UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Revista Científica

http://revistas.udistrital.edu.co/ojs/index.php/revcie/index

Artículo de investigación científica

Indicador de reputación para garantizar la seguridad de la interacción semántica entre objetos inteligentes del IoT mediante DAG y criptografía AES

Reputation Indicator to Ensure Security in Semantic Interaction between IoT Smart Objects Using DAG and AES Cryptography

Indicador de Reputação para Garantir a Segurança na Interação Semântica entre Objetos Inteligentes da IoT usando DAG e Criptografia AES

Carlos-Andrés Díaz-Santacruz[1]
Miguel-Ángel Niño-Zambrano[2]
Daniel-Guillermo Zarate-Guevara[3]
Samuel-Yesid Bulla-Ortega[4]

Recibido: 27 de agosto de 2024 **Aceptado:** 10 de octubre de 2024

Para citar este artículo: Díaz-Santacruz, C. A., Niño-Zambrano, M. A., Zarate-Guevara, D. G. y Bulla-Ortega, S. Y. (2024). Indicador de reputación para garantizar la seguridad de la interacción semántica entre objetos inteligentes del IoT mediante DAG y criptografía AES. *Revista Científica*, *51*(3), 62-86. https://doi.org/10.14483/23448350.22622

Resumen

En entornos de interacción semántica entre objetos inteligentes, la seguridad está ganando relevancia investigativa, pues este tipo de redes puede verse comprometido por nodos maliciosos o por la pérdida de confiabilidad. En los últimos años, las investigaciones han avanzado en el desarrollo de modelos de reputación que permitan a un nodo del Internet de las Cosas (IoT) evaluar la confiabilidad de otros nodos con base en información proporcionada por la propia red. Esta investigación propone un indicador de reputación para objetos inteligentes en el IoT, fundamentado en dos tecnologías prometedoras, i.e., el uso de grafos acíclicos dirigidos (DAG) y la criptografía Advanced Encryption Standard (AES). Estas tecnologías se integran con el objetivo de incrementar la seguridad de la información compartida sin comprometer la escalabilidad en entornos de interacción semántica cada vez más complejos. Los resultados de otras investigaciones sugieren que la solución propuesta podría incrementar el nivel de seguridad en la red, pues permite restringir los nodos que no cumplen con el criterio mínimo del indicador de reputación.

Palabras clave: indicador de reputación, DAG, criptografía AES, confiabilidad, IoT

1. Universidad de Ibagué (Ibagué, Colombia). andres.diaz@unibague.edu.co
2. Universidad del Cauca (Popayán, Colombia). manzamb@unicauca.edu.co
3. Universidad de Ibagué (Ibagué, Colombia). 2220162001@unibague.edu.co
4. Universidad de Ibagué (Ibagué, Colombia). 2220191038@unibague.edu.co

Abstract
In environments involving semantic interaction between intelligent objects, security is gaining increasing research relevance, as these types of networks can be compromised by malicious nodes or reliability loss. In recent years, research has advanced in developing reputation models that allow Internet of Things (IoT) nodes to assess the trustworthiness of other nodes based on information provided by the network itself. This study proposes a reputation indicator for intelligent objects in the IoT, based on two promising technologies, i.e., directed acyclic graphs (DAG) and Advanced Encryption Standard (AES) cryptography. These technologies are integrated in order to enhance the security of shared information without compromising scalability in increasingly complex semantic interaction environments. Findings from other studies suggest that the proposed solution could increase network security, as it allows restricting nodes that fail to meet the minimum reputation indicator criterion.
Keywords: reputation indicator, DAG, AES cryptography, reliability, IoT

Resumo
Em ambientes de interação semântica entre objetos inteligentes, a segurança está ganhando relevância investigativa, pois esse tipo de rede pode ser comprometido por nós maliciosos ou pela perda de confiabilidade. Nos últimos anos, as pesquisas avançaram no desenvolvimento de modelos de reputação que permitem a um nó da Internet das Coisas (IoT) avaliar a confiabilidade de outros nós com base em informações fornecidas pela própria rede. Esta pesquisa propõe um indicador de reputação para objetos inteligentes no IoT, fundamentado em duas tecnologias promissoras, ou seja, o uso de grafos acíclicos direcionados (DAG) e a criptografia Advanced Encryption Standard (AES). Essas tecnologias são integradas com o objetivo de aumentar a segurança das informações compartilhadas sem comprometer a escalabilidade em ambientes de interação semântica cada vez mais complexos. Os resultados de outras pesquisas sugerem que a solução proposta pode aumentar o nível de segurança na rede, pois permite restringir os nós que não atendem ao critério mínimo do indicador de reputação.
Palavras-chaves: indicador de reputação, DAG, criptografia AES, confiabilidade, IoT.

INTRODUCCIÓN

El desarrollo del IoT (*Internet of Things*) está ligado al concepto del *Internet del Todo* (IoE, *Internet of Everything*). Jamil *et al.* (2022) definen el IoE como un entorno en el que "se conectan millones de dispositivos físicos heterogéneos, elementos computacionales, objetos, animales y humanos que pueden configurar, compartir y autoorganizar sus recursos limitados para lograr un objetivo a nivel de sistema" (p. 2). En este entorno, las personas y los procesos se relacionan con los servicios de los objetos inteligentes, ya sean de su propiedad o del lugar en el que se encuentran. Esto exige una cooperación entre los distintos nodos y los mecanismos que incrementan la seguridad y la confiabilidad de datos y dispositivos, con el fin de que los servicios se ejecuten con la mayor calidad posible (Gurajena *et al.*, 2020). En otros estudios se ha propuesto el cálculo de la reputación para evaluar la confianza del nodo con el cual se está interactuando.

La *reputación* es la percepción o valoración que tienen las personas o grupos sobre una entidad, ya sea una persona, una empresa, un producto, un servicio o cualquier otro objeto o concepto. Esta valoración se basa en experiencias previas, comportamiento, desempeño y otros factores que influyen en cómo se percibe dicha entidad (Battah *et al.*, 2021).

Dado que los dispositivos inteligentes del IoT están habilitados para establecer comunicación y servicios con otros objetos inteligentes, las vulnerabilidades de seguridad de la información pueden aumentar en los servicios conjuntos. El concepto de *reputación* se ha trasladado al IoT como un elemento clave para establecer la confiabilidad de otros dispositivos y tomar decisiones que permitan establecer si es posible crear servicios conjuntos o implementar ciertos mecanismos de seguridad (Jamil *et al.*, 2022).

En vista de lo anterior, es necesario dotar al ecosistema del IoT de mecanismos de seguridad que protejan y regulen la información frente a entidades maliciosas y egoístas. Entre los mecanismos desarrollados para este fin se encuentra la adaptación de técnicas de seguridad de la información para proteger las redes del IoT. Las tecnologías utilizadas incluyen la criptografía liviana (Alshehri & Bamasag, 2022; Rana *et al.*, 2022); el *blockchain* adaptado para el IoT, conocido como *IOTA* (Alshehri & Bamasag, 2022; Hellani *et al.*, 2021a; Mazzocca *et al.*, 2024); e indicadores clave de rendimiento basados en KPI, que ayudan en la detección de irregularidades en las aplicaciones del IoT (Tariq *et al.*, 2023).

Normalmente, las tecnologías utilizadas para incrementar la confianza y la seguridad de la información tienen un impacto importante en la calidad del servicio, la reputación, los aspectos de seguridad, las relaciones sociales, el consumo de energía y la escalabilidad de la red, dados los tiempos de ejecución de los procesos de cada dispositivo en el IoT que buscan garantizar la seguridad de la red. Desarrollar una calificación de reputación que garantice que una entidad es confiable podría ser una estrategia importante para evitar reprocesos de aseguramiento de la información, evitar sobrecargar la red y garantizar una calidad del servicio adecuada. A esto último se le conoce como la *reputación de una entidad en el IoT* (Bernal Bernabe *et al.*, 2016) .

El enfoque de solución adoptado en este trabajo consiste en reunir las particularidades de la reputación en el entorno humano y llevarlas a una fórmula de características medidas en el entorno de los objetos inteligentes del IoT. Definida la reputación en el entorno humano, cuyos componentes clave son la credibilidad, la confiabilidad, la calidad, la responsabilidad, la imagen, la ética y los valores, es posible establecer un símil para el entorno del IoT. Los componentes correspondientes serían la confianza, la confiabilidad, la calidad del servicio, la seguridad, el desempeño, la percepción del usuario y la privacidad.

En las próximas secciones se describen los diferentes enfoques reportados en la literatura, y luego se presenta la propuesta que este trabajo ha adoptado para generar un modelo de reputación en un entorno de objetos inteligentes del IoT.

TRABAJOS RELACIONADOS

En la literatura se discuten varios enfoques para medir y gestionar la reputación en los sistemas de IoT. Por ejemplo, Gurajena *et al.* (2020) proponen un modelo de reputación basado en lógica difusa para identificar entidades maliciosas en entornos de IoT. Azad *et al.* (2018) presentan M2M-REP, un sistema de reputación que preserva la privacidad para redes descentralizadas del IoT, el cual agrega retroalimentación local encriptada para calcular puntuaciones de reputación globales. Patel y Jinwala (2022) introducen un protocolo RPL basado en reputación para detectar ataques de reenvío selectivo, evaluando el comportamiento de los nodos e incorporando la reputación en la selección de pares. Bordel *et al.* (2018) describen un modelo de reputación híbrido que combina observaciones implícitas y recomendaciones explícitas para identificar componentes maliciosos en sistemas complejos de IoT.

Los trabajos más relacionados con esta investigación tienen que ver con *blockchain* y criptografía. A partir del 2018 se evidencia un aumento en el procesamiento y la cantidad de datos en el IoT, así como en la necesidad de compartir servicios entre distintos objetos heterogéneos, lo cual supone graves

problemas de confianza y seguridad en este tipo de redes. Cabe anotar que los trabajos de Cai *et al.* (2024), Yang *et al.* (2024), Xu *et al.* (2018) y Zhou *et al.* (2024) desarrollan indicadores de reputación para la arquitectura del IoT mediante técnicas de *blockchain* y criptografía. Todos estos estudios emplean tecnología *blockchain* en entornos simulados como Ethereum, que permite la ejecución descentralizada de este tipo de programas (Liang *et al.*, 2019). Sin embargo, IOTA incorpora el *directed acyclic graph* (DAG), también conocido como *grafo acíclico dirigido* o *Tangle*, una estructura de datos que reemplaza la cadena de bloques tradicional, operando sin bloques ni mineros (Hellani *et al.*, 2021a). El DAG implementa diversas técnicas clave para garantizar la seguridad, la eficiencia y la escalabilidad de sistemas de IoT, especialmente en aplicaciones de objetos inteligentes y procesamiento semántico. Estas técnicas incluyen la confirmación de transacciones mediante aprobaciones múltiples (Son *et al.*, 2020), el algoritmo de selección de puntas con cadena de Markov (*Markov chain Monte Carlo*, MCMC) (Hellani *et al.*, 2021b), el uso del peso acumulativo para medir la relevancia de las transacciones (Hellani *et al.*, 2021a), pruebas de trabajo ligeras (*proof of work*, PoW) (Son *et al.*, 2020) y la distribución de tareas y equilibrio de carga entre nodos (Hellani *et al.*, 2021a). En este estudio se retoman diversas contribuciones de estos estudios, aunque se optó por desarrollar un indicador propio basado ellas, dada la arquitectura semántica que sustenta este trabajo (Guerrero-Narváez *et al.*, 2018).

Los estudios mencionados destacan la importancia de los sistemas de reputación para mejorar la seguridad del IoT, pues permiten evaluar la confianza, detectar entidades maliciosas y apoyar procesos de toma de decisiones. Los enfoques propuestos tienen como objetivo abordar desafíos como la preservación de la privacidad, las limitaciones de recursos y la naturaleza dinámica de los entornos del IoT, a la vez que mejoran la confiabilidad y seguridad general del sistema.

Concepto de *reputación*

Según Gurajena *et al.* (2020), la confianza y la reputación están relacionadas, pero son conceptos distintos. La *confianza* se refiere a la expectativa de un comportamiento positivo futuro por parte de una entidad, mientras que la *reputación* es una evaluación de su comportamiento pasado. Si una entidad ha interactuado de manera negativa, *i.e.*, ha presentado un comportamiento malicioso o ha brindado servicios de baja calidad a otras entidades, su reputación se verá afectada negativamente. En cambio, una reputación positiva es el resultado de interacciones pasadas satisfactorias. A medida que se detectan brechas de seguridad en una entidad, su reputación disminuye, lo cual afecta su capacidad para interactuar efectivamente con otras entidades en la red. Este aspecto se puede evaluar a partir de los informes de interacción de las entidades.

Se han planteado modelos de reputación con lógica difusa en los sistemas red de pares (*peer-to-peer*, P2P) (Kamvar *et al.*, 2003; Song *et al.*, 2005; Wang & Vassileva, 2003), dado que son redes anónimas y, por sus características, se parecen a las redes del IoT, en las que los participantes no se conocen inicialmente, pero utilizan mediciones relacionadas con la confianza global y las interacciones de los nodos.

En Kamvar *et al.* (2003) se establecen los elementos de diseño fundamentales para crear un indicador de reputación (esta investigación toma algunos y modifica otros):

1. El indicador debe basarse en un sistema autogestionado, *i.e.*, no hay una autoridad, sino que la reputación se calcula por la interacción entre pares.
2. No se asigna ningún beneficio a los nuevos nodos; estos inician desde cero, y se computa el indicador a partir de sus interacciones con otros.

3. El costo de cómputo debe ser mínimo en términos de infraestructura, almacenamiento y complejidad de los mensajes.
4. El indicador debe ser robusto frente a colectivos de pares maliciosos que se conocen entre sí.

Wang y Vassileva (2003) proponen las siguientes definiciones:

> Confianza: creencia de un par en las capacidades, honestidad y fiabilidad de otro par con base en sus propias experiencias directas; reputación: creencia de un compañero en las capacidades, honestidad y fiabilidad de otro, con base en las recomendaciones recibidas de otros compañeros. La reputación puede estar centralizada, calculada por un tercero de confianza como Better Business Bureau, o descentralizada, calculada de forma independiente por cada usuario tras pedir recomendaciones a otros usuarios. (p. 1)

Estos autores también presentan las principales características de la medición de la reputación, *i.e.*, contexto específico, polifacético y dinámica, dando a entender que la reputación puede adquirir complejidad adicional dependiendo de los contextos y servicios provistos por las entidades del IoT.

Los trabajos que utilizan técnicas de *blockchain* (Cai *et al.*, 2024; Yang *et al.*, 2024; Xu *et al.*, 2018; Zhou *et al.*, 2024) cuentan con un indicador de reputación y, en otros casos, con los datos del mismo. Partiendo de los propios datos y de metadatos, algunos trabajos utilizan la criptografía (Li *et al.*, 2024) para evitar el acceso no autorizado o para ocultar la información de los nodos que ofrecen servicios en una red pública. En este trabajo también se implementa *blockchain*, pero una variante más ligera (DAG), así como la técnica de criptografía simétrica Advanced Encryption Standard (AES). Estas dos técnicas se integran a las capas de una arquitectura de interacción semántica de objetos inteligentes (Guerrero-Narváez *et al.*, 2018), mediante un indicador modelado a partir del concepto *reputación* que se maneja en los entornos sociales humanos (Jøsang *et al.*, 2007; Resnick, 2001).

Indicadores de reputación propuestos en otros estudios

Gurajena *et al.* (2020) presentan una red jerárquica y descentralizada de agentes de reputación basada en lógica difusa, a fin de solventar las dificultades que emergen cuando no todos los objetos pueden almacenar información de reputación. En este trabajo se toman objetos inteligentes del IoT que tienen la capacidad de almacenar dicha información.

El resumen de las investigaciones sobre el cálculo de la reputación se presenta a continuación (Tabla 1), con la siguiente nomenclatura:

CR = Cálculo de la reputación
CRL = Cálculo de la reputación local
CRG = Cálculo de la reputación global
MER = Método de evaluación de la reputación
RM = Reputación multidimensional (múltiples propiedades)
AR = Agente raíz
ARep = Agente de reputación
UO = Usuario origen
UD = Usuario destino

Entity = Entidad
EO = Entidad origen
ED = Entidad destino
FIS = Sistema de inferencia difusa
PE = Peso de la entidad
PP = Peso de la propiedad a evaluar
CD = Conjuntos difusos
RD = Reglas difusas
VL = Variables lingüísticas QoS
SS = Sistema Sugeno (*singleton*)
LD = Lógica difusa
CoG = Centro de gravedad
NB = *Naive Bayes* (Bayes ingenuo)
TE = Transacción exitosa
TNE = Transacción no exitosa
K-NN = *K-Nearest Neighbors*
CBR = Razonamiento basado en casos
IB = Inferencia Bayesiana
SO = Autoobservación
PDR = Índice de entrega de paquetes
CRI = Cálculo de la reputación implícita o conocimiento directo
CRE = Cálculo de la reputación explícita o conocimiento indirecto
OD = Observaciones directas
OI = Observaciones indirectas
AP = Algoritmos de procesamiento
TI = Taxonomías de incertidumbre
MI = Modelos de incertidumbre
RECE = Recomendaciones explícitas
ID = Información difusa
PBR = Parámetros básicos de la red
EMA = Expresiones matemáticas algebraicas
ADR = Algoritmo de recomendación
TB = Cubo de fichas (*token bucket*)
TP = Fichas positivas (*positive tokens*)
TN = Fichas negativas (*negative tokens*)
TRP = Tasa de recomendaciones positivas
TRN = Tasa de recomendaciones negativas
RPNV = Recomendación positiva no validada
RNNV = Recomendación negativa no validada
TO = Tiempo de convergencia o de operación (*time slots*)
ACN = Algoritmo de cálculo de nobleza

Tabla 1. *Resultados de investigaciones sobre el cálculo de la reputación de un nodo IoT en la red*

Investigación	Conceptos de cálculo			Interacción		Fórmula de reputación	Algoritmos utilizados	Dimensiones medidas
	CR	MER	Entity	UO	UD			
(Gurajena *et al.*, 2020)	CRL, CRG	RM	E	AR	ARep	PE, **PP**, CD, RD, VL	FIS, LD, SS, CoG	competencia, credibilidad o disponibilidad, calidad de servicio (variables lingüísticas), fiabilidad, motivo, reciprocidad, incentivo, defecto, relevancia, valor de confianza
(Wang & Vassileva, 2003)	CRL, CRG	RM	E	Par 1 de nodos iniciales de red Bayesiana	Par 2 de nodos finales de red Bayesiana	PE	NB	velocidad de descarga, calidad del archivo, tipo de archivo
(Chen *et al.*, 2011)	CRL, CRG	RM	E	Nodo inicial	Nodo final	PE	LD	Calidad de Servicio
(Javanmardi *et al.*, 2015)	CRL, CRG	RM	E	Usuario origen	Usuario destino	PE	LD	calidad de servicio
(Bernal Bernabe *et al.*, 2016)	CRL, CRG	RM	E	Usuario origen	Usuario destino	PE	LD	calidad de servicio
(Mhetre *et al.*, 2016)	CRL, CRG	RM	E	Usuario origen	Usuario destino	PE	LD	calidad de servicio
(Bica *et al.*, 2020)	CRL, CRG	RM	TE, TNE	Nodo IoT inicial	Nodo IoT final	PE	K-NN, NB, CBR, LD IB, SO	temperatura, presión de aire, humedad, ruido, nivel de CO_2, relación de entrega de paquetes (PDR), fiabilidad
(Bordel *et al.*, 2018)	CRL,CRG	RM	E	Módulo, nodo o componente IoT	Módulo, nodo o componente IoT	PE, RI, RE, TB; TP, TN, TRP, TRN, RV, RNV, RPNV, RNNV, RECE, TO	OD, OI, TI, AP, MI, CRE, CRI, RI, ID, PBR, EMA, ADR, A	nobleza + solidaridad + relevancia, fiabilidad de la información, calidad de servicio, nivel de confianza, tasa de pérdida de paquetes, velocidad de convergencia, velocidad de creación de mensajes, inserción no autorizada de dispositivos, integridad de los datos, ataque de repetición, recogida de datos no autorizada, seguridad hacia adelante y hacia atrás

En síntesis, todas las investigaciones preliminares de este estudio emplearon el cálculo de la reputación local y global. *Reputación local* se refiere a mantener la percepción con la que cuenta un nodo IoT en el marco de una red de confianza, y la *reputación global* corresponde a la puntuación derivada de las opiniones, las transacciones, las experiencias pasadas y los comportamientos que ha tenido un nodo IoT en interacción con otros dentro de una red. Además, la fórmula de la reputación considera conceptos, dimensiones y algoritmos a la hora de calcular el aumento o la disminución de la calificación correspondiente.

Los últimos estudios presentados, que utilizan *blockchain* y algoritmos de criptografía, son la base de la Tabla 2, en la cual se presenta la fórmula de reputación y los algoritmos y dimensiones que se usaron para el cálculo, con la siguiente nomenclatura:

CR = Cálculo de la reputación
CRL = Cálculo de la reputación local
CRG = Cálculo de la reputación global
MER = Método de evaluación de la reputación
RM = Reputación multidimensional (múltiples propiedades)
UO = Usuario origen
UD = Usuario destino
Entity = Entidad
TE = Transacción exitosa
TNE = Transacción no exitosa
DRL = Algoritmo basado en diseño
FedAvg = Algoritmo FedAvg
PPÖ = Algoritmo de reparto de incentivos en línea
OOA = Algoritmo de subasta óptima *offline*
OGA = Algoritmo de subasta codiciosa en línea
RS = Selección aleatoria
ABE = Cifrado basado en atributos o encriptación para búsquedas
CA = Algoritmos de consenso
HE = Encriptación homomórfica
PPRM = Preservación de la privacidad en el proceso de intercambio de datos
PKC = Criptografía de clave pública
HOPE = Cifrado homomórfico y preservación del orden
AEDM = Mecanismo autónomo de cifrado y descifrado
SSA = Algoritmo para compartir secretos
DPHE = Privacidad diferencial y cifrado homomórfico
THE = Cifrado umbral homomórfico
EC = Algoritmo de cifrado EC-ElGamal
AC = Autoridad de certificación
BM = Miembros de *blockchain*
DMSC = Gestión de datos, contrato inteligente
RMSC = Gestión de la reputación, contrato inteligente

Tabla 2. *Resultados de investigaciones sobre el cálculo de la reputación*

Investigación	Conceptos de cálculo			Interacción		Fórmula de reputación	Algoritmos utilizados	Dimensiones medidas
	CR	MER	Entity	UO	UD			
(Cai *et al.*, 2024)	CRL,CRG	RM	TE, TNE	Usuarios del IoT	Usuarios del IoT	PPO	DRL, FedAvg, OOA, OGA, RS	Calidad de los datos enviados Sistema de incentivos de intercambio de modelos en línea que combina *blockchain* y aprendizaje federado.
(Yang *et al.*, 2024)	CRL,CRG	RM	CA, BM	Propietario de los datos (DO)	Usuario de Datos (DU)	PPRM	ABE, CA, HE, PKC HOPE AEDM, SSA, DPHE, THE, EC, DMSC,	Control de acceso detallado Confidencialidad Anonimato *Desvinculabilidad* *Infalsificabilidad* Eficiencia Escalabilidad

Estos estudios también calculan la reputación local y global, y definen su fórmula a partir de conceptos, dimensiones y algoritmos basados en *blockchain*, IOTA, criptografía simétrica y asimétrica y aprendizaje federado.

En la investigación realizada por Cai *et al.* (2024), el algoritmo calcula la reputación de los usuarios IoT, no la de los nodos. Sin embargo, los algoritmos propuestos podrían adaptarse a estos últimos, como se busca en este estudio. Yang *et al.* (2024) utilizan la plataforma de Ethereum, que emplea IOTA para crear el Tangle de las transacciones, para desplegar la red IoT. Adicionalmente, estos autores desarrollaron un sistema de almacenamiento de datos fuera de los bloques y un índice que se almacena en los bloques del *blockchain*, superando el problema de almacenamiento de los datos a compartir. Sin embargo, la reputación también se calcula sobre los usuarios propietarios de nodos, no sobre estos últimos.

A diferencia de las investigaciones anteriores, nuestro trabajo desarrolla un indicador de reputación para los nodos inteligentes del IoT que pueden tener o no un propietario visible. Además, desarrollamos nuestro propio Tangle con DAG, a fin de tener más control sobre las interacciones. Al igual que en trabajos anteriores, la criptografía permite asegurar los datos de las cadenas de bloques, pero bajo este enfoque también se aseguran los metadatos de los objetos inteligentes y sus contratos, representados como eventos, condiciones y acciones (ECA).

A partir el análisis comparativo de los estudios previos, la Figura 1 presenta una clasificación general de los conceptos y características que soportan el cálculo de la reputación de un nodo IoT.

En el primer nivel se identificaron las principales características empleadas para crear los indicadores de reputación, *i.e.*, cálculo de la reputación, método de evaluación, aumento y disminución del valor de reputación, datos analizados, interacción entre los nodos IoT, cálculos para la fórmula de reputación, algoritmos utilizados y dimensiones medidas. En cada característica se colocaron los elementos de los diferentes enfoques analizados. Estos elementos se tuvieron en cuenta a momento de elaborar la presente propuesta.

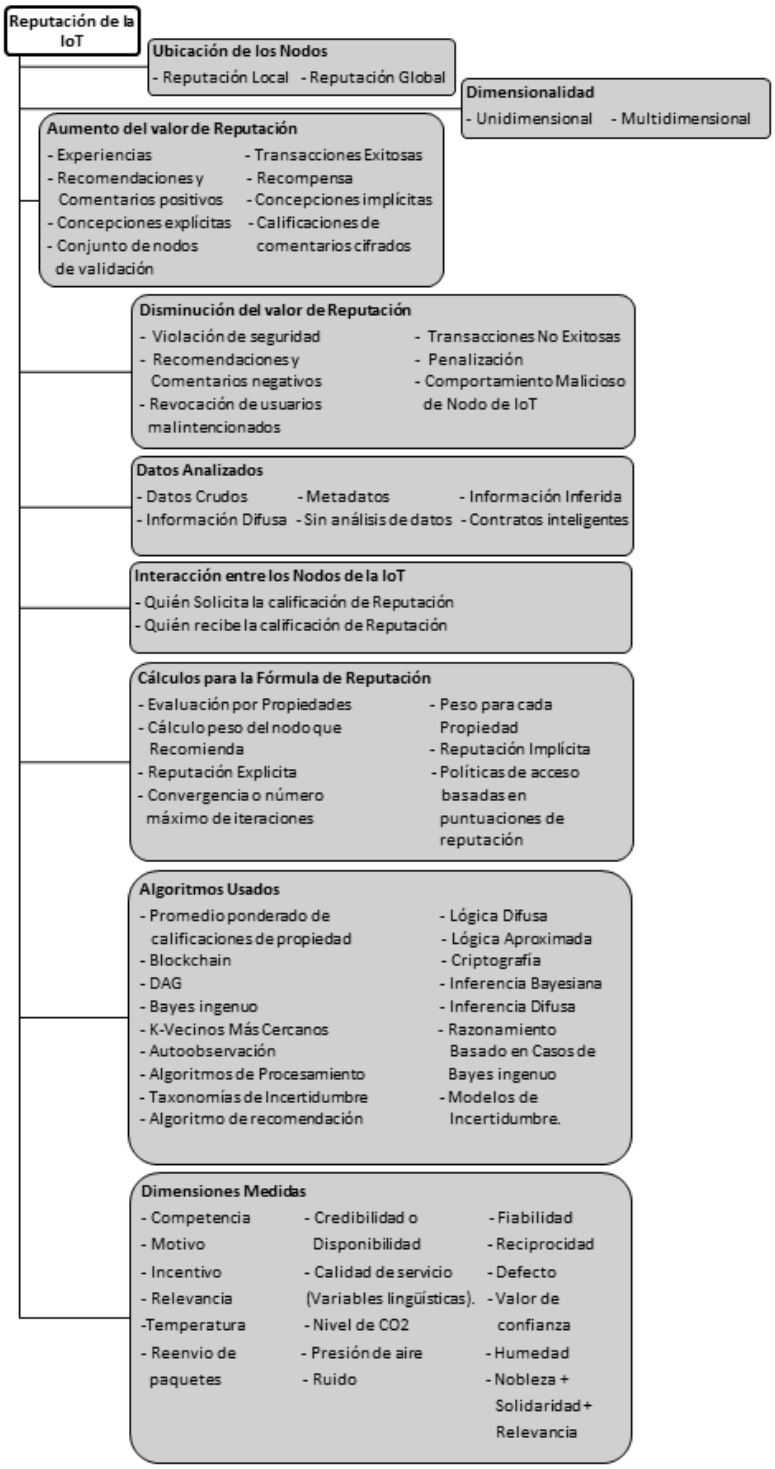

Figura 1. *Características para el cálculo de la reputación*

METODOLOGÍA

Esta investigación se basó en definir mecanismos de seguridad que permitan establecer una conexión segura entre dispositivos inteligentes en un entorno IoT, a la vez que se genera mayor confianza. De allí surge la necesidad de evaluar las conexiones mediante un indicador de reputación, en aras de saber si las decisiones que se toman durante los contratos inteligentes garantizan que se envíe o reciba información confiable de acuerdo con las reglas lógicas establecidas, sin que dicha información sea alterada durante el proceso. La metodología se basó en tres fases (Figura 2): una relacionada con la creación del modelo, la segunda con la creación del indicador de reputación y la última con la creación de la prueba de concepto.

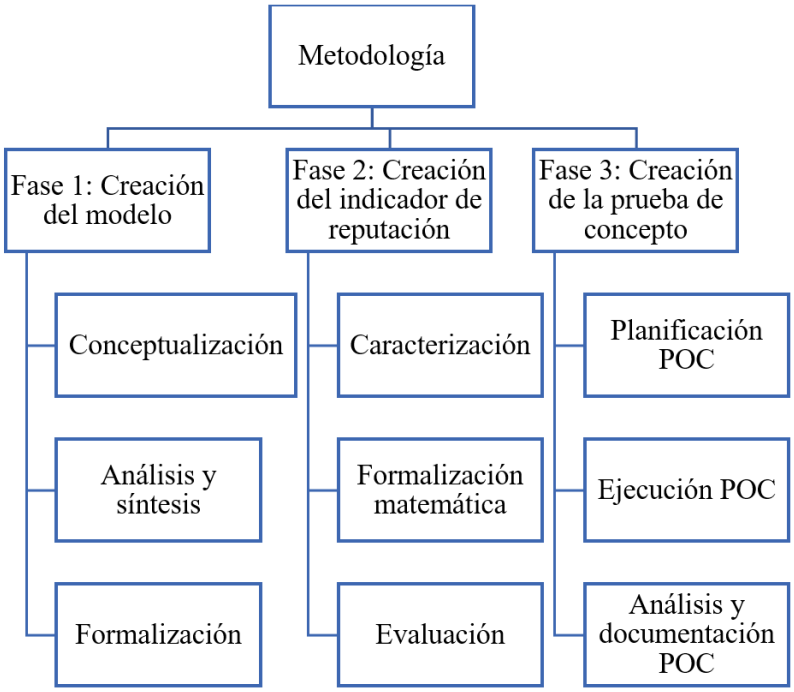

Figura 2. *Metodología usada en la investigación*

Fase 1

1. **Conceptualización del modelo**. Se utilizó un mapeo sistemático (Xu *et al.*, 2018) para ampliar el conocimiento sobre la tecnología IOTA, sus aplicaciones y los algoritmos de criptografía que se han implementado en dispositivos del IoT.
2. **Análisis y síntesis del modelo**. En esta fase se revisó la información obtenida durante la revisión bibliográfica y se procedió a extraer los conceptos clave, las relaciones entre ellos y los elementos a tener en cuenta para implementar el modelo de reputación.
3. **Formalización del modelo**. En esta fase se utilizaron diagramas de ingeniería, que permitieron describir y compartir el modelo de reputación creado.

Fase 2

1. **Formalización matemática**. Se propuso una fórmula matemática que permitió calcular la reputación de un objeto inteligente en el IoT a partir de las características y dimensiones definidas en el modelo.
2. **Formalización del indicador de reputación**. Se incluyó el cálculo del indicador de reputación en la arquitectura y el entorno de objetos inteligentes del IoT definido en los trabajos previos a esta propuesta.
3. **Evaluación de la prueba de concepto**. Este indicador se evaluó en una prueba de concepto para evidenciar su utilidad, la cual se llevó a cabo en un escenario simulado y en un entorno real desplegado.

Fase 3

Se siguió la metodología de prueba de concepto (POC) propuesta por Gubbi *et al*. (2013), que consiste en las siguientes fases:

1. **Planificación de la POC.** Se establecieron las características de los objetos a ser desplegados y los elementos a controlar en el experimento para medir la reputación.
2. **Ejecución de la POC.** Se ejecutó el escenario y se midió el indicador de reputación. Se recogieron resultados y datos en tiempo real para su posterior análisis.
3. **Análisis y documentación de la POC**. Se revisaron los datos obtenidos de la POC y se aplicaron técnicas estadísticas y analíticas para evaluar la idoneidad del indicador propuesto.

Con el fin de garantizar la reputación y la seguridad de los dispositivos inteligentes del IoT, en la arquitectura de modelo de interacción semántica (Guerrero-Narváez *et al*., 2018) se implementó una capa adicional de seguridad basada en la tecnología de registro distribuido de transacciones IOTA, cuyo funcionamiento se basa en el DAG, con una arquitectura denominada *Tangle* y la criptografía del algoritmo simétrico AES, la cual se utiliza para generar reglas automáticas en la interacción de los dispositivos del IoT mediante claves criptográficas y contratos inteligentes, que implican una menor carga de trabajo computacional al momento de desplegar transacciones y son acordes con los dispositivos del IoT.

RESULTADOS

Indicador de reputación propuesto

El objetivo de esta investigación fue desarrollar un indicador de reputación y confianza que identifique y seleccione las características asociadas a la reputación propia de los entornos humanos o empresariales (para este caso) y que defina su equivalente en el contexto de la interacción semántica entre objetos inteligentes en el IoT. Dichas características se pueden apreciar en la Tabla 3.

Tabla 3. *Características humanas aplicadas a entornos del IoT*

Característica humana	Definición	Característica IoT	Definición
Credibilidad	La confianza que las personas depositan en la entidad	Confianza	Seguridad y credibilidad en la interacción y comunicación de los dispositivos del IoT.
Confiabilidad	Consistencia y previsibilidad en el comportamiento y desempeño de la entidad	Confiabilidad	Consistencia y dependencia de los dispositivos del IoT para funcionar correctamente bajo condiciones establecidas.
Calidad	El nivel de excelencia percibido respecto a los productos o servicios ofrecidos.	Calidad del servicio	Medición del rendimiento y la eficiencia de los dispositivos del IoT en la prestación de servicios.
Responsabilidad	La percepción de cómo la entidad cumple con sus obligaciones y compromisos	Seguridad y desempeño	*Seguridad:* protección de los datos y las comunicaciones contra accesos no autorizados y amenazas cibernéticas. *Desempeño:* eficiencia y efectividad de los dispositivos del IoT en el cumplimiento de sus funciones.
Imagen	La percepción visual y conceptual que se tiene de la entidad, influenciada por el *branding* y el *marketing*	La percepción del usuario y de otros objetos del IoT	*Percepción del usuario:* evaluación subjetiva de los usuarios sobre la utilidad y la experiencia de uso de los dispositivos del IoT. *Percepción de otros objetos:* Evaluación objetiva de los otros objetos del IoT sobre la utilidad y la experiencia de uso de los dispositivos.
Ética y valores	La alineación de la entidad con principios éticos y valores reconocidos por la sociedad	Privacidad	Salvaguarda de la información personal y sensible en el entorno del IoT.

En vista de lo anterior, y según se muestra en la Tabla 4, es posible desarrollar o aplicar técnicas existentes para soportar y evaluar las características del IoT a través de indicadores.

Tabla 4. *Técnicas existentes para soportar y evaluar las características del IoT*

Característica	Técnicas usadas	Indicador
Confianza	• Modelo de reputación • Algoritmos de Bayes ingenuo • Redes de confianza • Sistemas de inferencia difusa • Calidad del servicio • Observaciones implícitas o explícitas • *Blockchain*	• Reputación • Confianza • Contexto
Confiabilidad	• Modelos probabilísticos de confiabilidad	• Tasa de fallos • Capacidad de recuperación • Restricciones de *hardware* y *software* • Condiciones tolerables de funcionamiento • Datos sucios de los sensores
Calidad del servicio	• Cálculo de calidad del servicio	• Latencia • Tasa de error • Disponibilidad de información
Seguridad	• Criptografía • Autenticación • Firma digital	• Integridad • Disponibilidad • Confiabilidad

Característica	Técnicas usadas	Indicador
Desempeño	• Indicadores cualitativos y cuantitativos	• Eficiencia • Eficacia • Calidad
Percepción del usuario	• Calificación de reputación	• Reputación de usuario
Percepción de objetos del IoT	• Círculo de confianza. • Calificación de la reputación	• Transacciones exitosas • Transacciones no exitosas
Privacidad	• Autorización • Identidad oculta • Control de acceso • Confianza • Prevención (perfil, ciclo de vida, uso indebido de datos, recolección de datos, localización)	• Número de accesos no autorizados

Cálculo del indicador de reputación

El indicador de reputación propuesto se fundamenta exclusivamente en los aspectos de confianza, seguridad y calidad del servicio (QoS), considerados pilares esenciales para la evaluación de la reputación en entornos como las redes IoT, los sistemas distribuidos y los servicios en línea. La *confianza* se define como el nivel de fiabilidad de un nodo, usuario o entidad, determinado a partir de interacciones previas y comportamientos históricos. Entre las métricas más comunes para medir la confianza están la tasa de transacciones exitosas *vs.* fallidas, las opiniones y recomendaciones de terceros (reputación global) y el nivel de consistencia en el cumplimiento de las expectativas. En el contexto del IoT, esto puede abarcar la precisión de los datos transmitidos y el cumplimiento de los contratos inteligentes. Por su parte, la *seguridad* evalúa la capacidad de un nodo o entidad para proteger la información y garantizar la integridad de las interacciones. Las métricas relevantes en este ámbito incluyen la tasa de incidentes de seguridad (*e.g.*, inserciones no autorizadas), el grado de cumplimiento de los protocolos de criptografía y la protección frente a ataques comunes, como los de repetición o de intermediario. En las redes IoT se analiza el nivel de cifrado implementado y la capacidad del sistema para resistir vulneraciones. Finalmente, la *QoS* mide la eficiencia y la efectividad con las que se presta un servicio. Las métricas típicamente empleadas para evaluar la QoS incluyen la velocidad de respuesta (o tiempo de operación), la tasa de entrega de paquetes (PDR), la estabilidad y disponibilidad del servicio, y variables lingüísticas asociadas a la satisfacción del usuario como el tiempo de espera o la latencia. En el ámbito IoT, estas métricas suelen estar orientadas a medir el éxito del envío y la recepción de datos entre nodos (Yan *et al.*, 2014).

A partir de las propuestas realizadas por los otros autores, se utilizó el teorema *naive Bayes*. Según se muestra en la Ecuación (1), este teorema supone la independencia ingenua, *i.e.*, que la presencia (o ausencia) de una característica particular no guarde relación con la presencia (o ausencia) de otra.

$$P(A|B) = P(B\backslash A).P(A) \,/\, P(B) \quad (1)$$

donde:

- P(A|B) es la probabilidad de A dado B
- P(B|A) es la probabilidad de B dado A
- P(A) es la probabilidad de A
- P(B) es la probabilidad de B

Decidimos basar la reputación en el concepto de *credibilidad del nodo*, *i.e.*, en la **confianza del nodo** (Tabla 3). A partir de los datos de la Tabla 4, definimos una relación tridimensional de la confiabilidad para cada nodo, con base en las calificaciones de otros nodos en función de la confianza, la seguridad y la calidad del servicio. Así garantizamos que se pudieran tomar los elementos principales de la reputación y combinarlos en el indicador propuesto.

Para calcular la probabilidad de que un nodo sea confiable o no confiable, el teorema de Bayes exige una tabla de entrenamiento de calificaciones de transacciones pasadas (Tabla 5). Para ello, se simplifica el concepto de *confiabilidad* a dos valores *confiable* y *no confiable*.

Tabla 5. *Datos de entrenamiento del escenario de estudio de una red de naive Bayes para calcular un indicador de confianza*

Transacción	Nodo servidor	Confianza	Seguridad	Calidad del servicio	Confianza del nodo
1	A	Alta	Alta	Buena	Confiable
2	A	Baja	Baja	Mala	No confiable
3	B	Media	Alta	Regular	Confiable
4	B	Alta	Media	Buena	Confiable
5	C	Baja	Baja	Mala	No confiable
6	C	Alta	Baja	Regular	No confiable

***Nodo servidor:** Es el nodo que ofrece el servicio y cuya confianza se debe calcular

Estos datos fueron obtenidos a partir de un grupo experto que estableció si los nodos eran confiables en función de los valores para cada una de las tres características seleccionadas. Seguidamente, se definieron las variables de las características seleccionadas y la variable objetivo, tal como se presenta a continuación:

Características (X):

- $X1$: Confianza (alta/media/baja)
- $X2$: Seguridad (alta/media/baja)
- $X3$: Calidad del Servicio (buena/regular/mala)

Variable objetivo (Y):

- *Y:* Confianza del nodo (confiable/no confiable)

Posteriormente, se calcularon las probabilidades de acuerdo con la Tabla 5. Primero, mediante las Ecuaciones (2) y (3), se calcularon las probabilidades *a priori* de cada clase. En este caso, se partió de cualquier nodo (confiable o no confiable).

$$P(confiable) = Nconfiable \,/\, Ntotal = 3 \,/\, 6 = 0.5 \quad (2)$$
$$P(Noconfiable) = NNoconfiable \,/\, Ntotal = 3 \,/\, 6 = 0.5 \quad (3)$$

Luego, se calcularon las probabilidades condicionales de cada característica para nodos confiables o no confiables.

Las Ecuaciones (4) a (9) se utilizaron para determinar la confianza.

$$P(Confianza = Alta|Confiable) = 2 / 3 = 0.67 \ (4)$$
$$P(Confianza = Media|Confiable) = 1 / 3 = 0.33 \ (5)$$
$$P(Confianza = Baja|Confiable) = 0 / 3 = 0.00 \ (6)$$
$$P(Confianza = Alta|NoConfiable) = 1 / 3 = 0.33 \ (7))$$
$$P(Confianza = Media|NoConfiable) = 0 / 3 = 0.00 \ (8)$$
$$P(Confianza = Baja|NoConfiable) = 2 / 3 = 0.67 \ (9)$$

Las Ecuaciones (10) a (15) se utilizaron para calcular la seguridad.

$$P(Seguridad = Alta|Confiable) = 2 / 3 = 0.67 \ (10)$$
$$P(Seguridad = Media|Confiable) = 1 / 3 = 0.33 \ (11)$$
$$P(Seguridad = Baja|Confiable) = 0 / 3 = 0.00 \ (12)$$
$$P(Seguridad = Alta|NoConfiable) = 0 / 3 = 0.00 \ (13)$$
$$P(Seguridad = Media|NoConfiable) = 0 / 3 = 0.00 \ (14)$$
$$P(Seguridad = Baja|NoConfiable) = 2 / 3 = 0.67 \ (15)$$

Las Ecuaciones (16) a (21) se utilizaron para determinar la QoS.

$$P(Calidad = Buena|Confiable) = 2 / 3 = 0.67 \ (16)$$
$$P(Calidad = Regular|Confiable) = 1 / 3 = 0.33 \ (17)$$
$$P(Calidad = Mala|Confiable) = 0 / 3 = 0.00 \ (18)$$
$$P(Calidad = Buena|NoConfiable) = 1 / 3 = 0.33 \ (19)$$
$$P(Calidad = Regular|NoConfiable) = 1 / 3 = 0.33 \ (20)$$
$$P(Calidad = Mala|NoConfiable) = 2 / 3 = 0.67 \ (21)$$

Según lo anterior, cada vez que llegue la solicitud de una nueva transacción entre dos nodos de la red IoT, *i.e.*, nodo que solicita el servicio (Nss) *vs*. nodo que ofrece el servicio (Nos), inicia un proceso de cálculo de reputación entre pares de nodos de la misma red, a partir de las transacciones pasadas entre ellos. Para esto, se consulta la información (variables y características) que tiene cada nodo de la red sobre el Nos, en caso de que haya interactuado con este, y se calcula su confiabilidad con la Ecuación (1).

Por ejemplo, la información de un nodo *i* de la red que ya ha interactuado con el Nos puede ser la siguiente:

- Confianza: Alta
- Seguridad: Media
- QoS: Buena

En este caso, se calcula la confiabilidad así:
En las Ecuaciones (22) y (23), se utiliza el teorema *naive* Bayes.

$$[P(Confiable|X) \backslash proporcionala P(X|Confiable) \cdot P(Confiable)] \ (22)$$
$$[P(NoConfiable|X) \backslash proporcional\ a\ P(X|NoConfiable).\ P(NoConfiable)] \ (23)$$

En la Ecuación (24) se calcula $P(X|Confiable)$ y en la (25) se determina $P(X|NoConfiable)$.

$$P(X|Confiable) = P(Confianza = Alta|Confiable).\ P(Seguridad = Media|Confiable).\ P(Calidad = Buena|Confiable)\ (24)$$
$$P(X|Confiable) = 0.67 * 0.33 * 0.67 = 0.148\ (24)$$

$$P(X|NoConfiable) = P(Confianza = Alta|NoConfiable).\ P(Seguridad = Media|NoConfiable).\ P(Calidad = Buena|NoConfiable)\ (25)$$
$$P(X|NoConfiable) = 0.33 * 0.33 * 0.00 = 0.00\ (25)$$

Finalmente, en las Ecuaciones (26) y (27) se calculan las probabilidades *a posteriori*.

$$P(Confiable \mid X) \backslash proporcional\ a\ 0.148 * 0.5 = 0.074\ (26)$$
$$P(No\ Confiable \mid X) \backslash proporcional\ a\ 0.00 * 0.5 = 0.00\ (27)$$

En las Ecuaciones (28) y (29) se normaliza para obtener probabilidades.

$$P(Confiable|X) = 0.074\ /\ (0.074+0.00) = 1.0\ (28)$$
$$P(NoConfiable|X) = 0.00\ /\ (0.074+0.0) = 0\ (29)$$

Por lo tanto, la confiabilidad del nodo *i* sobre el Nos sería clasificada como *confiable*, con una probabilidad del 100 %. Asimismo, se calcula la confiabilidad de cada par (nodo i *vs*. Nos). Posteriormente, a partir del conjunto de confiabilidades medidas, se puede calcular la reputación del Nos, como se presenta en la Ecuación (30). Así, el Nss, con el valor de reputación calculado para el Nos, puede decidir si realizar la transacción o no.

Indicador de reputación con *blockchain* y criptografía

De acuerdo con lo anterior, el indicador de reputación se basa en la confiabilidad calculada para cada nodo *i* de la red que interactuado con el Nos, cuya reputación se calcula así:

$$Reputacioni = \sum_{j=0}^{N} \frac{\text{Confiabilidadji * Wj}}{N}\ (30)$$

donde:

- i: el nuevo nodo cuya reputación se calcula.
- j: un nodo de la red que ha interactuado con el nuevo nodo.
- N: el número total de nodos de la red IoT.
- $Confiabilidad_{ji}$: la confiabilidad se calcula a través de la información provista por el nodo *j* sobre la interacción que tuvo con el nuevo nodo. Sin embargo, para que en esta fórmula el valor no sea cualitativo sino cuantitativo, se manejan los siguientes valores: (alto o buena) = 1, (medio o regular) = 0.5 y (bajo o mala) = 0.0.
- Wj es un peso que se le da a la confiabilidad de los nodos consultado y depende del grado de confianza que tenga el nodo solicitante con el nodo que provee la información. Por ejemplo, si el nodo es del mismo propietario, puede tomar un valor de 1.0, y, si es de otro propietario, se le podría dar un valor menor como 0.6.

Este indicador es consultado por el Nss cada vez que requiera hacer un contrato inteligente con la regla ECA con un Nos. A partir de la reputación calculada, decide o no realizar la transacción. Una vez que finaliza la misma, se invoca el algoritmo que recalcula la reputación del Nos, actualizando las características y aplicando los algoritmos DAG y AES.

Aplicación de los algoritmos de *blockchain* y criptografía en el cálculo de las características de los nodos

En el contexto de interacción semántica entre objetos inteligentes del IoT se generan contratos inteligentes con reglas ECA cuando dos objetos inteligentes se ponen de acuerdo para crear un nuevo servicio. Antes de crear el servicio, el Nss solicita el cálculo de la reputación del Nos a la red y, dependiendo del resultado, decide o no crear el contrato inteligente.

Para calcular la reputación con la Ecuación (30), primero se calculan las características, y se registran los datos en los diferentes nodos de la red, tal como se presenta a continuación.

De acuerdo con las características seleccionadas, se aplica una técnica para calcular los respectivos valores.

Confianza. Esta característica se calcula con el algoritmo DAG y se construye entre todos los nodos de la red IoT. El algoritmo de consenso actualiza la confianza del Nos a partir de la red de nodos del DAG. Cada Nss que tuvo una interacción exitosa con el Nos lleva un contador de interacciones exitosas y no exitosas. Una interacción es exitosa si el Nss considera la reputación y decide realizar el contrato inteligente. Acto seguido, la confianza del Nos sube o baja en un porcentaje medido por la relación entre el contador de interacciones exitosas y el contador de interacciones no exitosas, donde el primero nunca puede ser cero. La confianza toma valores entre 0.0 y 1.0. En la Tabla 6 se muestran los valores de confianza y seguridad asociados a los umbrales de clasificación.

Tabla 6. *Valores de confianza y seguridad asociados a los umbrales de clasificación*

Valor de confianza y seguridad	Umbral de clasificación
Mayor o igual a 0.0 y menor que 0.4	Baja
Mayor o igual a 0.4 y menor que 0.7	Media
Mayor o igual a 0.7 y menor o igual a 1.0	Alta

Seguridad. La transacción se realiza utilizando técnicas criptográficas a fin de preservar la confidencialidad de la información y su integridad. El algoritmo utilizado fue el de criptografía AES. El Nss encripta la información y el Nos la desencripta. En caso de que la desencriptación falle, se llevan contadores que almacenan la información de seguridad para las transacciones exitosas y no exitosas. El proceso de cálculo es similar al de la confianza, pues se utiliza la relación de las dos medidas y los mismos umbrales de clasificación.

Calidad del servicio. La QoS se calcula midiendo la cantidad de servicios satisfactorios, sobre el total de los servicios realizados. Esto, a partir de todas las interacciones entre el Nos y otros nodos IoT de la red. Un servicio es satisfactorio si su confianza y su seguridad fueron exitosas; de lo contrario, si falla alguna de estas características, se trata de un servicio no exitoso. En la Tabla 7 se definen los valores asociados a los umbrales de clasificación de la QoS.

Tabla 7. Valores del servicio asociados a los umbrales de clasificación de la QoS

Valor del servicio	Umbral de clasificación de la calidad del servicio
Entre 0.0 y 33.3 %	Mala
Mayor que 33.3% y menor que 66.7 %	Regular
Mayor que 66.7 %	Buena

Prueba de concepto a partir de un escenario de simulación

Se realizó una prueba de concepto mediante una simulación en el lenguaje Python, donde se definieron tres objetos IoT: temperatura (T), humedad (H) y luz (L). En la Tabla 8 se presentan los requerimientos no funcionales para el escenario IoT simulado, los cuales fueron parametrizados en cada nodo.

Tabla 8. *Requerimientos no funcionales parametrizados en cada nodo IoT*

Requerimiento no funcional	Descripción
Tiempo	El tiempo se definió de manera aleatoria.
Restricciones	Se definieron restricciones en cada nodo IoT.
Criptografía	Se implementó el algoritmo AES SHA-256 (32 bytes) para encriptar y desencriptar los metadatos observados por la salida en consola.
Verificación del DAG	Se verificó el DAG con el fin de evaluar el tiempo de la interacción simulada entre cada par de nodos IoT.

En la Figura 3 se muestra la interacción entre cada par de nodos IoT. La conexión se estableció por medio de contratos inteligentes con reglas ECA.

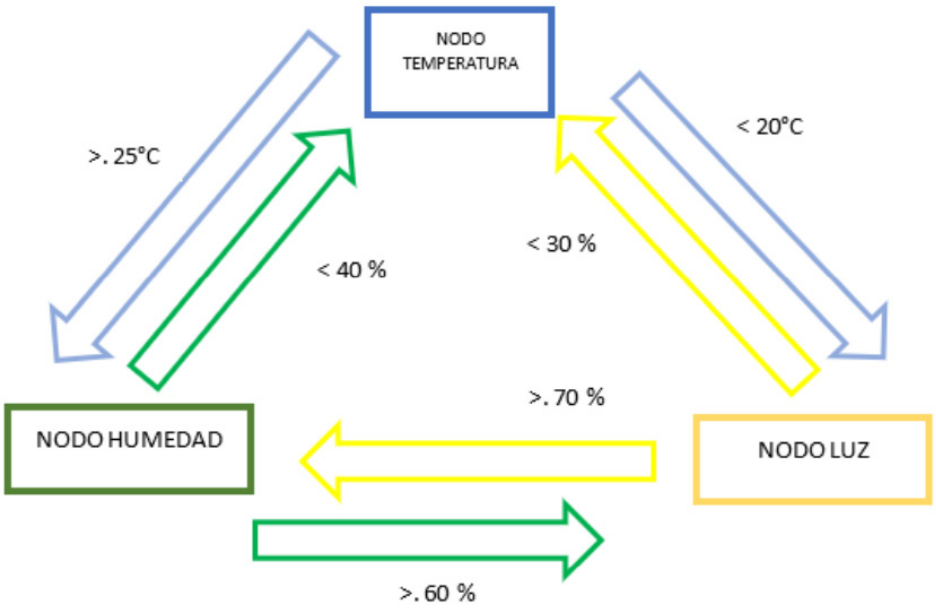

Figura 3. *Escenario de simulación con tres objetos inteligentes*

Se realizó una prueba inicial en el escenario IoT simulado, empleando el sistema de seguridad de información propuesto, que utiliza DAG y criptografía AES. Durante esta prueba, se verificaron las conexiones entre cada par de nodos IoT para asegurar que no presentaran fallas.

En la Tabla 9 se presenta una evaluación de las conexiones entre los nodos T, H y L para el escenario simulado, realizada durante un periodo de un minuto. Se establecieron un total de 15 conexiones entre los tres nodos, registrándose datos aleatorios cada diez segundos. Además, se verificó el cumplimiento de la regla ECA en cada nodo IoT.

Tabla 9. *Conexiones entre los nodos IoT de temperatura (T), humedad (H) y luz (L)*

Conexión 1	Conexión 2	Conexión 3	Conexión 4	Conexión 5	N° de conexiones
T→H	T →L	L →T	H →T	T → L	3
L→T	H → T	T → H	T →H	H → T	3
H →L	L →H	H → L	L →T	L → T	3

La Tabla 10 presenta los resultados de tres pruebas realizadas en el escenario simulado, con el sistema de seguridad de la información propuesto configurado en los tres nodos IoT. En cada prueba se modificó el tiempo de conexión de cada nodo IoT: en la prueba 1 se estableció un intervalo de 5 s, en la prueba 2 de 10 s y en la prueba 3 de 20 s. A partir de estos experimentos, se calculó y evaluó el tiempo promedio de conexión óptimo entre los tres nodos para la simulación, asegurando en todo momento la integridad y la confiabilidad del sistema.

Tabla 10. *Cálculo y evaluación del mejor tiempo promedio para la conexión de los tres nodos IoT en el escenario simulado*

Tiempo aleatorio de datos	Número de repeticiones										
	1	2	3	4	5	6	7	8	9	10	Promedio
5 s	27	13	16	4	3	7	2	8	1	6	8.7 s
10 s	11	10	3	32	54	19	40	29	22	1	22.1 s
20 s	42	1	22	19	41	1	42	39	9	2	21.8 s

Los datos obtenidos a partir de la ejecución de tiempos aleatorios (en segundos) para las tres pruebas indican que se efectuaron diez repeticiones por prueba. Se observó una relación proporcional entre el tiempo aleatorio de los datos y el tiempo promedio de conexión de los tres nodos IoT: a menor tiempo aleatorio de datos, menor es el tiempo promedio de conexión de los nodos, mientras que, a mayor tiempo aleatorio de datos, mayor es el tiempo promedio de conexión.

Planteamiento de un entorno IoT para conocer el índice de confianza

Según se muestra en la Tabla 11, la implementación del índice de confianza se efectuó por medio de un cálculo dinámico que valida la puntuación obtenida a partir de las siguientes condiciones:

Tabla 11. *Validación de la puntuación obtenida a partir de las condiciones para la implementación del índice de confianza en un entorno de objetos inteligentes del IoT*

Sistema de puntuación	**Puntuación base inicial** *(así se asegura que el dispositivo IoT empieza con un valor medio, confiable o no confiable)*	**50 puntos**
Factores positivos y negativos	Integridad del DAG (sin ciclos)	+20 puntos
	Encriptación/desencriptación exitosa	+20 puntos
	Actualización de datos	+10 puntos
	Error en la encriptación / desencriptación	-20 puntos
	Ciclo detectado en el DAG	-30 puntos
	Error en la solicitud de datos a otro dispositivo	-15 puntos
Puntuación mínima asegurada	**Umbral de puntuación mínima**	*Si después de sumar y restar puntos, el total es inferior a 10, se ajusta a 10. Esto garantiza que la puntuación nunca caerá a cero o a valores extremadamente bajos.*
Cálculo dinámico	**Índice de confianza**	*Cada vez que se recalcula el índice de reputación, se verifica si la puntuación es menor a 10. Si es así, se ajusta automáticamente a 10 para asegurar que siempre haya un valor mínimo.*

El valor de salida depende de esta calificación, y el sistema valida el dispositivo IoT como se muestra en la Tabla 12.

Tabla 12. *Valor de la salida de la puntuación, obtenido al evaluar la confiabilidad de un dispositivo IoT*

Valor de la salida de la puntuación	**Dispositivo IoT evaluado**
El valor de la puntuación es mayor o igual a 60	Confiable
El valor de la puntuación es menor que 60	No confiable

Ejemplo de un entorno IoT para conocer el índice de confianza

La implementación del índice de reputación en el escenario de ejemplo se llevó a cabo mediante un cálculo dinámico que validó la puntuación obtenida a partir de las condiciones de la Tabla 13. Se observa que el dispositivo IoT evaluado no es confiable.

Tabla 13. *Valor de la salida de la puntuación para el ejemplo propuesto*

Puntuación base	**Falla en la encriptación**	**Error en solicitud de datos**	**Valor de la salida de la puntuación**	**Dispositivo IoT evaluado**
50 puntos	-20 puntos	-15 puntos	15 puntos	No confiable

En la Figura 4 se presenta la ejecución del escenario del panel de objetos inteligentes, con los registros de interacción entre tres dispositivos del IoT y los datos del índice de reputación de cada uno. Como resultado, los tres dispositivos no son confiables. Además, por cada nodo IoT definido en el registro de interacción, se hace referencia a metadatos encriptados.

Figura 4. *Escenario del panel de objetos inteligentes*

La Figura 5 muestra cómo se usó el algoritmo AES SHA-256 (32 bytes) para encriptar y desencriptar los metadatos que se observan en la salida en los parámetros de la consola (*device_id, status, last_update, request_duration*), con el fin que no fuesen alterados durante el recorrido. Este proceso se realizó una vez cumplidas las reglas ECA y efectuada la conexión correspondiente a cada nodo IoT.

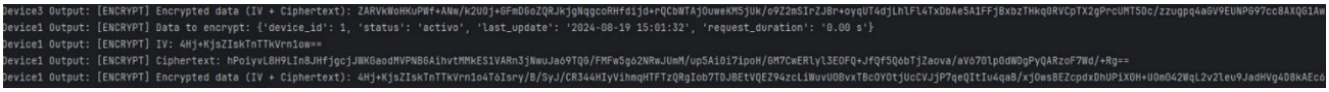

Figura 5. *Implementación de los parámetros de la consola device_id, status, last_update y request_duration*

Verificación e implementación del DAG

Una vez el nodo IoT recibe un dato aleatorio, decide si efectuará la conexión con otro nodo IoT teniendo en cuenta la regla ECA. Cuando la conexión se establece, este proceso queda registrado en el panel de objetos inteligentes.

En la consola del panel de objetos inteligentes, se evidencian las conexiones simultáneas entre los nodos IoT, y se observa un monitoreo del cumplimiento de las condiciones iniciales.

En la Figura 6 se observa que la consola del panel de objetos inteligentes detectó que un nodo IoT ya había establecido conexión con otro, y que el sistema quería establecer otra conexión con los mismos datos. Aquí se activa un evento por medio de una *excepción*, informando que no se permite establecer la conexión con un nodo IoT, pues el DAG hace referencia a conexiones acíclicas y no puede tomar un mismo camino porque se rompería su lógica.

Figura 6. *Verificación y validación del DAG en la conexión entre nodos IoT*

Cuando los datos aleatorios de las conexiones de los nodos IoT cambian (lo hacen cada cierto tiempo) y las reglas ECA son correctas, se establecen conexiones durante un tiempo fijo.

CONCLUSIONES

El indicador de reputación propuesto se basó en un enfoque de solución que reúne las particularidades de la reputación en el entorno humano y se basa en el concepto de *credibilidad del nodo*, *i.e.*, la confianza del nodo. Además, se definió una relación tridimensional de confiabilidad para cada nodo IoT, con base en las calificaciones de otros nodos respecto a la confianza, la seguridad y la calidad del servicio.

El uso del indicador de reputación propuesto permitió evaluar las interacciones entre los dispositivos inteligentes del IoT y la manera en que su resultado interviene en la decisión de efectuar una conexión. De acuerdo con la propuesta, se obtuvieron datos a partir de cálculos matemáticos, donde se evaluaron las interacciones posibles en los dispositivos, en aras de determinar si un nodo IoT era confiable o no.

Se realizó una prueba de concepto simulada con tres dispositivos inteligentes, en la cual fue posible enviar y recibir información entre los nodos IoT mediante la implementación del DAG y de encriptación AES. Se cálculo y evaluó el mejor tiempo promedio para la conexión de los tres nodos, garantizando seguridad y confianza. Se recomienda integrar más objetos inteligentes al escenario IoT simulado, con el propósito de evaluar la escalabilidad de la solución.

AGRADECIMIENTOS

Agradecemos la contribución del Semillero Internet de las Cosas y Computación Inteligente (IoTIC), adscrito al Grupo de Investigación y Desarrollo en Tecnologías de la Información (GTI) de la Universidad del Cauca, así como la del Semillero Espejo Internet de las Cosas y Computación Inteligente (IoTIC), adscrito al Grupo de Investigación Desarrollo Tecnológico (D+TEC) de la Universidad de Ibagué.

CONTRIBUCIÓN DE AUTORES

Díaz-Santacruz, Carlos-Andrés: conceptualización, metodología, investigación, redacción (borrador original, revisión y edición).
Niño-Zambrano, Miguel-Ángel: conceptualización, metodología, investigación, redacción (borrador original, revisión y edición), supervisión.

Zarate-Guevara, Daniel-Guillermo: investigación, análisis formal, software, validación, conservación de datos.
Bulla-Ortega, Samuel-Yesid: investigación, análisis formal, software, validación, conservación de datos.

REFERENCIAS

Alshehri, S., & Bamasag, O. (2022). AAC-IoT: Attribute access control scheme for IoT using lightweight cryptography and Hyperledger Fabric blockchain. *Applied Sciences (Switzerland), 12*(16), 8111. https://doi.org/10.3390/app12168111

Azad, M. A., Bag, S., & Hao, F. (2017). *M2M-REP: Reputation of machines in the Internet of Things* [Artículo de conferencia]. 12th International Conference on Availability, Reliability and Security. https://doi.org/10.1016/j.cose.2018.07.014

Battah, A., Iraqi, Y., & Damiani, E. (2021). Blockchain-based reputation systems: Implementation challenges and mitigation. *Electronics (Switzerland), 10*(3), 289. https://doi.org/10.3390/electronics10030289

Bernal Bernabe, J., Hernandez Ramos, J. L., & Skarmeta Gomez, A. F. (2016). TACIoT: Multidimensional trust-aware access control system for the Internet of Things. *Soft Computing, 20*(5), 1763-1779. https://doi.org/10.1007/s00500-015-1705-6

Bica, I., Chifor, B.-C., Arseni, Ş.-C., & Matei, I. (2020). Reputation-based security framework for Internet of Things. En E. Simion & R. Géraud-Stewart (Eds.), *Innovative Security Solutions for Information Technology and Communications* (pp. 213-226). Springer International Publishing. https://doi.org/10.1007/978-3-030-41025-4_14

Bordel, B., Alcarria, R., Martín De Andrés, D., & You, I. (2018). Securing Internet-of-Things systems through implicit and explicit reputation models. *IEEE Access, 6*, 47472-47488. https://doi.org/10.1109/ACCESS.2018.2866185

Cai, T., Li, X., Chen, W., Wei, Z., & Ye, Z. (2024). Blockchain-based federated learning for IoT sharing: Incentive scheme with reputation mechanism. En J. Chen, B. Wen & T. Chen (Eds.), *Blockchain and Trustworthy Systems. BlockSys 2023. Communications in Computer and Information Science* (vol. 1896, pp. 270-284). Springer. https://doi.org/10.1007/978-981-99-8101-4_19

Chen, D., Chang, G., Sun, D., Li, J., Jia, J., & Wang, X. (2011). TRM-IoT: A trust management model based on fuzzy reputation for the Internet of Things. *Computer Science and Information Systems, 8*(4), 1207-1228. https://doi.org/10.2298/csis110303056c

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645-1660. https://doi.org/10.1016/j.future.2013.01.010

Guerrero-Narváez, S., Niño-Zambrano, M. ángel, Riobamba-Calvache, D. J., & Ramírez-González, G. A. (2018). Test bed of semantic interaction of smart objects in the web of things. *Future Internet*, *10*(5), 42. https://doi.org/10.3390/fi10050042

Gurajena, C., Sibanda, K., & Chindenga, E. (2020). Security in the Internet of Things: Trust and reputation evaluation model. *Indian Journal of Computer Science and Engineering, 11*(5), 522-531. https://doi.org/10.21817/indjcse/2020/v11i5/201105263

Hellani, H., Sliman, L., Samhat, A. E., & Exposito, E. (2021a). Computing resource allocation scheme for DAG-based IOTA nodes. *Sensors, 21*(14), 4703. https://doi.org/10.3390/s21144703

Hellani, H., Sliman, L., Samhat, A. E., & Exposito, E. (2021b). Tangle the blockchain: Towards connecting blockchain and DAG. En IEEE (Ed.), *Proceedings of the Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE* (vol. 2021-October, pp. 63-68). IEEE Computer Society. https://doi.org/10.1109/WETICE53228.2021.00023

Jamil, B., Ijaz, H., Shojafar, M., Munir, K., & Buyya, R. (2022). Resource allocation and task scheduling in fog computing and Internet of Everything environments: A taxonomy, review, and future directions. *ACM Computing Surveys (CSUR), 54*, 1-38. https://doi.org/10.1145/3513002

Javanmardi, S., Shojafar, M., Shariatmadari, S., & Ahrabi, S. S. (2014). FR Trust: A fuzzy reputation-based model for trust management in semantic P2P grids. *International Journal of Grid and Utility Computing, 6*(1), 57-66. https://doi.org/10.1504/IJGUC.2015.066397

Jøsang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision Support Systems*, *43*(2), 618-644. https://doi.org/10.1016/j.dss.2005.05.019

Kamvar, S. D., Schlosser, M. T., & Garcia-Molina, H. (2003). *The Eigentrust algorithm for reputation management in P2P networks* [Artículo de conferencia]. 12th International Conference on World Wide Web, WWW '03. https://doi.org/10.1145/775152.775242

Li, J., Dai, M., Lu, Y., & Yang, S. (2024). Trusted reputation system for heterogeneous network resource sharing based on blockchain in IoT. *Wireless Networks, 31*, 1421-1433. https://doi.org/10.1007/s11276-024-03825-y

Liang, J., Li, L., & Zeng, D. (2019). Evolutionary dynamics of cryptocurrency transaction networks: An empirical study. *PLoS ONE*, *13*(8), e0202202. https://doi.org/10.1371/journal.pone.0202202

Mazzocca, C., Romandini, N., Montanari, R., & Bellavista, P. (2024). Enabling federated learning at the edge through the IOTA Tangle. *Future Generation Computer Systems, 152*, 17-29. https://doi.org/10.1016/j.future.2023.10.014

Mhetre, N. A., Deshpande, A. V., & Mahalle, P. N. (2016). Trust management model based on fuzzy approach for ubiquitous computing. *International Journal of Ambient Computing and Intelligence, 7*(2), 33-46. https://doi.org/10.4018/IJACI.2016070102

Patel, A., & Jinwala, D. (2022). A reputation-based RPL protocol to detect selective forwarding attack in Internet of Things. *International Journal of Communication Systems*, *35*(1), e5007. https://doi.org/https://doi.org/10.1002/dac.5007

Rana, M., Mamun, Q., & Islam, R. (2022). Lightweight cryptography in IoT networks: A survey. *Future Generation Computer Systems, 129*, 77-89. https://doi.org/10.1016/j.future.2021.11.011

Resnick, P., Zeckhauser, R., Friedman, E., & Kuwabara, K. (2001). Reputation systems. *Communications of the ACM*, *43*(12), 45-48. https://doi.org/10.1145/355112.355122

Song, S., Hwang, K., Zhou, R., & Kwok, Y. K. (2005). Trusted P2P transactions with fuzzy reputation aggregation. *IEEE Internet Computing, 9*(6), 24-34. https://doi.org/10.1109/MIC.2005.136

Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A critical cybersecurity analysis and future research directions for the Internet of Things: A comprehensive review. *Sensors, 23*(8), 4117. https://doi.org/10.3390/s23084117

Wang, Y., & Vassileva, J. (2003). *Trust and reputation model in peer-to-peer networks* [Artículo de conferencia]. Third International Conference on Peer-to-Peer Computing (P2P2003). https://doi.org/10.1109/PTP.2003.1231515

Xu, L. D., Xu, E. L., & Li, L. (2018). Industry 4.0: State of the art and future trends. International *Journal of Production Research, 56*(8), 2941-2962. https://doi.org/10.1080/00207543.2018.1444806

Yang, W., Hou, C., Zhang, Z., Wang, X., & Chen, S. (2024). Secure and efficient data sharing for IoT based on blockchain and reputation mechanism. *IEEE Internet of Things Journal, 11*(11), 20631–20647. https://doi.org/10.1109/JIOT.2024.3371063

Zhou, Z., Ye, F., Gao, J., Zhang, S., & Geng, X. (2024). Ensuring long-term trustworthy collaboration in IoT networks using contract theory and reputation mechanism on blockchain. *IEEE Internet of Things Journal, 11*(2), 2420-2437. https://doi.org/10.1109/JIOT.2023.3291826