BLOCKCHAIN® IN HEALTHCARE TODAY
PLATFORM APPROACHES IN HEALTHCARE

URSPRÜNGLICHE FORSCHUNG

Sichere und zuverlässige Fog-Enabled-Architektur unter Verwendung von Blockchain mit funktional verzerrter elliptischer Kurve Kryptographiealgorithmus für Gesundheitsdienste

Charu Awasthi, PhD Student[1]; Satya Prakash Awasthi, PhD[2]; und Prashant Kumar Mishra, PhD[3]

[1]Forschungsstipendiatin, Abteilung für Computertechnik, Poornima Universität, Jaipur, Indien; [2]Außerordentliche Professorin, Abteilung für Computertechnik, Poornima Universität, Jaipur, Indien; [3]Außerordentliche Professorin, Abteilung für Informatik und Ingenieurwesen, Pranveer Singh Institute of Technology, Kanpur, Indien

Korrespondierender Autor: Charu Awasthi, E-Mail: charuawasthi@gmail.com DOI:

https://doi.org/10.30953/bhty.v7.347

Schlüsselwörter: Blockchain, FB-ECC, Fog Computing, funktionaler Elliptische-Kurven-Kryptographie-Algorithmus, galaktischer Bienenvolk-Optimierungsalgorithmus, GBCOA, Gesundheitsdienste

Zusammenfassung

Fog Computing (FC) ist eine aufkommende Technologie, die die Leistungsfähigkeit und Effizienz von Cloud-Computing-Netzen erweitert, indem sie als Brücke zwischen der Cloud und dem Gerät fungiert. Fog-Geräte können eine enorme Menge an Informationen lokal verarbeiten, sind transportabel und können in einer Vielzahl von Systemen eingesetzt werden. Aufgrund ihrer Echtzeitverarbeitung und der Reaktion auf Ereignisse sind sie ideal für das Gesundheitswesen. Bei einer so großen Bandbreite an Merkmalen ergeben sich neue Bedenken hinsichtlich Sicherheit und Datenschutz. Aufgrund der sicheren Übertragung, Ankunft und des Zugangs sowie der Verfügbarkeit medizinischer Geräte ergeben sich neue Sicherheitsfragen im Gesundheitswesen. Folglich erfordert die FZ einen einzigartigen Ansatz für Sicherheits- und Datenschutzmetriken, der sich von den Standardmethoden des Cloud Computing unterscheidet. Daher schlägt dieser Artikel eine effektive Blockchain vor, die auf sicheren Gesundheitsdiensten in der FZ basiert. Hier sammeln die Fog Nodes die Informationen von den medizinischen Sensorgeräten und die Daten werden mit Hilfe von Smart Contracts im Blockchain-Netzwerk validiert. Zur Verschlüsselung der Daten schlagen wir einen funktional verzerrten elliptischen Kurven-Kryptographie-Algorithmus vor. Die Optimierung wird mit dem galaktischen Bienenvolk-Optimierungsalgorithmus durchgeführt, um das Verschlüsselungsverfahren zu verbessern. Die Leistung der vorgeschlagenen Methodik wird bewertet und mit den traditionellen Techniken verglichen. Es wird nachgewiesen, dass die Kombination von FC mit Blockchain die Sicherheit der Datenübertragung im Gesundheitswesen erhöht hat.

Eingereicht: 7. August 2024; Angenommen: Oktober 4, 2024; Veröffentlicht: December 31, 2024

Die jüngsten Durchbrüche in der elektronischen Kommunikation haben das Internet der Dinge (Internet of Things, IoT) mit der Entwicklung von Kleingeräten verändert, die das Internet nutzen und verbinden. die das Sammeln und Teilen von Informationen steuern. Dies ermöglicht die Schaffung winziger, kosteneffizienter und weniger leistungsfähiger multifunktionaler Sensorsysteme, die in der Lage sind, verschiedene Daten in zahlreichen Bereichen wie Verkehr, Gesundheitswesen und Industrie zu beobachten und zu übermitteln.[1]

Das IoT im Gesundheitswesen bietet mehrere Vorteile, darunter die Datenübertragung in Echtzeit und die Möglichkeit, den physiologischen Zustand von Patienten über verschiedene Zeiträume zu überwachen. Geräte, einschließlich Blutzuckermessgeräte, Elektroenzephalographie, Elektromyographie, tragbare Geräte usw. ermöglichen es den Gesundheitsdienstleistern, die Gesundheitsdaten eines Patienten vor Ort zu erfassen und je nach Gesundheitszustand des Patienten eine Entscheidung zu treffen.

Kliniken setzen das IoT bereits seit einigen Jahren ein und verfügen nun über IoT-Geräte im Gesundheitswesen in den Patientenzimmern und ihren Systemen. Klinische Einrichtungen, Kliniken und Unternehmen befassen sich jedoch nicht mit der Schutzbedrohung durch das IoT im Gesundheitswesen, das mit einem lokalen Netzwerk oder einem Weitverkehrsnetz verbunden ist. Die IoT-Geräte lassen sich leicht ausspionieren, was aufgrund schwacher Validierungs- und Verschlüsselungstechniken zu verschiedenen Problemen führen kann.

Daher wird die Blockchain für eine sichere und vertrauenswürdige Übertragung im IoT im Gesundheitswesen eingeführt. Abbildung 1 veranschaulicht den Rahmen des Fog Computing (FC).

Die Entwicklung von IoT-Systemen, insbesondere in der Gesundheitsbranche, erzeugt riesige Mengen an Informationen, die in der Cloud transportiert und gespeichert werden. Da Informationen in Echtzeit verarbeitet und gespeichert werden müssen, stellt die Handhabung solch großer Mengen an cloudbasierten Informationen einen Engpass dar.

Auch der Schutz von Informationen in der Cloud ist ein wichtiges Thema.[2]Die FZ-Idee war ein Versuch, dieses Problem zu lösen. Fog Computing ist eine Systemerweiterung des Cloud Computing. Die Hauptaufgabe von Fog ist es, das Funktionieren der Cloud zu begleiten. So stellt Fog beispielsweise Rechenressourcen für Geräte bereit, die sich näher am Rand des Netzwerks befinden. Das typische IoT-Cloud-Framework hat Probleme mit der Skalierbarkeit und Zuverlässigkeit, aber FC behebt diese Probleme.

Da die Fog-Knoten am Rande des Netzes arbeiten und geografisch weiter verstreut sind (siehe Abbildung 1), verbessern sie den Schutz und die Sicherheit der Informationen und minimieren die Verzögerung, was für Anwendungen wie medizinische Informationen entscheidend ist. Die Gesamtbandbreite zur Cloud wird ebenfalls minimiert, was zu einer verbesserten Servicequalität führt. Die Erkennung, Validierung und Verifizierung von IoT-Geräten im Gesundheitswesen in einem dezentralisierten Kontext kann durch die Integration von FC mit Blockchain gelöst werden.[3]Um dieses Problem anzugehen, stellen wir eine Fog-fähige Architektur vor, die Blockchain mit einem funktionalen FB-ECC-Algorithmus (Functional Biased Elliptic Curve Cryptography) für Gesundheitsdienste verwendet.

Verwandte Arbeiten

In diesem Artikel wird ein FB-ECC-Algorithmus zur Datenverschlüsselung vorgeschlagen, dessen Optimierung durch den galaktischen Bienenvolk-Optimierungsalgorithmus (GBCOA) erfolgt. Dieser Algorithmus wird mit verschiedenen Algorithmen verglichen, die in verschiedenen Artikeln zur Leistungsanalyse vorgeschlagen werden.

Tabelle 1 enthält die wichtigsten Beobachtungen von Forschern zu verwandten Beobachtungen von nebelfähigen Architekturen. Die Zusammenfassungen der verwandten Literatur deuten darauf hin, dass die Integration von Fog-Architekturen mit Blockchain, die die Fähigkeiten von IoT-Geräten nutzen, ein interessanter Bereich ist, wenn wir einen geeigneten Algorithmus für die ordnungsgemäße Funktion einbauen können.

Ngabo et al.[4]erklärten, dass das Hauptziel ihrer Arbeit darin besteht, Schutzmechanismen gegen medizinische Data-Mining-Angriffe zu entwickeln, die durch die Sensorebene und die Informationsspeicherung in der Cloud-Datenbank des IoT entstehen. Ein Blockchain-Schutzverfahren mit öffentlicher Genehmigung, das digitale ECC-Signaturen verwendet, um eine verteilte Ledger-Datenbank (Server) zu unterstützen, um unveränderlichen Schutz und Transparenz bei der Übertragung zu bieten sowie die Manipulation von Patientendaten auf der Nebelschicht des IoT zu schützen.

Baniata und Kertesz[5]präsentierten eine gründliche Literaturanalyse und Kategorisierung der FC-Blockchain (FC-BC)-Kombination - der aktuelle Stand der Technik der FC-BC-Kombination. Die Autoren erörtern und gliedern die relevanten Arbeiten nach Erscheinungsjahr und Gebiet sowie nach den verwendeten Algorithmen, BC-Funktionen und der Position der BC in der FC-Architektur. Untersuchungen, Bewertungen und zukünftige Schwierigkeiten für die BC-FC-Kombination werden vom Autor detailliert dargestellt.

Tariq et al.[6]versuchten, die Probleme des künftigen Schutzes digitaler Infrastrukturen zu einem Zeitpunkt anzugehen, zu dem dieser noch in der Entwicklung ist. Der funktionsabhängige Nebelrahmen wird mit dem Aufkommen der Architektur, die große Mengen an Informationen erzeugt, geschaffen.

Außerdem werden die Notwendigkeit eines zusätzlichen Schutzes von Fog-fähigen IoT-Geräten sowie die Herausforderungen des FZ-Schutzes und der Vertraulichkeit großer Datenmengen im Zusammenhang mit Fog-fähigem IoT diskutiert. Dann wird die Berücksichtigung der ergänzenden

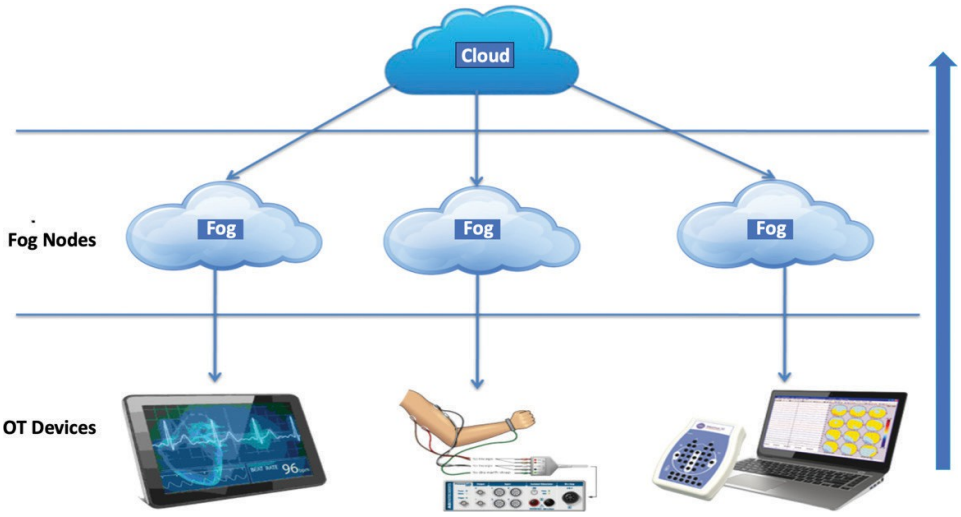

Abb. 1. Architektur des Fog Computing.

Citation: Blockchain im Gesundheitswesen heute 2024, **7**: 347 - https://doi.org/10.30953/bhty.v7.347

Tabelle 1. Beobachtungen von Forschern auf dem Gebiet der nebelfähigen Architektur

Quelle	Beobachtung der obersten Zeile
Ngabo et al.[4]	Das Hauptziel ist die Entwicklung von Schutzmechanismen gegen medizinische Data-Mining-Angriffe, die durch die Erfassungsschicht und die Informationsspeicherung in der Cloud-Datenbank des IoT entstehen.
Tariq und Kollegen[6]	befassen sich mit Fragen im Zusammenhang mit dem Schutz künftiger digitaler Infrastrukturen.
Banerjee et al.[7]	Verbesserte Nutzererfahrung und Ausfallsicherheit der Dienste in Notfällen.
Fernández et al.[8]	Implementierung eines Systems, das das kommerzielle CGM um IoT-Funktionen erweitert, um eine Fernüberwachung der Patienten zu ermöglichen.
Muthanna et al.[9]	schlugen einen Rahmen für SDN zur Regulierung und Verwaltung einer Edge-Computation-Ebene von Nebelknoten vor.
Srivastava et al.[10]	Diskutierten über FC, Blockchain und das IoT im Gesundheitswesen
Yánez et al.[11]	schlugen einen neuen kontextbewussten Ansatz für die Zuweisung von Informationen innerhalb der Kette in IoT-Blockchain-Netzwerken vor.
Kumari et al.[12]	Sie untersuchten die Funktionen des Fog- und Cloud-Computing und des IoT bei der Bereitstellung kontinuierlicher kontextbezogener Dienste für Endnutzer.
Pareek et al.[13]	stellten fest, dass das IoT viele Geräte weltweit miteinander verbindet.
Hanumantharaju et al.[14]	stellt fest, dass das IoT Patienten und Gesundheitsdienstleistern dabei helfen kann, in Kontakt zu bleiben und ihrer Gemeinschaft eine klare, wertorientierte Versorgung zu bieten.
Mayer et al.[15]	schlagen ein architektonisches FZ-Paradigma vor, das Blockchain, Fog Computing und das IoT für den Gesundheitsbereich integriert.

FC: Fog Computing; CGM: kontinuierliche Glukoseüberwachung; IoT: Internet der Dinge; SDN: Software-definiertes Netzwerk.

Es werden die gegenseitigen Abhängigkeiten zwischen Blockchain und FC sowie ihre Rolle bei der Bewältigung einer breiten Palette von Schutzproblemen im IoT erörtert. Infolgedessen bietet diese Studie eine Taxonomie der Arten von Angriffen auf nebeltiefe IoT-Systeme, vergleicht die jüngsten Beiträge in diesem Bereich im Hinblick auf ihren Schutzdienst und gibt Empfehlungen für künftige Forschung.

Banerjee et al.[7]verbesserten das Benutzererlebnis und die Ausfallsicherheit der Dienste im Notfall; FZ-Techniken wurden eingesetzt, um das Internet der Dinge mit Echtzeitberechnungen in Randnetzen zu verbinden. Fog-Edge-Computing mit seinem verteilten Design und seiner Nähe zu den Endnutzern kann schnellere Reaktionszeiten und qualitativ hochwertigere Dienste für die IoT-Nutzung liefern. FZ, IoT und maschinelles Lernen sind in jedem Teil des von den Forschern entwickelten Paradigmas zur Verbesserung der Qualität der Gesundheitsversorgung enthalten. Die Blockchain-Technologie wird eingesetzt, um den Schutz der Architektur zu gewährleisten.

Fernández et al.[8]implementierten ein System, das den kommerziellen kontinuierlichen Glukosemonitor (CGM) um IoT-Funktionen erweitert, um die Fernüberwachung von Patienten zu ermöglichen und sie so über potenziell gefährliche Umstände zu informieren. Zur Erfassung von CGM-Blutzuckermessungen werden Mobiltelefone verwendet, um Messungen an eine entfernte Cloud oder verstreute Knoten im Nebel zu senden. Dazu gehört auch ein dezentralisiertes Speichersystem, das die erfassten Informationen sammelt, verarbeitet und speichert, um genaue, vertrauenswürdige und cyber-sichere Informationen mit medizinischen Wissenschaftlern, Ärzten und Pflegepersonal zu teilen.

GlucoCoin wurde als Anreizsystem für Einzelpersonen geschaffen, dem System neue Informationen und digitales Geld zur Verfügung zu stellen. Unter Verwendung einer Blockchain, die in der Lage ist, intelligente Verträge auszuführen, kann dieses System den Kauf von CGM-Sensoren automatisieren oder Nutzer entschädigen, die ihre Informationen zur Verfügung stellen, damit das System funktioniert.

Muthanna et al.[9]schlugen einen Rahmen für softwareseitig definierte Netzwerke (SDN) vor, um eine Randberechnungsschicht von Nebelknoten zu regulieren und zu verwalten und eine hohe Verfügbarkeit und Zuverlässigkeit für verzögerte IoT-Anwendungen zu gewährleisten. OpenFlow-Switches mit Ressourcenbeschränkungen werden in dem SDN-Netzwerk verwendet, das über verteilte Kontrollinstanzen verfügt. Eine vertrauenswürdige Dezentralisierung kann durch den Einsatz der Blockchain erreicht werden. OpenFlow-Switches werden in Abhängigkeit von ihrer aktuellen Arbeitslast durch eine Informations-Offload-Technik rechnerische Verarbeitungsaufgaben zugewiesen. Es wurde ein Verkehrsmodell für das gesamte Netzwerk vorgeschlagen. Der Algorithmus wird mit Hilfe von Simulationen und einem Testbed getestet.

Srivastava et al.[10]diskutierten FC, Blockchain und das IoT im Gesundheitswesen. Im Gegensatz zum Cloud Computing, das zwischen Cloud- und Endnutzergeräten, den sogenannten IoT-Geräten, operiert, erweitert FC die Kapazität des Cloud Computing auf die Ausführung von Funktionen wie Verarbeitung, Speicherung und Interaktion über das Internet. Es bietet überlegene Möglichkeiten der Informationsspeicherung mit Echtzeitzugriff, geringerer Verzögerung, größerer Reaktionsfähigkeit, besserer Fehlertoleranz und einem geschützten und verborgenen Kontext. Nebel, Zugang, Informationsschnittstelle, Anwendung und Schutzschichten sind im IoT-System in fünf Ebenen unterteilt. Die Autoren heben die Blockchain-Technologie und Konsensmechanismen hervor, um den Informationsschutz im Gesundheitswesen zu verbessern.

Yánez et al.[11]schlugen einen neuen kontextbewussten Ansatz für die Zuweisung von Informationen innerhalb der Kette in IoT-Blockchain-Netzwerken vor. Darüber hinaus schaffen sie einen Datencontroller mit Fuzzy-Logik, der den RoA-Wert einer Anfrage anhand mehrerer Kontextmerkmale wie Qualität und Quantität der Informationen und der Netzwerke, über die sie gesendet werden, schätzt. Der Entwurf und die Implementierung des Mechanismus führten auch zur Verfeinerung von zwei beliebten IoT-Blockchain

architektonische Merkmale. Die Datenzuweisungsmethode wird in den Blockchain-abhängigen Cloud- und Fog-Architekturen instanziiert und mit Fog Bus evaluiert, um die Wirksamkeit unseres Ansatzes zu zeigen. Anhand von realen Anwendungen im Gesundheitswesen vergleichen sie unsere Methode auch mit aktuellen Entscheidungsfindungsprozessen.

Kumari et al.[12]untersuchten die Funktionen des Fog- und Cloud-Computing und des IoT bei der Bereitstellung kontinuierlicher kontextbezogener Dienste für Endnutzer, wann und wo sie benötigt werden. Für das Sammeln, Verarbeiten und Übertragen von Informationen in Echtzeit schlagen sie ein dreischichtiges patientenorientiertes Gesundheitssystem vor. Es bietet Endnutzern Informationen über die Verwendung von Fog-Geräten und Gateways im Ökosystem des Gesundheitswesens 4.0 für aktuelle und zukünftige Anwendungen.

Pareek et al.[13]erwähnten, dass das IoT viele Geräte auf der ganzen Welt miteinander verbindet. Um die Gesundheitssysteme zu entlasten, können IoT-abhängige Technologien dazu beitragen, die Gesundheitskosten zu senken und die Rechenleistung und Verarbeitungsgeschwindigkeit zu erhöhen. Im IoT erfordern größere und anspruchsvollere Datenmengen im Gesundheitswesen den Einsatz von Cloud Computing. Verzögerungen, Bandbreitennutzung, Echtzeit-Reaktionslatenz, Sicherheit und Vertraulichkeit sind nur einige der Probleme, die bei der Integration des IoT in die Cloud auftreten. Wenn es um Cloud Computing geht, müssen viele Bedenken und Herausforderungen angegangen werden, bevor eines der IoT-Fog-basierten Systemmodelldesigns bewertet werden kann.

Hanumantharaju et al.[14]erwähnten, dass die Rolle des IoT Patienten und Gesundheitsdienstleistern helfen könnte, in Kontakt zu bleiben und ihrer Gemeinschaft eine klare, wertabhängige Pflege zu bieten, indem sie es für beide einfacher machen, in Kontakt zu bleiben. Die FZ kann als Grundlage für den Einsatz des IoT im Gesundheitswesen dienen. Die Experten diskutierten über das Gesundheitswesen 4.0. Die Forscher werden untersuchen, wie die FZ-Taxonomie die beste Antwort auf das Gesundheitswesen 4.0 in Bezug auf die Informationserfassung und -auswertung, den Schutz und die Vertraulichkeit sowie die e-Gesundheitsdienste sein könnte.

Mayer et al.[15]schlugen ein FZ-Architekturparadigma vor, das Blockchain, FZ und das IoT für den Gesundheitsbereich integriert. Die FZ-Architektur und ihre differenzierten Ansätze zur Überwindung von IoT-Beschränkungen sind die bedeutendsten Beiträge.

Die Literaturrecherche legt nahe, dass die Integration von Fog-Architektur und Blockchain unter Nutzung der Fähigkeiten von IoT-Geräten ein interessanter Bereich ist, wenn wir einen geeigneten Algorithmus für ein reibungsloses Funktionieren entwickeln können.

In diesem Artikel wird ein FB-ECC-Algorithmus zur Datenverschlüsselung vorgeschlagen, dessen Optimierung durch die GBCOA erfolgt. Dieser Algorithmus wird mit verschiedenen Algorithmen verglichen, die in verschiedenen Artikeln zur Leistungsanalyse vorgeschlagen wurden.

Vorgeschlagene Methode

Ein effektiver blockchain-abhängiger geschützter Gesundheitsdienst in der FZ wird in diesem Abschnitt kurz erläutert.

Der Fog-Knoten sammelt die Informationen von den medizinischen Sensorgeräten und die Daten werden mithilfe von Smart Contracts im Blockchain-Netzwerk validiert. Um die Daten zu verschlüsseln, wird der FB-ECC-Algorithmus vorgeschlagen. Um den Verschlüsselungsprozess zu optimieren, wird der GBCOA implementiert. Die Leistung der vorgeschlagenen Methodik wird bewertet und mit dem traditionellen Ansatz verglichen. Abbildung 2 zeigt die Flussdarstellung der implementierten Techniken.

In dieser Infrastruktur lassen sich vier Ebenen erkennen: die IoT-Ebene, die Nebelschicht mit Blockchain, die Cloud-Ebene und die Datenanalyseschicht. Die Gesundheitsinformationen der Patienten werden mit Hilfe von medizinischen Sensorgeräten erfasst. Über kabelgebundene oder drahtlose Medien, einschließlich ZigBee und Wi-Fi, kann jedes medizinische IoT-Gerät mit einem einzigen Fog-Knoten verbunden werden. Fog-Knoten setzen voreingestellte Schutzstandards durch, um angeschlossene IoT-Geräte und -Dienste zu kontrollieren, und dienen als Vermittler zwischen der Cloud und der Blockchain, der einen Autorisierungsindex für Informationsabfragen ermöglicht.

Datenvalidierung mit Smart Contract

Obwohl der Begriff früher im Zusammenhang mit Protokollen zwischen Fremden im Internet verwendet wurde, sind Smart Contracts Beispiele für Verträge, die auf der Ethereum-Blockchain implementiert sind. Ein intelligenter Vertrag hat die folgenden Regeln:

1. Aushandeln der Bedingungen der Vereinbarung
2. Automatische Validierung der Vereinbarung
3. Umsetzung der vereinbarten Bedingungen

Ein intelligenter Vertrag besteht aus vielen Funktionen, auf die von außerhalb der Blockchain oder über andere intelligente Verträge zugegriffen werden kann. Durch die Verwendung der Blockchain in Verbindung mit der Smart-Contract-Technologie müssen sich die Transaktionsparteien nicht mehr auf ein zentralisiertes System verlassen. Jeder verbundene Teilnehmer im Netzwerk hat eine Kopie der intelligenten Verträge, da diese auf der Blockchain gespeichert sind. Wenn ein Smart Contract durch ein erlaubtes oder vereinbartes Ereignis ausgelöst wird, kann er die vereinbarte gespeicherte Prozedur ausführen. Jede Vertragsübertragung sowie der gesamte Prüfpfad der Aktivitäten werden in chronologischer Reihenfolge für den späteren Zugriff gespeichert. Jeder Versuch einer Partei, einen Vertrag oder eine Transaktion auf der Blockchain zu verändern, wird von allen anderen Teilnehmern erkannt und verhindert. Das System funktioniert auch dann weiter, wenn eine der Parteien ausfällt, ohne dass es zu einem Verlust von Informationen oder Integrität kommt. Auf diese Weise entsteht ein riesiges, sicheres, logisches Computersystem ohne die Gefahren, Kosten oder Vertrauensprobleme, die mit einem zentralisierten Paradigma verbunden sind.

Blockverifizierung mit Stellar-Konsens-Protokollen

Das Stellar-Konsensprotokoll ist ein dezentrales Konsensprotokoll, bei dem die Knoten in einem Netzwerk nicht über die

Citation: Blockchain im Gesundheitswesen heute 2024, 7: 347 - https://doi.org/10.30953/bhty.v7.347

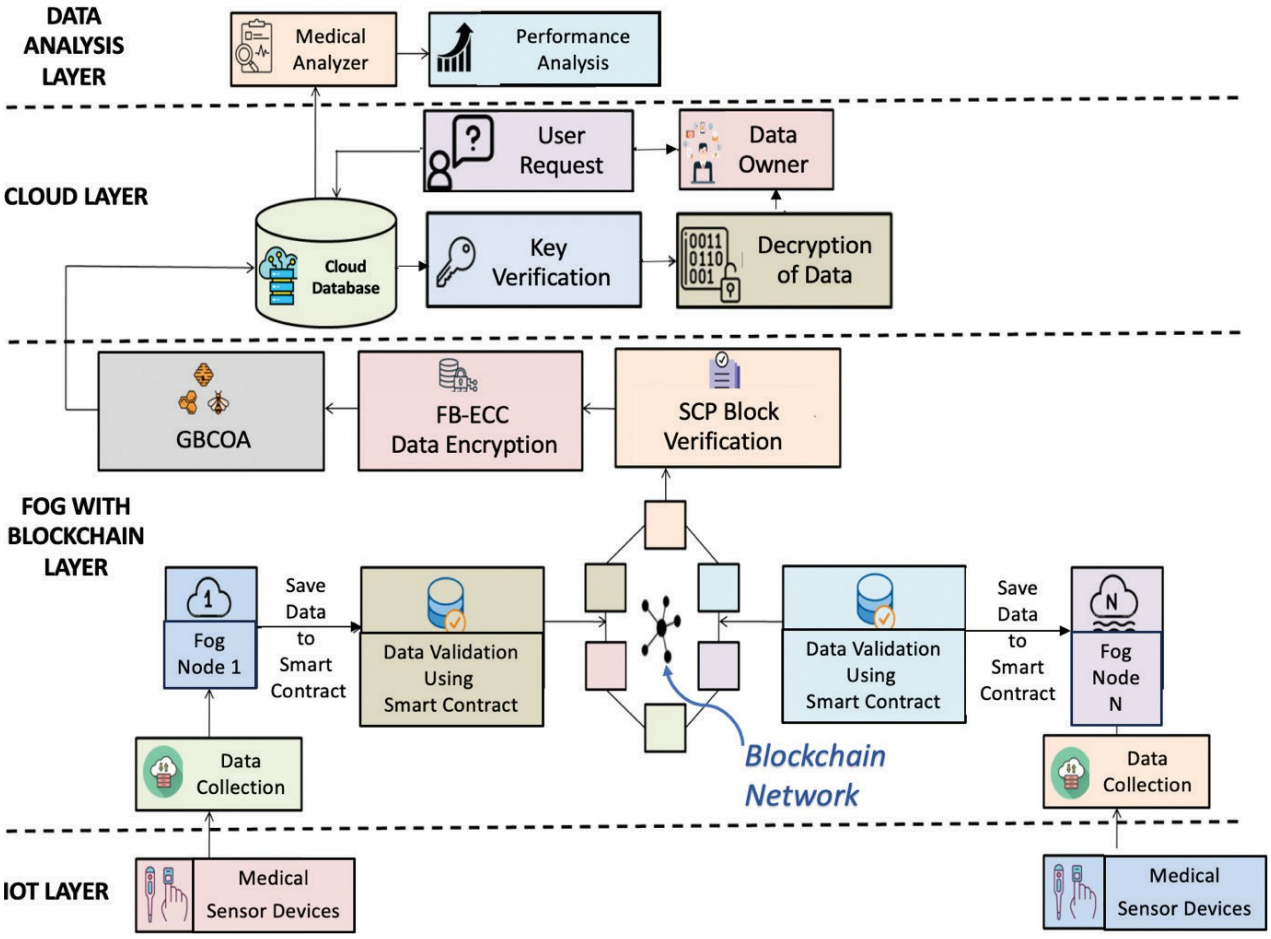

Abb. 2. Flussdarstellung der implementierten Techniken. FB-EEC: funktional verzerrter Elliptik-Kurven-Kryptograph; FC-BC: Fog Computing-Blockchain; GBCOA: galaktischer Bienenvolk-Optimierungsalgorithmus; IoT: Internet of Things.

[16]Die Idee einer "Quorum-Scheibe", die ursprünglich durch dieses Protokoll eingeführt wurde, bezieht sich auf eine Sammlung von Knoten, die einander vertrauen. Ein "Quorum" ist eine Gruppe von Knoten, die groß genug ist, um einen Konsens herbeizuführen, während ein "Quorum-Slice" eine Teilmenge eines Quorums ist, die einen oder mehrere Knoten dazu bringt, zuzustimmen.

Jeder Knoten, der diese Werte erhält, prüft den Block auf einen einzigen Wert unter ihnen, was dazu führt, dass ein einziger Wert zur Validierung des Blocks verwendet wird. Die Knoten beginnen in dieser Phase damit, den Block daraufhin zu überprüfen, ob sie die in der vorherigen Phase gewählten Werte akzeptieren oder abbrechen sollen. Wenn sich eine Gruppe von Knoten nicht einigen kann, wird der Wert zur Authentifizierung an einen größeren Block übertragen.

Datenverschlüsselung mit dem Algorithmus der Functional Biased Elliptic Curve Cryptography

FB-ECC ist eine bekannte Kryptographietechnik mit öffentlichem Schlüssel, die zuverlässig und sicher die Vertraulichkeit und das Geheimnis verschlüsselter medizinischer Informationen wahrt. Für die Verschlüsselung und Entschlüsselung werden identische Schlüssel verwendet (Tabelle 2).

FB-ECC ist eine gängige Verschlüsselungsmethode mit öffentlichem Schlüssel, bei der unterschiedliche Schlüsselpaare für Ver- und Entschlüsselungsvorgänge verwendet werden, z. B. die zufällige Erstellung öffentlicher und privater Schlüssel. Kryp-tographietechniken mit öffentlichen Schlüsseln, wie FB-ECC, sind ebenfalls in diese Technologie integriert. Die Autorisierung und Klarheit neuer Transaktionen hängt von der verstreuten Zustimmung (mehr als 50 %) zwischen den Nutzern ab, was dieser Technik einen Vorteil gegenüber der Public-Key-Kryptographie verleiht. Da nur der geheime FB-ECC-Schlüssel die tatsächliche Information zurückgeben kann, können die verborgenen medizinischen Informationen nicht von einer unbefugten Person abgerufen werden.

In der asymmetrischen Schlüsselkryptographie spielt die FB-ECC-Technik eine entscheidende Rolle bei der Durchführung der Public-Key-Kryptographie. Darüber hinaus wird ein numerischer Ausdruck unter Verwendung des definierten Basispunkts, der Kurve und der höchsten Grenze einer Primzahlfunktion erstellt, und die Verschlüsselung erfolgt mit Hilfe der folgenden FB-ECC-Gleichung:

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

Tabelle 2. Ein Algorithmus für die funktional vorgespannte elliptische Kurvenverschlüsselung

Eingabe: Eingabedaten (dI), privater Schlüssel (K).

Ausgabe: Verschlüsselte Daten (Ed).

1: Zufällige Erzeugung des öffentlichen Schlüssels (Pk);

2: $P_k = A * G_d$/* die Funktion der Generierung Go in Abhängigkeit von der Kurvengleichung, Go wird aus der Abbildungsfunktion extrahiert.

3: Generieren Sie die Chiffren Cs als Cs← RM * Go;

4:Die verschlüsselten Daten (E_d) werden erstellt als $E_d \leftarrow S_M * Pa) + (d_{(P)}, W)$;/* W /* W bezeichnet den Basispunkt auf der Kurve.

5: Die verschlüsselten Daten (E_d) werden in die öffentliche Cloud-Umgebung hochgeladen

Anmerkung: Siehe Text für mehr Kontext.

Die ganzen Zahlen sind durch b und c gekennzeichnet. Die Gesamtstärke des Verschlüsselungsprozesses wird jedoch durch die Erstellung eines Schlüssels bestimmt, der von jedem kryptografischen Algorithmus abhängt. Der erste Prozess ist die Erstellung des öffentlichen Schlüssels, der zur Verschlüsselung der Informationen verwendet wird, die normalerweise vom Empfänger empfangen werden. Der zweite Prozess besteht in der Erzeugung eines privaten Schlüssels, der die Entschlüsselung der ursprünglichen Information auf der Seite des Empfängers ermöglicht. W ist der Startpunkt der Kurve, und A ist die gewählte Zufallszahl im Bereich von 1-(m - 1):

$$S = A \; x \; W \tag{2}$$

Der öffentliche Schlüssel wird als S dargestellt, während der private Schlüssel mit A bezeichnet wird.

Die Verschlüsselung ist eine Methode zur Umwandlung von tatsächlichen Informationen in chiffrierte Informationen und wird verwendet
um den Schutz zu erhöhen. Die FB-ECC ist die am häufigsten verwendete Technik in der Cloud-Sicherheit, um Schutz zu bieten
je nach der Komplexität der Probleme. Die Verschlüsselung
Die Stärke des Verfahrens wird durch die Schlüsselgenerierung bestimmt

Prozess, der eine bessere Lösung für Informationen bieten kann, indem er mehr Vertraulichkeit bei der Übertragung von geheimen Schlüsseln zwischen verschiedenen Kommunikationseinheiten unterstützt. Die ursprüngliche Eingangsinformation dI und der private Schlüssel K werden in diesem Verschlüsselungsverfahren als Eingaben geliefert, und die Generierungsfunktion (Go) erstellt den öffentlichen Schlüssel (Pk). Infolgedessen werden die Chiffren Cs mit Hilfe der 4-Bit-Zufallszahlen Rm und Go erstellt. Die Eingabedaten dI werden dann mit dem Basispunkt W der Kurve verschlüsselt, gefolgt von der Erzeugung des öffentlichen Schlüssels Pk und der Zufallszahl Rm.

Galactic Bee Colony Optimierungsalgorithmus

Der GBCOA simuliert die Bewegung von Sternen, Galaxien und Supergalaxien, um machbare Alternativen in einem bestimmten Suchraum zu finden. Wie Sterne in Galaxien kommunizieren sie miteinander. Der Agent ist durch das galaktische Bienenvolk in zwei Ebenen unterteilt. Die Sterne werden auf der ersten Ebene dargestellt, während die Galaxien auf der zweiten Ebene dargestellt werden. Mit Ausnahme der Startpopulation der zweiten Ebene, die aus den besten Lösungen von der ersten Stufe, hat jede Stufe ihren Suchmechanismus. Auf jeder Stufe können mehrere Suchtechniken verwendet werden. In allen Stufen haben sich die Forscher für die Bienenvolk-Optimierungsmethode entschieden. So verwendet auf der ersten Ebene jede Teilpopulation BCO, um die optimale Antwort zu finden, und sendet sie dann an die höhere Ebene, um Superbienen zu bilden. Die Superbienen werden als Startpopulation für einen neuen BCO-Lauf verwendet, um die optimale Lösung zu finden. Das mehrschichtige BCOA-Verfahren wird in (3) dargestellt:

$$s_q^p \in S : q = 1, 2, ..., M$$

$$b_p \in S_p : b_p = best\left(S_p\right)$$

$$G = \bigcup_{p=1}^{M} b_p \tag{3}$$

Die erste Subpopulation von N Lösungen wird in der ursprünglichen galaktischen Bienen-Optimierungstechnik im Durchlaufverfahren erzeugt. S^p bezeichnet die j-te Lösung der i-ten Teilpopulation. S_q bezeichnet die i-te Teilpopulation. $b_{(p)}$ (best($S_{p)}$) bezeichnet die große Lösung der Teilpopulation S_p. Die Menge G bezeichnet die Superpopulation, die aus den besten Lösungen aus den Teilpopulationen besteht.

Die besseren Lösungen aus jeder Teilpopulation in Stufe 1 werden als erste Population von Stufe 2 verwendet. Stufe 2 wird L2 mal ausgeführt, dann wird das in Stufe 2 identifizierte gute Ergebnis als letzte Lösung der Epoche vereinbart. Der gesamte Algorithmus wird epochenweise ausgeführt, dann werden die bisher in den Epochen ermittelten guten Ergebnisse als letztes Ergebnis des Algorithmus festgelegt.

Cloud-Datenbank

Bei diesem Paradigma kommuniziert ein zentraler Server für Gesundheitsdaten mit einem Speicher oder einer Datenbank für medizinische Daten. Der Patient ist Eigentümer der Informationen, zu denen auch sensible persönliche Daten gehören. Die Krankenakte des Patienten, die häufig in solchen Dokumenten enthalten ist, kann unter anderem biometrische Daten, physische, psychologische und geistige Gesundheitsprobleme, persönliche Anamnese, Allergien, verwendete Medikamente, Gesundheitszustände, frühere medizinische Therapien und Krankheiten enthalten. Finanzielle Daten, einschließlich

Citation: Blockchain im Gesundheitswesen heute 2024, **7**: 347 - https://doi.org/10.30953/bhty.v7.347

Bankkonto-, Kredit- und Debitkartennummern sowie die Identität des Patienten können in den medizinischen Unterlagen enthalten sein.[17]

Der Schutz der Sicherheit und Vertraulichkeit elektronischer Gesundheitsdaten gilt als ein Kernelement des Gesundheitsinformationsmanagements. Das Hauptziel des Gesundheitsdatensystems besteht darin, zu gewährleisten, dass die Informationen bei Bedarf zugänglich sind und dass sie beim Speichern oder Versenden nicht missbräuchlich verwendet, offengelegt, erworben, verändert oder zerstört werden.

Die Sicherheits- und Datenschutzstandards arbeiten zusammen, um geeignete Kontrollen und Schutzmaßnahmen zu gewährleisten. Die Patienten-Identifikationsnummer wird zur Identifizierung der Krankenakte in der Krankenaktenablage oder Datenbank verwendet. Unter den genannten Kennungen sind die Gesundheitsdaten des Patienten persönlich identifizierbar. Die Daten des Patienten können allein oder in Verbindung mit weiteren Daten verwendet werden. Die Patienteninformationen werden in Datenbanken auf dem virtuellen Computer in der privaten Cloud gespeichert.

Für das Informationsmanagement umfasst die private Cloud-Architektur Rechen-, Speicher- und Netzwerkdienste. Bei der Übermittlung von Gesundheitsdaten an die Cloud werden die Verschlüsselungs- und Hash-Operationen gemäß dem Sicherheitsrahmen der privaten Cloud durchgeführt. Die eigentlichen Gesundheitsdaten werden in einer Datenbank aufbewahrt, während der für die Verschlüsselung erforderliche Schlüssel in einer anderen Datenbank gespeichert wird. Dadurch wird der Zugriff eines Angreifers auf kritische Patienteninformationen, die in der Cloud-Datenbank für elektronische Patientenakten gespeichert sind, eingeschränkt. Der vorgeschlagene Rahmen schützt die sensiblen Daten der Patienten, indem er die Vertraulichkeit und Integrität der Informationen gewährleistet. Infolgedessen können Nutzer des Gesundheitswesens Daten entschlüsseln und von jedem Ort und zu jeder Zeit auf wichtige Informationen zugreifen.

Leistungsanalyse

Die Leistungsbewertungskriterien des vorgeschlagenen Modells für die sichere Speicherung verschlüsselter medizinischer Informationen in einem FC-Framework, das Blockchain und einen funktionalen, voreingenommenen ECC-Algorithmus verwendet, werden beschrieben. Die Schlüsselerzeugungszeit (KGT), die Verschlüsselungszeit (ET), die Entschlüsselungszeit (DT) und das Sicherheitsniveau werden verwendet, um den geschützten Speicherbereich dieses vorgeschlagenen Algorithmus-Systems zu bewerten. Die entsprechenden Formeln zur Schätzung der verschiedenen Zeiten sind in den Gleichungen (4), (5) und (6) angegeben.

Verschlüsselungszeit

Die Verschlüsselungszeit wird als die für die Verschlüsselung der Informationen benötigte Zeit in Millisekunden beschrieben. Sie wird wie folgt berechnet:

Verschlüsselungszeit= Endzeit - Startzeit

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

Dabei steht ITT für die Information Transferring Time (Informationsübertragungszeit), während ET für die Encryption Time (Verschlüsselungszeit) steht. Die hier berechnete ET ist die Zeit, die die Information brauchte, um die ursprüngliche Information zu verschlüsseln und in eine verschlüsselte Information umzuwandeln. Dabei bezeichnet ENDT die Endzeit und STARTT die Startdauer des Verschlüsselungsverfahrens.

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

Abbildung 3 zeigt die Verschlüsselungszeit der vorgeschlagenen Technik unter Verwendung der funktional voreingenommenen ECC-Methode. Die Forscher fanden heraus, dass sich die Verschlüsselungszeit mit zunehmender Anzahl der Bits im Schlüssel verbessert. Die von uns vorgeschlagene Architektur benötigt dagegen viel weniger Zeit für die Verschlüsselung als herkömmliche Verfahren wie Advanced Encryption Standard (AES), Data Encryption Standard (DES) und Rivest-Shamir-Adleman (RSA).

Entschlüsselungszeit

Die Zeit, die zum Entschlüsseln der verschlüsselten Informationen erforderlich ist, wird als Entschlüsselungszeit bezeichnet und wie folgt berechnet:

Entschlüsselungszeit= Endzeit - Startzeit

Hier wird die DT (Entschlüsselungszeit) als die Dauer in Millisekunden berechnet, die die verwendeten Informationen zur Entschlüsselung der verschlüsselten Informationen benötigen, und sie wird mit Gleichung (6) berechnet.

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

Abbildung 4 zeigt die Entschlüsselungszeiten des vorgeschlagenen Rahmens im Vergleich zu herkömmlichen Methoden Die Entschlüsselungsdauer steigt mit zunehmender Schlüsselgröße aufgrund der Einführung störender Informationen auf dem Cloud-Server und verschiedener

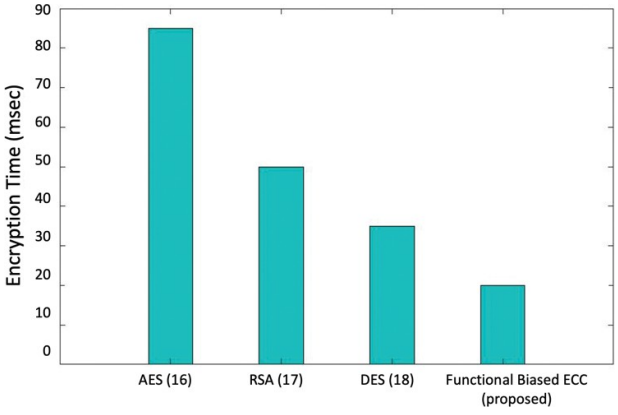

Abb. 3. Analyse der Schlüsselgenerierungszeit. AES: Advanced Encryp-tion Standard, DES: Data Encryption Standard, ECC: Ellip-tische Kurvenkryptographie, RSA: Rivest-Shamir-Adleman.

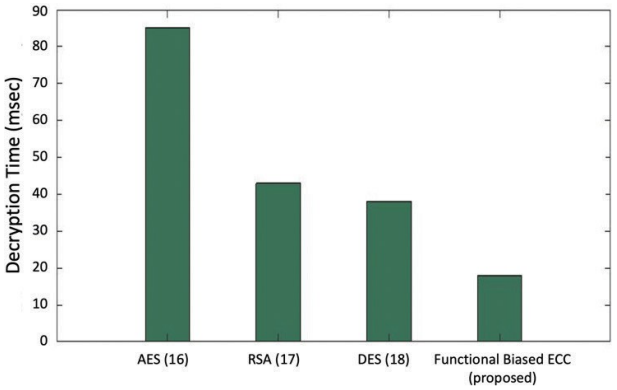

Abb. 4. Analyse der Entschlüsselungszeit. AES: Advanced Encryption Standard, DES: Data Encryption Standard, ECC: Ellip-tische Kurvenkryptographie, RSA: Rivest-Shamir-Adleman.

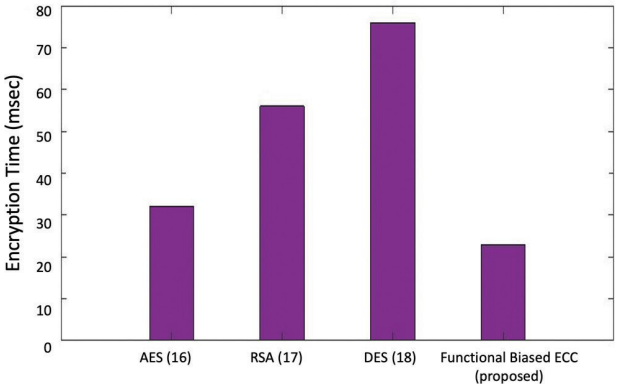

Abb. 5. Analyse der Schlüsselerzeugungszeit. AES: Advanced Encryption Standard, DES: Data Encryption Standard, ECC: Elliptische Kurven Kryptographie, RSA: Rivest-Shamir-Adleman.

Schlüsselwörter. Im Vergleich zu traditionellen Ansätzen wie AES, DES und RSA hat sich gezeigt, dass die von uns vorgeschlagene Methode auch bei größeren Schlüsseln weniger Zeit zur Entschlüsselung benötigt.

Schlüsselgenerierungszeit

Aus Abbildung 5 geht hervor, dass der vorgeschlagene Algorithmus zur Verschlüsselung mit elliptischen Kurven im Vergleich zu herkömmlichen Verfahren wie AES, DES und RSA weniger Zeit in Anspruch nimmt.

Sicherheitsniveau

Abbildung 6 vergleicht die vorgeschlagene funktional verzerrte ECC mit konventionellen sicheren Speicheralgorithmen wie DES, RSA und AES in Bezug auf das Sicherheitsniveau. Im Vergleich zu herkömmlichen Methoden bieten die vorgestellten Alternativen ein höheres Maß an Sicherheit.

Die Abbildungen 3 bis 6 veranschaulichen den Vergleich zwischen verschiedenen Algorithmen wie AES, RSA, DES und der vorgeschlagenen Methode FB ECC in Bezug auf verschiedene Parameter wie z. B. :

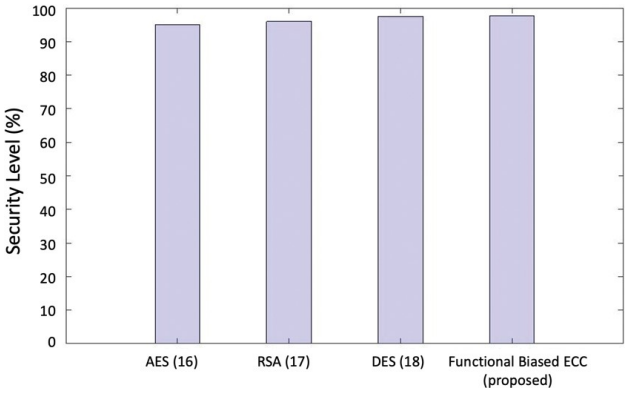

Abb. 6. Analyse der Sicherheitsstufen. AES: Advanced Encryption Standard, DES: Data Encryption Standard, ECC: Elliptische Kurvenkryptographie, RSA: Rivest-Shamir-Adleman.

i) Verschlüsselungszeit
ii) Entschlüsselungszeit
iii) Schlüsselgenerierungszeit
iv) Sicherheitsniveau

Die Gesamtanalyse der Algorithmen zeigt, dass sie bei allen vier besprochenen Parametern viel bessere Ergebnisse als herkömmliche Algorithmen liefern.

Schlussfolgerung

Für die sichere Speicherung medizinischer Patientendaten in nebelfähigen Cloud-Datenbanken wird ein Modell zur sicheren Speicherung medizinischer Informationen entwickelt und in dieses System integriert. Medizinische Informationen werden von zahlreichen Patienten gesammelt, die die E-Healthcare-Gadgets in diesem System unterstützen.

Die FB-ECC-Technik wird verwendet, um einen privaten Server einzurichten, der für die Kommunikation Ent- und Verschlüsselung benötigt. Die funktionale FB-ECC-Methode wird in dieser Forschung verwendet, um die Verschlüsselungs-, Entschlüsselungs- und Schlüsselerzeugungsverfahren auf einer geschützten Speicherarchitektur auszuführen. Im Vergleich zu bestehenden Ansätzen übertreffen die vorgeschlagenen Techniken diese in Bezug auf Sicherheit, Verschlüsselung, Entschlüsselung und KGT. Der vorgeschlagene Verschlüsselungsalgorithmus, FB-ECC, hat ein Sicherheitsniveau von 98,64 %. Es hat sich gezeigt, dass die Kombination von FC mit Blockchain die Sicherheit der Informationsübertragung im Gesundheitswesen verbessert hat. Da nur der funktional verzerrte geheime ECC-Schlüssel die tatsächlichen Informationen zurückgeben kann, können die verborgenen medizinischen Informationen nicht von Unbefugten abgerufen werden.

Zukünftige Studien in diesem Bereich könnten die Entwicklung eines neuen kryptografischen Algorithmus umfassen, der einen verbesserten Verschlüsselungsansatz von FB-ECC mit einem höheren Maß an Sicherheit darstellt.[18]

Finanzierung

Für die Erstellung dieses Artikels wurden keine finanziellen Mittel verwendet.

Citation: Blockchain im Gesundheitswesen heute 2024, **7**: 347 - https://doi.org/10.30953/bhty.v7.347

Interessenkonflikte

Es bestehen keine Interessenkonflikte.

Mitwirkende

Die Autoren sind für die Entwicklung dieses Artikels verantwortlich.

Datenverfügbarkeitserklärung (DAS), gemeinsame Nutzung von Daten, Reproduzierbarkeit und Datenrepositorien

Die Daten sind nicht verfügbar.

Anwendung von KI-generiertem Text oder verwandter Technologie

Es wurde keine KI verwendet.

Referenzen

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. Scanning the issue. 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-basierter Sicherheitsmechanismus für medizinische Daten in der Fog-Computing-Architektur des Internets der Dinge. 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. In: 2020 International Conference on Artificial Intelligence and Signal Processing (AISP). 2020 Jan 10 (pp. 1-6). IEEE [zitiert 2024 Aug 05]. Verfügbar unter: 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. Secure and reliable IoT networks using fog computing with software-defined networking and block-chain. 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. Anwendung von Fog Computing, Internet der Dinge und Blockchain-Technologie in der Gesundheitsbranche. In: 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. Data allocation mechanism for Internet-of-Things systems with 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. Fog computing for Healthcare 4.0 environment: opportunities and challenges. 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. Fog computing in health-care: a review. In 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. Technologien für Fog Computing im Gesundheitswesen 4.0: Herausforderungen und künftige Implikationen. In: 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: eine Fog-Computing-Architektur, die Blockchain und Internet der Dinge für persönliche Gesundheitsdaten integriert. IEEE Access. 2021 Sep 1;9:122723-37. https:// doi.org/10.1109/ACCESS.2021.3109822
16. Munirathinam T, Ganapathy S, Kannan A. Cloud- und IoT-basiertes System zur Wahrung der Privatsphäre in der elektronischen Gesundheitsfürsorge unter Verwendung eines sicheren Speicher-Algorithmus und 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. An IoT based secure patient health monitoring system. Comput Mater Contin. 2022 Jan 1;70(2):3637-52. https://doi.org/10.32604/cmc.2022.020614