena de bloques (blockchain) capaz de ejecutar contratos inteligentes, este sistema puede automatizar la compra de sensores de MCG o compensar a los usuarios que faciliten información para permitir el funcionamiento del sistema.

Muthanna et al.[9]propusieron un marco para redes definidas por software (SDN) con el fin de regular y gestionar una capa de computación de borde de nodos de niebla y proporcionar una gran disponibilidad y fiabilidad para aplicaciones de IoT retrasadas. En la red SDN se utilizan conmutadores OpenFlow con restricciones de recursos, que tienen controladores dispersos. Se puede lograr una descentralización fiable con el uso de la cadena de bloques. A los conmutadores OpenFlow se les asignarán tareas de procesamiento computacional en función de su carga de trabajo actual mediante una técnica de descarga de información. Se ha propuesto un modelo de tráfico para la red en su conjunto. El algoritmo se prueba mediante simulación y un banco de pruebas.

Srivastava et al.[10]analizaron la computación en nube, la cadena de bloques y la IO en la sanidad. A diferencia de la computación en nube, que opera entre la nube y los dispositivos de usuario final conocidos como dispositivos IoT, la computación en nube amplía la capacidad de la computación en nube para ejecutar funciones como el procesamiento, el almacenamiento y la interacción a través de Internet. Ofrece facilidades superiores de almacenamiento de información con acceso en tiempo real, menor retardo, mayor capacidad de respuesta, mejor tolerancia a fallos y un contexto protegido y oculto. Las capas de niebla, acceso, interacción de la información, aplicación y protección se fragmentan en cinco niveles en el sistema IoT. Los autores destacaron la tecnología blockchain y los mecanismos de consenso para mejorar la protección de la información en el contexto sanitario. Yánez et al.[11]sugirieron un nuevo enfoque consciente del contexto para la asignación de información en la cadena en redes IoT-blockchain. Además, crean un controlador de datos mediante lógica difusa, que estima el valor RoA de una solicitud utilizando varias características del contexto, como la calidad y cantidad de la información y las redes por las que se envía. El diseño y la aplicación del mecanismo también llevaron a perfeccionar dos populares IoT-blockchain

características arquitectónicas. El método de asignación de datos se instantiza en las arquitecturas de nube y niebla dependientes de blockchain y se evalúa utilizando Fog Bus para mostrar la eficacia de nuestro enfoque. Utilizando usos sanitarios del mundo real, también comparan nuestro método con los procesos actuales de toma de decisiones.

Kumari et al.[12]examinan las funciones de la computación en la nube y en la niebla y del IoT en la prestación de servicios continuos contextualizados a los usuarios finales cuando y donde los necesiten. Para la recopilación, el procesamiento y la transferencia de información en tiempo real, sugieren un marco de atención sanitaria de tres capas orientado al paciente. Proporciona a los usuarios finales información sobre el uso de dispositivos de niebla y pasarelas en el ecosistema de Sanidad 4.0 para usos presentes y futuros.

Pareek et al.[13]mencionan que la IO conecta muchos aparatos en todo el mundo. Para aliviar la presión sobre los sistemas sanitarios, las tecnologías dependientes de la IO pueden ayudar a reducir los gastos sanitarios, así como a aumentar la computación y la velocidad de procesamiento. En la IO, los conjuntos de información sanitaria cada vez más sofisticados requieren el uso de la computación en nube. Retraso, uso de ancho de banda, latencia de reacción en tiempo real, seguridad y confidencialidad son sólo algunos de los problemas que plantea la integración de IoT con la nube. Cuando se trata de la computación en nube, hay que abordar muchas preocupaciones y retos antes de poder evaluar cualquiera de los diseños de modelos de sistemas basados en IoT-Fog.

Hanumantharaju et al.,[14]mencionan que el papel de la IoT podría ayudar a pacientes y proveedores sanitarios a mantenerse en contacto y ofrecer a su comunidad una atención clara y dependiente del valor, simplificando el contacto entre ambos. La FC puede servir de base para el uso de la IO en la atención sanitaria. Los expertos debatieron sobre la sanidad 4.0. Los investigadores estudiarán cómo la taxonomía FC puede ser la mejor respuesta a la sanidad 4.0 en términos de recopilación y evaluación de información, protección y confidencialidad, y servicios de sanidad electrónica.

Mayer et al.[15]propusieron un paradigma arquitectónico de FC que integra blockchain, FC e IoT para el ámbito sanitario. En su mayor parte, la arquitectura de FC y sus enfoques diferenciales para superar las restricciones de IoT son las contribuciones más significativas.

La revisión de la literatura relacionada sugiere que la integración de la arquitectura de niebla con blockchain utilizando las capacidades de los dispositivos IoT es un dominio interesante si podemos incorpo-rar un algoritmo adecuado para su correcto funcionamiento.

Este artículo propone un algoritmo FB-ECC para el cifrado de datos, con optimización realizada por el GBCOA. Este algoritmo se compara con varios algoritmos propuestos en diferentes artículos para su análisis de rendimiento.

Método propuesto

En esta sección se explica brevemente un servicio eficaz de atención sanitaria protegida dependiente de blockchain en FC.

El nodo de niebla recopila la información de los dispositivos sensores médicos y los datos se validan mediante contratos inteligentes en la red blockchain. Para cifrar los datos, se propone el algoritmo FB-ECC. Para optimizar el proceso de cifrado, se implementa el GBCOA. Se evalúa el rendimiento de la metodología propuesta y se compara con el enfoque tradicional. La figura 2 muestra la ilustración del flujo de las técnicas aplicadas.

En esta infraestructura pueden detectarse cuatro niveles: la capa IoT, la capa de niebla con blockchain, la capa de nube y la capa de análisis de datos. La información sanitaria de los pacientes se adquiere utilizando dispositivos de sensores médicos. Con medios accesibles por cable o inalámbricos, incluidos ZigBee y Wi-Fi, cada equipo médico IoT puede vincularse a un único nodo Fog. Los nodos Fog imponen normas de protección preestablecidas para controlar los dispositivos y servicios IoT conectados, además de servir de intermediario entre la Nube y la Blockchain, permitiendo el índice de autorización para las consultas de información.

Validación de datos mediante contrato inteligente

Aunque la palabra se utilizaba anteriormente en el contexto de protocolos entre desconocidos en Internet, los contratos inteligentes son ejemplos de contratos implementados en la blockchain de Ethereum. Un contrato inteligente tiene las siguientes reglas

1. Negociar las condiciones del acuerdo
2. Validar el acuerdo automáticamente
3. Implementar las condiciones acordadas

Un contrato inteligente se compone de muchas funcionalidades a las que se puede acceder desde fuera de la cadena de bloques o a través de otros contratos inteligentes. El uso de la cadena de bloques junto con la tecnología de contratos inteligentes elimina la necesidad de que las partes de la transacción dependan de un sistema centralizado. Cada participante vinculado en la red tiene una réplica de los contratos inteligentes, ya que se mantienen en la cadena de bloques. Cuando se inicia por un evento permitido o acordado, un contrato inteligente puede realizar el procedimiento almacenado acordado. Cada transferencia de contrato, así como toda la pista de auditoría de las actividades, se guardan en orden cronológico para su acceso futuro. Cualquier parte que intente alterar un contrato o transacción en la blockchain será detectada e impedida por todos los demás participantes. El sistema sigue funcionando incluso si una de las partes se bloquea, sin pérdida de información ni de integridad. Como resultado, se crea un sistema informático enorme, seguro y lógico sin los peligros, gastos o dificultades de confianza asociados a un paradigma centralizado.

Verificación de bloques mediante protocolos de consenso Stellar

El Protocolo de Consenso Stellar es un protocolo de con-senso descentralizado en el que los nodos de una red no tienen

Citación: Blockchain en la sanidad hoy 2024, 7: 347 - https://doi.org/10.30953/bhty.v7.347

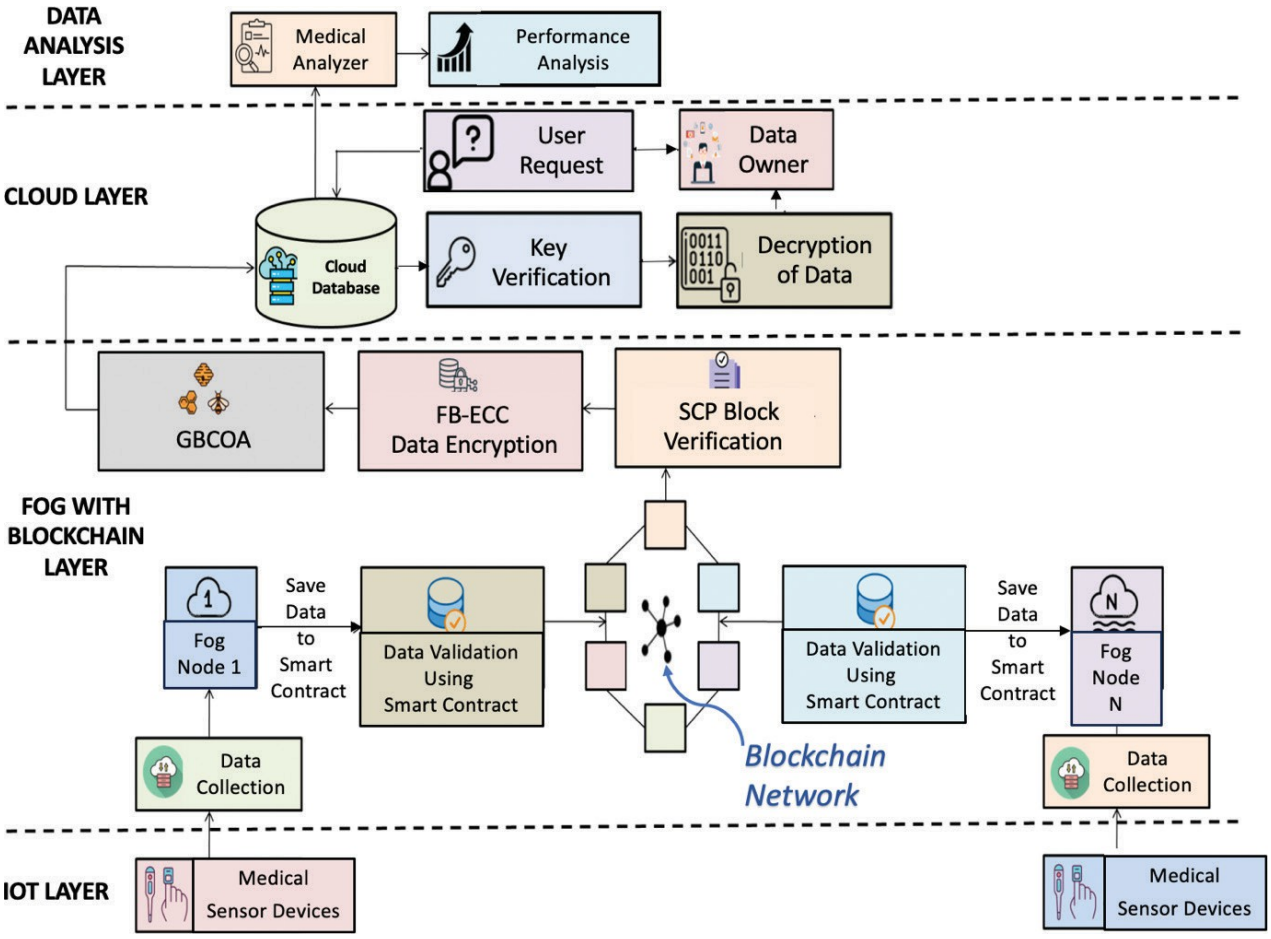

Fig. 2. Ilustración del flujo de las técnicas aplicadas. FB-EEC: criptógrafo de curva elíptica con sesgo funcional; FC-BC: cadena de bloques de computación de niebla; GBCOA: algoritmo de optimización de colonias de abejas galácticas, IoT: Internet de las cosas.

confianza en todos los nodos de la red y, en su lugar, pueden elegir en qué nodos confían.[16]La idea de un "quórum", establecida inicialmente por este protocolo, se refiere a un conjunto de nodos que confían unos en otros. Un "quórum" es un grupo de nodos lo suficientemente grande como para establecer un consenso, mientras que una "porción de quórum" es un subconjunto de un quórum que persuade a uno o más nodos para que se pongan de acuerdo.

Cada nodo que obtenga estos valores comprobará el bloque buscando un único valor entre ellos, lo que dará como resultado un único valor que se utilizará para validar el bloque. A lo largo de esta etapa, los nodos comienzan a comprobar el bloque para decidir si aceptan o rechazan los valores elegidos en la etapa anterior. Si un grupo de nodos no se pone de acuerdo, el valor se transfiere a un bloque mayor para su autenticación.

Cifrado de datos mediante el algoritmo de criptografía de curva elíptica con sesgo funcional

La FB-ECC es una conocida tecnología de criptografía de clave pública que mantiene de forma fiable y segura la confidencialidad y el secreto de la información médica codificada. Se utilizan claves idénticas para el cifrado y el descifrado (Tabla 2).

El FB-ECC es un método común de cifrado de clave pública que utiliza pares de claves distintas para los procedimientos de cifrado y descifrado, como la creación aleatoria de claves públicas y privadas. Las técnicas de criptografía de clave pública, como la FB-ECC, también están integradas en esta tecnología. La autorización y la claridad de las nuevas transacciones dependen del acuerdo disperso (superior al 50%) entre sus usuarios, lo que confiere a esta técnica una ventaja sobre la criptografía de clave pública. Dado que sólo la clave secreta FB-ECC puede devolver la información real, la información médica que se oculta no puede ser recuperada por ningún individuo no autorizado.

En la criptografía de clave asimétrica, la técnica FB-ECC desempeña un papel crucial en la criptografía de clave pública. Además, se crea una expresión numérica utilizando el punto base definido, la curva y el límite superior de una función de números primos, y el cifrado se realiza utilizando la siguiente ecuación FB-ECC:

$$k^2 = l^3 + bl + c \quad (1)$$

Tabla 2. Algoritmo criptográfico de curva elíptica con sesgo funcional

Entrada: Datos de entrada (dI), clave privada (K).

Salida: Datos cifrados (Ed).

1: Generación aleatoria de la clave pública (Pk);

2: $P_k = A * G_d$/* la función de generación Go dependiendo de la ecuación de la curva, Go se extrae de la función de mapeo.

3: Se generan los cifrados Cs como Cs← RM * Go;

4:Los datos cifrados (E_d) se crean como $E_d \leftarrow (S_M * Pa) + (d_{(P)}, W)$;/* W /* W denota el punto base en la curva.

5:Los datos cifrados (E_d) se cargan en el entorno de la nube pública

Nota: Véase el texto para mayor contexto.

Los números enteros se indican con la *b* y la *c*. Sin embargo, la fuerza global del proceso de cifrado viene determinada por la producción de una clave que depende de cada algoritmo criptográfico. El proceso inicial consiste en fabricar la clave pública que se utilizará para cifrar la información, que normalmente se recibe del receptor. El segundo proceso es generar una clave privada que permita descifrar la información original en el lado del receptor. *W* es el punto inicial de la curva, y *A* es el número entero aleatorio elegido dentro del intervalo 1-(m - 1):

$$S = A \times W \tag{2}$$

La clave pública se representa como *S*, mientras que la clave privada se significa como *A*.

El cifrado es un método de transformación de información real en información cifrada, y se utiliza

para aumentar la protección. El FB-ECC es la técnica m á s utilizada en seguridad en la nube para proporcionar protección en función de la complejidad de los problemas. El cifrado

viene determinada por la generación de la clave

que puede ofrecer una mejor solución para la información, al favorecer una mayor confidencialidad en la transmisión de claves secretas entre varias entidades de comunicación. La información original de entrada dI y la clave privada K se suministran como entradas en este procedimiento de cifrado, y la función generadora (Go) crea la clave pública (Pk). Como consecuencia, el cifrado Cs se crea utilizando los números aleatorios de 4 bits Rm y Go. A continuación, los datos de entrada dI se codifican utilizando el punto base de la curva *W*, seguido de la generación de la clave pública Pk y el número aleatorio Rm.

Algoritmo de optimización de colonias de abejas galácticas

El GBCOA simula el movimiento de estrellas, galaxias y supergalaxias para encontrar alternativas viables en un espacio de búsqueda determinado. Como las estrellas en las galaxias, se comunican entre sí. El agente está dividido en dos niveles por la colonia galáctica de abejas. Las estrellas se muestran en el primer nivel, mientras que las galaxias se representan en el segundo. Salvo la población inicial del segundo nivel, que se extrae de las mejores soluciones de

el primer n i v e l , cada nivel tiene su mecanismo de búsqueda. En cada etapa pueden utilizarse varias técnicas de búsqueda. En todas las e t a p a s , los investigadores optaron por emplear el método de optimización de colonias de abejas. Así, en el primer nivel, cada subpoblación utiliza BCO para encontrar la respuesta opti-mal, y luego la envía al nivel superior para construir superabejas. Las superabejas se utilizan como población inicial en una nueva ejecución de BCO para encontrar la solución óptima. La huelga multicapa BCOA se representa en (3):

$$\begin{aligned} & s_q^p \in S : q = 1, 2, \ldots, M \\ & p \\ & b_p \in S_p : b_p = \underset{M}{mejor}\left(S_p\right) \\ & G = \bigcup_{p=1} b_p \end{aligned} \tag{3}$$

La primera subpoblación de N soluciones se genera de forma aleatoria en la técnica original de optimización de la abeja galáctica. S^p es la jésima solución de la i-ésima subpoblación. S^q $_p$ denota la i-ésima subpoblación. $b_{(p)}$ (best($S_{p)}$) indica la gran solución de la subpoblación S_p. El conjunto G denota la superpoblación que comprende las mejores soluciones procedentes de las subpoblaciones.

Las mejores soluciones obtenidas de cada subpoblación en la etapa 1 se utilizan como la primera población de la etapa 2. La etapa 2 se ejecuta L2 veces y el mejor resultado identificado en la etapa 2 se considera la última solución de la época. El algoritmo total se ejecuta un número de épocas y los mejores resultados identificados hasta el momento en las épocas se consideran el último resultado del algoritmo.

Base de datos en la nube

En este para-digma, un servidor centralizado de historiales médicos se comunica con un repositorio o base de datos de historiales médicos. El paciente es el propietario de la información, que incluye datos personales sensibles. El historial médico del paciente, que suele figurar en estos documentos, también puede incluir datos biométricos, problemas de salud física, psicológica y mental, antecedentes personales, alergias, medicamentos utilizados, afecciones médicas, terapias médicas previas y enfermedades, entre otras c o s a s . Datos financieros, incluidos

Citación: Blockchain en la sanidad hoy 2024, **7**: 347 - https://doi.org/10.30953/bhty.v7.347

cuenta bancaria, números de tarjetas de crédito y débito, así como la identidad del paciente, pueden incluirse en los historiales médicos.[17]

La protección de la seguridad y la confidencialidad de los historiales médicos electrónicos se considera un elemento central de la gestión de la información sanitaria. Su principal objetivo es garantizar que la información sea accesible cuando se requiera y que no se utilice, divulgue, adquiera, modifique o destruya indebidamente mientras se guarda o envía.

Las normas de seguridad y privacidad colaboran para garantizar los controles y salvaguardias adecuados. El número de iden-tificación del paciente se utiliza para identificar la historia clínica en el almacén o base de datos de historias clínicas. Bajo las identificaciones indicadas, la información sanitaria del paciente es personalmente identificable. Los datos del paciente pueden utilizarse solos o junto con otros datos adicionales. La información del paciente se almacena en bases de datos en el ordenador virtual de la nube privada.

Para la gestión de la información, la arquitectura de nube privada incluye computación, almacenamiento y servicios de red. Al enviar la información sanitaria a la nube, las operaciones de cifrado y hash se realizan de acuerdo con el marco de seguridad de la nube privada. La información real de los historiales médicos se guarda en una base de datos, mientras que la clave necesaria para el cifrado se guarda en otra. Como resultado, se restringe el acceso de un atacante a la información crítica del paciente almacenada en la base de datos de historiales médicos electrónicos en la nube. Como resultado, el marco sugerido salvaguarda los datos sensibles del paciente garantizando la confidencialidad e integridad de la información. Como consecuencia, los usuarios del sistema sanitario pueden descifrar los datos y acceder a información crucial desde cualquier lugar y en cualquier momento.

Análisis del rendimiento

Se describen los criterios de evaluación del rendimiento del modelo propuesto para el almacenamiento seguro de información médica cifrada en un marco de FC que emplea blockchain y un algoritmo ECC de sesgo funcional. El tiempo de generación de claves (KGT), el tiempo de cifrado (ET), el tiempo de descifrado (DT) y el nivel de seguridad se utilizan para evaluar la sección de almacenamiento protegido de este sistema de algoritmos sugerido. Además, en las ecuaciones (4), (5) y (6) se dan las fórmulas pertinentes para estimar los distintos tiempos.

Tiempo de cifrado

El tiempo de cifrado se describe como el tiempo necesario para cifrar la información en milisegundos. Se calcula de la siguiente manera

Tiempo de cifrado= Tiempo final - Tiempo inicial

$$KGT = ITT + ET \quad (4)$$

Donde ITT representa el tiempo de transferencia de la información, mientras que ET significa tiempo de cifrado. El ET com-putado aquí es el tiempo que tardó la información en codificar la información original y transformarla en información codificada. Donde ENDT denota el tiempo final y STARTT indica la duración inicial del procedimiento de encriptación.

$$ET = ENDT - STARTT \quad (5)$$

La figura 3 muestra el tiempo de cifrado de la técnica sugerida utilizando el método funcional ECC sesgado. Los investigadores descubrieron que el tiempo de cifrado mejoraba a medida que aumentaba el número de bits de la clave. Por otra parte, la arquitectura que proponemos t a r d a mucho menos en cifrar que los métodos tradicionales, como Advanced Encryption Standard (AES), Data Encryption Standard (DES) y Rivest-Shamir-Adleman (RSA).

Tiempo de descifrado

El tiempo necesario para descifrar la información cifrada se denomina tiempo de descifrado y se calcula de la siguiente manera:

Tiempo de descifrado= Tiempo final - Tiempo inicial

Aquí, el DT (tiempo de descifrado) se computa como la cantidad de tiempo que tarda la información utilizada en descifrar la información cifrada en milisegundos, y se calcula utilizando la Ecuación (6).

$$DT = ENDT - STARTT \quad (6)$$

La duración del descifrado aumenta al aumentar el tamaño de la clave debido a la introducción de información perturbadora en el servidor de la nube y a diversos factores.

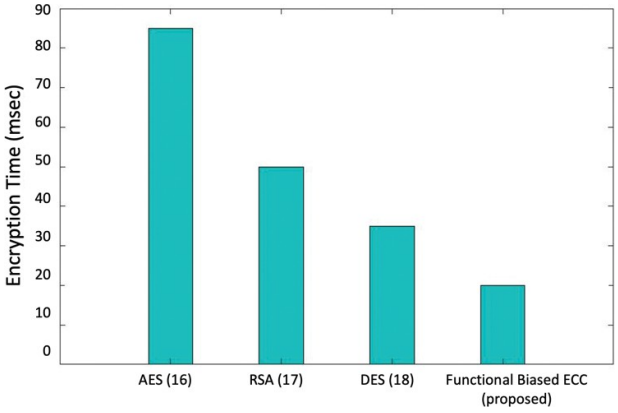

Fig. 3. Análisis del tiempo de generación de claves. AES: Advanced Encryp-tion Standard, DES: Data Encryption Standard, ECC: criptografía de curva elíptica, RSA: Rivest-Shamir-Adleman.

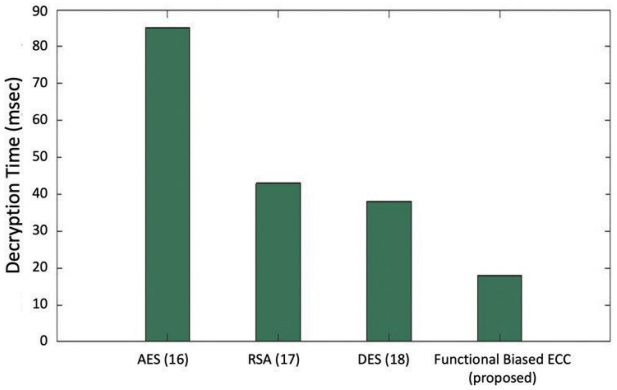

Fig. 4. Análisis del tiempo de descifrado. AES: Advanced Encryp-tion Standard, DES: Data Encryption Standard, ECC: criptografía de curva elíptica, RSA: Rivest-Shamir-Adleman.

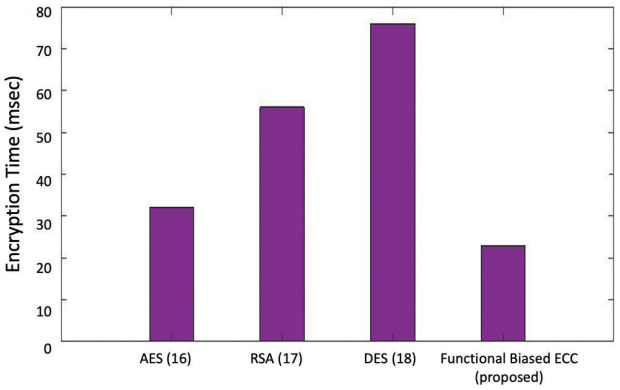

Fig. 5. Análisis del tiempo de generación de claves. AES: Advanced Encryp-tion Standard, DES: Data Encryption Standard, ECC: criptografía de curva elíptica, RSA: Rivest-Shamir-Adleman.

palabras clave. En comparación con enfoques tradicionales como AES, DES y RSA, se ha demostrado que nuestra metodología sugerida tarda menos en descifrarse incluso con claves más grandes.

Tiempo de generación de claves

En la Figura 5 se puede observar que, en comparación con los enfoques tradicionales como AES, DES y RSA, el algoritmo de cifrado de curva elíptica con sesgo funcional de almacenamiento seguro propuesto consume menos tiempo.

Nivel de seguridad

La Figura 6 compara el ECC funcionalmente sesgado propuesto con algoritmos de almacenamiento seguro convencionales como DES, RSA y AES en términos de nivel de seguridad. En comparación con las metodologías tradicionales, las alternativas presentadas ofrecen un mayor grado de seguridad.

Las figuras 3 a 6 ilustran las comparaciones entre varios algoritmos como AES, RSA, DES con el método propuesto FB ECC en varios parámetros como:

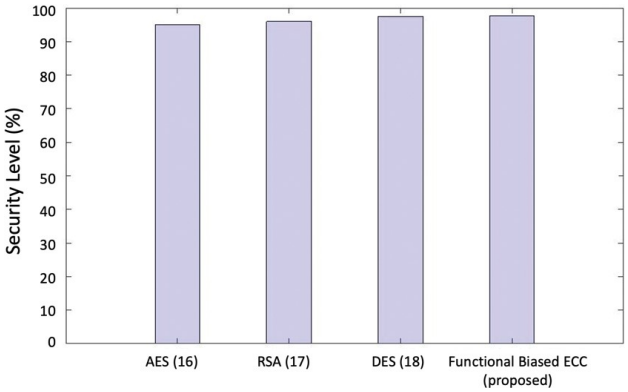

Fig. 6. Análisis del nivel de seguridad. Análisis del nivel de seguridad. AES: Estándar de cifrado avanzado, DES: Data Encryption Standard, ECC: criptografía de curva elíptica, RSA: Rivest-Shamir-Adleman.

i) Tiempo de cifrado
ii) Tiempo de descifrado
iii) Tiempo de generación de claves
iv) Nivel de seguridad

El análisis general de los algoritmos muestra que ofrece resultados mucho mejores que los algoritmos tradicionales en los cuatro parámetros analizados.

Conclusión

Para almacenar de forma segura la información médica de los pacientes en bases de datos en la nube habilitadas para niebla, se diseña e incluye en este sistema un modelo seguro de almacenamiento de información médica. En este sistema se recopila información médica de numerosos pacientes compatibles con los dispositivos de atención sanitaria electrónica.

La técnica FB-ECC se utiliza para desplegar un servidor privado que requiere descifrado y cifrado para com-putar. El método FB-ECC funcional se utiliza en esta investigación para ejecutar los procedimientos de cifrado, descifrado y generación de claves en la arquitectura de almacenamiento protegido. En comparación con los enfoques existentes, las técnicas propuestas los superan en términos de seguridad, cifrado, descifrado y KGT. El algoritmo de cifrado propuesto, FB-ECC, tiene un nivel de seguridad del 98,64%. Se ha demostrado que la combinación de FC con blockchain ha mejorado la seguridad de la transferencia de información en la atención sanitaria. Dado que sólo la clave secreta ECC con sesgo funcional puede devolver la información real, la información médica oculta no puede ser recuperada por ningún individuo no autorizado.

Los estudios futuros en esta área podrían incluir el desarrollo de un nuevo algoritmo criptográfico, que es un enfoque de cifrado sugerido a nivel mejorado de FB-ECC con un mayor grado de seguridad[18]

Financiación

No se han utilizado fondos para la preparación de este artículo.

Conflictos de intereses

No hay conflictos de intereses.

Colaboradores

Los autores son responsables de la elaboración de este artículo.

Declaración de disponibilidad de datos (DAS), intercambio de datos, reproducibilidad y repositorios de datos

Los datos no están disponibles.

Aplicación de texto generado por IA o tecnología relacionada

No se ha utilizado IA.

Referencias

1. Bouachir O, Aloqaily M, Tseng L, Boukerche A. Blockchain and fog computing for cyberphysical systems: the case of smart industry. Computer. 2020 Sep;53(9):36-45. https://doi.org/10.1109/MC.2020.2996212
2. Eskandarian A. Escaneando la cuestión. IEEE Trans Intell Transp Syst. 2023 Sep 1;24(9):8899-918. https://doi.org/10.1109/TITS.2023.3299370
3. Onasanya A, Elshakankiri M. Smart integrated IoT health-care system for cancer care. Wireless Netw. 2021;27:4297-312. https://doi.org/10.1007/s11276-018-01932-1
4. Ngabo D, Wang D, Iwendi C, Anajemba JH, Ajao LA, Biamba C. Blockchain-based security mechanism for the medical data at fog computing architecture of internet of things. Electronics. 2021 Aug 30;10(17):2110. https://doi.org/10.3390/electronics10172110
5. Baniata H, Kertesz A. A survey on blockchain-fog integration approaches. IEEE Access. 2020 Jun 1;8:102657-68. https://doi.org/10.1109/ACCESS.2020.2999213
6. Tariq N, Asim M, Al-Obeidat F, Zubair Farooqi M, Baker T, Hammoudeh M, et al. The security of big data in fog-enabled IoT applications including blockchain: a survey. Sensors. 2019 Apr 14;19(8):1788. https://doi.org/10.3390/s19081788
7. Banerjee A, Mohanta BK, Panda SS, Jena D, Sobhanayak S. A secure IoT-fog enabled smart decision making system using machine learning for intensive care unit. En: 2020 International Conference on Artificial Intelligence and Signal Processing (AISP). 2020 Jan 10 (pp. 1-6). IEEE [citado 2024 Aug 05]. Disponible en: https://www.researchgate.net/publication/340896382_A_Secure_IoT-Fog_Enabled_Smart_Decision_Making_system_using_Machine_Learning_for_Intensive_Care_unit.
8. Fernández-Caramés TM, Froiz-Míguez I, Blanco-Novoa O, Fraga-Lamas P. Enabling the internet of mobile crowdsourc-ing health things: a mobile fog computing, blockchain and IoT based continuous glucose monitoring system for diabetes melli-tus research and care. Sensors. 2019 Jul 28;19(15):3319. https://doi.org/10.3390/s19153319
9. Muthanna A, Ateya A, Khakimov A, Gudkova I, Abuarqoub A, Samouylov K, et al. Redes de IoT seguras y fiables utilizando computación de niebla con redes definidas por software y cadena de bloques. J Sensor Actuator Netw. 2019 Feb 18;8(1):15. https://doi.org/10.3390/jsan8010015
10. Srivastava A, Jain P, Hazela B, Asthana P, Rizvi SW. Application of fog computing, Internet of Things, and blockchain technol-ogy in healthcare industry. En: Fog Computing for Healthcare 4.0 Environments: Technical, Societal, and Future Implications. 2021:563–91. https://doi.org/10.1007/978-3-030-46197-3_22
11. Yánez W, Mahmud R, Bahsoon R, Zhang Y, Buyya R. Mecanismo de asignación de datos para sistemas de Internet de las Cosas con blockchain. IEEE Internet Things J. 2020 Feb 10;7(4):3509-22. https://doi.org/10.1109/JIOT.2020.2972776
12. Kumari A, Tanwar S, Tyagi S, Kumar N. Computación de niebla para el entorno Healthcare 4.0: oportunidades y desafíos. Comput Elect Eng. 2018 Nov 1;72:1-3. https://doi.org/10.1016/j.compeleceng.2018.08.015
13. Pareek K, Tiwari PK, Bhatnagar V. Computación en la niebla en el cuidado de la salud: una revisión. En IOP Conference Series: Materials Science and Engineering 2021 Mar 1 (Vol. 1099, No. 1, p. 012025). IOP Publishing.
14. Hanumantharaju R, Pradeep Kumar D, Sowmya BJ, Siddesh GM, Shreenath KN, Srinivasa KG. Enabling technologies for fog computing in healthcare 4.0: challenges and future impli-cations. En: Fog Computing for Healthcare 4.0 Environments: Technical, Societal, and Future Implications. 2021:157-76.
15. Mayer AH, Rodrigues VF, da Costa CA, da Rosa Righi R, Roehrs A, Antunes RS. Fogchain: a fog computing architec-ture integrating blockchain and internet of things for personal health records. IEEE Access. 2021 Sep 1;9:122723-37. https://doi.org/10.1109/ACCESS.2021.3109822
16. Munirathinam T, Ganapathy S, Kannan A. Cloud and IoT based privacy preserved e-Healthcare system using secured stor-age algorithm and deep learning. J Intell Fuzzy Syst. 2020 Jan 1;39(3):3011-23. https://doi.org/10.3233/JIFS-191490
17. Al Hamid HA, Rahman SM, Hossain MS, Almogren A, Alamri A. A security model for preserving the privacy of medical big data in a healthcare cloud using a fog com-puting facility with pairing-based cryptography. IEEE Access. 2017 Sep 28;5:22313-28. https://doi.org/10.1109/ ACCESS.2017.2757844
18. Yadav K, Alharbi A, Jain A, Ramadan RA. Un sistema seguro de monitorización de la salud del paciente basado en IoT. Comput Mater Contin. 2022 Jan 1;70(2):3637-52. https://doi.org/10.32604/cmc.2022.020614