ISSN 2007-9737

Un sistema transactivo de energía ciberseguro usando cadenas de bloques de múltiples niveles

Juan C. Olivares-Rojas, Enrique Reyes-Archundia, José A. Gutiérrez-Gnecchi

Instituto Tecnológico de Morelia,
División de Estudios de Posgrado e Investigación,
México

{juan.or, enrique.ra, jose.gg3}@morelia.tecnm.mx

Resumen. Los incidentes de ciberseguridad son cada vez más frecuentes debido al alto grado de penetración que tienen las tecnologías de la información y las comunicaciones en nuestra vida diaria. Una de las infraestructuras críticas que más se ha beneficiado en los últimos años de la amplia integración de tecnologías ha sido la red inteligente. Los sistemas de medición inteligentes permiten, entre otras cosas, monitorear el consumo de energía y las lecturas de producción que se traducen en transacciones monetarias. La alteración y manipulación de las lecturas de los medidores inteligentes se reflejan en pérdidas económicas para las empresas de servicios públicos y pérdida de confianza en los usuarios finales. Este trabajo presenta una arquitectura de ciberseguridad basada en una cadena de bloques multicapa capaz de adaptarse a la arquitectura de los sistemas de medición inteligente a través de un esquema de computación distribuida borde-niebla-nube. La arquitectura propuesta es altamente escalable a los distintos componentes de los sistemas de medición inteligente y mejora el rendimiento de las cadenas de bloques en aspectos como el almacenamiento y el procesamiento. Esta cadena de bloques utiliza su propio algoritmo de consenso de prueba de eficiencia, que permite beneficiar a los usuarios finales mediante un uso más eficiente de su consumo de energía considerando la calidad de la energía, el pronóstico de la demanda y el apoyo para la detección de robo y fraude energético. El algoritmo de consenso utiliza la misma arquitectura propuesta para determinar las recompensas de los usuarios mediante análisis de datos y técnicas de aprendizaje automático. Todo esto sienta las bases para un sistema de medición más inteligente, más transaccional y ciberseguro. La arquitectura desarrollada fue probada para garantizar la ciberseguridad de las transacciones realizadas en los sistemas de medición inteligente. Los resultados obtenidos sugieren que el uso de una arquitectura de cadenas de bloque permite mejorar la ciberseguridad de los sistemas de medición inteligente y brindar a los usuarios finales una mayor confianza en sus transacciones energéticas, pudiendo recibir mejores incentivos económicos al hacer un uso más eficiente de su consumo energético.

Palabras clave. Cadenas de bloque, ciberseguridad, sistemas transactivos de energía.

A Cybersecurity Transaction Energy System Using Multi-Tier Blockchain

Abstract. Cybersecurity incidents are becoming more frequent due to the high degree of penetration that information and communication technologies have in our daily lives. One of the critical infrastructures that has benefited the most in recent years from the broad integration of technologies has been the smart grid. Smart metering systems allow, among other things, the monitoring of energy consumption and production readings that are translated into monetary transactions. The tampering and manipulation of the smart meter readings are reflected in economic losses for the utilities and loss of confidence in the end-users. This work presents a cybersecurity architecture based on a multitier blockchain capable of adapting to smart metering systems' architecture through an edge-fog-cloud distributed computing scheme. The proposed architecture is highly scalable to the various components of smart metering systems and improves the performance of blockchains in aspects such as storage and processing. This blockchain uses its own consensus algorithm proof-of-efficiency, which allows benefiting end-users through more efficient use of their energy consumption considering the power quality, the forecast of the demand, and the support for detecting theft and energy fraud. The consensus algorithm uses the same architecture proposed to determine users' rewards through data analytics and machine learning techniques.

ISSN 2007-9737

All of this lays the foundation for a more intelligent, more transactional, and cybersecure metering system. The architecture developed was tested to guarantee the cybersecurity of the transactions carried out in the smart metering systems. The results obtained suggest that using a blockchain architecture allows improving the cybersecurity of smart metering systems and giving end-users greater confidence in their energy transactions, being able to receive better economic incentives by making more efficient use of their energy consumption.

Keywords. Blockchain, cybersecurity, transactive energy systems.

1. Introducción

Una de las áreas de mayor transformación ha sido la red eléctrica; la cual tenía demasiados años sin sufrir modificaciones. El uso de las tecnologías de la cuarta revolución industrial (4RI) ha traido consigo a que la red eléctrica se haya vuelto más inteligente, motivo por el cual ha pasado a denominarse como Red Eléctrica Inteligente (REI).

La REI ha permitido no solo automatizar procesos y operaciones de los sistemas eléctricos de potencia, sino que a su vez ha permitido que el suministro de energía eléctrica sea más confiable, barato y sobre todo menos contaminante al fomentar el uso energías limpias [1].

El concepto de la REI se empezó a manejar a finales de la década de los 2000 y vino de la mano del uso de los denominados medidores inteligentes (MI). Los MI evolucionan del medidor electrónico al agregarle capacidades de comunicaciones y procesamiento al sistema embebido del medidor, convirtiéndose en un dispositivo de IoT bastante robusto.

Los MI permiten monitorear el consumo de energía eléctrica en todo momento, además de automatizar operaciones como los procesos de facturación, así como los cortes y reconexiones del servicio sin la intervención manual de operadores [2].

Para ello, se requiere además de los MI de un conjunto de elementos denominado como Sistemas de Medición Inteligente (SMI) siendo la Infraestructura de Medición Avanzada (AMI, por sus siglas en inglés), la implementación mejor conocida.

Recientemente se han agregado nuevas funciones entre las que se encuentran la medición de energía producida a través de sistemas de generación distribuida (DER, por sus siglas en inglés), el manejo de tarifas eléctricas por uso horario y en tiempo real, así como la integración con sistemas de gestión de energía y de respuesta a la demanda [3].

Sin embargo, a pesar de las enormes ventajas que traen consigo la REI y los SMI también se presentan nuevos retos y oportunidades derivado del uso de las tecnologías de la 4RI, uno de ellos, la ciberseguridad.

De acuerdo con la Comisión Federal de Eléctricidad (CFE) [4] se estima el nivel de pérdidas no técnicas (errores de medición, facturación, robo y fraude de energía eléctrica) a nivel nacional en un 25.2%.

Aunque los MI y los SMI presentan arquitecturas de ciberseguridad para la confidencialidad, integridad y disponibilidad de los datos, nunca es suficiente debido al incremento de las amenazas y vulnerabilidades que presenta cualquier sistema informático.

Los SMI son sistemas complejos y muy heterogéneos por lo que las vulnerabilidades se presentan de forma muy diversa y en diversos puntos de su infraestructura. Por ejemplo, los mismos dispositivos eléctricos que ahora tienen capacidades de comunicación (dispositivos IoT) en el hogar pueden inducir fallas de ciberseguridad.

Por otra parte, los MI que poseen capacidades de cómputo y almacenamiento son una de los principales activos de información en tratar de ser atacados.

Además de lo anterior, se pueden presentar fallas de ciberseguridad en los medios de transmisión de datos y en la infraestructura tecnológica de las empresas eléctricas.

La ciberseguridad es un área bastante estudiada en la literatura y en el campo de las REI y SMI no es nuevo. Existen diversos enfoques utilizados en tratar de garantizar la protección de los activos de información, desde el uso de criptografía para cifrar y descifrar la información, hasta mecanismos de análisis de tráfico en redes de datos como lo son los cortafuegos (firewalls), por mencionar algunos.

Tabla 1. Estado del arte de ciber seguridad en Sistemas de Medición Inteligente

Trabajo	Técnica	C	I	D	Enfoque
[9]	Blockchain multifirma	Si	Sí	Si	Privacidad
[11]	Criptomoneda	No	Sí	No	Comercializacion
[13]	Blockchain doble	Sí	Sí	Si	Criptografía ligera
[15]	Blockchain doble	Sí	Sí	Sí	Computación borde
[16]	Blockchain	Sí	Sí	No	Protección de datos
[17]	Blockchain modular	Sí	Sí	Sí	Utilizar diversos algoritmos de consenso
[18]	Libro mayor distribuido	No	Sí	Sí	Fragmentos de datos
Este trabajo	Blockchain multinivel	Sí	Sí	Sí	Computación borde-niebla-nube Ligero y Escalable Protección de datos en SMI

En los últimos años, ha surgido el concepto de blockchain (cadenas de bloques) que trata sobre la combinación de diversas tecnologías para garantizar confianza en las transacciones de cualquier sistema informático [5].

Entre los principales componentes de la cadena de bloques se encuentran las técnicas de criptografía asimétrica para el manejo de firmas digitales para garantizar la identidad de los usuarios, el manejo de funciones de resumen (hash) para garantizar integridad de los datos, así como métodos de validación de transacciones denominados algoritmos de consenso [6], entre otros.

Como se puede apreciar, el uso de cadenas de bloque provee enormes ventajas que permiten garantizar la confidencialidad, integridad y disponibilidad de los datos en sistemas de transacciones, por lo que su uso en la REI se ha ido incrementando en los últimos años [7].

Sin embargo, el uso de cadena de bloques por si solo presenta algunos retos que aunados a los retos presentes en los SMI hace necesario tomar en cuenta nuevas consideraciones referentes a la ciberseguridad y al desempeño de las cadenas de bloques.

En este trabajo se propone un SMI transactivo utilizando una cadena de bloques multinivel, el cual permite garantizar la ciberseguridad de los datos de medición de consumo y producción de energía eléctrica.

El trabajo que se propone utiliza para la validación de transacciones, un algoritmo de consenso propio denominado Proof-of-Efficiency (PoEf, prueba de eficiencia) basado en una plataforma de analítica de datos multinivel que al igual que la arquitectura de cadena de bloques propuesta, aprovecha las arquitecturas de cómputo distribuido de borde-niebla-nube.

Los resultados de la analítica de datos además de validar transacciones de consumo/producción de energía eléctrica, permiten recompensar a los usuarios que hacen un uso más eficiente de su consumo y producción de energía eléctrica con base en factores de calidad de la energía, esto trae consigo un modelo transactivo de energía beneficioso para los usuarios finales y la empresa eléctrica gubernamental al eliminar subsidios y reducir costos en ambas partes.

Finalmente, la solución propuesta fue probada a través de diversos ataques pertinentes a las cadenas de bloques utilizando una arquitectura de gemelos digitales.

2. Estado del arte

En la literatura científica y en ambientes de desarrollo e innovación tecnológica, el estudio de la ciberseguridad en la REI y otras infraestructuras críticas ha sido ampliamente analizado desde hace varios años.

Desde técnicas de criptografía robustas y ligeras para MI y otros dispositivos electrónicos

inteligentes (IED, por sus siglas en inglés) hasta Sistemas de Prevención y Detección de Intrusos (IPS/IDS).

En general el uso de técnicas de ciberseguridad combinadas ha demostrado ser mucho más eficaz que utilizar un solo mecanismo de seguridad. Por este motivo, el uso de las cadenas de bloque ha proliferando en los últimos años, como medio para garantizar seguridad y confianza en sistemas transaccionales particularmente donde existe flujo de dinero [8].

En [9] se muestra Priwatt, un sistema de comercialización de energía a través del uso de de blockchain, multi-firmas y flujos de mensajes anónimos.

Existes diversos trabajos enfocados en generar criptomonedas y métodos financieros para REI, como en [10] en donde muestra NRGcoin. La cual es una criptomoneda que ayuda a la comercialización de energía limpia usando la infraestructura de la cadena de bloques.

Otra implementación es Helios que define una criptomoneda y un protocolo de consenso descentralizado [11]. En [12, 13] se presenta una arquitectura ligera para preservar y comparticir privacidad con un blockchain doble para sistemas de precios inteligentes en REI.

El uso de múltiples cadenas se está haciendo cada vez más común en la literatura [14, 15]. Otros tipos de trabajo radica en el monitoreo de las operaciones de REI, como por ejemplo en GridMonitoring [16]. En dicho trabajo se muestra una implementación de un blockchain para protección de los datos en REI.

La referencia [17], muestra la implementación de la cadena de bloques Phantom que permite la inclusión de diversos algoritmos de consenso en diferentes niveles.

En [18] se muestra la implementación de libros mayores de contabilidad fragmentados (parciales) y completos; todo esto con el objeto de tener una cadena de bloques más eficiente para el manejo de diversas entidades y dispositivos, particularmente de vehículos eléctricos.

En [19] se presenta una propuesta de arquitectura de blockchain basada en la nube y en el nuevo concepto de cómputo en niebla. En esta arquitectura las operaciones de la cadena de bloques se encuentran en la nube.

La información fluye desde la capa de dispositivos hacia la nube a través de la capa de niebla. En la capa de niebla utilizando el paradigma de Redes Definidas por Software (SDN, por sus siglas en inglés) se forma una especie de cadena de bloques para problemas más concretos.

En [20] se muestra la implementación de un mecanismo de cadena de bloques para la detección de malware en dispositivos móviles. Lo novedoso de esta propuesta es que permite la interconexión de otras cadenas públicas a través de un consorcio de cadenas de bloques. Otras implementaciones de cadenas de bloque en consorio para REI se muestra en [21].

Muchas implementaciones de cadenas de bloques se han implementado en entornos hogareños en combinación con mecanismos de seguridad y privacidad de la información [22-24]. Existen diversas implementaciones comerciales de cadenas de bloques dentro del área de la REI y SMI [25-27], particularmente enfocadas en energía transactiva de par a par.

Existe una gran cantidad de patentes del área de cadenas de bloques para REI y SMI, particularmente de China, Corea del Sur, Estados Unidos, entre otros [28-34]; enfocados principalmente en sistemas transactivos de energía. Sin embargo, la mayoría de las implementaciones carecen de una arquitectura modular que pueda garantizar de forma eficiente la seguridad de los datos en los diversos componentes de los SMI, particularmente en los MI.

En la Tabla 1, se muestran los principales trabajos relacionados en la ciber seguridad en SMI. Las columnas C, I y D; corresponden a los objetivos primarios de ciber seguridad de Confidencialidad, Integridad y Disponibilidad respectivamente. Este trabajo aporta una arquitectura de ciberseguridad basada en blockchain de múltiples niveles que puede adaptarse con facilidad a los SMI de forma distribuida y escalable basado.

La arquitectura propuesta garantiza la protección de los datos de medición ante diversos ciber ataques y permite la comercialización de la energía privilegiando la eficiencia y calidad de la energía.

3. Arquitectura propuesta

Conceptualización de los SMI dentro de una arquitectura borde-niebla-nube

La arquitectura de cómputo distribuido borde-niebla-nube se ha empezado a utilizar en diversos sistemas ciberfísicos particularmente en la REI. Una de nuestras aportaciones ha sido describir a los SMI dentro de una arquitectura distribuida de borde-niebla-nube como se visualiza en la Figura 1.

La arquitectura propuesta se basa en la arquitectura AMI adaptándose a la arquitectura de cómputo distribuida borde-niebla-nube.

La arquitectura propuesta para proteger los datos de medición se muestra en la Figura 2.

Se puede apreciar que conceptualmente se tienen al menos 4 cadenas de bloques (BC1, BC2, BC3, BCn) representando las áreas de HAN/BAN/IAN (aunque este trabajo se centra en HAN), NAN, FAN/WAN (que pueden crecer de forma variable dependiendo de la densidad de CD y a su extensión geográfica), y finalmente, el Head-End (representando por el centro de datos de la empresa eléctrica).

En HAN, existen EI (SA en inglés) que permiten medir su consumo energético y reportarlo al MI para generar una cadena de bloques por hogar, oficina o industria. El consumo de todos los electrodomésticos convencionales se almacena en el MI. Otro componente importante son los DER que permiten producir energía. El excedente de producción de energía se inyecta en la red y la transacción se guarda en la cadena de bloques.

La red de MI está dentro de NAN. Cada MI está asociado con una HAN particular y que todos los MI están asociados con un CD. En NAN se forma otra blockchain con los datos de todos los MI de la red. Los datos almacenados aquí son solo un resumen de los datos de cada MI ya que la privacidad de los datos debe protegerse a toda costa.

La Figura 3 muestra que el MI y el CD necesitan una BD para almacenar los datos de las transacciones realizadas. La BD del CD es mayor que el del MI y SA. La cadena de bloques propuesta en varios niveles se utiliza para garantizar la seguridad de los datos.

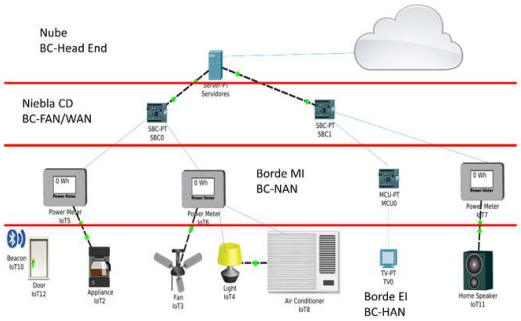

Fig. 1. Un SMI dentro de una arquitectura borde-niebla- nube

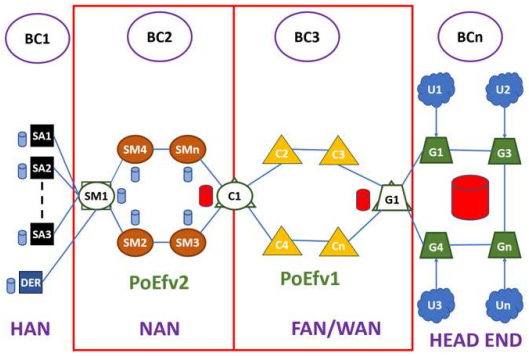

Fig. 2. Arquitectura propuesta basada en las cuatro áreas elementales de AMI

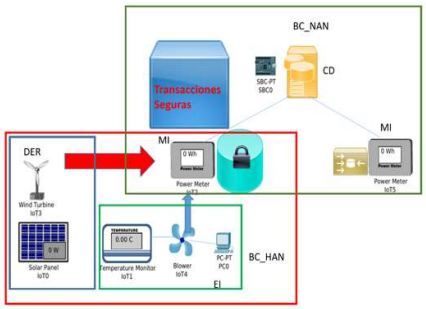

Fig. 3. Almacenamiento de datos general de la arquitectura de cadena de bloques propuesta

Todos los niveles en la arquitectura de almacenamiento de datos usan una cadena de bloques. En este caso, EI, MI, y CD tienen BD. De manera general los datos que se almacenan son los valores de la señal eléctrica, particularmente los registros de consumos y producción se guardan como transacciones en la cadena de bloques, más adelante en esta misma

sección se describen las estructuras de datos manejadas en cada capa. El siguiente nivel de la arquitectura está en FAN/WAN donde el CD resume los datos de cada WAN y por lo tanto requiere una mayor capacidad de almacenamiento.

Finalmente, en los servidores de la empresa eléctrica, los datos de todos los clientes se almacenan en una cadena de bloques que puede ser interoperable con otras empresas de servicios públicos.

3.2. Algoritmo prueba de eficiencia (PoEf) versión 2: Sistema de análisis de datos multinivel para SMI

Está basado en la arquitectura borde-niebla-nube descrita en la sección anterior. El nivel de borde está representado por EI, DER y MI. En la actualidad, los EI y DER rara vez se consideran porque no incluyen capacidades de hardware para procesar y almacenar datos.

Sin embargo, debido a las tendencias actuales en el desarrollo de dispositivos IoT, se considera que la introducción comercial de dispositivos EI con mayores capacidades de IoT, almacenamiento y procesamiento de datos proliferará durante la próxima década y, por lo tanto, es importante abordar la importancia de EI y DER, como parte de la arquitectura general. De manera similar, los MI incluyen regularmente una capacidad de almacenamiento BD embebida limitada y capacidades limitadas de procesamiento de datos.

El nivel de niebla está representado por CD que procesan datos en tiempo real obtenidos del MI. El nivel de nube está representado por MDMS y la infraestructura de TIC de todas las empresas de servicios públicos para almacenar y procesar macrodatos. La arquitectura propuesta se muestra en la Figura 4.

La arquitectura propuesta comprende cuatro áreas principales de comunicación de datos AMI (HAN, NAN, FAN/WAN, Head-End) en 3 secciones. La sección 1 es el nivel de borde. La sección 2 representa los niveles de niebla. La sección 3, compuesta por la cabecera, representa el nivel de nube.

Las áreas delimitadas por cuadrados representan cargas (E, EI, DER); los círculos

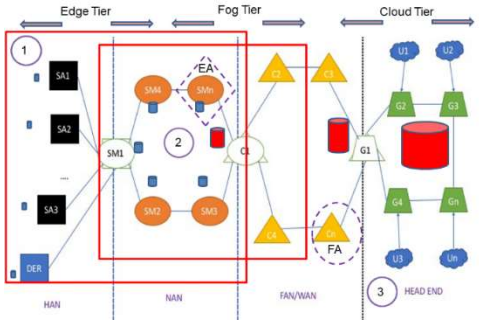

Fig. 4. Diagrama de alto nivel de la arquitectura propuesta

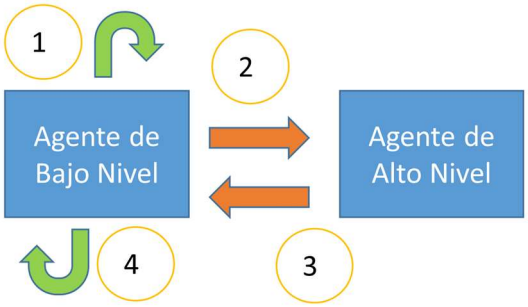

Fig. 5. El aprendizaje por reforzamiento en la arquitectura propuesta

representan MI, los triángulos representan CD, los cilindros representan BD, los trapezoides representan los Servidores Gateway (G) de la empresa de servicios públicos y las nubes representan las redes de comunicación de datos externas de las otras empresas de servicios públicos.

La Analítica en el Borde (EA por sus siglas en inglés) está representado dentro de cada MI y la Analítica en la Niebla (FA por sus siglas en inglés) está representado para cada CD. La comunicación de datos entre cada componente de la arquitectura se realiza a través de la misma red y protocolos de comunicación de datos.

El análisis de datos se realiza en el nivel más cercano. En la EA, el análisis de datos se realiza en línea utilizando la transmisión de datos para procesar diferentes aplicaciones de análisis de datos.

La arquitectura utiliza aprendizaje automático (ML, por sus siglas en inglés de Machine Learning) para calcular los nuevos parámetros de las

diferentes aplicaciones de análisis de datos de acuerdo con las capacidades computacionales utilizando Aprendizaje por Reforzamiento (RL, por sus siglas en inglés de Reinforcemnet Learning). Los agentes son los procesos que se ejecutan en los MI, CD y Servidores de la empresa eléctrica.

Los entornos dependen de las diferentes variables de cada aplicación de análisis de datos en la arquitectura propuesta.

Las acciones corresponden a las diferentes tareas para predecir, clasificar, actividades de aprendizaje. Constantemente, la arquitectura monitorea los diferentes estados de los algoritmos de análisis de datos.

Las recompensas son los valores que optimizan los diferentes algoritmos de análisis de datos en la arquitectura propuesta según las políticas.

Las políticas y las funciones de valor intentan minimizar o maximizar el rendimiento de la aplicación analítica de datos.

La arquitectura es flexible y cada nivel se puede utilizar como una variante de algoritmos para el análisis de datos. La Figura 5 muestra el procedimiento de aprendizaje.

El proceso comienza en el nivel inferior del Agente. El Agente en los niveles inferiores (Al) ejecuta sus aplicaciones de análisis de datos y evalúa su política (π) y la función de valor correspondiente (Vf) para estimar si el nuevo estado (S) tiene una mejor recompensa (R) usando sus parámetros locales.

A continuación, el Al emite una solicitud al Agente en el nivel superior (Au) preguntando sobre los parámetros globales de sus vecinos. En consecuencia, Au informa los parámetros a la Al que emitió la solicitud.

Finalmente, la Al ajusta sus parámetros de acuerdo con la nueva información y evalúa si los parámetros actualizados tienen una mejor recompensa.

Los niveles inferior y superior dependen del contexto actual de la aplicación de análisis de datos en la arquitectura. La combinación de niveles inferiores y superiores podría ser (SA / DER => MI), (MI => CD), (CD => CD) y (CD => G), que son los niveles inmediatos, pero todos los niveles están conectados directamente entre sí.

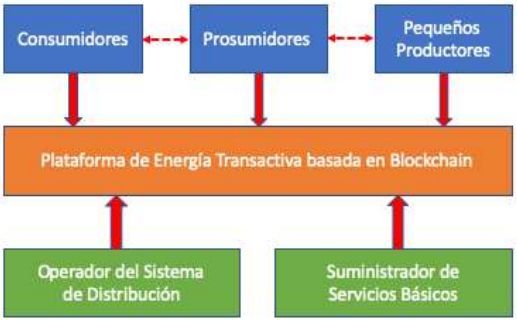

Fig. 6. Modelo Propuesto de Mercados Eléctrico Minorista Transactivo

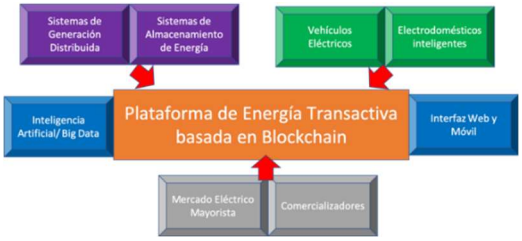

Fig. 7. Interfaces de la plataforma de energía transactiva propuesta

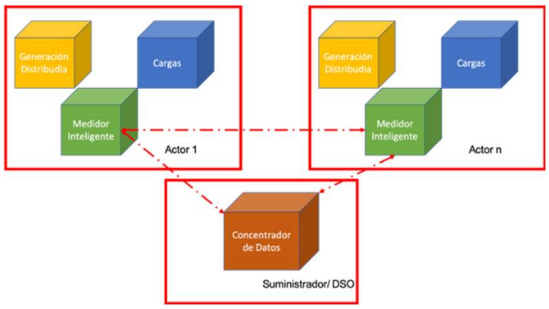

Fig. 8. Interacciones de la plataforma de energía transactiva propuesta

Por ejemplo, los MI (nivel de borde) son retroalimentados directamente por CD (nivel de niebla) e indirectamente por G (nivel de nube).

La segmentación de la arquitectura en niveles permite un mejor rendimiento de la analítica de datos de acuerdo con las capacidades de hardware de cada dispositivo, utilizando los datos cuando se necesitan en el momento que se requiera.

La plataforma de análisis de datos multinivel para SMI se probó para tres aplicaciones analíticas de datos: pronóstico del consumo de

energía, predicción de la calidad de la energía y predicción del robo de energía.

A continuación, se describen cada una de las aplicaciones.

3.3. Algoritmo prueba de eficiencia (PoEf) versión 3: Sistema transactivo de energía

Un modelo de Energía Transactiva (TE, por sus siglas es inglés) está compuesto por dos elementos: mecanismos de control y de mercado con el propósito de equilibrar dinámicamente la oferta y la demanda.

En la Figura 6 se muestra un modelo general de energía transactiva basado en mercados minoristas de electricidad. En donde además de los participantes tradicionales (incluyendo prosumidores) se encuentra la plataforma de energía transactiva.

La Plataforma de Energía Transactiva contiene además de componentes de la cadena de bloques dos elementos primordiales: un sistema de almacenamiento de datos masivos con su respectivo módulo de analítica de datos e interfaces de comunicación hacia otros componentes del mercado eléctrico no tan presentes en el mercado minorista como los comercializadores y agregadores más comunes en el mercado eléctrico mayorista, tal y como se muestra en la Figura 7.

En la Figura 8 se muestra de manera general la interacción de cada actor participante en el mercado eléctrico transactivo con sus componentes principales.

La 9 muestra una descripción detallada de la arquitectura TES en el dispositivo MI. En la parte inferior las tres partes mencionadas en el MG: Almacenamiento, Cargas y DER.

En el medio está la capa de software representada por la interfaz gráfica de usuario (GUI, por sus siglas en inglés) y el aprendizaje automático (ML) / analítica de datos (DA).

En la parte superior se encuentran los otros componentes principales de un TES, el Calendarizador y Temporizador, la interconexión con el operador de la red, y finalmente, el módulo de Comercialización de Energía responsable del registro de las transacciones de energía entre los prosumidores y otros participantes del mercado.

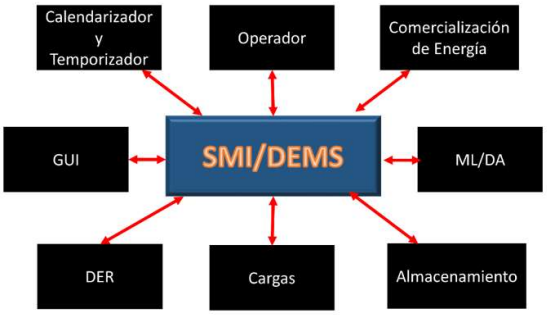

Fig. 9. Arquitectura TES en profundidad

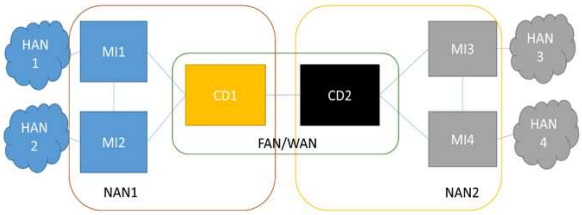

Fig. 10. La arquitectura implementada para las pruebas

Fig. 11. Arquitectura de hardware del MI

La idea general de TE es equilibrar los mercados regulados con la reducción de los picos y llenar los valles.

TE generalmente es un modelo complejo porque los mercados de energía incluyen muchas variables independientes y causalidades que son difíciles de modelar.

Esta complejidad se refleja en las tarifas eléctricas que son difíciles de entender para el prosumidor en la mayoría de los casos. Se simplificó este modelo para mejorar las tarifas

eléctricas y promover la eficiencia energética entre los prosumidores.

Conceptualizamos simplemente un TE como se describe en Ecuación 1:

$$TE = Señales\ Economicas + Incentivos - Costos. \quad (1)$$

4. Pruebas y resultados

En general, las cadenas de bloques garantizan la ciberseguridad en diversos campos como Confidencialidad, Integridad, Disponibilidad, privacidad, entre otros.

Para probar la arquitectura se diseñaron diversos escenarios de prueba tomando en cuenta que la implementación de la arquitectura propuesta se centra en los niveles NAN y FAN/WAN de AMI.

Los autores implementaron un SMI con cuatro SM y dos CD. Cada red NAN tiene dos MI. La Figura 10 muestra la arquitectura de cadena de bloques utilizada para las pruebas. Los dispositivos de las cuatro HAN son los mismos.

La arquitectura de hardware elegida para el MI es una Raspberry Pi Model 3b con la tarjeta de energía Smart Pi Sensor [35]. El hardware para CD es una PC con 4GB en RAM, un disco duro de 1TB y microprocesador Intel core i5 a 3.8GHz conectado a una red FastEthernet mediante cableado UTP-Cat6.

La selección de hardware se eligió basándose en pruebas previas que determinan la mejor SBC para un MI. En la Figura 11, se muestra el MI conformado por la integración del SBC Raspberry Pi y la tarjeta de energía SmartPi

El sistema de Blockchain se ha implementado en lenguaje Python utilizando PostgreSQL 8.4 en MI y CD. El algoritmo hash utilizado es SHA-256. El contenido de la transacción está cifrado con AES-128 y RSA de 1024 bits se usa para las firmas en PKI. La Figura 12 muestra el diagrama de bloques de la implementación de la cadena de bloques en NAN.

Además, la arquitectura se probó en un modelo CD Texas Instruments TMDSDC3359 y en un MI Texas Instrument EVM430-F6779 utilizando la biblioteca de energía y procesando datos en una placa Raspberry Pi.

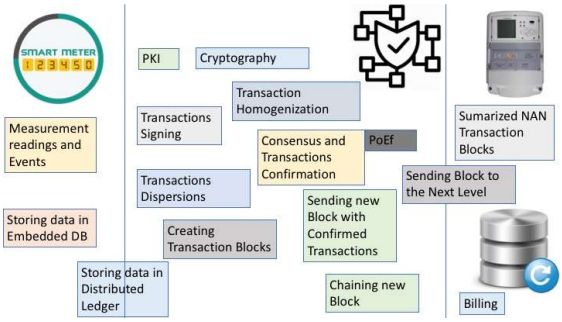

Fig. 12. Diagrama de bloques de la implementación de Blockchain en NAN

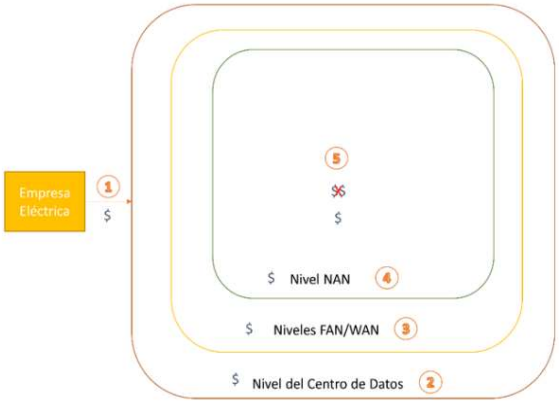

Fig. 13. Escenario de ataque de precio falso

Para MI legados, es necesario agregar una placa de módulo de expansión para expandir la memoria RAM y la tarjeta SD para ejecutar el sistema operativo Linux embebido con Python y BD embebidas.

Las comunicaciones utilizaron una VPN en cada capa de la cadena de bloques. De antemano, se usaron algunas herramientas de prueba de vulnerabilidades para verificar la ciberseguridad de todos los nodos.

4.1. Problemas generales de ciberseguridad en SMI

Para probar la manipulación de datos, se modificó en el MI2 una transacción que corrompe algunas lecturas. Todos los nodos, incluidos los coordinadores, pudieron verificar la manipulación de datos y evitar la transacción alterada.

En relación con la privacidad de los datos, en el libro mayor solo se almacenan el ID de los nodos:

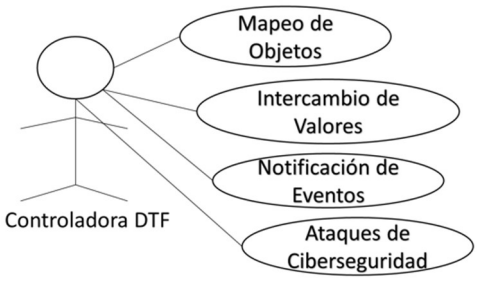

Fig. 14. Escenario de ataque de precio falso

EI, DER, MI y CD. Por lo tanto, la información es pseudoanónima y es tan segura como cualquier cadena de bloques.

Por confidencialidad, todos los nodos deben estar registrados en su coordinador y utilizar la infraestructura PKI para la firma de transacciones.

Solo las claves públicas/privadas correctas pueden acceder a la información. La disponibilidad de los datos se probó a través de un ataque DoS realizado nuevamente en los nodos de la cadena de bloques. Se comprobó que cuando al menos un nodo está disponible, los datos de la cadena de bloques podrían restaurarse.

Para probar la inyección de datos falsos, los autores diseñaron un escenario con ataques de precios en el nivel NAN de la cadena de bloques como se muestra en la Figura 13.

La empresa eléctrica envía un nuevo precio a la cadena de bloques (paso 1) y el precio se almacena en cada nivel (paso 2 al 4), por lo tanto, para manipular un precio de señal es necesario manipular todos los bloques de cada capa (paso 5). Los nodos siempre comparan su precio con sus coordinadores y descartan precios falsos.

La señal de precio se almacena en cada nivel de la cadena de bloques, para manipularla; es necesario modificar todos los bloques de la cadena de bloques. De manera general, la propuesta arquitectónica protege los datos de medición inteligente de manera adecuada.

4.2. Problemas generales de ciberseguridad en Blockhain

Para probar un ataque MitM, se utilizó un escenario simple en el que un nodo malicioso en el nivel NAN de blockchain quiere escuchar mensajes no autorizados. El nodo malicioso no puede escuchar ni escribir ninguna transacción debido a que no tiene las credenciales correctas para ingresar a la red de la cadena de bloques.

El ataque del 51% es un problema grave de ciberseguridad en cadenas de bloques. El algoritmo de consenso propuesto funciona con un consenso de mayoría simple y podría ser vulnerable a este tipo de ataque.

Para mitigar este ataque, la arquitectura propuesta ha implementado un sistema de alarmas para reportar transacciones de consumo/producción anormales. Estas alertas deben ser verificadas y analizadas para un mejor funcionamiento del sistema.

4.3. Problemas de ciberseguridad la arquitectura propuesta

El rol de coordinador de nodo es la parte más vulnerable de la arquitectura propuesta debido a su naturaleza centralizada. Por este motivo, es necesario saber cómo se detecta una falla de un nodo coordinador.

Las fallas en los nodos coordinadores se detectan si la validación de las transacciones no ocurre correctamente. Todas las transacciones son confirmadas por la mayoría de nodos y el coordinador.

Para probar la ciberseguridad en los nodos coordinadores, los autores propusieron un escenario en la cadena de bloques de nivel FAN/WAN donde el coordinador está atacando usando DoS. Los resultados obtenidos muestran que el rol de coordinador puede pasar al segundo coordinador sin problemas solo con un retraso en la confirmación de las transacciones.

4.4. Pruebas de rendimiento

Respecto a los gastos generales, lo más visible está relacionado con el espacio en disco. Un MI normal tiene un promedio de 100 bytes por transacción cada 15 minutos. Una transacción con blockchain de varios niveles en el nivel NAN implica 375 bytes por transacción. Esto es 3 veces más grande.

La sobrecarga en el procesamiento no es relevante debido a que el tiempo promedio en el algoritmo PoEf se redondea a 1 minuto en NAN y

1.5 minutos en FAN/WAN y el tiempo para los informes de AMI es de 15 minutos.

Sobre la escalabilidad, la arquitectura propuesta podría incrementarse utilizando más nodos. Los autores han comprobado con la simulación de procesos que más de 2,000 nodos MI (una cantidad común en AMI para cada CD) podrían funcionar en el nivel NAN sin problemas de rendimiento.

4.5. Problemas generales de ciberseguridad en usando Gemelos digitales

Recientemente ha surgido el concepto de Gemelos Digitales (DT, por sus siglas en inglés) que permite la interacción entre objetos físicos y virtuales, considerando un objeto virtual como una réplica del objeto físico permitiendo que ambos interactúen como si fuera uno solo.

DT trae enormes ventajas ya que el mundo físico interactúa de la misma forma con el mundo virtual, alterando cualquier cambio en la realidad de los dos mundos.

Para la realización de las pruebas, se utilizaron dispositivos electrodomesticos (cargas), así como dispositivos de microgeneración de energía eléctrica. Dado que es difícil tener una gran cantidad de dispositivos, los DT son una opción sumamente útil para esto.

Por tal motivo, se desarrolló un marco de trabajo para DT compuesto principalmente por un controlador DT. El DT Framework Controller (DTFC) se encarga de mapear objetos reales con su representación virtual, intercambiar valores entre DT, notificar eventos y alarmas entre todos los objetos y simular ciber amenazas y ataques.

La Figura 14 muestra los casos de uso descritos anteriormente del DTFC. En el caso de los electrodomésticos, se ha agregado un módulo de comunicación WiFi y procesamiento de variables eléctricas a través de un microcontrolador Arduino y sensores de corriente y voltaje.

Además, se han agregado un sensor de temperatura y un potenciómetro para controlar un aparato para encender o cambiar de velocidad. Para la implementación del sistema se modeló un DT de un MI, una plancha de 6 posiciones y una licuadora de 4 velocidades.

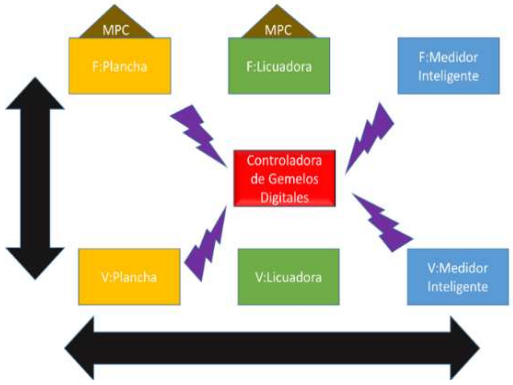

Fig. 15. Arquitectura del prototipo de DT implementado para las pruebas

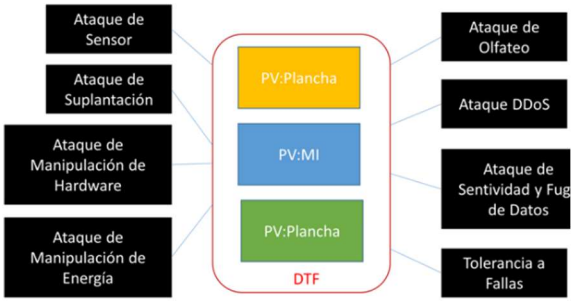

Fig. 16. Pruebas utilizando DT

La arquitectura del DT propuesto se muestra en la Figura 15. Se puede ver que hay seis objetos. Tres de los mundos físicos representados por la letra inicial P y que son la plancha, licuadora y un MI. Cada objeto físico tiene su componente virtual idéntico representado por la letra inicial V.

Los electrodomésticos en el mundo físico tienen un Módulo de Procesamiento y Comunicaciones (MPC), que permite mapear con su contraparte tangible a través del controlador DT.

El núcleo de la arquitectura es el controlador DT, que concentra información de objetos físicos con objetos virtuales para mapear cualquier cambio. La comunicación se realiza en ambos sentidos y con todos los objetos, tanto físicos como virtuales.

Se utilizó el formato de Notación de Objetos de JavaScript (JSON, por sus siglas en inglés) para mapear los datos. Aquí hay un ejemplo de mapeo de los datos de DT en el MI:

```
{
   ID: 0x0001,
   Name: "Smart_Meter",
   On: 0,
   Voltage: 1,
   Current: 2,
   Power: 3,
   Consumption: 4
}
```

Existen datos de identificación particulares y valores que representan cada uno de los datos. En el caso de un MI, la posición 0 del potenciómetro indica que el dispositivo está apagado, mientras que las otras posiciones indican variables de energía eléctrica que se quiere monitorear.

En el caso de la licuadora, los estados del potenciómetro indican las diferentes velocidades, mientras que en la plancha indican tipos de ropa para planchar. El calor de la plancha se monitorea con el sensor de temperatura.

Para cada objeto físico, es necesario un proceso de mapeo para obtener un objeto virtual. El objeto JSON representa un objeto virtual y el controlador DT puede agregarlo manualmente o descubrirlo.

La implementación del DT se realiza en python debido a su sencillez y alta portabilidad con otras plataformas. Cada objeto físico tiene configurada una dirección IP y se registra en el controlador mediante mapeo de datos. Una vez que se han producido los cambios, se muestran en la interfaz de DT y se reflejan en los objetos físicos y virtuales.

La comunicación entre objetos físicos es directa. No es necesaria una modificación en el sistema físico. En este caso, el SMI funciona con normalidad e interactúa con otro EI. La comunicación entre objetos virtuales se realiza directamente a través de la plataforma DT.

El controlador DT se encarga de comunicar los cambios de los objetos virtuales a los físicos y viceversa. Además, el controlador DT siempre supervisa la interacción entre los objetos físicos y virtuales y refleja los cambios.

La plataforma DT puede detectar algunas amenazas cibernéticas, como ataque de sensor, ataque de nodo de suplantación, ataque de manipulación de hardware, ataque de manipulación de energía, rastreo, denegación de servicio distribuido (DDoS), fuga de datos confidenciales y tolerancia a fallas. Cada tipo de amenaza se describe a continuación y cómo la plataforma DT puede ayudar a probar la ciberseguridad en un HI.

Tabla 2. Base de datos del medidor inteligente para grabar registros de Consumo y Producción

Marca de tiempo	Consumo (kWh)	Producción (kWh)
2019/04/11 10:00:00	0.109	0
2019/04/11 10:01:00	0.083	0
2019/05/10 09:59:00	0.116	0.054

Ataque de sensor

Cada dispositivo registrado en la plataforma debe registrar cada sensor. La plataforma DT registra los datos de los sensores de cada dispositivo en una base de datos histórica. La plataforma DT monitorea estos datos históricos y envía una alarma si el sensor tiene un comportamiento anómalo probable que pueda considerarse como un posible ataque.

Ataque de parodia (*spoof*)

Cada dispositivo registrado en la plataforma registra y toma una identificación única de la función de hardware. La plataforma DT monitorea esta identificación única de forma continua y evita un posible dispositivo de suplantación.

Ataque de manipulación de hardware

Cada dispositivo registrado en la plataforma debe verificar en su PCM un proceso de seguridad responsable de verificar todos los componentes de hardware si están conectados o desconectados.

Ataque de manipulación de energía

Similar al ataque de sensor, la plataforma DT monitorea el consumo histórico de cada dispositivo registrado. Si el consumo varía en un valor atípico, se envía una notificación al usuario.

Ataque de olfateo (*sniffing*)

La plataforma DT siempre monitorea la conexión de red de todos los dispositivos registrados, tanto físicos como virtuales. Cuando se detecta una nueva conexión, la plataforma DT registra la nueva conexión y notifica a los usuarios.

Tabla 3. Base de datos del MI para registro de predicciones de Consumo y Producción

Marca de tiempo	Predicción de consumo (kWh)	Delta de consume (kWh)	Predicción de producción (kWh)	Delta de produccion (kWh)
2019/04/11 10:00:00	0.115	0.06	0	0
2019/05/11 10:01:00	0.080	-0.03	0	0
2019/05/11 22:03:00	0.099	+0.11	0.066	-0.07
2019/05/12 09:59:00	0.116	-0.04	0.054	0.05

Tabla 4. Base de datos CD database para grabación de predicciones de consumo y producción en NAN

Marca de tiempo	SM_ID	Consumo predicho	Delta consumo	Predicción de producción	Delta de producción
2019/04/11 10:00:00	1	0.115	0.06	0	0
2019/04/11 10:00:05	2	0.094	-0.03	0.112	-0.02
2019/04/11 10:00:09	3	0.204	0.03	0	0
2019/04/11 10:00:13	4	0.149	0.04	0	0

La comunicación entre objetos físicos y virtuales se cifra mediante firmas RSA.

Ataque distribuido de denegación de servicio (DDoS)

La plataforma DT tiene un firewall integrado responsable de verificar las conexiones de red. Solo los dispositivos registrados, tanto físicos como virtuales, pueden conectar cada uno. La plataforma DT registra la frecuencia de comunicación de cada dispositivo y notifica a los usuarios del uso anormal.

Ataque sensible y de fuga de datos (SDL)

La plataforma DT solo permite que los dispositivos registrados y autorizados vean y exporten la información. La plataforma DT requiere otorgar permisos para acceder a datos sensibles.

Tolerancia a fallos

El cuello de botella en los sistemas centralizados es el proceso del servidor, en nuestro caso, el controlador DT. La plataforma DT puede conectarse con otros controladores DT como respaldo.

Cuando la plataforma DT detecta una falla, si existe un controlador DT auxiliar, el controlador auxiliar se conmuta como un nuevo controlador DT.

Los controladores DT auxiliares verifican la base de datos con toda la información actualizada. Se desarrolló un escenario de ciberseguridad para probar aspectos de ciberseguridad en HI.

El escenario de prueba está relacionado con la manipulación de datos de forma física y lógica. El escenario de prueba tiene en cuenta los diversos ataques y amenazas mencionados anteriormente en esta sección.

4.2 Robo de Energía

La principal aplicación de la parte analítica del algoritmo de consenso desarrollado es el monitoreo del robo de energía.

La medición del consumo y la producción de energía seda a una velocidad de 1 muestra por minuto y da como resultado una base de datos de 43,200 registros en el MI.

La Tabla 2 muestra un ejemplo de registros de base de datos obtenidos para consumo y producción de energía de un MI.

La metodología funciona de la siguiente manera: cuando se obtienen nuevos datos, se compara con los datos predichos y posteriormente se compara con los datos observados calculando la desviación del error y la tasa de aprendizaje mediante un proceso RL.

En esta aplicación de análisis de datos, los estados son Al y los diferentes Au.

Las acciones se clasifican o ajustan. Las recompensas son dos valores (1 ó -1) dependiendo de la función de valor que dan las métricas de error como una matriz de confusión (las clasificaciones correctas dan 1 recompensa, las clasificaciones incorrectas dan -1).

El entorno y las políticas mapean la transición entre Al y diferentes Au de acuerdo con las capacidades del hardware y los Vf (s). Por último, la función de aprendizaje se obtiene comprobando Al(s) con Vf (s) mediante la observación.

Los resultados obtenidos muestran que la arquitectura propuesta en esta aplicación analítica de datos puede aprender de manera efectiva debido a que el proceso de clasificación tiene una puntuación de 90.53% de casos correctos y con RL se mejoró a 98.17%.

Además, se utilizan dos repositorios de datos más en MI y CD para almacenar las predicciones y calcular el porcentaje de la diferencia entre los datos de consumo/producción de energía como se muestra en las Tabla 3 y la Tabla 4.

La Tabla 5 muestra los resultados de la predicción del Robo de Energía en comparación con las observaciones. Los valores en las predicciones de consumo y producción se expresan en porcentajes indicando los datos correctos clasificados.

La Tabla 6 muestra el número general de clasificaciones correctas e incorrectas en la detección de ladrón de energía en consumo y producción de energía. Los resultados son una media de 30 experimentos en los 4 MI.

Los resultados obtenidos muestran que la arquitectura propuesta en esta aplicación analítica de datos puede aprender de manera efectiva debido a que el proceso de detección de ladrones de energía tiene un puntaje general de producción/consumo de 88.16% de casos correctos y con RL se mejoró a 90.61%.

Tabla 5. Resultados CD en aplicación analítica de datos para predicción de robo de energía

SM_ID	Consumo predicho	Predicción de producción
1	88.35	93.12
2	89.12	92.15
3	87.23	92.63
4	90.01	92.27

Tabla 6. Matriz de confusión de detección de robo de energía

		Predicción	
		Positivos	**Negativos**
Observación	**Positivos**	19421	2009
	Negativos	2047	19723

5. Conclusiones

La medición de energía eléctrica y en general de cualquier sistema de medición es vital para la facturación y cobro de los servicios que se brindan. La correcta medición del sumistro eléctrico es fundamental para la confianza entre las empresas eléctricas y los usuarios finales.

En este sentido, la ciberseguridad de las transacciones y datos del SMI es sumamente importante para el éxito de los SMI. La introducción de cadenas de bloques a SMI en particular en AMI como un mecanismo de seguridad cibernética y confiable puede traer múltiples beneficios, siendo una de estas mitigaciones de manipulación de BD.

Para poder implementar la cadena de bloques en SMI, la cadena de bloques debe adaptarse a todas las capas de SMI, particularmente en lo que respecta a SMI y otros dispositivos de IoT que se administran en REI.

En este trabajo, se ha propuesto una arquitectura novedosa para SMI de diseño seguro utilizando cadenas de bloque. Esta arquitectura propone el uso de una cadena de bloques multinivel en SMI (HAN, NAN, FAN/WAN, centro de datos) utilizando un algoritmo de consenso ligero privado: Prueba de Eficiencia, que está optimizado para dispositivos IoT y de baja energía (limitados en recursos) pero también adaptable a otros dispositivos en SMI. Esta arquitectura propone el uso de BD en el MI que actualmente no es común.

La protección de datos se logra mediante el uso de una cadena de bloques de varios niveles y una estructura de datos simple que incluye el cifrado de las transacciones de energía.

La arquitectura propuesta podría usarse para la próxima generación de sistemas AMI porque incluye una ciberseguridad más sólida para la

manipulación de datos en las transacciones de energía.

Por otra parte, la próxima generación de aplicaciones para REI y SMI necesita un procesamiento analítico mejorado. Una solución posible y factible consiste en segmentar AMI en niveles para aumentar las capacidades de procesamiento, almacenamiento y comunicación.

Además, la velocidad y la granularidad de los datos también son importantes para procesar el análisis de datos de forma eficaz. La arquitectura propuesta en este documento mostró que la arquitectura borde-niebla-nube es una solución viable para aplicaciones de SMI que ofrece ventajas de procesamiento de datos mediante el uso de múltiples niveles.

La metodología resultante puede realizar análisis de datos para una variedad de aplicaciones en SMI. Los resultados sugieren que otros procesos relacionados con la producción, transmisión, distribución y consumo de energía pueden beneficiarse de la implementación de la arquitectura propuesta.

Además, este trabajo demostró que era posible implementar una arquitectura de SMI de varios niveles para el análisis de datos utilizando datos en tiempo real y en tiempo diferido.

La arquitectura propuesta es versátil y se puede utilizar para implementar diferentes procedimientos de formación y aprendizaje para el desarrollo de modelos en línea y fuera de línea capaces de adaptarse a diferentes entornos mediante el uso del aprendizaje por refuerzo.

Agradecimientos

Juan C. Olivares-Rojas agradece al Tecnológico Nacional de México por el apoyo brindado en la licencia beca-comisión para estudios de posgrado otorgado. Los autores agradecen al Tecnológico Nacional de México a través de los fondos de investigacion 3601.18-P, 6385.19-P, 8000.20-P, 10285.21-P y 13537.22-P.

Referencias

1. **Dilep, G. (2020).** A survey on smart grid technologies and applications. Renewable Energy, Vol. 146, pp. 2589–2625. DOI: 10.1016/j.renene.2019.08.092.
2. **Rokan, B., Kotb, Y. (2020).** Towards a real IoT-based smart meter system. Advances in Intelligent Systems and Computing, Vol. 1045, pp. 139–154. DOI: 10.1007/978-981-15-0029-9_11.
3. **Amara, A., Tamani, N, Ghamri-Doudane, Y, Islem, N. (2020).** Anomaly-based framework for detecting power overloading cyberattacks in smart grid AMI. Computers and Security, Vol. 96. DOI: 10.1016/j.cose.2020.101896.
4. **Secretaría de Energía (2017).** Programa de redes eléctricas inteligentes (PRODEREI). https://www.gob.mx/cms/uploads/attachment/file/250609/2017_Programa_de_Redes_El_ctricas_Inteligentes.pdf.
5. **Meng, W., Wolfgang, E., Wang, Q, Wang, Y., Han, J. (2018).** When intrusion detection meets blockchain technology: A review. IEEE Access, Vol. 6, pp. 10179–10188. DOI: 10.1109/ACCESS.2018.2799854.
6. **Hasankhani, A., Mehdi, S., Bisheh-Niasar, M., Shafie-Khah, M., Asadolahi, H. (2021).** Blockchain technology in the future smart grids: A comprehensive review and frameworks. International Journal of Electrical Power & Energy Systems, Vol. 129. DOI: 10.1016/j.ijepes.2021.106811.
7. **Agung, A., Handayani, R. (2020).** Blockchain for smart grid. Journal of King Saud University - Computer and Information Sciences, Vol. 34, No. 3, pp. 666–675. DOI: 10.1016/j.jksuci.2020.01.002.
8. **Agarkar, A., Agrawal, H., (2019).** A review and vision on authentication and privacy preservation schemes in smart grid network. Security and Privacy, Vol. 2, No. 2. DOI: 10.1002/spy2.62.
9. **Aitzhan, N. Z., Svetinovic, D. (2018).** Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous nessaging streams. IEEE Transactions on Dependable and Secure Computing, Vol. 15, No. 5, pp. 840–852. DOI: 10.1109/TDSC.2016.2616861.
10. **Mihaylov, M., Jurado, S., Avellana, N., Van-Moffaert K., Magrans, I., Nowé, A. (2014).**

NRGcoin: Virtual currency for trading of renewable energy in smart grids. 11th International Conference on the European Energy Market. pp. 1–6. DOI: 10.1109/EEM.2014.6861213.

11. **Helios (2022).** Helios Protocol. https://heliosprotocol.io/.
12. **Li, K., Yang, Y., Wang, S., Shi, R., Li, J. (2021).** A lightweight privacy-preserving and sharing scheme with dual-blockchain for intelligent pricing system of smart grid. Computers and Security, Vol. 103. DOI: 10.1016/j.cose.2021.102189.
13. **Kamal, M., Tariq, M. (2019).** Light-weight security and blockchain based provenance for advanced metering infrastructure. IEEE Access, Vol. 7, pp. 87345–87356. DOI: 10.1109/ACCESS.2019.2925787.
14. **Oprea, S. V., Bara, A., Andreescu, A. I. (2020).** Two novel blockchain-based market settlement mechanisms embedded into smart contracts for securely trading renewable energy. IEEE Access, Vol. 8, pp. 212548–212556. DOI: 10.1109/ACCESS.2020.3040764.
15. **Chen, S., Yang, L., Zhao, C., Varadarajan, V., Wang, K. (2020).** Double-blockchain assisted secure and anonymous data aggregation for fog-enabled smart grid. Engineering. Vol. 8. DOI: 10.1016/j.eng.2020.06.018.
16. **Gao, J., Omono, K., Bosteng, E., Smahi, A., Xia, Q., Xia, H., Zhang, X., Dong, G. (2018).** GridMonitoring: Secured sovereign blockchain based monitoring on smart grid. IEEE Access, Vol. 6, pp. 9917–9925. DOI: 10.1109/ACCESS.2018.2806303.
17. **Sompolinsky, Y., Zohar, A. (2018).** PHANTOM: A scalable BlockDAG protocol. http://diyhpl.us/~bryan/papers2/bitcoin/Phantom:%20A%20scalable%20block%20DAG%20protocol%20-%202018.pdf.
18. **Cebe, M., Erdin, E., Akkaya, K., Aksu, H., Uluagac, S., (2018).** Block4Forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles. IEEE Communications Magazine, Vol. 56, No. 10, pp. 50–57. DOI: 10.1109/MCOM.2018.1800137.
19. **Sharma, P. K., Chen, M., Park, J. H. (2018).** A software defined fog node based distributed blockchain cloud architecture for IoT. IEEE Access, Vol. 6, pp. 115–124, DOI: 10.1109/ACCESS.2017.2757955.
20. **Gu, J., Sun, B., Du, X., Wang, J., Zhuang, Y., Wang, Z. (2018).** Consortium blockchain-based malware detection in mobile devices. IEEE Access, Vol. 6, pp. 12118–12128. DOI: 10.1109/ACCESS.2018.2805783.
21. **Fan, M., Zhang, X. (2019).** Consortium blockchain based data aggregation and regulation mechanism for smart grid. IEEE Access, Vol. 7, pp. 35929–35940. DOI: 10.1109/ACCESS.2019.2905298.
22. **Yang, Q., Wang, H. (2021).** Privacy-preserving transactive energy management for IoT-aided smart homes via blockchain. IEEE Internet of Things Journal. DOI: 10.1109/JIOT.2021.3051323.
23. **Afzal, M., Huang, Q., Amin, W., Umer, K., Raza, A., Naeem, M. (2020).** Blockchain enabled distributed demand side management in community energy system with smart homes. IEEE Access, Vol. 8, pp. 37428–37439, DOI: 10.1109/ACCESS.2020.2975233.
24. **Zhang, S., Rong, J., Wang, B. (2020).** A privacy protection scheme of smart meter for decentralized smart home environment based on consortium blockchain. International Journal of Electrical Power and Energy Systems, Vol. 121. DOI: 10.1016/j.ijepes.2020.106140.
25. **GridPlus (2022).** Grid+. https://gridplus.io/
26. **PowerLedger (2022).** Powerledger. https://power ledger.io/
27. **Jiangsu Rongze Information Technology Co (2020).** Power system electricity consumption usage data statistics management system based on block chain. Patente CN111475581A, https://patents.google.com/patent/CN111475581A/en?oq=CN111475581+A.
28. **North China Electric Power University (2019).** Distributed generation energy

management method based on block chain double-chain structure. Patente CN111062596A, https://patents.google.com/patent/CN111062596A/en?oq=CN111062596+A.

29. **China Southern Power Grid Co Ltd Institute of Information Engineering of CAS (2019).** Block chain-based electricity consumption client credit management method and system. Patente CN110704531A, https://patents.google.com/patent/CN110704531A/en?oq=CN110704531+A.
30. **Chung Ang University Industry Academic Cooperation Foundation (2018).** Blockchain-based secure smart grid management system. Patente KR20200063623A, https://patents.google.com/patent/KR20200063623A/en?oq=KR20200063623+A.
31. **Timothy MAYNE, Serge UMANSKY (2017).** Method of matching renewable energy production to end-user consumption via blockchain systems. Patente US20190164236A1, https://patents.google.com/patent/US20190164236A1/en?oq=US20190164236+A1.
32. **International Business Machines Corp (2018).** Method or system for management of a device for energy consumption by applying blockchain protocol. Patente US20190353685A1, https://patents.google.com/patent/US20190353685A1/en?oq=US20190353685+A1.
33. **Accenture Global Solutions Ltd (2016).** Device, method and system for autonomous selection of a commodity supplier through a blockchain distributed database. Patente US20170206522A1,https://patents.google.com/patent/US20170206522A1/en?oq=US20170206522+A1.
34. **nD-enerserve GmbH (2022).** SmartPi, https://blog.enerserve.eu/category/smartpi/installation-smartpi/, Última consulta: enero 2022.

Article received on 24/01/2022; accepted on 18/04/2023.
Corresponding author is Juan C. Olivares-Rojas.