UNIVERSIDAD TÉCNICA DE MACHALA
UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

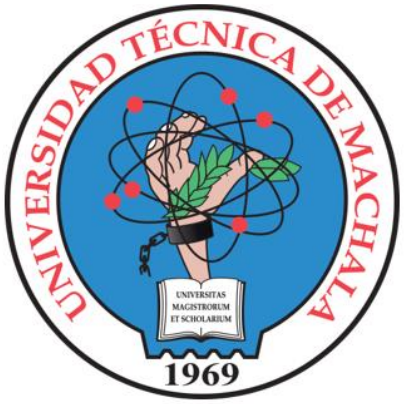
MAESTRÍA EN SOFTWARE

CONTROL DE ILUMINACIÓN IOT USANDO BLOCKCHAIN

ING. JOFFRE MANUEL AYALA MENDIETA

ING. DIXYS HERNANDEZ, PH.D.

MACHALA, FECHA



UNIVERSIDAD TÉCNICA DE MACHALA
UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

CONTROL DE ILUMINACIÓN IOT USANDO BLOCKCHAIN

ING. JOFFRE MANUEL AYALA MENDIETA

PROYECTO TECNOLÓGICO AVANZADO

TUTOR: ING. DIXYS HERNANDEZ, PH.D.

MACHALA, FECHA

DEDICATORIA

Dedico el presente con todo mi afecto trabajo a Dios, a mi madre Nancy, a mis hijos Lorena y Alejandro y en especialmente a mi querida Karen. Sin ellos este trabajo no habría sido posible. Su amor, apoyo y comprensión se han convertido en pilar fundamental de mi vida. Todo lo que he hecho, haga o haré en mi vida siempre será con profundo amor y con ferviente deseo de aportar en la vida de cada uno de ustedes.

Ing. Joffre Manuel Ayala Mendieta

AGRADECIMIENTO

Agradezco a Dios por haber permitido llegar a este especial momento de mi vida, por los triunfos y momentos difíciles que me han enseñado a valorarlo más y reconocer el valor que aporta en mi vida. A Karen por su afecto, apoyo y comprensión ante las dificultades que se han presentado a lo largo de estos años. A mi madre Nancy por ser quien me ha acompañado durante toda mi formación académica y de vida. A Eduardo y mi hermana María quienes con su consejos y apoyo me han guiado y apoyado para culminar mi formación académica y así cumplir con uno de mis objetivos. A mis compañeros de maestría, por su continua demostración de perseverancia y su ejemplo de superación continua sin desmayar ante los obstáculos que se puedan presentar. A todos los docentes que forman parte de la Maestría en Software de la UTMACH por haber compartido sus conocimientos de manera abierta y desinteresada. Mi especial agradecimiento a mi tutor y jefe de grupo de investigación Ing. Dixys Hernandez, phd por su apoyo, asesoramiento e inspiración para continuar con mi formación académica y enseñarme que los problemas que se presenten no son obstáculos, sino oportunidades de superación.

Ing. Joffre Manuel Ayala Mendieta

RESPONSABILIDAD DE AUTORIA

Declaro que lo realizado durante el proyecto ha sido generado mediante la indagación exhaustiva en la que se han citado las fuentes correspondientes. Las ideas, resultados y conclusiones son de responsabilidad del autor y fueron generadas tras el proceso investigativo y aplicación del proyecto.

JOFFRE MANUEL AYALA MENDIETA

Firmado digitalmente por JOFFRE MANUEL AYALA MENDIETA
Fecha: 2021.03.13 00:49:17 -05'00'

JOFFRE MANUEL AYALA MENDIETA

C.I. 0704877638

REPORTE DE SIMILITUD

Tesis maestria

INFORME DE ORIGINALIDAD

0%	0%	0%	0%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

Excluir citas	Apagado	Excluir coincidencias	Apagado
Excluir bibliografía	Apagado		

CERTIFICACION DEL TUTOR

Por medio de la presente apruebo que el trabajo de titulación titulado "Control de iluminación IOT usando Blockchain" del autor Joffre Manuel Ayala Mendieta, en opción al título de Master en Software, sea presentada al Acto de Defensa.

DIXYS LEONARDO HERNANDEZ ROJAS

Firmado digitalmente por DIXYS LEONARDO HERNANDEZ ROJAS
Fecha: 2021.03.13 00:53:25 -05'00'

Dixys Leonardo Hernandez Rojas

C.I: 0923026298

Machala, 10 de enero de 2021

CESIÓN DE DERECHOS

Yo, JOFFRE MANUEL AYALA MENDIETA, Declaro que estoy de acuerdo con ceder los derechos de autoría del presente trabajo investigativo a la Universidad Técnica de Machala. Cualquier uso ya sea total o parcial debe ser realizado con la autorización previa de la institución previamente mencionada.

JOFFRE MANUEL AYALA MENDIETA

Firmado digitalmente por JOFFRE MANUEL AYALA MENDIETA
Fecha: 2021.03.13 00:49:50 -05'00'

JOFFRE MANUEL AYALA MENDIETA

C.I. 0704877638

RESUMEN

El presente trabajo realiza la implementación de un sistema de internet de las cosas (IoT – Internet of things) con una arquitectura cliente servidor utilizando Blockchain para la seguridad en el almacenamiento de datos de un sistema de iluminación en entorno de laboratorio. Existen problemas de seguridad en IOT entre las que resaltan la vulnerabilidad de los datos en almacenamiento y transporte. Se han propuesto distintos métodos aplicados a seguridad, sin embargo, en los años recientes se ha promovido el uso de Blockchain aún por las características que estas plataformas proveen a los sistemas entre las que constan inmutabilidad de los datos, almacenamiento distribuido y encriptación de los datos. En el presente proyecto se utiliza una plataforma de Blockchain para asegurar el almacenamiento y transmisión de datos. Se ha seleccionado a IOTA como plataforma para tal objeto. Siguiendo la estructura de IOT, se establece un middleware que ha sido creado con NodeJS y el dispositivo IOT (Smart transducer) mediante el uso del lenguaje de programación C. Para el desarrollo del middleware se ha tomado un modelo monolítico con almacenamiento utilizando Blockchain, un Smart Transducer basado en Arduino que proporciona iluminación mediante un led con un sensor lumínico y la medición de desempeño y seguridad del sistema. Tras el análisis de los resultados, se concluye que el uso de Blockchain provee alta seguridad a un sistema IOT. Sin embargo, Se debe tomar en cuenta que el uso de recursos y tiempo de respuesta presentan retos a resolver.

Palabras clave: Blockchain, IOT, Seguridad de datos

ABSTRACT

This paper implements an Internet of things (IoT) system with a client-server architecture using Blockchain for the security of data storage in a lighting system in a laboratory environment. There are security issues in IoT among which stand out the vulnerability of data in storage and transport. Different methods applied to security have been proposed, however, in recent years the use of Blockchain has been promoted due to the characteristics that these platforms provide to the systems, among which are data immutability, distributed storage and data encryption. In the present project, a Blockchain platform is used to secure data storage and transmission. IOTA has been selected as the platform for this purpose. Following the IOT framework, a middleware is established which has been created with NodeJS and the IOT device (Smart transducer) by using C programming language. For the development of the middleware, a monolithic model has been taken with storage using Blockchain, an Arduino based Smart Transducer that provides illumination using a led with a light sensor and the performance and security measurement of the system. After the analysis of the results, it is concluded that the use of Blockchain provides high security to an IOT system. However, it should be noted that the use of resources and response time present challenges to be solved.

Keywords: Blockchain, IOT, data security.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Desde el inicio de su uso hasta la actualidad, la iluminación ha sido una prioridad para la humanidad. Esta garantiza que las personas puedan estar alerta del entorno que los rodea en todo momento brindado una sensación de seguridad. Dentro de los diferentes sistemas de iluminación existentes en la actualidad es de gran importancia poder diferenciar los de mayor relevancia existentes en la actualidad, los cuales son: iluminación pública e iluminación privada. Cada tipo de iluminación cumple un objetivo distinto para la sociedad, siendo el primero utilizado para iluminar los espacios públicos y el segundo con un espectro de usos muy amplio, entre los que se destacan la iluminación industrial y de hogares. Existen una constante que no puede dejarse de lado en cualquiera de los casos y es que existe un aumento progresivo del consumo eléctrico generado[1] . Este consumo eléctrico desmesurado por el continuo y amplio uso de la iluminación podría llegar a saturar los sistemas eléctricos. Por tal razón este debería ser controlado de manera automatizada para permitir una adecuada mitigación de problemas. Para tal motivo la comunidad científica oferta una solución mediante un control completo con el uso de un sistema de internet de las cosas (IoT) aplicado a la iluminación[2]. Recolectar los datos de consumo de esta resulta de especial importancia puesto que permite mantener un control sobre el uso y a futuro establecer formas de optimización del recurso.

Esta propuesta surge tras la proliferación de dispositivos con la capacidad de interactuar entre sí y ejecutar tareas de censado y manipulación de entorno. Estos dispositivos han traído a la vida una nueva forma de manejar los datos generados, esto es lo que se conoce como IOT [3]. En este campo es mucho lo que se ha realizado, pues abarca áreas del conocimiento muy diversas que van desde la agricultura, con proyectos de agricultura de precisión, hasta medicina y asistencia de personas con discapacidades físicas. Este avance se refleja claramente en los trabajos de Park [4], Yuan [5] y Huh [6] que utilizan el IOT con otros campos de conocimiento para resolver problemas de índole muy diversa. De esta manera

queda demostrado que IOT se ha establecido como una tecnología madura y por tanto viable para la solución del problema que se había planteado en la investigación.

A pesar de que los datos generados por los sistemas IOT son de alto valor y continen información sensible en muchos ámbitos, varios trabajos realizados en este campo no implementan un sistema de seguridad robusto. El acceso a estos es un objetivo de alto valor para los hackers alrededor de todo el mundo, pues expone información de las vidas diarias de los usuarios. Estas vulnerabilidades son muy visibles en el trabajo de Park [4], pues no se ha tomado en cuenta ningún tipo de seguridad para el sistema en sí mismo. El trabajo de Yuan [5] es otro ejemplo de este punto, pues se ha utilizado un middleware para proporcionar una incipiente seguridad del sistema. Sin embargo, no hay una adecuada identificación de los usuarios ni se toma en cuenta ningún framework para la seguridad IoT. Finalmente el trabajo de Huh [6] implementa un sistema de encriptado de datos basado en Ethereum, una plataforma de blockchain que permite brindar robustez y seguridad en el sistema. Incluso en este trabajo no se ha implementado ningún framework de seguridad. Quedó claro en trabajos posteriores que existen plataformas que no son óptimas para realizar estas tareas, tal como se demuestra con Ethereum[7], [8]. Queda determinado que existe inseguridad en varios aspectos dentro de IoT [9]. Esta se genera debido a que actualmente no existen dispositivos que estén en la capacidad de defenderse ante intrusiones o ataques de manera nativa [9]. Ante esta afirmación varias investigaciones se han desarrollado como una incipiente competencia alrededor del tema. Este tan importante asunto ha sido ignorado por la mayoría de productores de pequeño y mediano tamaño siendo adoptado únicamente por aquellas de alto rango y capacidad [10].

En el trabajo realizado por Mazzei [11] se asegura que la implementación de un sistema de Blockchain puede ser fácilmente adaptado a sistemas legados o sistemas nuevos sin ningún tipo de inconveniente. Blockchain también brinda grandes ventajas a sistemas de gran escala de IoT[12]. Pero surge una limitante para el uso de esta tecnología, y esta es la limitada capacidad de procesamiento que poseen los nodos de IoT [13].Por la misma razón no se puede realizar la implementación de protocolos de seguridad de alto consumo de recursos.

Es innegable que el uso de Blockchain facilita el mejoramiento de la seguridad y refuerza la filosofía de defensas en profundidad pero esta tecnología por sí misma no es suficiente, debe ser combinada con otros sistemas de seguridad [14]. Esto se debe a que existe un gran vacío en la seguridad que se requiere para las aplicaciones que funcionan en red [15]. La inseguridad en este tipo de sistemas llega incluso a mostrarse en el trabajo de Kolias [16] en el que se demuestra que existen formas en las que se puede utilizar IoT como una forma para atacar otras estructuras del mismo tipo.

Se debe tomar en cuenta la limitada capacidad que disponen los dispositivos IoT para la implementación de cualquier protocolo de seguridad. Por tal razón se utilizará como base la investigación de Dorri [17] y [13]. Es también importante tomar dentro de las limitaciones existentes en IoT las descritas por Chiang [18] en su trabajo. En este se consideran cinco restricciones para el uso de computación en la niebla aplicada a IoT: Latencia, ancho de banda, dispositivos con bajos recursos, interrupción de conexión al servidor y retos de seguridad actual. La presente investigación se realiza como continuación a la investigación de Chiang [18], principalmente basado en uno de los problemas de IoT identificado como falta de seguridad cuando se realizan operaciones en red [19]. Para tal objetivo se toman en cuenta los trabajos de Huh [6] en el que se desarrolló la plataforma Ethereum para implementaciones puntuales de domótica, cubriendo climatización e iluminación para IoT utilizando la plataforma Ethereum, en la investigación se tomó en cuenta únicamente ataques de tipo DoS y errores de sincronización. Por otra parte, en la investigación de Pavithran[7] se postula el uso de Hyperledge Fabric como la mejor solución tomando en cuenta los criterios de seguridad requeridos para IoT. También existe la alternativa de uso de Consortium Blockchain propuesta por Arif [8]. En conjunto con los trabajos anteriormente mencionado se toma en cuenta el de Lindgren [20], en el que se utiliza un sistema de hash pero que sin embargo no ha logrado obtener resultados eficientes en identificación end-to-end. Silvano [21] en un estudio más reciente postula que para comunicación maquina a máquina (M2M) la nueva tendencias es el uso de IOTA, debido a que este posee gran capacidad de transaccionalidad en comparación con otras tecnologías de Blockchain y además posee un costo cero para el intercambio de datos en una red descentralizada. Se busca a la vez de prevenir ataques utilizando Blockchain, poder detectar posibles intrusiones.

Basados en las afirmaciones de Minoli [14] la presente investigación utilizará la tecnología de Blockchain en un proyecto de iluminación por lo cual se tomará en cuenta el trabajo de Huh [6] para poder obtener mayor seguridad en IoT. La principal diferencia con el trabajo de Vinayakumar [22] es que se implementará una red de sensores inteligentes descentralizada sobre un sistema distribuido mediante Blockchain que garantizará la seguridad [15] como se demostró en el trabajo de Mirsky [23], Cui [24] y Santis [13].

En el trabajo de Ammar [25], mismo en el que se cubren diferentes frameworks utilizados para IoT, se destaca la eficiencia de varios de ellos en sistemas de seguridad. La presente investigación busca crear un sistema IoT utilizando Weave de Google en conjunción con un sistema de Blockchain implementado sobre IOTA. Tomando en cuenta también las diferentes formas de implementación propuestas por Dedeoglu [26].

Por lo anteriormente expuesto y con el incentivo de colaborar en combatir la obsolescencia como se estipula en el objetivo 3.7 del plan nacional de desarrollo [27] que exhorta al incentivo de producción y consumo responsable con el medio ambiente y a la meta establecida en el mismo objetivo que busca incrementar la productividad de tecnologías evitando la obsolescencia programática y con la finalidad de realizar un adecuado tratamiento de los datos generados [28] como dicta el artículo 66 numeral 19 de la Constitución de la República del Ecuador [29] se realizó la presente investigación que propone un sistema un control de iluminación IoT mediante la implementación de Blockchain para mejorar la seguridad con mira en la hipótesis de que el uso de Blockchain incrementa la seguridad de los datos en un sistema IoT comparado a métodos tradicionales y a su vez permitir que los procesos puedan ser realizados de manera autónoma o manual según sea el deseo del usuario. Para tal objetivo se creó un smart transducer (Mote), un middleware y una aplicación web. La aplicación web fue creada con arquitectura monolítica cliente servidor para el procesamiento de datos y ejecución de comandos de cambio en los actuadores con almacenamiento basado en Blockchain que permitirá comunicación mediante un Gateway para el tratamiento de los datos recolectados basado en REST-API con los motes, mismos

que poseen sensores lumínicos que permiten el censado de la luz ambiental y relays que permiten la gestión del suministro energético a las luminarias led.

La investigación se realizó en un ambiente de laboratorio tomando como objeto de estudio los medios de almacenamiento y seguridad de los datos. Tras la aplicación de las pruebas pertinentes se concluye que Blockchain en la plataforma IOTA brinda un alto nivel de seguridad en el almacenamiento y transporte de la información. Sin embargo, se debe tener en cuenta la alta latencia en la comunicación que implica la transferencia por lo que no es apto para un sistema en tiempo real. Se recomienda el uso de un almacenamiento intermedio para realizar lotes de transferencias periódicas basadas en la importancia de los datos.

La investigación se desarrolla en un total de 4 capítulos. El capítulo primero tiene como objetivo establecer el estado del arte de todas las tecnologías utilizadas para el desarrollo del trabajo de titulación. El capítulo segundo brinda una clara visión de todas las metodologías y materiales utilizados en el desarrollo del trabajo. En el capítulo tercero se da a conocer los resultados generados durante el proceso. Y finalmente en el capítulo cuarto se realiza la discusión sobre los resultados obtenidos con trabajos previos y se brinda un preámbulo de sugerencia para trabajos futuros.

CAPITULO I: MARCO TEÓRICO

En el presente capítulo se establecen los aspectos relevantes del marco teórico mediante la descripción de los antecedentes históricos en la sección 1.1, para posteriormente abordar los antecedentes conceptuales en la sección 1.2 y finalmente se detallarán los antecedentes contextuales de la investigación realizada.

1.1. Antecedentes Históricos de la investigación

Los antecedentes históricos permiten conocer a profundidad el objeto de estudio y establecer conocimientos fundamentales para la adecuada comprensión el proyecto. Es por tanto de vital importancia determinar una adecuada selección de preguntas de investigación que serán consultadas, el uso de una metodología de revisión bibliográfica de comprobada eficiencia y el estudio de fuentes bibliográficas con garantía de calidad técnica.

1.1.1. Preguntas de investigación

Se establecen preguntas de alto impacto para el proyecto a desarrollar, basado en la línea de investigación. Especificar adecuadamente las preguntas de investigación es la base de cualquier investigación ya que de estas dependen todos los resultados obtenidos durante la investigación y el análisis de los datos[30]. Son por tanto el eje que guiará la investigación. Ante las necesidades específicas establecidas para el presente proyecto se establecen las siguientes preguntas de investigación:

- ¿Qué problemas tienen los sistemas IoT en seguridad?
- ¿Cómo se puede mitigar los ataques?
- ¿Cuáles son las métricas utilizadas para medir las vulnerabilidades en IoT?
- ¿Blockchain ayuda optimiza la seguridad en IoT?
- ¿Cuáles son las características deseables de Blockchain aplicables a IoT?
- ¿Cuántas tecnologías de Blockchain se adaptan a las necesidades de IoT?

1.1.2. Proceso de Búsqueda

El proceso de búsqueda se ha realizado mediante la aplicación del método de revisión sistemática de la literatura para ingeniería de software propuesto por Barbara Kitchenham [30]. Dicho artículo ha sido ampliamente aceptado dentro del área de ingeniería de software y representa para el presente estudio la guía metodológica para la adecuada investigación. El uso de método anteriormente mencionado se obtiene garantía de calidad en los resultados.

El proceso de búsqueda se realizará mediante la investigación en fuentes ampliamente aceptadas en la comunidad científica. Por tal motivo se utilizarán revistas científicas de alto impacto y actas de congresos de relevancia.

1.1.3. Criterios de inclusión y exclusión

Los criterios de inclusión y exclusión sirven como un mecanismo de control para verificar que los resultados obtenidos dentro de la revisión sistemática de la literatura se mantengan apegados a las necesidades establecidas por el proyecto de investigación. Cada uno de los criterios debe ser cumplido por las publicaciones para formar parte importante del estudio.

1.1.3.1. Inclusión

Se establecen para el presente proyecto los siguientes cirterios de inclusión tomando en cuenta la línea de investigación, la periodicidad requerida para que un estudio sea valido y fuentes necesarias para garantizar que la información sea válida en el mundo científico.

- Estudios relativos a la seguridad en informática (Software y hardware)
- Estudios relacionados a la seguridad de la información.
- Publicaciones a partir del año 2015.
- Fuentes primarias únicamente (Artículos científicos y conferencias)

1.1.3.2. Exclusión

Los criterios de exclusión representan un segundo pilar para fundamentación. Estos ayudan a filtrar estudios de poca relevancia o que puedan resultar inentendibles para el investigador.

- Estudios no incluidos en las bases de datos seleccionadas
- Estudios duplicados
- Fuentes secundarias o terciarias
- Estudios no presentados en inglés o español

1.1.4. Grupo de control

Debido a su similaridad a la investigación presentada el grupo de control permite tener un eje fundamental para el desarrollo del proyecto y servirán como línea base para el aporte que se brindará. Cada uno de los artículos presenta aspectos relevantes para la investigación que pueden ser tomados en cuenta para tener una investigación de calidad.

- Xu, Z., Jiao, T., Wang, Q., Van, C. B., Wen, S., & Xiang, Y., 2019, An Efficient Supply Chain Architecture Based on Blockchain for High-value Commodities, International Symposium on Blockchain and Secure Critical Infrastructure, 1, 81-83.
- Zinonos, Z., Christodoulou, P., Andreou, A., & Chatzichristofis, S., 2019, ParkChain: An IoT Parking Service Based on Blockchain, International Conference on Distributed Computing in Sensor Systems, 15, 687-693.
- Mishra, S., & Tyagi, A. K, 2019, Intrusion Detection in Internet of Things (IoTs) Based Applications using Blockchain Technology, International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 3, 123-128.
- Koshy, P., Babu, S., & Manoj, B. S., 2020, Sliding Window Blockchain Architecture for Internet of Things, IEEE Internet of Things Journal, 7, 3338-3348.

1.1.5. Cadena de búsqueda

La cadena de búsqueda permite realizar la investigación en las diversas bases de datos científicos. La adecuada selección de una cadena de búsqueda es fundamental para tener una investigación exitosa. Se deben tomar en cuenta por tal motivo las palabras clave correspondientes al proyecto, las bases de datos científicas que serán consultadas y los criterios de inclusión y exclusión.

Ante lo expuesto se determina que la cadena de búsqueda se realizará sobre el título para mitigar la aparición de resultados que, aunque pueden resultar cercanos, no abarcan de manera profunda los tópicos de interés. Y tras el análisis de las bases de datos y criterios de inclusión y exclusión previamente establecidos se determina que la cadena de búsqueda como se muestra a continuación:

intitle:(blockchain IoT "security framework") site:(sciencedirect.com OR ieee.org OR springer.com OR acm.org OR mdpi.com)

1.1.6. Selección de estudios

Una vez realida la investigación con los parámetros establecidos previamente se realiza un segundo filtro a los resultados. Para la selección de los estudios de mayor relevancia se contemplaron las siguientes preguntas de validación.

a. ¿Se cumple con los criterios de inclusión y exclusión descritos como apropiados?
b. ¿Se cubren todos los estudios relevantes?
c. ¿Los revisores evaluaron la calidad y valides de los estudios incluidos?
d. ¿Fueron descritos los datos o estudios de manera adecuada?

1.1.7. Resultados de la revisión

Autores	Año	Título	Journal	Número	Páginas
Ibba, S., Pinna, A., Seu, M., & Pani, F. E.	2017	CitySense: blockchain-oriented smart cities	Scientific Workshops	17	44201
Khan, M. A., & Salah, K.	2018	IoT security: Review, blockchain solutions, and open challenges	Future Generation Computer Systems	82	395-411
Biswas, S., Sharif, K., Li, F., Nour, B., & Wang, Y.	2018	A scalable blockchain framework for secure transactions in IoT	IEEE Internet of Things Journal	6(3)	4650-4659
Lin, J., Shen, Z., Zhang, A., & Chai, Y.	2018	Blockchain and IoT based food traceability for smart agriculture	International Conference on Crowd Science and Engineering	3	44202
Scriber, B. A.	2018	A framework for determining blockchain applicability	IEEE Software	35	70-77
Noby, D. A., & Khattab, A.	2018	A Survey of Blockchain Applications in IoT Systems	Conference on Computer Engineering and Systems	14	83-87

Tsolakis, A. C., Moschos, I., Votis, K., Ioannidis, D., Dimitrios, T., Pandey, P., ... & García-Castro, R.	2018	A Secured and Trusted Demand Response system based on Blockchain technologies	Innovations in Intelligent Systems and Applications	-	-
Roy, S., Ashaduzzaman, M., Hassan, M., & Chowdhury, A. R.	2018	Blockchain for IoT security and management: current prospects, challenges and future directions	Conference on Networking, Systems and Security	5	44205
Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H.	2018	Blockchain technologies for the internet of things: Research issues and challenges	IEEE Internet of Things Journal	6	2188-2204
Lu, Y.	2019	The blockchain: State-of-the-art and research challenges.	Journal of Industrial Information Integration	15	80-90
McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D.	2019	Blockchain in healthcare applications: Research	Journal of Network and Computer Applications	135	62-75

		challenges and opportunities			
Gu, K., Wang, L., & Jia, W.	2019	Autonomous Resource Request Transaction Framework Based on Blockchain in Social Network	IEEE Access	7	43666-43678
Jindal, A., Aujla, G. S. S., Kumar, N., & Villari, M	2019	GUARDIAN: Blockchain-based secure demand response management in smart grid system	Transactions on Services Computing	13	613-624
Xu, Z., Jiao, T., Wang, Q., Van, C. B., Wen, S., & Xiang, Y.	2019	An Efficient Supply Chain Architecture Based on Blockchain for High-value Commodities	International Symposium on Blockchain and Secure Critical Infrastructure	1	81-83
Sargsyan, G., Castellon, N., Binnendijk, R., & Cozijnsen, P.	2019	Blockchain Security by Design Framework for Trust and Adoption in	IEEE World Congress on Services	2642	15-20

		IoT Environment			
Zinonos, Z., Christodoulou, P., Andreou, A., & Chatzichristofis, S.	2019	ParkChain: An IoT Parking Service Based on Blockchain	International Conference on Distributed Computing in Sensor Systems	15	687-693
Mishra, S., & Tyagi, A. K	2019	Intrusion Detection in Internet of Things (IoTs) Based Applications using Blockchain Technolgy	International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)	3	123-128
Gourisetti, S. N. G., Mylrea, M., & Patangia, H.	2019	Evaluation and Demonstration of Blockchain Applicability Framework	IEEE Transactions on Engineering Management	-	-
Wu, M., Wang, K., Cai, X., Guo, S., Guo, M., & Rong, C.	2019	A comprehensive survey of blockchain: From theory to IoT applications and beyond	IEEE Internet of Things Journal	6	8114-8154
Medhane, D. V., Sangaiah, A. K.,	2020	Blockchain-enabled	IEEE Internet of Things Journal	7	6143 – 6149

Hossain, M. S., Muhammad, G., & Wang, J.		Distributed Security Framework for Next Generation IoT: An Edge-Cloud and Software Defined Network Integrated Approach			
Seshadri, S. S., Rodriguez, D., Subedi, M., Choo, K. K. R., Ahmed, S., Chen, Q., & Lee, J.	2020	IoTCop: A Blockchain-based Monitoring Framework for Detection and Isolation of Malicious Devices in Internet-of-Things Systems	IEEE Internet of Things Journal	14	44210
Wu, Y., Dai, H. N., & Wang, H.	2020	Convergence of Blockchain and Edge Computing for Secure and Scalable IoT Critical			

		Infrastructures in Industry 4.0			
Hassija, V., Chamola, V., Garg, S., Dara, N. G. K., Kaddoum, G., & Jayakody, D. N. K.	2020	A blockchain-based framework for lightweight data sharing and energy trading in V2G network	IEEE Transactions on Vehicular Technology	69	5799 - 5812
Hu, J., Reed, M., Thomos, N., AI-Naday, M. F., & Yang, K.	2020	Securing SDN controlled IoT Networks Through Edge-Blockchain	IEEE Internet of Things Journal	-	-
Hasegawa, Y., & Yamamoto, H.	2020	Reliable IoT Data Management Platform Based on Real-World Cooperation Through Blockchain	IEEE Consumer Electronics Magazine	-	-
Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A.	2020	Integration of blockchain and cloud of things: Architecture, applications and challenges	IEEE Communications Surveys & Tutorials	-	-
Singh, M., Aujla, G. S. S., Singh,	2020	Deep Learning based	IEEE Transactions on	-	-

A., Kumar, N., & Garg, S.		Blockchain Framework for Secure Software Defined Industrial Networks	Industrial Informatics		
Sodhro, A. H., Pirbhulal, S., Muzammal, M., & Zongwei, L.	2020	Towards Blockchain-Enabled Security Technique for Industrial Internet of Things Based Decentralized Applications	Journal of Grid Computing	1	44210
Kumari, A., Gupta, R., Tanwar, S., & Kumar, N.	2020	A taxonomy of blockchain-enabled softwarization for secure UAV network	Computer Communications	161	304-323
Koshy, P., Babu, S., & Manoj, B. S.	2020	Sliding Window Blockchain Architecture for Internet of Things	IEEE Internet of Things Journal	7	3338-3348.
Ferrag, M. A., Shu, L., Yang, X.,	2020	Security and Privacy for	IEEE Access	8	32031-32053

Derhab, A., & Maglaras, L.		Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges			

Tabla 1 Resultados de la revisión bibliográfica.

Fuente: Autor

1.2. Antecedentes conceptuales

Los antecedentes conceptuales permiten obtener una vista clara de todos los aspectos abordados dentro de la investigación. En estos se declaran las hipótesis de investigación junto con el establecimiento de las redes de categorías de variables y la fundamentación teórica correspondiente a las mismas.

1.2.1. Hipótesis de la investigación

Tras el análisis de la literatura mostrada en la sección 1.1.7 se clarifica el panorama investigativo. Con las definiciones bien internalizadas combinadas con el estudio de las preguntas de investigación se posee suficiente claridad para las hipótesis. Para la presente investigación se establecen la hipótesis fundamental que guiará el desarrollo del proceso. Se establece también la hipótesis nula correspondiente a la planteada anteriormente. Esta será analizada tras la presentación y el análisis de los resultados obtenidos con la investigación realizada.

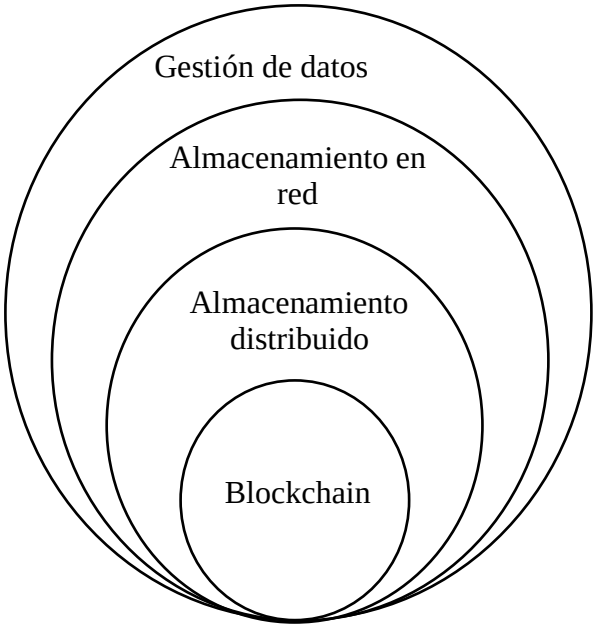
Ha: El uso de Blockchain incrementa la seguridad de los datos en un sistema de iluminación IOT.

Ho: El uso de Blockchain en un sistema IoT no incrementa la seguridad de los datos en un sistema de iluminación IOT.

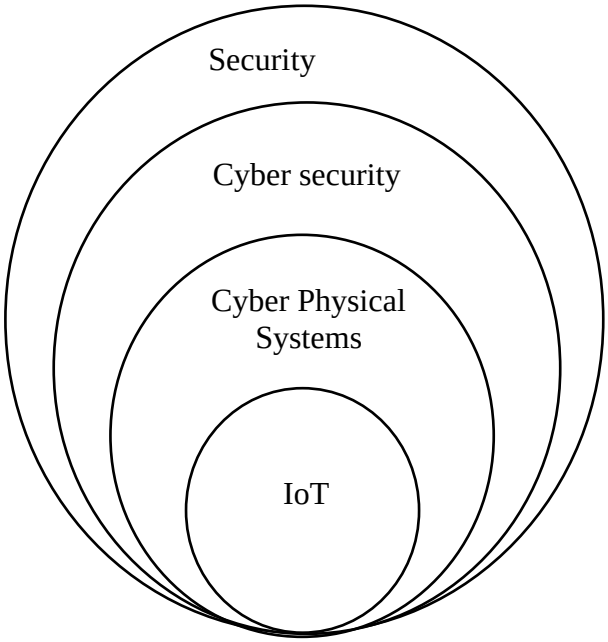
Para establecer como verdadera una u otra hipótesis estas fueron probadas durante la realización del proyecto. La validez de las hipótesis anteriormente mencionadas se muestra en el capítulo IV, discusión de resultados.

1.2.2. Red de categorías de las variables

Variable independiente



Variable dependiente



1.2.3. Fundamentación Teórica de la Variable Independiente

Para el presente estudio se ha considerado como variable independiente los métodos de almacenamiento.

Multiples alternativas se han considerado para el desarrollo del presente proyecto pasando desde las más tradicionales implementado bases de datos relacionales hasta bases de datos no estructuradas, en muchos casos incluso mediante el uso de ficheros planos o almacenamiento en memoria [31].

Se establece en la actualidad una nueva tendencia en almacenamiento. Para aplicaciones que requieran de un nivel de seguridad superior se propone el uso de almacenamiento distribuido sobre la nube. Dentro de estos se ha dado gran relevancia al uso de blockchain para garantizar la inmutabilidad de las transacciones [32].

1.2.3.1. Blockchain

Blockchain es una tecnología presentada por primera vez en 2009. Ha tomado gran relevancia en el mundo científico por su forma de almacenamiento que brinda características muy deseables. Blockchain permite el intercambio de valores sin la necesidad de una autoridad central [33][34] mismo que incluye aplicaciones distribuidas [35] o, en el caso específico del proyecto en desarrollo, redes IoT [36].

Blockchain es en estructura básica una base de datos descentralizada, distribuida , compartida e inmutable a través de la red[9][37]. Es manejada como una lista de registros expandible donde se puede únicamente agregar información al final [38]. Sin embargo requiere de un gran poder computacional debido a que requiere de un mecanismo de consenso que se basa en realizar múltiples operaciones matemáticas complejas [39][40][41].

Se demuestra también los beneficios de Blockchain en IoT en áreas muy variadas que van desde sistemas de cultivo agrícola hasta cuidados médicos [42][43] Llegando inclusive a la valoración de un total de 23 proyectos realizados con esta tecnología [44].

Tipos de Blockchain

Blockchain puede ser clasificada de por el acceso de usuarios a la red y por la privacidad de las transacciones realizadas dentro de las mismas. Cada una de ellas está subdividida en dos muy marcadas formas [45].

Por acceso de usuarios:

- Sin permisos: No requiere de autenticación o aprobación de ingreso a la red, es decir, cualquier usuario puede unirse e interactuar con la red sin restricción alguna.
- Permisionadas: Existe un filtro de ingreso para los usuarios. Permite determinar que qué usuarios pueden tener participación dentro del Blockchain.
-
- Por privacidad de transacciones:
- Publicas: Toda la información puede ser leída y usada sin restricción alguna.
- Privadas: Solo usuarios autorizados pueden acceder a la información del Blockchain.

Beneficios

Blockchain brinda múltiples beneficios que hacen muy apetecible su implementación en proyectos [46]. Debido a la naturaleza de los proyectos se debe verificar si alguno de los presentes beneficios es realmente requeridos, en caso contrario se podría optar por un método de almacenamiento alternativo [32].

- Transparencia: Los datos almacenados dentro del Blockchain son inmutables sin importar la situación que pueda presentarse. Esto brinda transparencia al registro de transacciones realizadas pudiendo considerarse como un registro de transacciones.
- Rastreabilidad: Dada la forma en la que se almacena la información dentro de la Blockchain siempre se puede saber el origen de la información revisando la composición de los bloques.
- Apertura: Se puede obtener la información requerida sin importar la ubicación debido a su naturaleza distribuida.

- Autonomía: Los sistemas de Blockchain son autorregulados, no requieren de ninguna entidad supervisora que gestione el almacenamiento o apruebe el mismo.

Generaciones

Muchos son los cambios sufridos por Blockchain desde su creación en 2009. Tan marcados han sido estos cambios que se pueden diferenciar un total de tres generaciones bien definidas en esta tecnología [47].

- Primera generación o Etapa de embrión: Caracterizada por las Criptomoneda y por su peculiaridad de ser de código abierto. Esta generación fue representada por BitCoin como principal exponente.
- Segunda generación o generación de contrato inteligente: Caracterizada por brindar plataformas de negocio y plataformas industriales con la habilidad de manejo de valores digitales. Su principal exponente fue Hyperledger.
- Tercera generación: Genera ecosistema de Blockchain mediante la creación de aplicaciones distribuidas, sistemas corporativos descentralizados autónomos y organizaciones autónomas distribuidas.

Soluciones tecnológicas con smart contracts y digital assets

Para poder ser aplicables al área de IOT se requiere de manera obligatoria que la plataforma soporte el uso de contratos inteligentes y de activos digitales. En la actualidad existen multitud de opciones para plataformas de Blockchain. Se establecen como las principales soluciones a Hyperledger, Eris, Stellar, Ripple, Tendermint y Ethereum [9] sin embargo hay contendientes tecnológicos nacidos en los años recientes tales como Xuperchain y Corda, e IOTA que fue diseñado específicamente para que sea altamente adaptable a las condiciones de un ambiente IOT [21].

Estructura de los bloques

En Blockchain cada una de las transacciones se encuentran embebidas en bloques que almacenan muchas de las mismas. El número de transacciones incluidas dentro de un bloque depende mucho de la transaccionalidad necesaria por el sistema o por las necesidades específicas de cada proyecto. Los bloques se encuentran estructurados de la siguiente manera [48].

- Hash: Hash generado por todas las transacciones almacenadas dentro del bloque que se ha creado.
- Marca de tiempo: Dato de tiempo de creación del bloque.
- Nonce: Llave única valida para una sola transacción.
- Transacciones: Datos almacenados dentro del bloque

Limitaciones

Como ha quedado demostrado anteriormente Blockchain brinda características muy deseables para sistemas altamente sensibles donde la seguridad de la información toma gran valor. Sin embargo, existen ciertas limitantes en la implementación de este tipo de plataformas [43] como se muestra a continuación:

- Falta de estandarización: Es una tecnología relativamente nueva e inmadura, por tal razón falta estandarización en la mayoría de las implementaciones.
- Fuga de privacidad en el almacenamiento estandarizado: Al ser descentralizado posiblemente pueden darse fugas de información.
- Manejo de llaves: El manejo de llaves puede ser comprometida por errores ya sean de programación o de los desarrolladores.
- Escalabilidad y sobre encabezados de IoT: En muchos casos las soluciones de Blockchain implican un ancho de banda exageradamente alto.

Plataformas

Nguyen [49] menciona mencionan las siguientes plataformas de Blockchain como sobresalientes

- Microsoft azure blockchain
- IBM Blockchain
- Amazon blokchain
- Oracle blockchain
- Hewlett-Packard
- Alibaba Blockchain
- Baido Blockchain
- Huawei Blockchain
- Google Blockchain
- SAP

Sin embargo cabe recalcar que existen ciertas plataformas que emergen en la actualidad que están específicamente diseñadas para IoT y con un costo de transacción cero [21].

1.2.4. Fundamentación Teórica de la Variable Dependiente

Para el presente estudio se ha considerado como variable dependiente la privacidad e integridad de los datos en una arquitectura en la nube.

La computación en la nube está siendo ampliamente adoptada pero es a su vez más vulnerable a las amenazas de seguridad, ya que comparte recursos físicos entre varios clientes utilizando la tecnología de virtualización. Esto sumado a que no posee una estandarización de tecnologías de encriptación[50]. Mucho se ha propuesto sobre temas de integridad y seguridad pero no se ha logrado determinar un método de almacenamiento que cumpla con todas las caracteristicas deseadas para la computación en la nube[51].

1.2.4.1. IOT

El internet de las cosas ha dejado de ser un termino novedoso para establecerse como una tecnología madura [52]. El internet de las cosas ha tenido un incremento significativo de presencia en el mundo actual[53]. IOT permite abordar ámbitos en multitud de áreas [54], incluyendo procesos tan delicados como juicios en tiempo real y cuidados médicos[55][56][57]. IoT se encuentra cada vez más vinculado a diferentes sistemas de alto impacto [58]. Al estar desplegado alrededor del mundo en sistemas tan diversos y numerosos se genera una gran cantidad de datos [59] que en muchos casos pueden resultar vitales.

Un aplicativo IoT está compuesto por diversos dispositivos heterogéneos que están embebidos entre actuadores y sensores interconectados en red que pueden ser utilizados en ámbitos domésticos e industriales [60][61]. Este tipo de dispositivos se generalmente conectan en redes de sensores inteligentes [62]. Los smart transducersse caracterizan por tener bajo consumo energético, una memoria muy pequeña y una capacidad de procesamiento baja que es compensada a través del uso de Gateways [9].

Arquitectura

IoT se divide en cuatro capas con las siguientes tecnologías [9]:

- Aplicación: HTTP, XML, JSON, RESTFUL, MQTTO, COAP, XMPP.
- Red y transporte: IPV4, IPV6, 6LOWPAN, RPL, TCP/UDP, TLS, DTLS, AERON, ROLL.
- Dispositivos físicos y comunicación: ZIGBEE, BLUETOOTH, WIFI, 4G/5G, LTE, VSAT, LORAWAN, NB-IOT, WEIGHTLESS, ETHERNET.
- Autenticación y manejo de llaves: OAYTH2, OPENID, OMA DM, LWM2M, TR-069, PKI

Arquitectura de red dirigida por software

Se establece como posibilidad de implementación de un entorno IOT el uso de una arquitectura de red dirigida por software (*Software driven network* - SDN) para aumentar la escalabilidad del proyecto y retirar la limitante de registro dependiente de un ente

regulador[63]. Este tipo de arquitectura cuenta con la siguiente estructura de dispositivos que interactúan en la red:

- Dispositivos iot: Interactuan con el ambiente y pueden intercambiar datos entre ellos.
- Hubs de iot: Conectan a los dispositivos IoT con los nodos de frontera.
- Switches SDN: Detecta cambios y ejecuta los planes de los controladores SDN.
- Agentes de Blockchain: Proveen el servicio de Blockchain.
- Nodos de frontera: Los nodos de frontera proveen servicio de cómputo y de almacenamiento.
- Controlador SDN: Realizan cálculos y buscan objetivos predefinidos.
- Arquitectura

La arquitectura tradicional se divide en la cinco capas, ver *figura 1*.

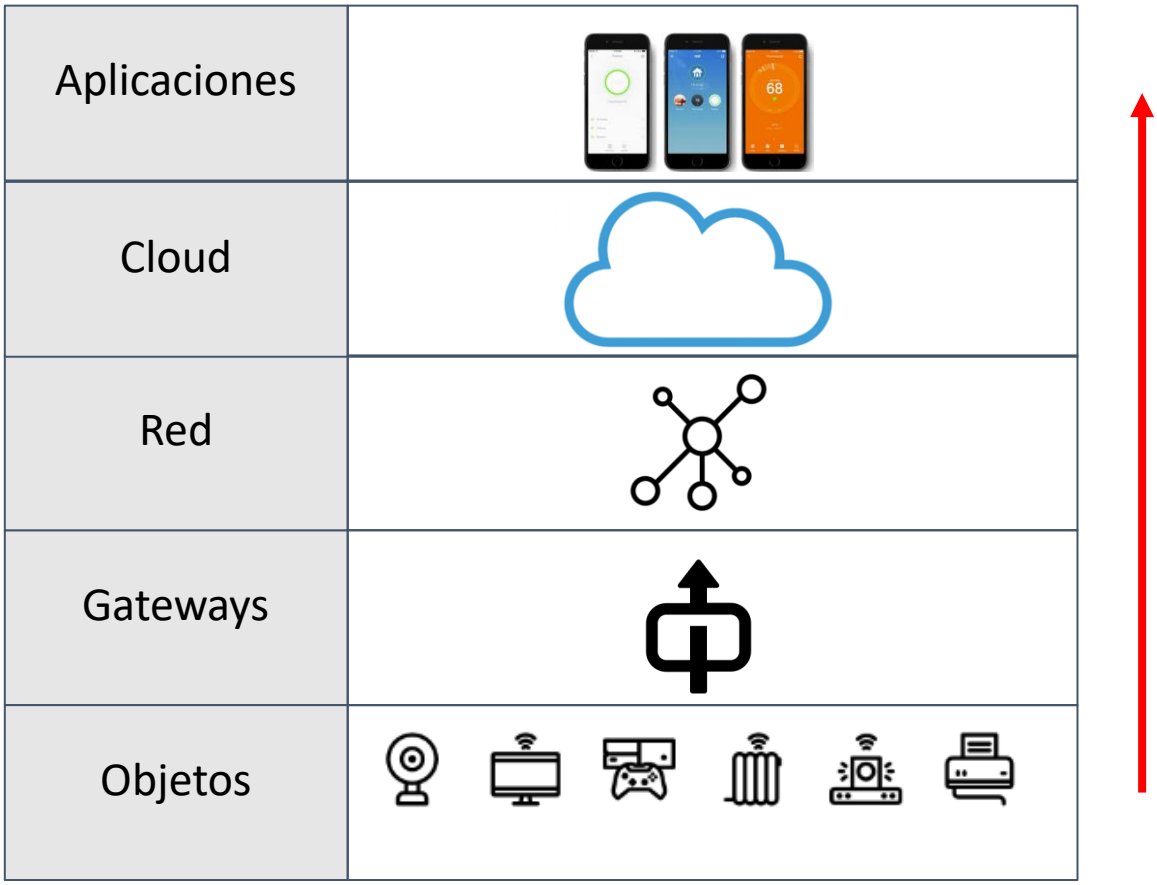


Figura 1 Capas de IoT

Fuente: Autor

Capa de objetos: Se encuentran los Smart transducers, dispositivos que recolectan información mediante sensores y cambian su entorno mediante actuadores. Estos generan los datos de valor en IoT.

Capa de Gateways: Cumple la función de interprete entre los objetos y la cloud. Recibe mensajes y los codifica dándoles formato y seguridad que sea aceptable para el servidor.

Capa de red: Capa en la que se transportan los datos, puede ser basada en diferentes protocolos.

Cloud: En ella se almacena la información y se generan las decisiones que tomarán los objetos a futuro basados en la misma.

Capa de aplicaciones: En esta capa se utiliza la información recolectada, ya sea para dar reportes, análisis, inteligencia de negocio, entre muchos otros usos.

Seguridad en IOT

Pese a ser utilizado de manera intensiva IOT posee severos problemas de seguridad entre los que se identifican 19 clasificados en cinco de riesgo de bajo nivel, diez de nivel intermedio y cuatro de alto nivel [9] [64].

Restricciones

IOT se compone de dispositivos heterogéneos pero todos comparten restricciones bien marcadas que se convierten en un reto al momento de intentar utilizar tecnologías altamente demandantes como Blockchain [58].

- Latencia: Los dispositivos IOT generalmente no poseen la capacidad de manejo de hilos, por lo que el tiempo de consenso, que suele variar de entre 3 hasta 10 minutos, puede llegar a bloquear la funcionalidad de los mismos.
- Aplicabilidad: Los dispositivos IOT son altamente heterogéneos por lo que muchos no podrán aceptar ciertos lenguajes de programación y ejecutar clientes de Blockchain.
- Restricciones de recursos: Debido a la baja capacidad de almacenamiento y procesamiento de los dispositivos IOT ejecutar las operaciones relacionadas a Blockchain es un reto.

1.3. Antecedentes contextuales de la investigación

La investigación se realiza para un sistema IOT para el control de iluminación en un entorno de laboratorio. Se estableció este como inicio para una cadena de investigaciones futuras que se desarrollaran basándose en los resultados obtenidos en la presente.

1.3.1. Delimitación del contexto del estudio

El estudio se realizará sobre un sistema de iluminación IoT para lo cual se realizaron las siguientes actividades:

- Implementar un sistema monolítico para servidor con almacenamiento o basado en Blockchain.
- Crear un mote basado en Arduino.
- Mesurar el desempeño y seguridad.

1.3.2. Propuesta de solución y contribuciones

Como se pudo notar en secciones previas IOT se toma como una tecnología madura que tiene vacíos fundamentales en la seguridad. Se han realizado investigaciones en años recientes para poder obtener confianza en el almacenamiento y transporte de la información pero aun queda un amplio camino por recorrer.

La presente investigación incide en los problemas de autenticación y comunicación, seguridad de transporte de punto a punto, establecimiento de sesión, violación de privacidad en IoT en la nube. Estos problemas se encuentran, como se puede apreciar en la *figura 2*, en las capas de red, Gateway y nube; y serán resueltos mediante el uso de IOTA.

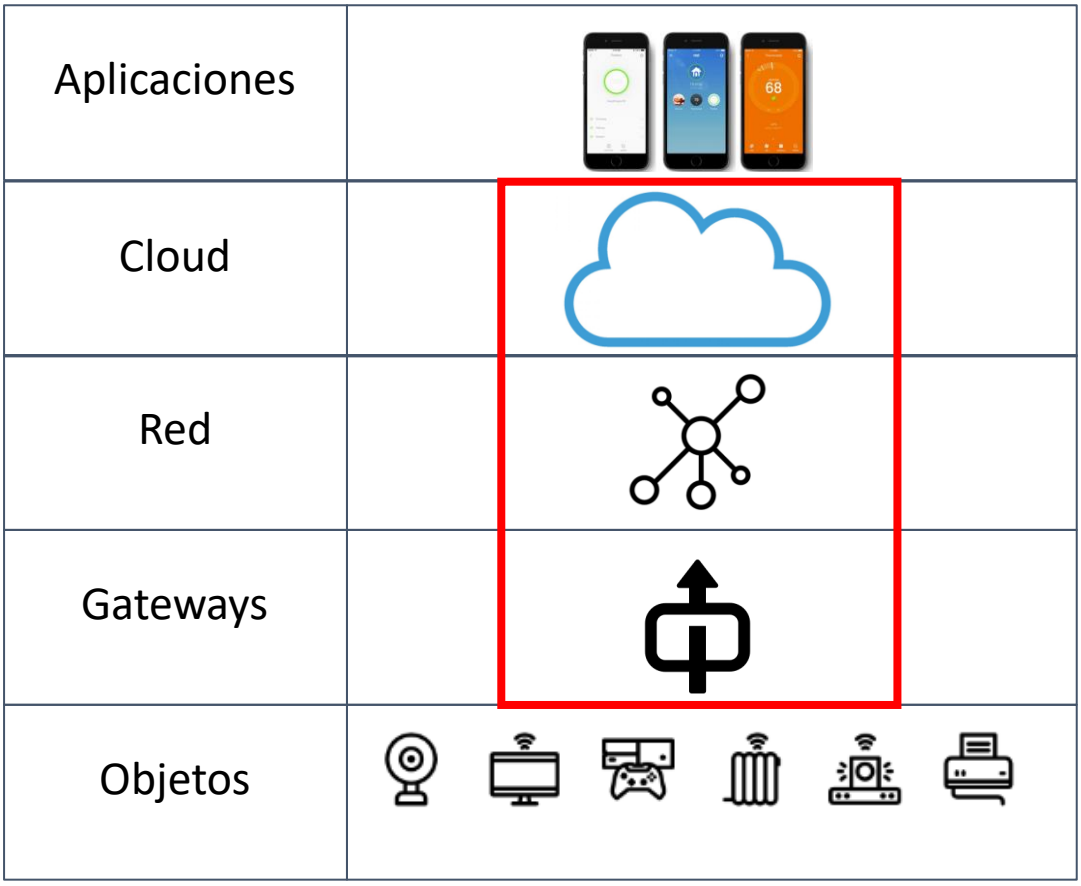


Figura 2 arquitectura de la propuesta.

Fuente: Autor

Por tal razón la presente investigación realizó la creación una arquitectura cliente servidor que implementó un sistema de Blockchain, en este caso IOTA, para la encriptación y seguridad en la transmisión y almacenamiento de datos en IoT, vea *figura 3*.

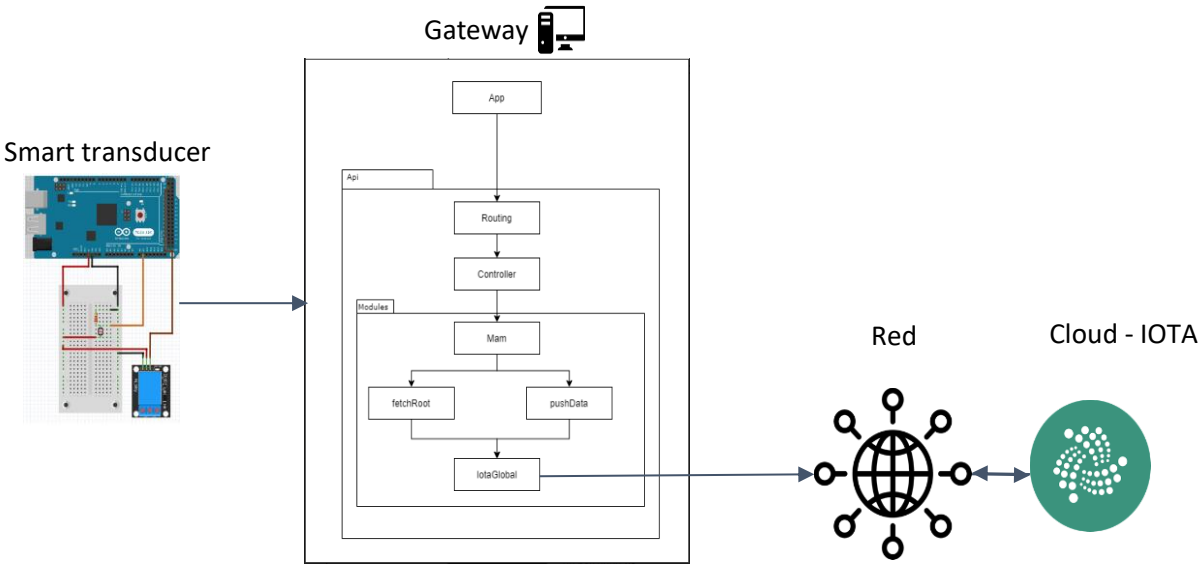


Figura 3 Arquitectura de control de iluminación

Fuente: Autor

1.3.3. Organización del documento

El presente documento se organiza en capítulo I en el que se presentará el marco teórico; capitulo II que establecerá la metodología y los materiales utilizados para el proyecto; capitulo III en el que se describirán los resultados obtenidos en el estudio Y el capítulo IV donde se realizará la discusión de los resultados obtenidos en el estudio realizado.

CAPITULO II: MATERIALES Y MÉTODOS

En el presente capítulo se describen de manera detallada los materiales y métodos utilizados para realizar la presente investigación mismos que podrían ser replicados en futuras investigaciones con temática similar a la presentada en el presente proyecto. En este se desarrollarán las secciones 2.1 tipo de estudio, 2.2 paradigma o enfoque desde el cual se realizó, 2.3 población y muestra, 2.4 métodos teóricos con los materiales utilizados. 2.5 métodos empíricos con los materiales utilizados y 2.6 técnicas estadísticas para el procesamiento de los datos obtenidos.

2.1. Tipo de estudio o investigación realizada

2.1.1. Experimental

Para poder realizar las mediciones de la variación de las variables se establece un modelo experimental, en el que se manipularán deliberadamente la transaccionalidad para verificar el comportamiento del Blockchain ante distintas situaciones. *(ver tabla 2)*.

Fase	Descripción
Baja transaccionalidad	Se genera una petición única y se mide el desempeño de la plataforma en una situación ideal.
Alta transaccionalidad	Se desarrollará una ronda de peticiones máximas para verificar el desempeño de la plataforma.

Tabla 2 fases de experimentación del proyecto.

Fuente: Autor

2.2. Paradigma o enfoque en el cual se realizó

2.2.1. Cuantitativo

Los resultados del presente proyecto de investigación se presentan de manera cuantitativa tomando en cuenta que los escenarios utilizarán como métrica la latencia, es decir, el tiempo transcurrido entre el envío de los datos y la recepción de los datos del servidor. Se puede apreciar en la *figura 4* los escenarios propuestos desde un nivel arquitectónico.

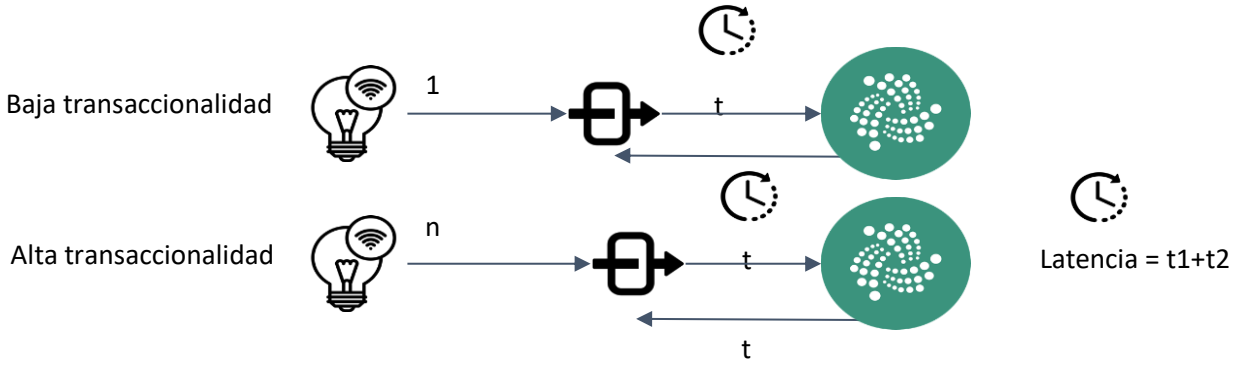


Figura 4 Escenarios y métrica.

Fuente: Autor

2.3. Cálculo de la población y muestra

La población a analizar será de un conjunto de datos enviados a través de siete smart transducers de IoT implementados sobre tarjetas electrónicas Arduino. Adicionalmente se analizará también un conjunto de dos Gateways implementados.

Al ser una población que aumenta con el tiempo, es decir, los mensajes siguen fluyendo entre los dispositivos de manera permanente, se ha determinado que la población es infinita. Se ha tomado como parámetros el 95% de confianza y 10% de margen de error, con tales argumentos se define la recolección de datos utilizando la fórmula de muestra en una población infinita (ver *figura 5)*.

$$n = \frac{z^2 * p * q}{e^2} = \frac{1.96^2 * 0.5 * 0.5}{0.1^2} = 96.04$$

Figura 5 cálculo de la muestra.

Fuente: Autor

2.4. Métodos teóricos con los materiales utilizados

Por la naturaleza del proyecto investigativo propuesto se utilizarán métodos de recolección y análisis de datos que sean adaptados para dispositivos electrónicos y que permitan verificar la transaccionalidad y la seguridad de los mismos. Por tal razón se han determinado los métodos y técnicas de recolección de datos que se muestran en la *figura 6.*

Figura 6 métodos y técnicas de recolección de datos.

Fuente: Autor

El seguimiento de datos transaccionales será realizado tras el envío de cada mensaje por parte de los dispositivos IOT (*smart transducers)* al Gateway que comunicará con la nube. El monitoreo de tráfico se realizará de manera continua durante todo el tiempo de ejecución del prototipo para analizar fluctuaciones en tiempos de entrega de los paquetes y revisar intentos de envío de paquetes por fuentes desconocidas. Adicionalmente también se ejecutarán artefactos con sensores que son los smart transducers de la red de sensores inalámbricos y proporcionan una serie de datos obtenidos mediante sensores y actuadores. Finalmente, también se ejecutará software a manera de middleware y motor de reglas simple.

2.5. Técnicas estadísticas para el procesamiento de datos observados

2.5.1. Experimento

Se establecen los escenarios de experimentación como se muestran en la *tabla 2, sección 2.1.1.* Para cada uno de estos escenarios se establecerá una infraestructura de red como de sensores. El almacenamiento de la infraestructura de red establecida variará en cada uno de los escenarios de prueba, manipulando la variable independiente para verificar el comportamiento de la variable dependiente.

2.5.2. Artefacto

Como parte del proyecto investigativo se desarrollará tres artefactos entregables. El primero es el software correspondiente a los Gateways sobre un computador de escritorio. El segundo es el firmware de los smart transducers basados en Arduino.

2.5.3. Prototipo

Se realizará un prototipó electrónico con tarjetas Arduino, mismo que contendrá un sensor para poder realizar el levantamiento de los datos y un actuador que cambiará acorde a las mediciones.

2.5.4. Recolección de datos

La recolección de datos se realizará en la red de área local (LAN) y en internet (WAN) ver *figura 7*. Para establecer métricas de seguridad se realizará un análisis de paquetes enviados.

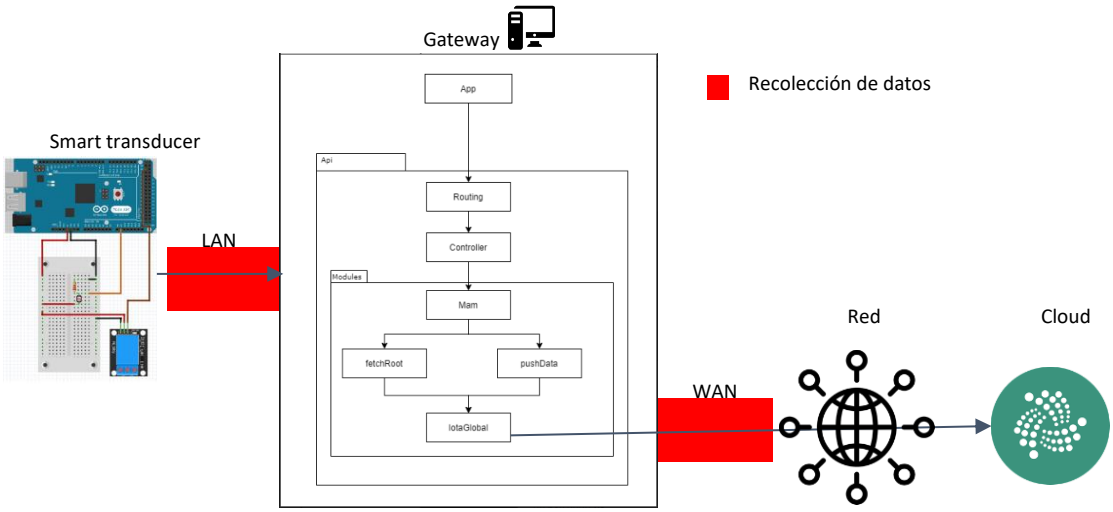


Figura 7 Escenario de recolección de datos.

Fuente: Autor

2.5.5. Herramientas utilizadas

Se utilizarán un conjunto de herramientas con propósitos bien establecidos. RStudios se utilizará para análisis de datos. Wireshark para análisis de paquetes. Jmeter para pruebas de carga y postman para envío y recepción de paquetería ver *figura* 8.

Figura 8 herramientas de recolección y análisis de datos.

Fuente: Autor

2.6. Técnicas estadísticas para el procesamiento de datos obtenidos y Medidas de tendencia central

Para el análisis estadístico se utilizan medidas de tendencia central para caracterizar el comportamiento de las variables previa manipulación y de esa manera poder obtener resultados concluyentes. De esta manera se tomarán en cuenta los valores obtenidos de la latencia de las comunicaciones.

CAPITULO III: RESULTADOS

En el presente capítulo se describen de manera detallada los productos generados en el proyecto investigativo. Se iniciará con la descripción del proceso de selección del Blockchain, seguidamente se realizará la estructura del Gateway en la sección 3.2, posteriormente se describirá la creación de los smart transducers en la sección 3.3 y finalmente se describirán las pruebas realizadas en la sección 3.4.

3.1. Selección del Blockchain

En el mercado actual existe varias plataformas de Blockchain pero pocas son adaptables a IOT. Se requiere que la tecnología seleccionada cuente con capacidades de realizar contratos digitales y digitalización de activos.

Tras un exhaustivo análisis de la literatura se ha podido realizar un resumen gráfico para la mejor comprensión de las distintas tecnologías de Blockchain existente. Estos pueden resumirse en dos aspectos importantes: Tiempo en el mercado, lo que establecería madurez de la tecnología; y adaptabilidad a IOT, mediante la seguridad de red y adaptabilidad a este tipo de tecnología.

Se muestra en la línea de tiempo (ver figura 9) que existen tecnologías muy variadas que se han desarrollado en el área de Blockchain durante los últimos años, algunas de las cuales se consideran inmaduras por su corto periodo en el mercado, sin embargo tienen prestaciones de alto impacto para IOT.

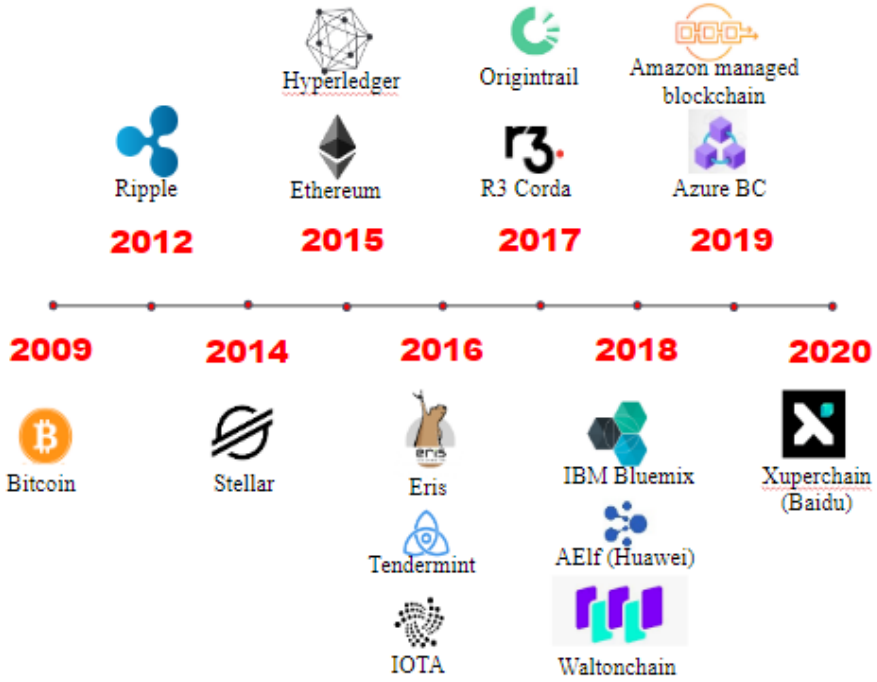


Figura 9 Línea de tiempo de Blockchain

Fuente: Autor

Existe también, adicionalmente a la madurez de las tecnologías, la adaptabilidad de las plataformas a proyectos de IOT basados en su capacidad de brindar diferentes funcionalidades de alta utilidad para este tipo de proyectos, tales como contratos inteligentes, digitalización de activos y que tantos recursos requieren para un correcto funcionamiento ya que IOT tiene la limitante de dispositivos con capacidades limitadas. También se toma en cuenta la seguridad en red que ofrecen y la capacidad de establecer una privacidad de distintos niveles para las transacciones realizadas dentro de la plataforma y el sistema criptográfico utilizado para las comunicaciones entre el cliente y el servidor. Todos estos aspectos han sido resumidos en la capacidad que tienen las plataformas de adaptarse a IOT (ver figura 10) para facilitar la selección de una plataforma.

.

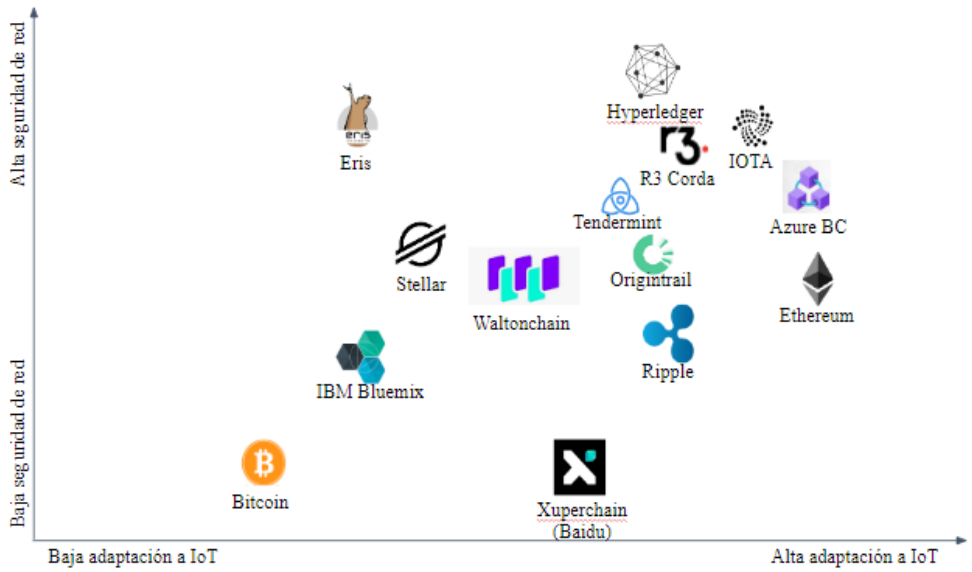


Figura 10 capacidad de plataformas aplicadas a IOT

Fuente: Autor

Los claros contendientes para uso dentro de IOT son R3 de Corda, Hyperledger, en sus versiones de Fabric y Sawtooth e IOTA. Para la selección se ha tomado finalmente un criterio fundamental para la naturaleza del proyecto, la transaccionalidad y costos de envío. La transaccionalidad del proyecto de la forma y naturaleza en la que fue concebido es muy alta, y requiere por tanto un sistema que permita realizarlas de manera rápida con un mecanismo de consenso que permita esta facilidad. El segundo factor, costo de transacciones se determina como fundamental puesto que al ser un proyecto IOT está diseñado para ser escalable, por tal motivo al escalar en dispositivos, también escalan los costos de transacciones hacia el Blockchain.

Se ha seleccionado como tecnología a utilizar durante el desarrollo del proyecto a IOTA, ya que esta tiene una velocidad de transacción alta debido al sistema de consenso que aplica y además posee un costo cero de transacciones, haciéndolo ideal para el proyecto en cuestión.

3.2. Diseño arquitectónico del proyecto

El proyecto consta de un smart transducer basado en Arduino que conforman la red local, esta red se conecta con un middleware ejecutado sobre un Servidor. El middleware se encarga de interpretar los datos, encriptarlos y enviarlos al Blockchain (ver *figura 11)*.

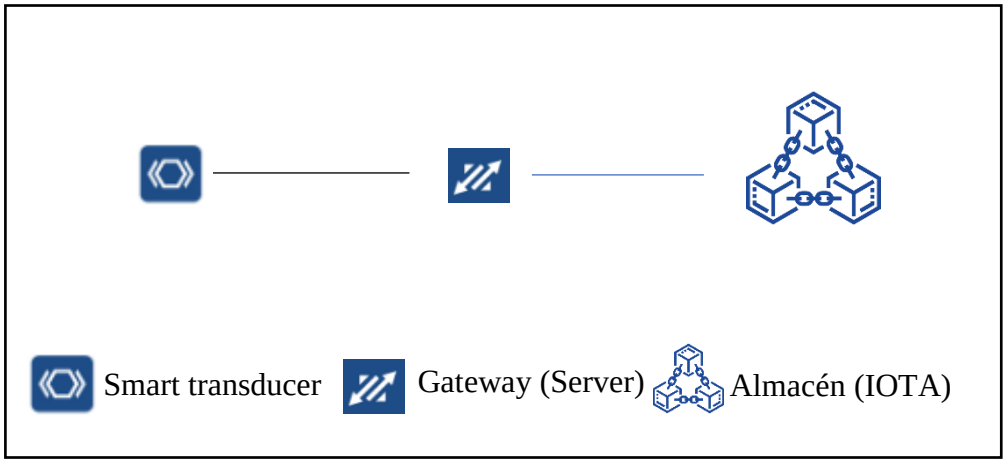


Figura 11 infraestructura de red experimental.

Fuente: Autor

3.3. Gateway

El Gateway ha sido construido de manera monolítica con la arquitectura modelo vista controlador. Establece comunicación con internet y con los smart transducers mediante un REST API. A continuación se lo describe utilizando el modelo "4+1" que brinda las vistas lógicas, de desarrollo, de proceso y física del sistema, tal como fue propuesto por Philippe Kruchten [65].

3.3.1. Vista lógica

El Gateway se encuentra construido con seis clases que permiten realizar las operaciones necesarias para el correcto funcionamiento del mismo *(ver figura 12)*. La clase app instancia express como framework para el middleware y se encarga también de gestionar el puerto de conexión del API REST, mismo que puede estar definido por el entorno o direcciona al puerto 6001 en caso de no existir. Utiliza también la clase Routing para las request que llegen al servidor. Routing a su vez establece las rutas a tomar para las diferentes rutas URL ingresadas por los clientes y las redirige a la función correspondiente en la clase Mam. Mam se encarga de gestionar los métodos que se utilizarán. Mam cumple la función de biblioteca de métodos y clases, permitiendo de esta manera centralizar el direccionamiento que llevará a PushData o a Fetch Root. FetchData se encargar del envío de datos hacia IOTA utilizando el input enviado por el usuario y convirtiendo estos mensajes a trytes. FetchRoot se encarga de la lectura de datos dentro de IOTA utilizando para esto la raíz que provee el usuario en su petición. Las clases FetchRoot y PushData utilizan para su funcionamiento la clase IotaGlobal. IotaGlobal contiene los parámetros de conección al Blockchain, incluyendo credenciales, direcciones IP, raíz y brinda también una instanciación del cliente de IOTA, mismo que es requerido por todas las acciones que vayan a realizar alguna interacción con el mismo. También posee la funcionalidad de actualizar el objeto cliente de IOTA con un fichero almacenado dentro del servidor para garantizar la estabilidad y permanencia de los datos dentro del servidor.

Se debe recordar que IOTA utiliza el algoritmo de árbol de Merkle y por tanto, el estado del objeto es de especial importancia para todas las transacciones de escritura a realizar dentro del sistema.

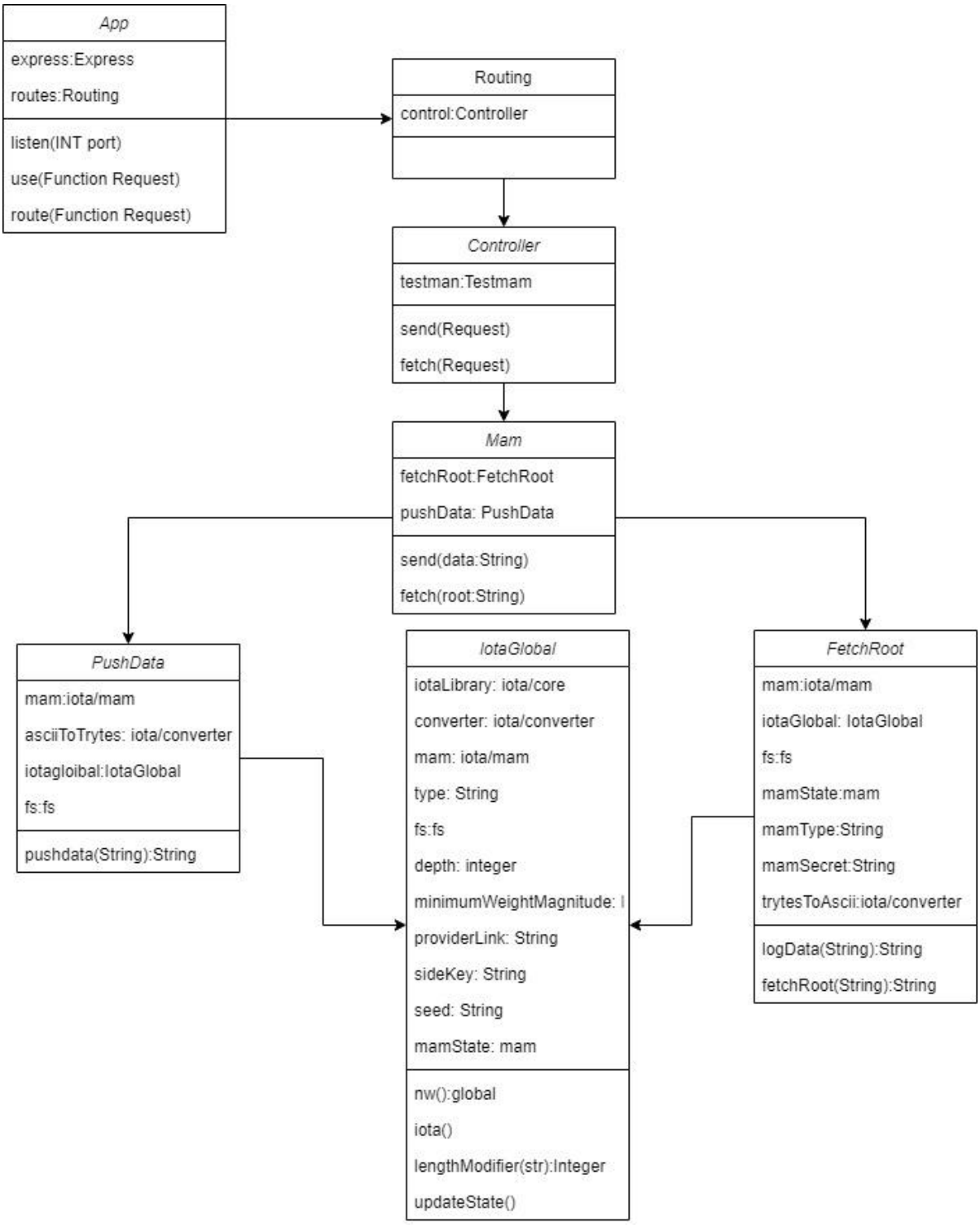


Figura 12 Diagrama de clases del Gateway.

Fuente: Autor

3.3.2. Vista de Desarrollo

Como se mencionó al inicio de la sección, el middleware ha sido desarrollado con una arquitectura basada en modelo vista controlador de manera monolítica. Las clases por tanto cumplen un rol específico en el funcionamiento del software, siendo vista establecido por la clase app; controlador está conformado por las clases Routing y Controller y modelo está conformada por Mam, FetchRoot, PushData, y IotaGlobal*(ver figura 13)*.

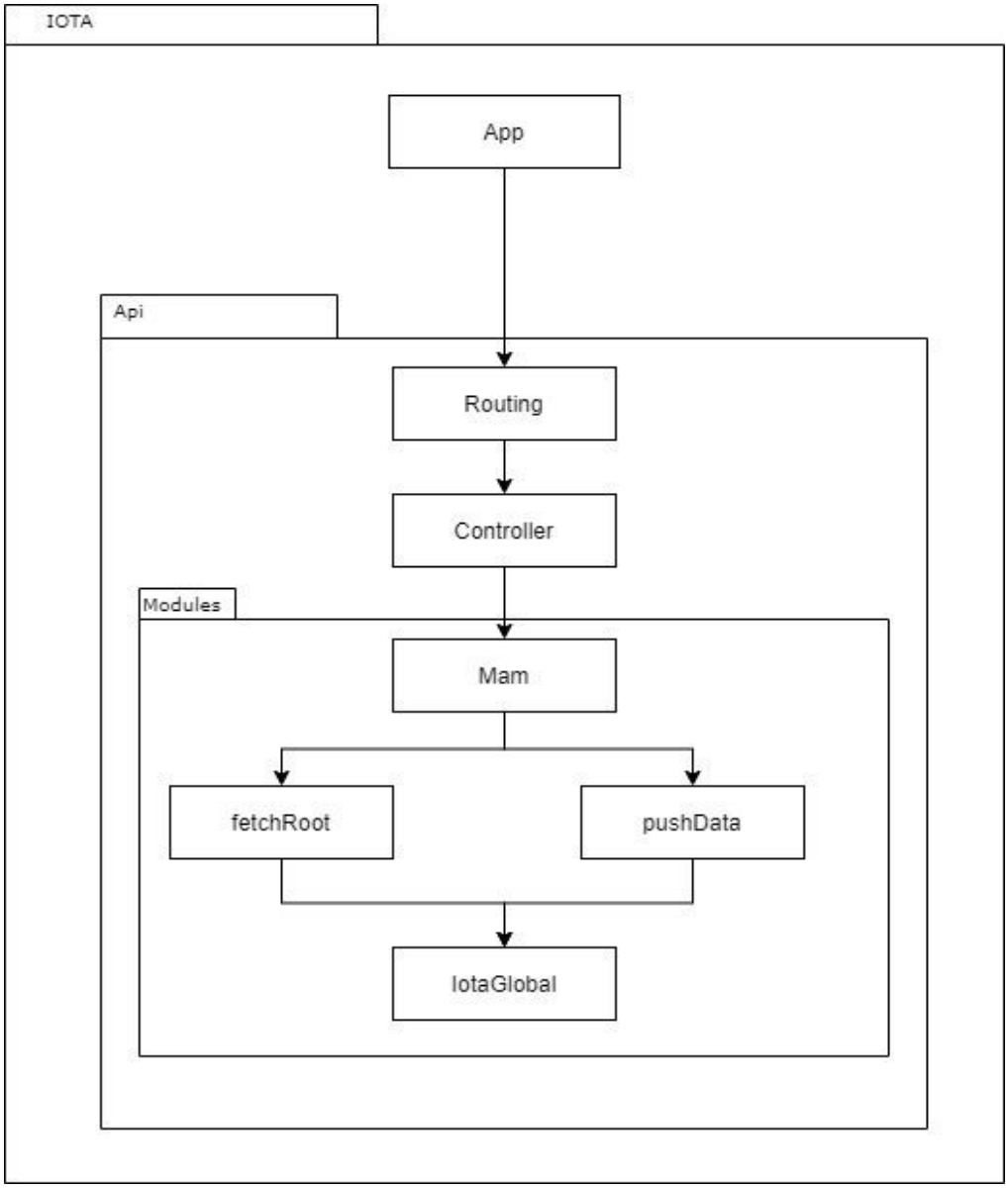


Figura 13 Diagrama de paquetes del Gateway

Fuente: Autor

3.3.3. Vista de proceso

El proceso de funcionamiento del Gateway es relativamente sencillo, se puede describir fácilmente con un diagrama de flujo *(ver figura 14)*. En el caso de llegada de una petición al servidor, este tiene que inicialmente establecer la url a la que ha sido realizada. Si la url pide un push, se obtiene los datos de la petición, misma que debe ser JSON, se procede a hacer la petición de las credenciales para el envío y finalmente se envían los datos a IOTA. Si se solicita un fecth se debe obtiene la raíz ingresada, posteriormente se realiza la petición de las credenciales y se devuelven los datos que se obtuvieron al usuario.

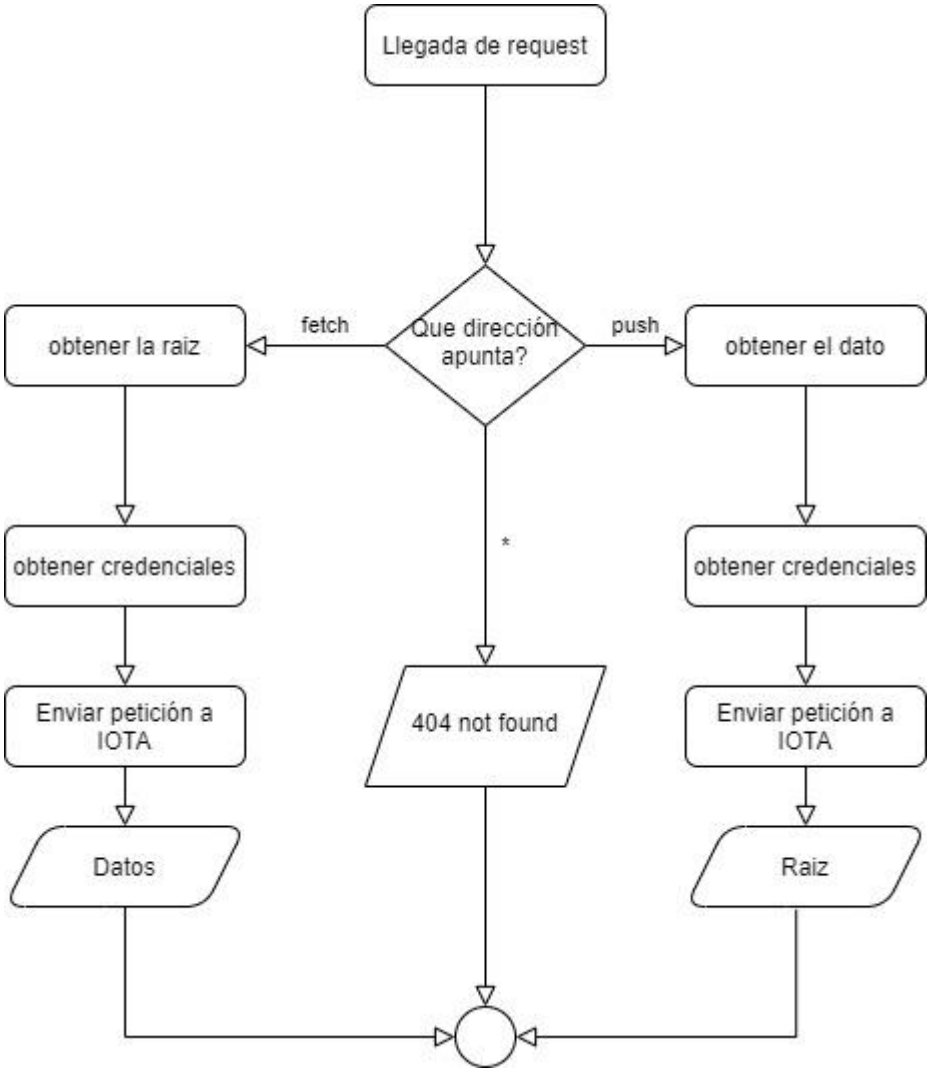


Figura 14 Diagrama de flujo de Gateway

Fuente: Autor

3.3.4. Vista física

El despliegue del proyecto se establece en tres componentes principales, el Gateway, los Smart transducers y el Blockchain. El Gateway tiene comunicación de entrada y salida con los smart transducers y permite a su vez comunicación de los usuarios con el sistema. El Blockchain se comunica también con el Gateway, pero únicamente recepta peticiones del mismo *(ver figura 15)*.

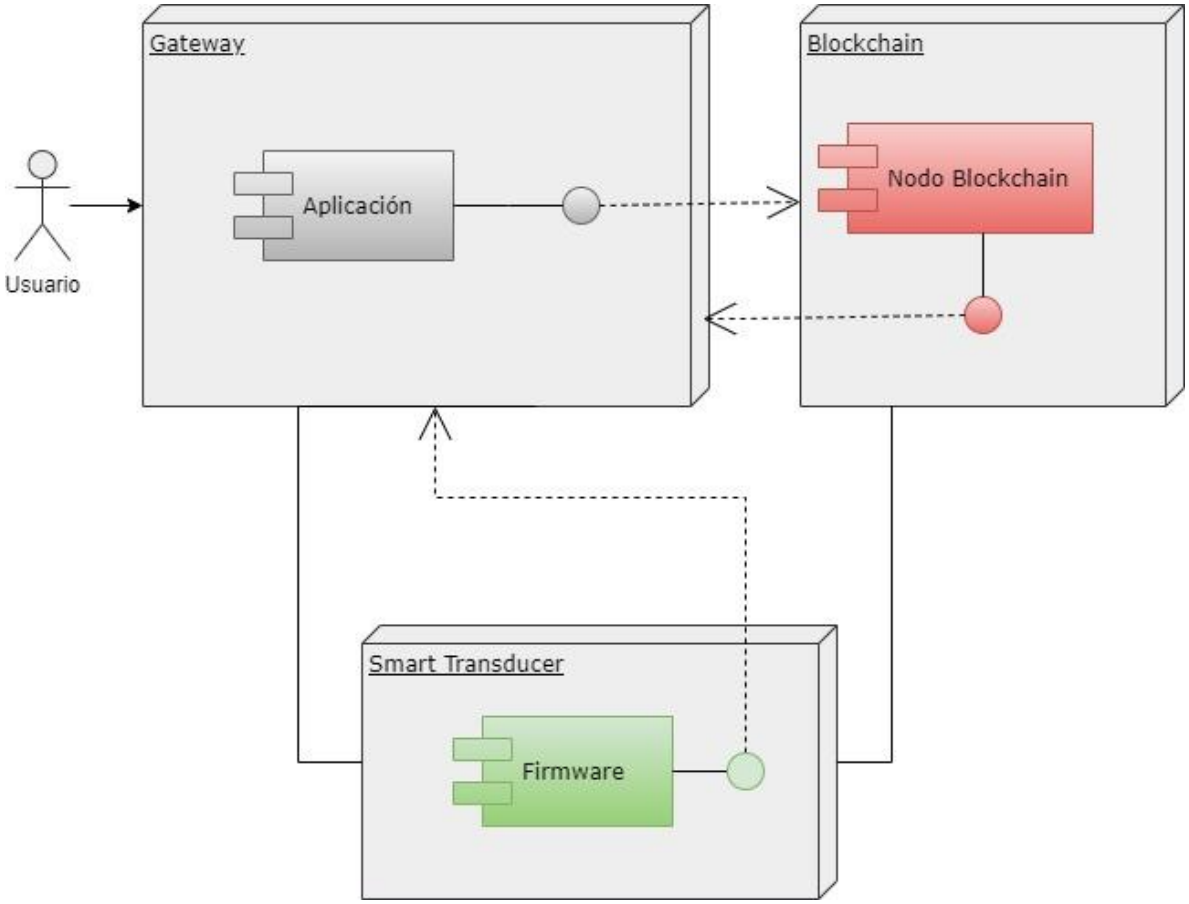


Figura 15 Diagrama de despliegue del proyecto

Fuente: Autor

3.4. Smart transducers

Los smart transducers realizan tres funciones dentro del sistema: sensado de datos del ambiente mediante un sensor lumínico, gestión de estado de actuadores que permite en este caso realizar el encendido y apagado de un relay al que estará conectado la fuente de luz y también gestiona la mensajería mediante HTTP mediante el envío de mensajes POST al

middleware y recepción de las raíces que este devuelve mediante el uso de un ETHERNET SHIELD.

Se utilizarán para este propósito placas Arduino MEGA en conjunto con una placa de relay KY-09 y un sensor lumínico de elaboración propia con el uso de una fotocelda y una resistencia de 10kΩ (*ver figura 16).*

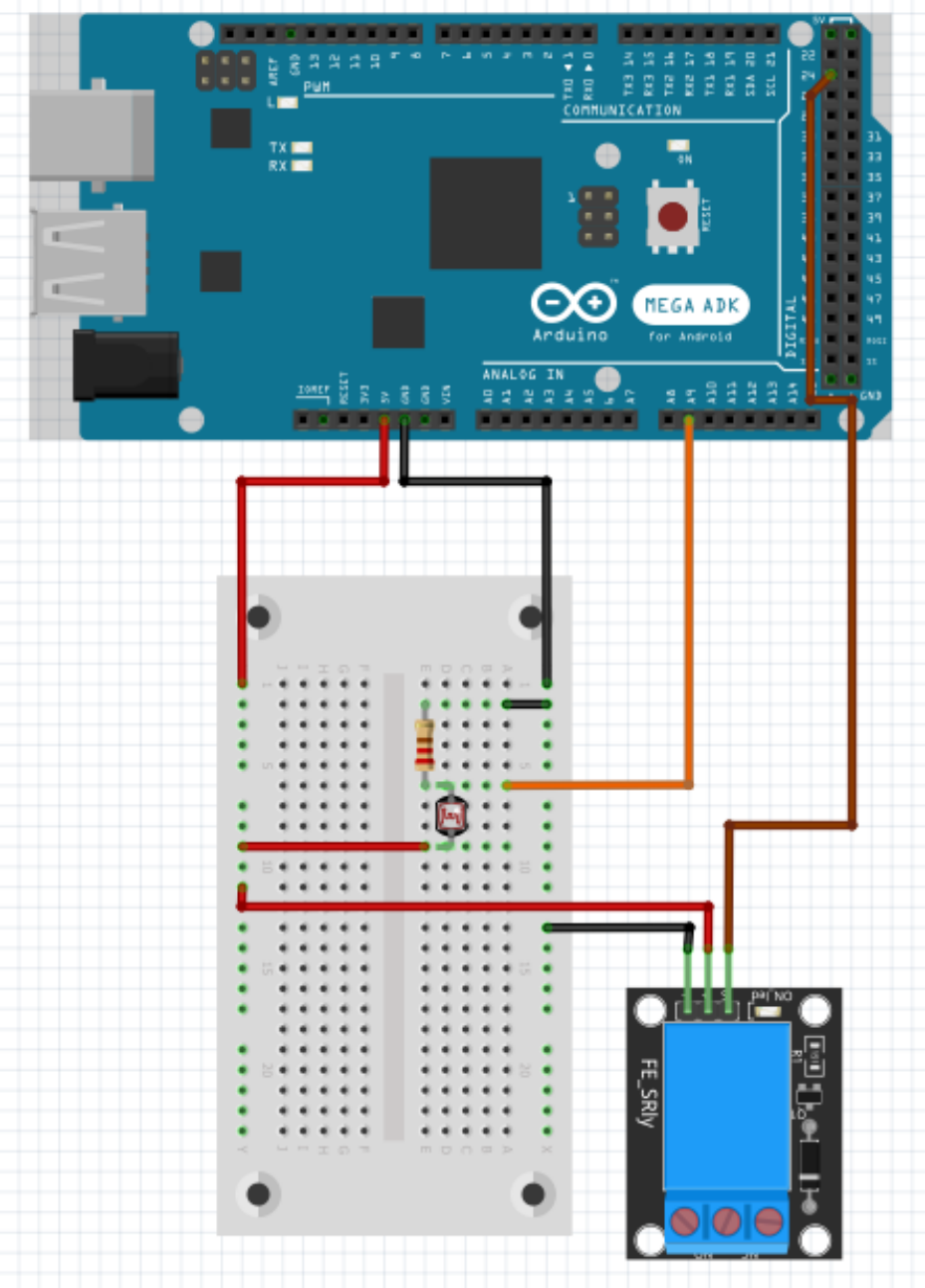


Figura 16 Diagrama de conexión de smart transducer Arduino

Fuente: Autor

El diagrama esquemático permite visualizar las conexiones requeridas por el smart transducer *(ver figura 17)* basado en las necesidades mostradas en el diagrama anterior.

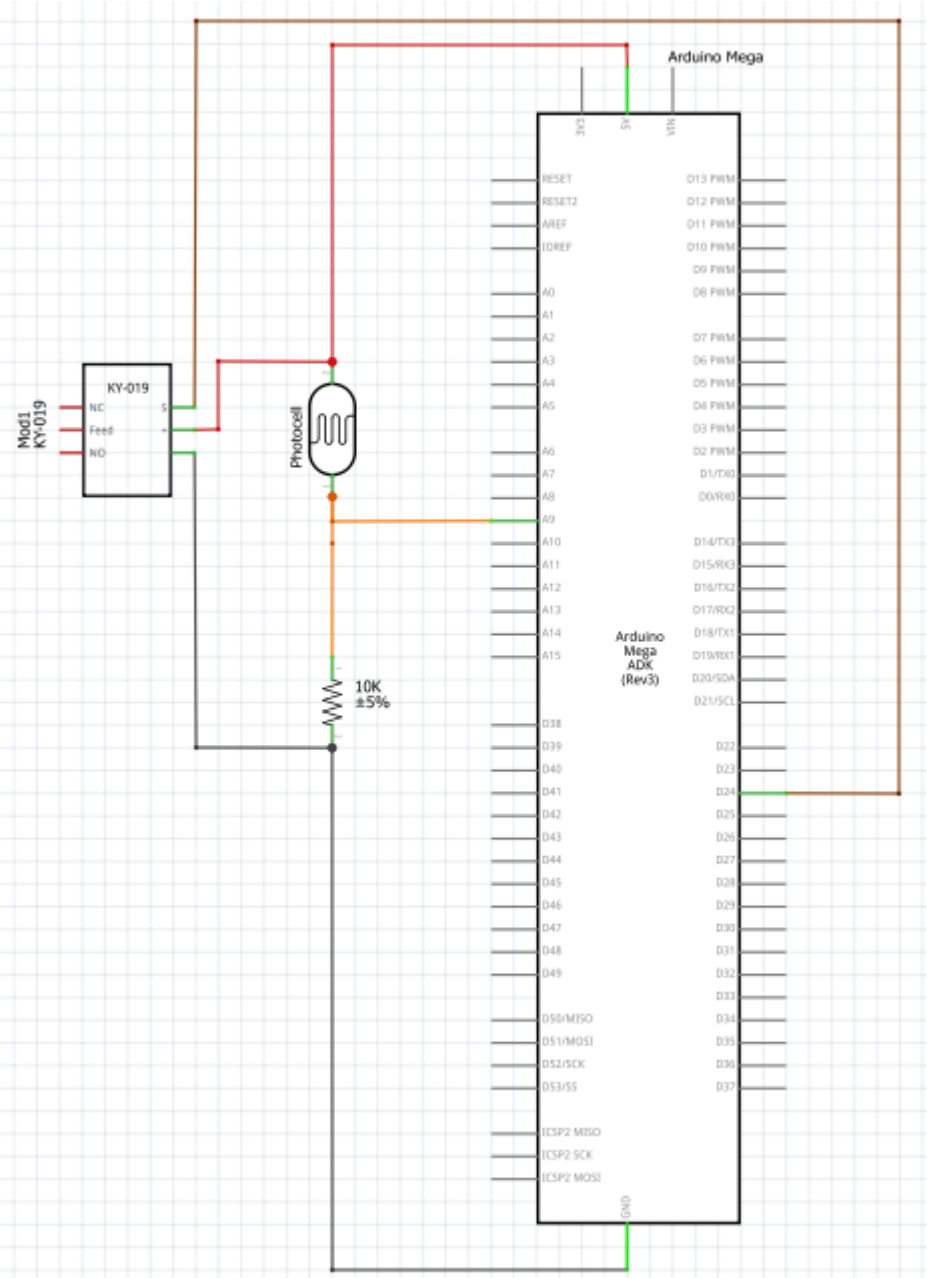


Figura 17 Diagrama circuital de smart transducer Arduino

Fuente: Autor

El prototipo en funcionamiento ha sido adaptado para lograr que se cumplan las necesidades específicas de iluminación de la habitación realizando una calibración del sensor a un valor analógico de 300 unidades en un rango de 0-1023.

El prototipo en cuestión permanece en un lazo permanente en el que se ejecutarán las operaciones principales correspondientes al funcionamiento del prototipo. Por cuestiones referidas a un nivel práctico el prototipo puede funcionar sin conexión a internet. La información se almacenará únicamente cuando el prototipo tenga acceso a una red, ya sea inalámbrica o cableada que le permita conectarse directamente con el middleware *(ver figura 18).*

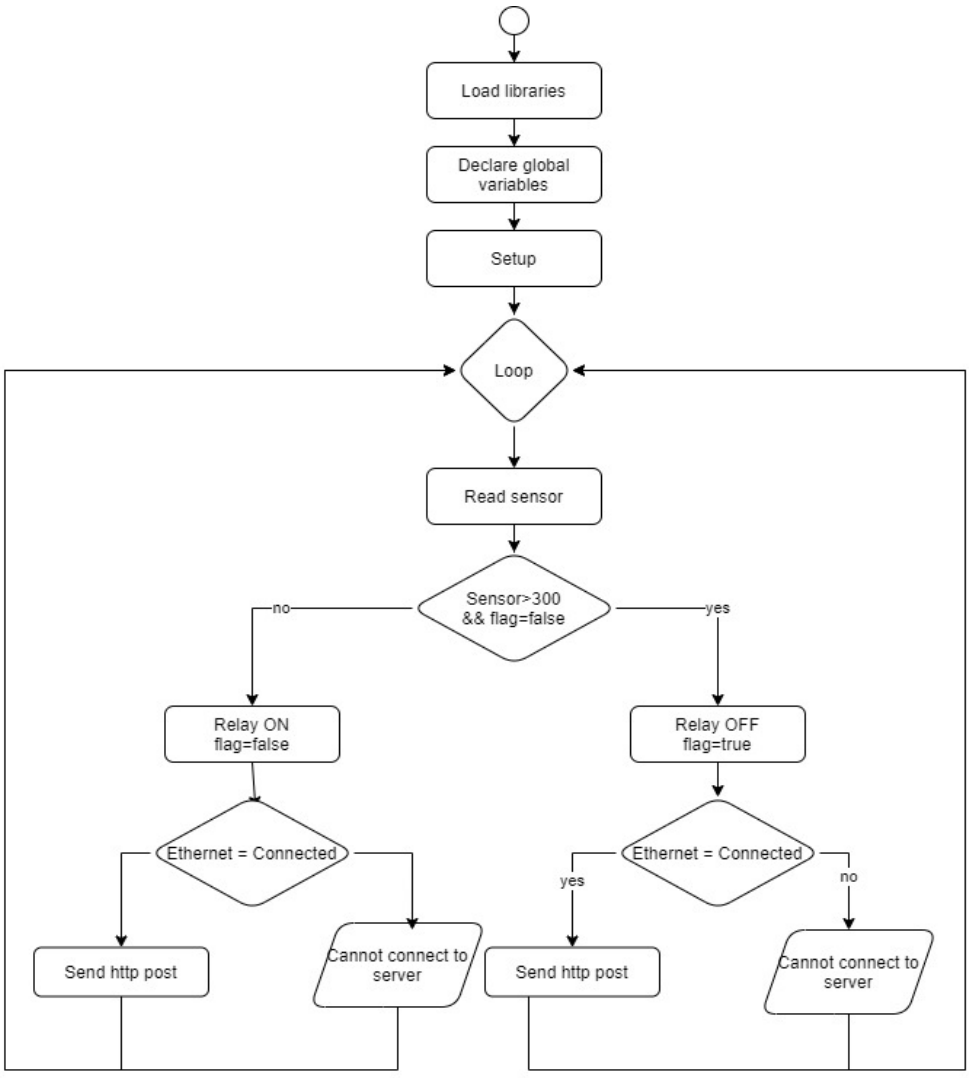


Figura 18 Diagrama de flujo firmware Arduino

Fuente: Autor

CAPITULO IV: DISCUSIÓN DE RESULTADOS

En la redacción del presente capítulo se presentarán de manera simplificada los hallazgos del presente proyecto. Se inicia en la sección 4.1 con la descripción de los hallazgos fundamentales de la investigación, seguidamente se desarrollan las conclusiones y recomendaciones surgidas del proyecto en la sección 4.2 y finalmente se describe futuras investigaciones de IOT con Blockchain en la sección 4.3.

4.1. Hallazgos fundamentales

Durante la realización del presente proyecto se ha logrado implementar de manera exitosa un sistema IOT basado en tres componentes. El Smart transducer diseñado utilizando un Arduino Mega, un relé que se encargará de gestionar el suministro eléctrico al sistema de iluminación y un sensor creado con el uso de resistencias y una fotocelda. El middleware del sistema está basado en un API creado con servicios REST implementado sobre NODE JS v.12.18.4 con una arquitectura monolítica. que se encarga del manejo de mensajería, almacenamiento y lectura de datos de la plataforma de Blockchain IOTA. Finalmente el almacenamiento se realiza sobre IOTA, utilizando su cliente MAM.

Tras la correcta implementación del sistema se realizaron pruebas de rendimiento y aseguramiento de encriptación de los datos mediante el uso de JMeter y Wireshark.

Para rendimiento se realizaron pruebas de carga y de tiempo de respuesta Las pruebas mostraron resultados muy marcados en ambos aspectos. El sistema de IOTA muestra un tiempo de respuesta promedio de 3105ms con una concurrencia de un usuario. Esto es un tiempo adecuado tomando en cuenta las diferentes operaciones que son realizadas para la seguridad del sistema. Para un sistema con alta transaccionalidad puede resultar inadecuado debido a que este efecto puede causar un cuello de botella en las transacciones.

Ante esta aseveración se han realizado pruebas de carga para verificar la cantidad de usuarios concurrentes que podrían conectarse al middleware sin causar ningún inconveniente determinando que en un sistema ejecutado en Windows 10 PRO con un procesador Intel Core i7-4790 @ 3.60GHz con 8GB compartidos con el sistema operativo y las operaciones nativas de este puede soportar una concurrencia de 59 usuarios sin fallos. Esta capacidad es aceptable

para el proyecto desarrollado. Debido a la necesidad de escalabilidad que puede generarse a futuro esto podría convertirse en un problema importante. Se realizaron las mediciones de rendimiento en la prueba de carga y se obtuvieron tiempos de respuesta con una media de 21526.597ms, tiempo considerablemente alto para la realización de transacciones dentro del sistema.

Se realizaron pruebas de encriptación sobre las transacciones al servidor de IOTA, determinando un nivel de seguridad muy alta basada en TLS, firma única, árbol de Merkle y uso de un sistema de datos basado en una triada correspondiente a un tryte.

4.1.1. Prototipo en funcionamiento

El prototipo fue creado y probado brindando resultados satisfactorios a las necesidades de iluminación. Permitiendo que se puedan realizar cambios en los actuadores de manera automática mediante el censado de la información ambiental en la placa microcontroladora.
El prototipo electrónico puede realizar sus actividades mediante el censado de datos ambientales para activar o desactivar un relay que permite a su vez abrir un circuito. Para el presente proyecto se estableció únicamente un LED como forma de iluminación. Esto puede ser modificado a gusto y necesidad de cada uno de los posibles usos *(ver figuras 19, 20)*

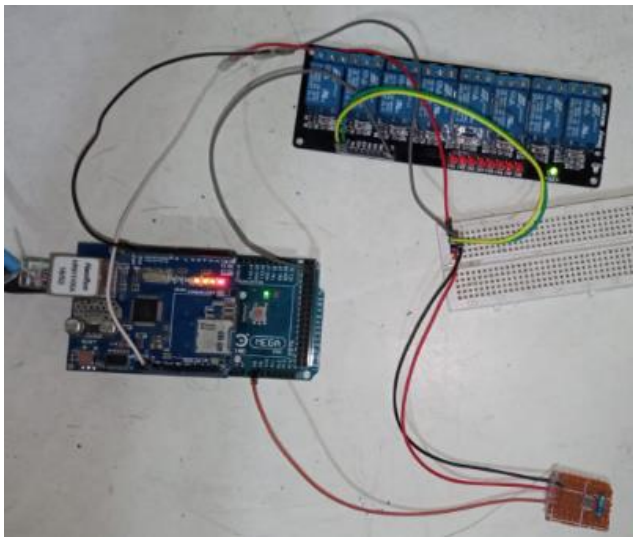


Figura 19 Prototipo electrónico con iluminación al sensor.

Fuente: Autor

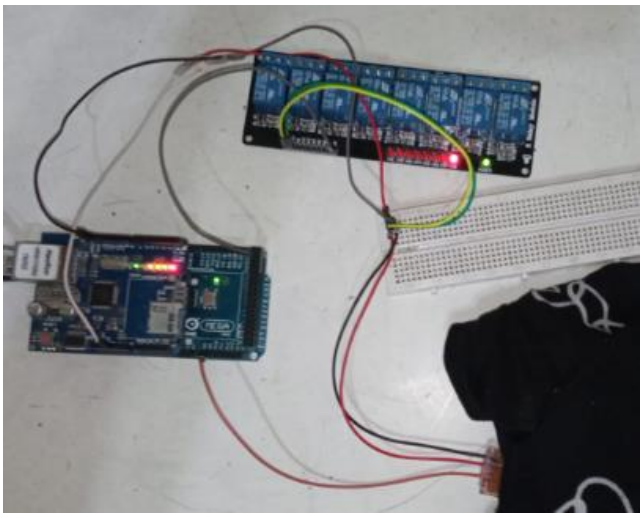


Figura 20 prototipo electrónico sin iluminación al sensor.

Fuente: Autor

Se ha creado dentro del firmware del prototipo electrónico un sistema de mensajería que permite visualizar la dirección IP asignada por DHCP *(ver figura 21)* para de esta manera poder realizar futuros rastros a la comunicación.

```
Initialize Ethernet with DHCP:
12:04:39.180 ->  DHCP assigned IP >> 192.168.10.103
```

Figura 21 asignación de IP mediante DHCP en el prototipo electrónico

Fuente: Autor

Se puede también visualizar los mensajes intercambiados con el middleware mediante mensajería HTTP (Ver figuras 22, 23).

```
12:04:40.655 -> Sending to Server:
12:04:40.655 -> POST /send HTTP/1.1Host: 192.168.10.107
12:04:40.703 -> Content-Type: application/x-www-form-urlencoded
12:04:40.749 -> User-Agent: Arduino/1.0
12:04:40.795 -> Content-Length: 57
12:04:40.795 -> data={"data":"{"DISPOSITIVO":"LUZ1","SENSORVALUE1","0"} }
```

Figura 22 envio de Request tipo POST al servidor a la dirección /send

Fuente: Autor

```
12:04:47.449 -> HTTP/1.1 200 OK
12:04:47.495 -> X-Powered-By: Express
12:04:47.495 -> Content-Type: application/json; charset=utf-8
12:04:47.542 -> Content-Length: 83
12:04:47.588 -> ETag: W/"53-4FCNulKjDxQIwDGL/VI1afqYS18"
12:04:47.588 -> Date: Tue, 05 Jan 2021 17:04:49 GMT
12:04:47.635 -> Connection: keep-alive
12:04:47.681 ->
12:04:47.681 -> "IDCREPVGAJOUMWLOGSXYCFLFBUAKOCZQA9GNCYPYXVJQTSDA
```

Figura 23 respuesta del servidor al POST enviado

Fuente: Autor

El contenido del mensaje varía acorde al estado al que se haya modificado el actuador *(ver figura 22, 24)*

```
12:05:20.776 -> Sending to Server:
12:05:20.776 -> POST /send HTTP/1.1Host: 192.168.10.107
12:05:20.821 -> Content-Type: application/x-www-form-urlencoded
12:05:20.868 -> User-Agent: Arduino/1.0
12:05:20.914 -> Content-Length: 57
12:05:20.914 -> data={"data":"{"DISPOSITIVO":"LUZ1","SENSORVALUE1","1"} }
12:05:24.684 -> HTTP/1.1 200 OK
12:05:24.684 -> X-Powered-By: Express
12:05:24.731 -> Content-Type: application/json; charset=utf-8
12:05:24.776 -> Content-Length: 83
12:05:24.776 -> ETag: W/"53-tvdetSygAUVQZEMShQuhHKJ5Fps"
12:05:24.822 -> Date: Tue, 05 Jan 2021 17:05:26 GMT
12:05:24.868 -> Connection: keep-alive
12:05:24.914 ->
12:05:24.914 -> "ILBQBFDCIGXYJIQCEOMAZHRQEJEVOQVYHTSPTY9EMLHIBJMSOTYNQRMK
```

Figura 24 interacción de mensajes para estado ON

Fuente: Autor

Cada uno de los mensajes que se envía desde el prototipo electrónico se muestra también dentro del servidor junto con la actualización del estado del cliente de IOTA *(ver figura 25, 26).*

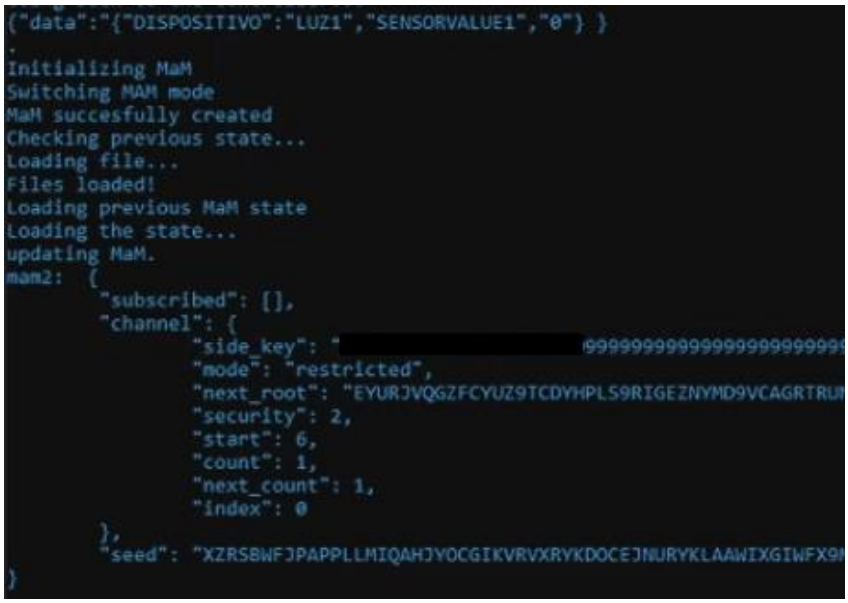


Figura 25 Recepción de mensaje de actuador OFF

Fuente: Autor

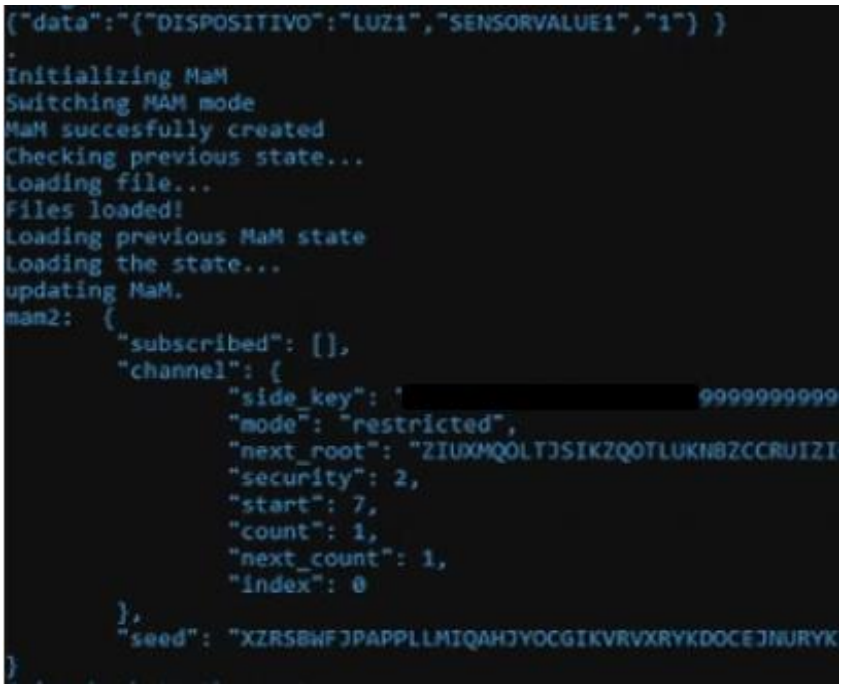


Figura 26 Recepción de mensaje actuador ON

Fuente: Autor

Finalmente para la lectura de datos se puede realizar una request de tipo POST a la dirección /fetch con el argumento root y la raíz que se va a buscar *(ver figura 27)*

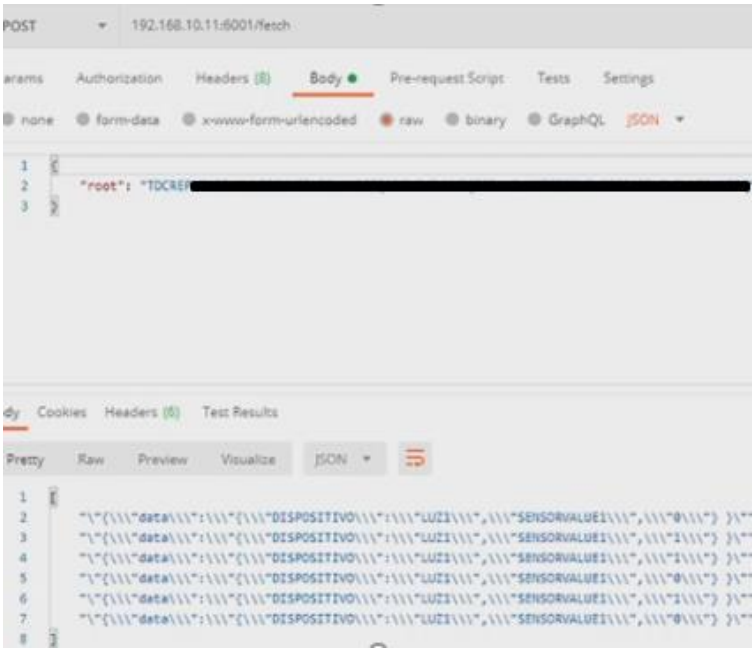


Figura 27 lectura de datos en mediante POST

Fuente: Autor

El servidor también mostrará mensajería de los datos que se devuelven al cliente *(ver figura 28)*

Figura 28 lectura de datos en el middleware

Fuente: Autor

4.1.2. Mediciones de rendimiento

4.1.2.1. Envío de datos

Se realizaron las mediciones correspondientes al rendimiento de envío de peticiones al Blockchain con resultados que oscilan entre 2890ms a 3520ms. *(ver tabla 3)*

Parámetro	Tiempo (ms)
Valor mínimo	2890
Valor Máximo	3520
Mediana	3060
Media	3105
Primer cuartil	3005
Tercer cuartil	3180

Tabla 3 Estadística descriptiva del dataset

Fuente: Autor

La distribución de los tiempos de respuesta se encuentra en un rango bien definido y es fácilmente apreciable en un diagrama de distribución correspondiente a los tiempos de respuesta de la simulación *(ver figura 29).*

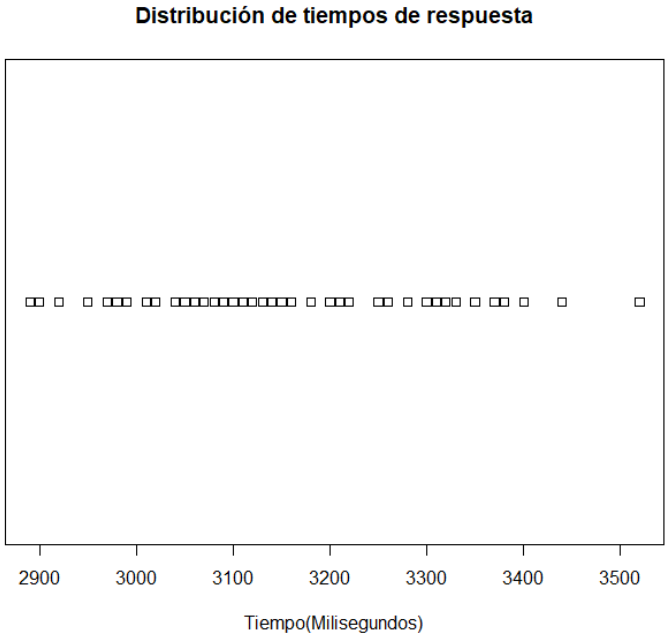


Figura 29 Diagrama de cajas de tiempos de respuesta

Fuente: Autor

Esto se puede apreciar de mejor manera mediante el uso de un diagrama de *cajas (ver figura 30)* donde incluso se puede notar que existe un valor fuera del rango determinado lo cual puede deberse a problemas de conexión desde la ubicación del middleware. Se debe recordar que la velocidad de transmisión de los datos también depende de la velocidad de transmisión de datos que posee el middleware.

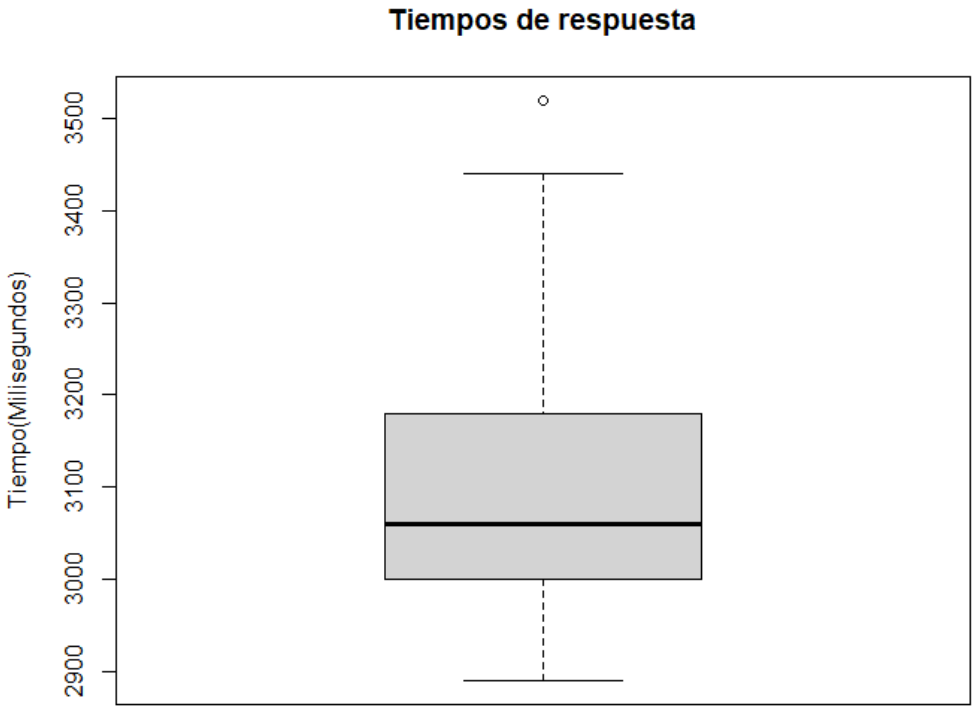


Figura 30 Diagrama de cajas para tiempos de respuesta

Fuente: Autor

Se puede apreciar las frecuencias de los datos con un histograma (ver figura 31) donde se puede notar que la mayoría de los valores se encuentran en un rango de entre 3000 ms y 3100 ms. Se debe notar que estos valores se ven influenciados por la transaccionalidad que está teniendo IOTA en el momento de la captura de los datos e inclusive por la velocidad de transmisión de los datos.

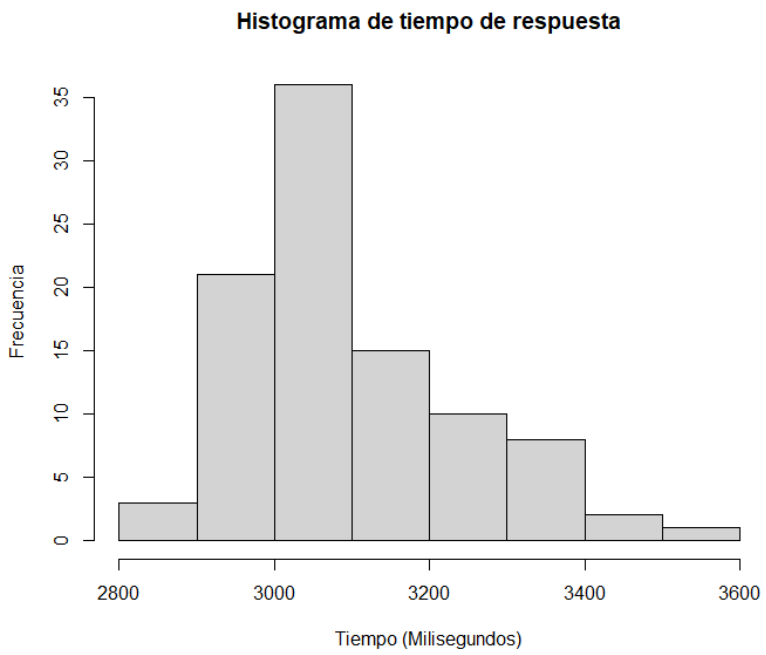


Figura 31 Histograma de tiempos de respuesta

Fuente: Autor

Finalmente se puede apreciar la curva formada por los datos para verificar la curtosis de la distribución de los datos *(ver figura 32)*.

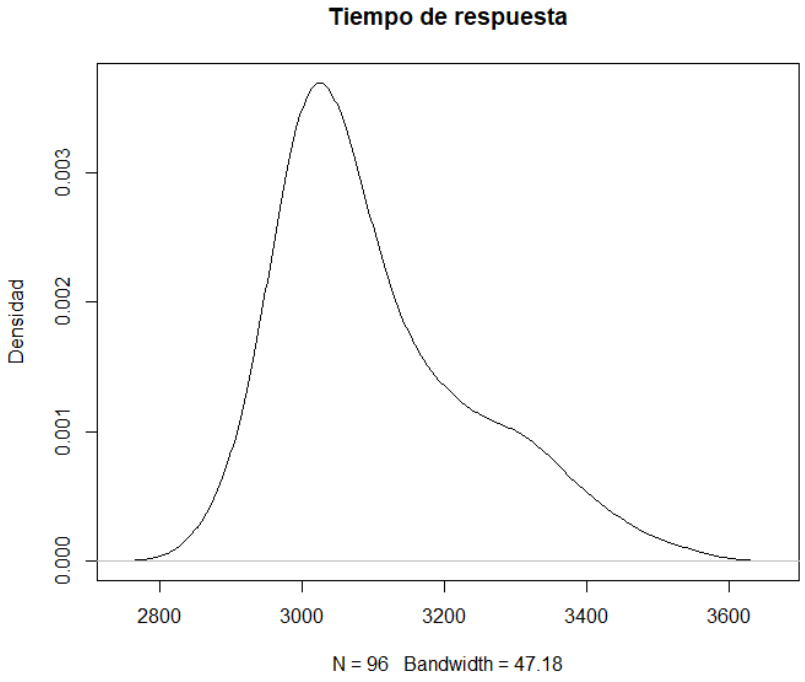


Figura 32 Diagrama de densidad de tiempos de respuesta.

Fuente: Autor

4.1.2.2. Lectura de datos

La lectura de datos toma un tiempo promedio de 566ms por cada uno de los mensajes almacenados dentro del Blockchain.

4.1.3. Pruebas de carga

Las pruebas de carga fueron realizadas con un ordenador con características muy limitadas (ver tabla 4) y mediante una simulación de usuarios realizada en JMeter se determina que pueden existir un total de 59 usuarios conectados de manera concurrente al servicio realizando transacción de envío de datos cada uno de ellos puede poseer una diferencia de tiempo de envio de 1 segundo.

CPU	Intel Core i7-4790 @ 3.60GHz
RAM	8GB
Sistema operativo	Windows 10 Pro

Tabla 4 Características del middleware

Fuente: Autor

Durante las pruebas de carga se obtuvieron las medidas de tendencia central con la concurrencia de usuarios anteriormente mencionada (ver tabla 5). Se puede notar un alto incremento en latencia con una media de 21.526,597 milisegundos, lo que representa cerca de 22 segundos para procesamiento de transacción.

Mínimo	6697 ms
Máximo	41237 ms
Media	21526.597 ms
Desviación estándar	6478.113 ms

Tabla 5 Medidas de tendencia central en prueba de carga

Fuente: Autor

Se puede apreciar las frecuencias de los datos con un histograma *(ver figura 33)* donde se puede notar que la mayoría de los valores se encuentran mayormente ubicados alrededor de 23967 ms.

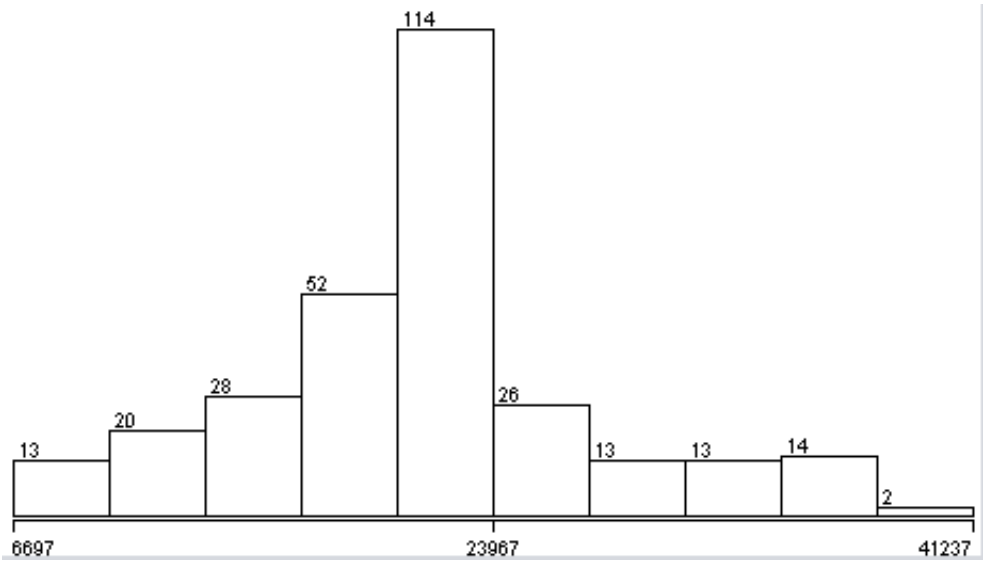


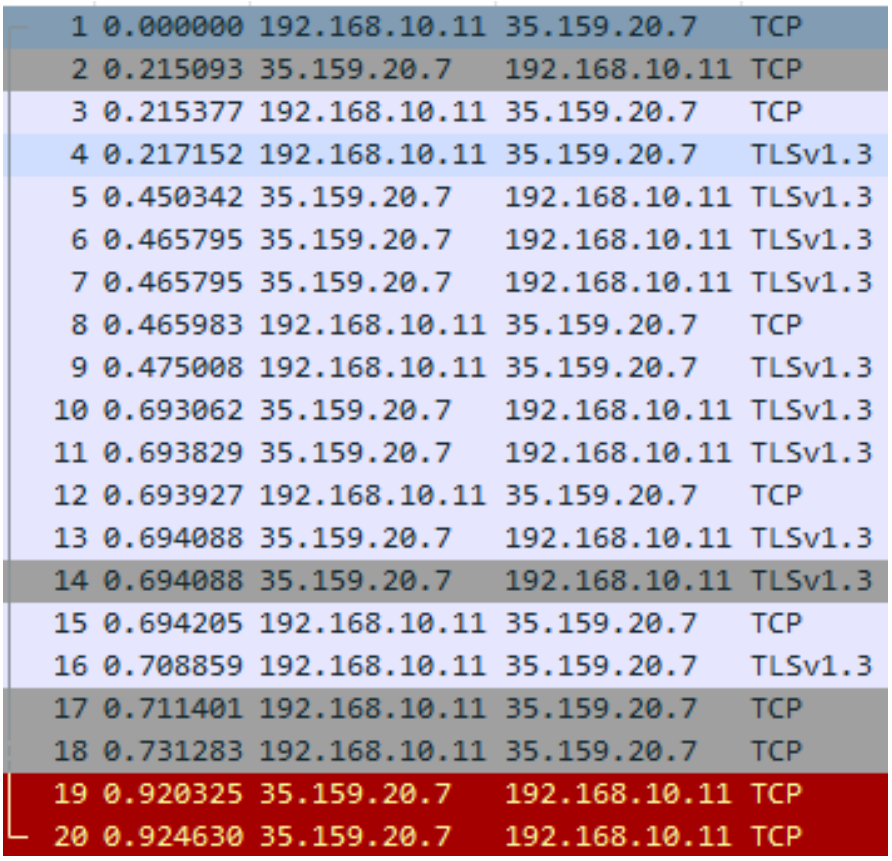
Figura 33 Histograma de frecuencia para pruebas de carga.

Fuente: Autor

4.1.4. Seguridad de datos

La seguridad de los datos en la conexión con IOTA se encuentra garantizada por el uso de su propio algoritmo de encriptación basado en la firma única y el árbol de Merkle para generar la misma.

Es importante el correcto análisis del tráfico de red generado por el middleware dado que de este podrían devenir futuros ataques de tipo *"man in the middle"* mediante la escucha y desciframiento de los paquetes enviados para su almacenamiento en la nube o por los paquetes leídos para su uso en el middleware. Estos datos han sido obtenidos mediante el uso de la herramienta Wireshark *(ver figura 34).*



1	0.000000	192.168.10.11	35.159.20.7	TCP
2	0.215093	35.159.20.7	192.168.10.11	TCP
3	0.215377	192.168.10.11	35.159.20.7	TCP
4	0.217152	192.168.10.11	35.159.20.7	TLSv1.3
5	0.450342	35.159.20.7	192.168.10.11	TLSv1.3
6	0.465795	35.159.20.7	192.168.10.11	TLSv1.3
7	0.465795	35.159.20.7	192.168.10.11	TLSv1.3
8	0.465983	192.168.10.11	35.159.20.7	TCP
9	0.475008	192.168.10.11	35.159.20.7	TLSv1.3
10	0.693062	35.159.20.7	192.168.10.11	TLSv1.3
11	0.693829	35.159.20.7	192.168.10.11	TLSv1.3
12	0.693927	192.168.10.11	35.159.20.7	TCP
13	0.694088	35.159.20.7	192.168.10.11	TLSv1.3
14	0.694088	35.159.20.7	192.168.10.11	TLSv1.3
15	0.694205	192.168.10.11	35.159.20.7	TCP
16	0.708859	192.168.10.11	35.159.20.7	TLSv1.3
17	0.711401	192.168.10.11	35.159.20.7	TCP
18	0.731283	192.168.10.11	35.159.20.7	TCP
19	0.920325	35.159.20.7	192.168.10.11	TCP
20	0.924630	35.159.20.7	192.168.10.11	TCP

Figura 34 Transacciones realizadas por el cliente IOTA

Fuente: Autor

Como se puede notar se realiza una conexión segura utilizando TLSv1.3 adicionalmente a la encriptación de datos nativa dentro del servidor de IOTA. De esta manera se garantiza la confiabilidad del envío de los mensajes y se evitan ataques de tipo "*Man in the middle"*.

Existe un factor de riesgo adicional que se debe tomar en cuenta para la implementación de un sistema IoT. En las comunicaciones realizadas dentro de la red de área local se debe también asegurar algún tipo de encriptación que garantice que los datos se mantengan ocultos. En caso contrario, el intercambio de mensajes dentro de la red local se podría ver vulnerada *(ver figura 35).*

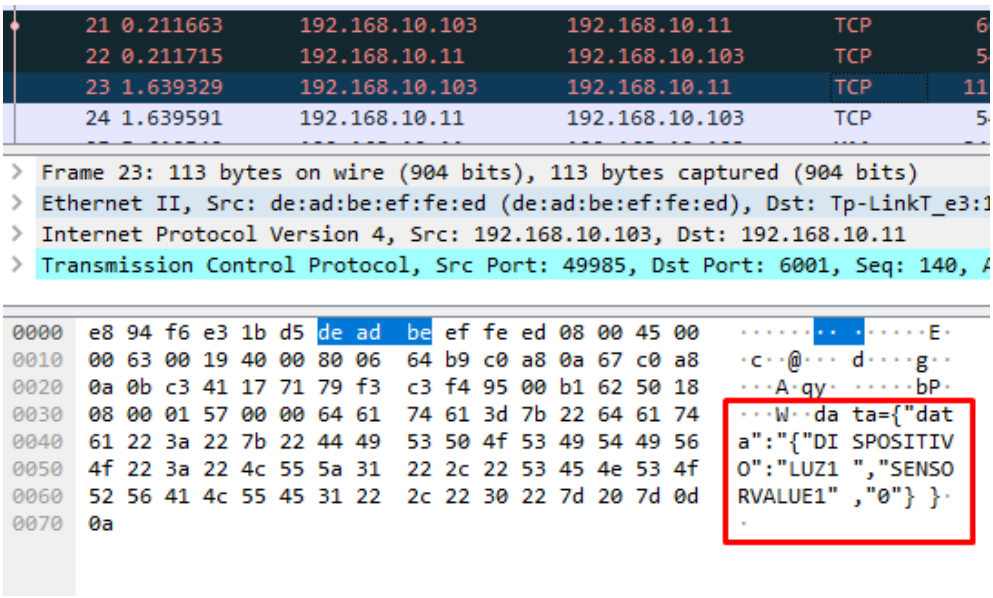


Figura 35 Envío de datos mediante POST en LAN

Fuente: Autor

Es importante notar que debido a los bajos recursos que poseen ciertos Smart transducers no se puede utilizar algoritmos de encriptación, lo que deja como opción de seguridad el proteger la red de área local evitando el posible ingreso de personas no autorizadas mediante un adecuado filtrado de MACs o la aplicación de un sistema de detección de intrusiones.

4.2. Relación con trabajos previos

Se puede evidenciar que en trabajos previos de IOT con Blockchain se han tomado en cuenta ciertos factores específicos para cada uno de sus investigaciones. Se ha dejado de lado el panorama superior. Es decir, pese a que los resultados investigativos han sido óptimos, no se ha determinado ciertos factores que se describen a continuación.

4.2.1. Concurrencia

Dentro del desarrollo de la investigación actual queda demostrado que el tiempo de respuesta promedio del Blockchain es de 3060ms. Este tiempo de transaccionalidad es ideal para sistemas de baja concurrencia tales como el presentado por Zinonos [41], pero no en general no es pertinente su uso en sistemas que requiera de transacciones continuas.

4.2.2. Medio de almacenamiento

Como se menciona en el apartado 4.2.1. Concurrencia, Blockchain no es adecuado para todos los sistemas IOT. Cada sistema debe determinar si su naturaleza permite por transaccionalidad el uso de Blockchain. Se debe aplicar un estudio como el descrito por Scriber [44] y en caso de requerir mayor seguridad se puede tomar en cuenta la segmentación de la información en bloques de mayor tamaño para minimizar la transaccionalidad al servidor.

4.2.3. Seguridad

Pese a que la seguridad de Blockchain es muy alta, esta solamente cubre la comunicación que se realiza con el nodo del Blockchain. La seguridad dentro de la red local aun queda expuesta. Por tanto, se deben aplicar las medidas de seguridad necesarias para evitar la intrusión tal como se muestra en el trabajo de Vinayakumar [22].

4.3. Conclusiones y recomendaciones

La investigación concluyó de manera satisfactoria con el cumplimiento de todos los objetivos tal como fue planificado. Tras el análisis de los resultados queda afirmado que el uso de Blockchain incrementa la seguridad de los datos en un sistema de iluminación IOT.

La investigación estableció que:

- El uso de Blockchain incrementa la seguridad de almacenamiento y transporte en WAN de datos en un sistema de iluminación IOT.
- Blockchain es aplicable a IoT.
- Se obtienen beneficios en persistencia de datos por ser distribuida.
- Se dificulta la realización de ataques al ser validada por el algoritmo de consenso.
- La naturaleza de los proyectos a realizar determina la selección de una plataforma de Blockchain.
- Se observa una gran diferencia en latencia de baja (3105 ms) con alta (21526 ms) transaccionalidad.

Ante dichas afirmaciones y la experiencia en la realización del proyecto se recomienda que:

- Se debe conocer el sistema que se va a desarrollar previo a la selección de un medio de almacenamiento. El uso de Blockchain no queda siempre justificado ya que conlleva un uso de recursos superior a otros medios de almacenamiento.
- No existe una Blockchain genérica que pueda cumplir con los requerimientos de cualquier tipo de proyectos. Cada plataforma de Blockchain puede ajustarse a diversos proyectos mayormente por el tipo de algoritmo de consenso que este implica.
- El sistema de encriptación en la comunicación con el nodo suele ser una característica heredada de la plataforma de Blockchain. Sin embargo, debe ser verificada para comprobar una comunicación segura.
- La red local debe ser asegurada. Los clientes Blockchain cubren únicamente la red WAN, por tanto la seguridad LAN debe ser prioridad en todos los proyectos.

4.3.1. Implicaciones para IOT

El proyecto demuestra que se brinda una seguridad muy alta a las transacciones realizadas en IOT, garantizando que la información permanezca privada. Se debe tomar en cuenta que la tecnología de Blockchain también es susceptible a cierto tipo de ataques, por tanto la selección de una plataforma adecuada juega un papel fundamental en que tan bien se desarrolle el sistema.

IOTA demostró ser una opción altamente competitiva permitiendo obtener un nivel de seguridad resistente incluso a computación cuántica, lo que la hace una de las plataformas lideres para el almacenamiento de bloques con un consumo de recursos muy bajo. Esto se adapta perfectamente a IOT, sin embargo, pueden existir requerimientos de proyectos que hagan viable el uso de Hyperledger o de Corda.

IOT ha sido considerada como una tecnología muy insegura debido a la falta de capacidad de procesamiento de los Smart Transducers, mismo que limitaba la posibilidad de encriptación de los datos. Sin lugar a dudas IOTA deja de lado esta limitante, lo cual dará a

IOT un mayor impacto en la comunidad científica y será aplicado a un espectro mucho mayor de sectores tanto personales como empresariales.

4.3.2. Almacenamiento y rendimiento

Aunque IOT puede beneficiarse de la seguridad brindada por Blockchain la velocidad de almacenamiento se ve altamente impactada. Por tal razón se debe realizar un análisis previo de la importancia de la información que se genera y del impacto que podría tener la manipulación de la misma, ya que, en caso de ser un sistema de poco impacto del tiempo de transacción no sería justificado.

4.3.3. Recomendaciones

- Se debe conocer el sistema que se va a desarrollar previo a la selección de un medio de almacenamiento. El uso de Blockchain no queda justificado en caso de que la información generada sea de baja importancia pues este requiere de un uso alto de recursos.
- La selección del Blockchain a utilizar depende de la naturaleza del proyecto. No existe una Blockchain genérica que pueda cumplir con los requerimientos de cualquier tipo de proyectos. Cada plataforma tiene características que lo diferencian, por tanto, son mayormente aplicables a proyectos específicos.
- El sistema de encriptación en la comunicación con el nodo suele ser una característica heredada de la plataforma de Blockchain. En caso de no serlo se debe establecer una robusta encriptación de datos para evitar ataques en la red.
- La red local debe ser asegurada mediante encriptación, bloqueo de puertos, y cualquier método de seguridad que se considere consistente. Se pueden realizar ataques en caso de que exista infiltración en la red.

4.4. El futuro

El proyecto realizado solo representa el inicio de una cadena de investigación sobre seguridad en IOT. Como proyectos futuros se consideran varios aspectos mencionados a continuación

4.4.1. Almacenamiento intermedio

Para sistemas con una muy alta transaccionalidad se requiere un almacenamiento intermedio que pueda servir para forjar bloques con transacciones que pueden ser establecidas por periodicidad o por cantidad de transacciones. Este almacenamiento intermedio puede ser realizado en memoria, en un fichero, base de datos relacional, no relacional, on premise o en la nube. Una vez cumplido el parámetro de almacenamiento se forja un bloque a ser enviado a la plataforma de Blockchain. Esto presumiblemente mejoraría de manera notable el flujo de las transacciones y por tanto el desempeño de las aplicaciones.

4.4.2. Replicación

El middleware se podría beneficiar de tecnologías de replicación para garantizar la disponibilidad del servicio y a su vez mejorar el rendimiento en horas de alta transaccionalidad. Para esto se puede aplicar el uso de contenedores y replicación mediante la gestión en tiempo real de contenedores para presumiblemente mejorar el desempeño de los sistemas.

4.4.3. Microservicios

Basado en la premisa anterior, se debería dividir el middleware en microservicios que tengan tareas específicas para de esta manera, presumiblemente, se pueda garantizar un flujo mucho más rápido de la información y facilitando la replicación de los microservicios en alta demanda permitiendo optimizar el uso de recursos.

4.4.4. Continuous Integration y Continuous Delivery (CI/CD)

Acompañado de los microservicios se debe implementar un sistema de CI/CD, para facilitar el mantenimiento del middleware y permitiendo que este pueda ser mejorado de manera permanente y sencilla.

BIBLIOGRAFÍA

[1] K. Shi *et al.*, "Detecting spatiotemporal dynamics of global electric power consumption using DMSP-OLS nighttime stable light data," *Appl. Energy*, vol. 184, pp. 450–463, 2016, doi: 10.1016/j.apenergy.2016.10.032.

[2] A. Seyyedabbasi, "Decrease Electricity Consumption in Rooms with IoT Technology," *Int. J. Inf. Syst. Comput. Sci.*, vol. 9, no. 1, pp. 1–4, 2020, doi: 10.30534/ijiscs/2020/01912020.

[3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013, doi: 10.1016/j.future.2013.01.010.

[4] K. H. Park *et al.*, "Robotic smart house to assist people with movement disabilities," *Auton. Robots*, vol. 22, no. 2, pp. 183–198, 2007, doi: 10.1007/s10514-006-9012-9.

[5] Y. J. Fan, Y. H. Yin, L. Da Xu, Y. Zeng, and F. Wu, "IoT-based smart rehabilitation system," *IEEE Trans. Ind. Informatics*, vol. 10, no. 2, pp. 1568–1577, 2014, doi: 10.1109/TII.2014.2302583.

[6] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," *Int. Conf. Adv. Commun. Technol. ICACT*, pp. 464–467, 2017, doi: 10.23919/ICACT.2017.7890132.

[7] D. Pavithran, K. Shaalan, J. N. Al-Karaki, and A. Gawanmeh, "Towards building a blockchain framework for IoT," *Cluster Comput.*, 2020, doi: 10.1007/s10586-020-03059-5.

[8] S. Arif, M. A. Khan, and S. U. Rehman, "Investigating Smart Home Security : Is Blockchain The Answer ?," vol. 4, pp. 1–15, 2020, doi: 10.1109/ACCESS.2020.3004662.

[9] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Futur. Gener. Comput. Syst.*, vol. 82, pp. 395–411, 2018, doi: 10.1016/j.future.2017.11.022.

[10] B. D. Davis, J. C. Mason, and M. Anwar, "Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study," *IEEE Internet Things J.*, vol. 4662, no. c, pp. 1–1, 2020, doi: 10.1109/jiot.2020.2983983.

[11] D. Mazzei *et al.*, "A Blockchain Tokenizer for Industrial IOT trustless applications,"

Futur. Gener. Comput. Syst., vol. 105, pp. 432–445, 2020, doi: 10.1016/j.future.2019.12.020.

[12] N. M. Kumar and P. K. Mallick, "Blockchain technology for security issues and challenges in IoT," *Procedia Comput. Sci.*, vol. 132, pp. 1815–1823, 2018, doi: 10.1016/j.procs.2018.05.140.

[13] L. De Santis, V. Giovanni, P. Ii, V. Giovanni, and P. Ii, "Blockchain-Based Infrastructure to enable Trust in IoT environment," pp. 1–6, 2020.

[14] D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for IoT security," *Internet of Things*, vol. 1–2, pp. 1–13, 2018, doi: 10.1016/j.iot.2018.05.002.

[15] Y. Qian *et al.*, "Towards decentralized IoT security enhancement: A blockchain approach," *Comput. Electr. Eng.*, vol. 72, pp. 266–273, 2018, doi: 10.1016/j.compeleceng.2018.08.021.

[16] Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas, "DDoS in the IoT: Mirai and Other Botnets," *Computer (Long. Beach. Calif).*, p. 79, 2017.

[17] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," *2017 IEEE Int. Conf. Pervasive Comput. Commun. Work. PerCom Work. 2017*, pp. 618–623, 2017, doi: 10.1109/PERCOMW.2017.7917634.

[18] M. Chiang and T. Zhang, "Fog and IoT: An Overview of Research Opportunities," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 854–864, 2016, doi: 10.1109/JIOT.2016.2584538.

[19] E. Reilly, M. Maloney, M. Siegel, and G. Falco, "An iot integrity-first communication protocol via an ethereum blockchain light client," *Proc. - 2019 IEEE/ACM 1st Int. Work. Softw. Eng. Res. Pract. Internet Things, SERP4IoT 2019*, no. April, pp. 53–56, 2019, doi: 10.1109/SERP4IoT.2019.00016.

[20] H. Lindgren *et al.*, "Hash-Chain Based Authentication for IoT Devices and REST Web-Services," *Adv. Intell. Syst. Comput.*, vol. 476, no. ISAmI 2016, pp. V–VI, 2016, doi: 10.1007/978-3-319-40114-0.

[21] W. F. Silvano and R. Marcelino, "Iota Tangle: A cryptocurrency to communicate Internet-of-Things data," *Futur. Gener. Comput. Syst.*, vol. 112, pp. 307–319, 2020,

doi: 10.1016/j.future.2020.05.047.

[22] R. Vinayakumar, K. P. Soman, and P. Poornachandrany, “Applying convolutional neural network for network intrusion detection,” *2017 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2017*, vol. 2017-Janua, pp. 1222–1228, 2017, doi: 10.1109/ICACCI.2017.8126009.

[23] Y. Mirsky, T. Golomb, and Y. Elovici, “Lightweight collaborative anomaly detection for the IoT using blockchain,” *J. Parallel Distrib. Comput.*, vol. 145, pp. 75–97, 2020, doi: 10.1016/j.jpdc.2020.06.008.

[24] Z. Cui *et al.*, “A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN,” *IEEE Trans. Serv. Comput.*, vol. 13, no. 2, pp. 241–251, 2020, doi: 10.1109/TSC.2020.2964537.

[25] M. Ammar, G. Russello, and B. Crispo, “Internet of Things: A survey on the security of IoT frameworks,” *J. Inf. Secur. Appl.*, vol. 38, pp. 8–27, 2018, doi: 10.1016/j.jisa.2017.11.002.

[26] V. Dedeoglu *et al.*, “Blockchain Technologies for IoT,” *Adv. Appl. Blockchain Technol.*, vol. 60, pp. 55–89, 2019.

[27] Secretaría Nacional de Planificación y Desarrollo, “Plan Nacional de Desarrollo 2017-2021-Toda una Vida,” p. 84, 2017.

[28] T. Lin *et al.*, “Implementation of high-performance blockchain network based on cross-chain technology for IoT applications,” *Sensors (Switzerland)*, vol. 20, no. 11, pp. 1–23, 2020, doi: 10.3390/s20113268.

[29] República del Ecuador, *Constitución del Ecuador*. 2008.

[30] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, “Systematic literature reviews in software engineering - A systematic literature review,” *Inf. Softw. Technol.*, vol. 51, no. 1, pp. 7–15, 2009, doi: 10.1016/j.infsof.2008.09.009.

[31] A. Siddiqa, A. Karim, and A. Gani, “Big data storage technologies: a survey,” *Front. Inf. Technol. Electron. Eng.*, vol. 18, no. 8, pp. 1040–1070, 2017, doi: 10.1631/FITEE.1500441.

[32] P. Sharma, R. Jindal, and M. D. Borah, “Blockchain Technology for Cloud Storage: A Systematic Literature Review,” *ACM Comput. Surv.*, vol. 53, no. 4, 2020, doi:

10.1145/3403954.

[33] S. Biswas, K. Sharif, F. Li, B. Nour, and Y. Wang, “A scalable blockchain framework for secure transactions in IoT,” *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4650–4659, 2019, doi: 10.1109/JIOT.2018.2874095.

[34] A. Jindal, G. S. Aujla, N. Kumar, and M. Villari, “GUARDIAN: Blockchain-Based Secure Demand Response Management in Smart Grid System,” *IEEE Trans. Serv. Comput.*, vol. 13, no. 4, pp. 613–624, 2020, doi: 10.1109/TSC.2019.2962677.

[35] A. C. Tsolakis *et al.*, “A Secured and Trusted Demand Response system based on Blockchain technologies,” *2018 IEEE Int. Conf. Innov. Intell. Syst. Appl. INISTA 2018*, 2018, doi: 10.1109/INISTA.2018.8466303.

[36] S. Roy, M. Ashaduzzaman, M. Hassan, and A. R. Chowdhury, “BlockChain for IoT security and management: Current prospects, challenges and future directions,” *Proc. 2018 5th Int. Conf. Networking, Syst. Secur. NSysS 2018*, pp. 1–9, 2019, doi: 10.1109/NSysS.2018.8631365.

[37] K. Gu, L. Wang, and W. Jia, “Autonomous Resource Request Transaction Framework Based on Blockchain in Social Network,” *IEEE Access*, vol. 7, no. c, pp. 43666–43678, 2019, doi: 10.1109/ACCESS.2019.2908627.

[38] D. A. Noby and A. Khattab, “A survey of blockchain applications in IoT systems,” *Proc. - ICCES 2019 2019 14th Int. Conf. Comput. Eng. Syst.*, pp. 83–87, 2019, doi: 10.1109/ICCES48960.2019.9068170.

[39] V. Hassija, V. Chamola, S. Garg, D. N. G. Krishna, G. Kaddoum, and D. N. K. Jayakody, “A Blockchain-Based Framework for Lightweight Data Sharing and Energy Trading in V2G Network,” *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5799–5812, 2020, doi: 10.1109/TVT.2020.2967052.

[40] M. Singh, G. S. S. Aujla, A. Singh, N. Kumar, and S. Garg, “Deep Learning based Blockchain Framework for Secure Software Defined Industrial Networks,” *IEEE Trans. Ind. Informatics*, vol. 3203, no. c, pp. 1–1, 2020, doi: 10.1109/tii.2020.2968946.

[41] Z. Zinonos, P. Christodoulou, A. Andreou, and S. Chatzichristofis, “ParkChain: An IoT parking service based on blockchain,” *Proc. - 15th Annu. Int. Conf. Distrib. Comput. Sens. Syst. DCOSS 2019*, pp. 687–693, 2019, doi:

10.1109/DCOSS.2019.00123.

[42] J. Lin, A. Zhang, Z. Shen, and Y. Chai, “Blockchain and IoT based food traceability for smart agriculture,” *ACM Int. Conf. Proceeding Ser.*, pp. 1–6, 2018, doi: 10.1145/3126973.3126980.

[43] T. McGhin, K. K. R. Choo, C. Z. Liu, and D. He, “Blockchain in healthcare applications: Research challenges and opportunities,” *J. Netw. Comput. Appl.*, vol. 135, no. February, pp. 62–75, 2019, doi: 10.1016/j.jnca.2019.02.027.

[44] B. A. Scriber, “A Framework for Determining Blockchain Applicability,” *IEEE Softw.*, vol. 35, no. 4, pp. 70–77, 2018, doi: 10.1109/MS.2018.2801552.

[45] G. Sargsyan, N. Castellon, R. Binnendijk, and P. Cozijnsen, “Blockchain security by design framework for trust and adoption in IoT environment,” *Proc. - 2019 IEEE World Congr. Serv. Serv. 2019*, pp. 15–20, 2019, doi: 10.1109/SERVICES.2019.00018.

[46] Z. Xu, C. B. Van, T. Jiao, S. Wen, Q. Wang, and Y. Y. Xiang, “An efficient supply chain architecture based on blockchain for high-value commodities,” *BSCI 2019 - Proc. 2019 ACM Int. Symp. Blockchain Secur. Crit. Infrastructure, co-located with AsiaCCS 2019*, pp. 81–88, 2019, doi: 10.1145/3327960.3332384.

[47] Y. Lu, “The blockchain: State-of-the-art and research challenges,” *J. Ind. Inf. Integr.*, vol. 15, no. April, pp. 80–90, 2019, doi: 10.1016/j.jii.2019.04.002.

[48] Y. Wu, H.-N. Dai, and H. Wang, “Convergence of Blockchain and Edge Computing for Secure and Scalable IIoT Critical Infrastructures in Industry 4.0,” *IEEE Internet Things J.*, no. September, pp. 1–1, 2020, doi: 10.1109/jiot.2020.3025916.

[49] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, “Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges,” *IEEE Commun. Surv. Tutorials*, no. c, pp. 1–1, 2020, doi: 10.1109/comst.2020.3020092.

[50] N. Vurukonda and B. T. Rao, “A Study on Data Storage Security Issues in Cloud Computing,” *Procedia Comput. Sci.*, vol. 92, pp. 128–135, 2016, doi: 10.1016/j.procs.2016.07.335.

[51] Q. Zhou, X. Qin, G. Liu, H. Cheng, and H. Zhao, “An efficient privacy and integrity preserving data aggregation scheme for multiple applications in wireless sensor networks,” *Proc. - 2019 IEEE Int. Conf. Smart Internet Things, SmartIoT 2019*, pp.

291–297, 2019, doi: 10.1109/SmartIoT.2019.00051.

[52] D. L. Hernández-Rojas, T. M. Fernández-Caramés, P. Fraga-Lamas, and C. J. Escudero, *A plug-and-play human-centered virtual TEDS architecture for the web of things*, vol. 18, no. 7. 2018.

[53] D. Hernández-Rojas, B. Mazon-Olivo, J. Novillo-Vicuña, C. Escudero-Cascon, A. Pan-Bermudez, and G. Belduma-Vacacela, "IoT android gateway for monitoring and control a WSN," *Commun. Comput. Inf. Sci.*, vol. 798, pp. 18–32, 2018, doi: 10.1007/978-3-319-72727-1_2.

[54] B. Mazon-Olivo, D. Hernández-Rojas, J. Maza-Salinas, and A. Pan, "Rules engine and complex event processor in the context of internet of things for precision agriculture," *Comput. Electron. Agric.*, vol. 154, no. February, pp. 347–360, 2018, doi: 10.1016/j.compag.2018.09.013.

[55] D. V. Medhane, A. K. Sangaiah, M. S. Hossain, G. Muhammad, and J. Wang, "Blockchain-Enabled Distributed Security Framework for Next-Generation IoT: An Edge Cloud and Software-Defined Network-Integrated Approach," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6143–6149, 2020, doi: 10.1109/JIOT.2020.2977196.

[56] P. Koshy, S. Babu, and B. S. Manoj, "Sliding Window Blockchain Architecture for Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3338–3348, 2020, doi: 10.1109/JIOT.2020.2967119.

[57] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the internet of things: Research issues and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, 2019, doi: 10.1109/JIOT.2018.2882794.

[58] S. S. Seshadri *et al.*, "IoTCop: A Blockchain-based Monitoring Framework for Detection and Isolation of Malicious Devices in Internet-of-Things Systems," *IEEE Internet Things J.*, vol. 14, no. 8, pp. 1–1, 2020, doi: 10.1109/jiot.2020.3022033.

[59] Y. Hasegawa and H. Yamamoto, "Reliable IoT Data Management Platform Based on Real-World Cooperation Through Blockchain," *IEEE Consum. Electron. Mag.*, vol. 14, no. 8, 2020, doi: 10.1109/MCE.2020.3011646.

[60] A. H. Sodhro, S. Pirbhulal, M. Muzammal, and L. Zongwei, "Towards Blockchain-Enabled Security Technique for Industrial Internet of Things Based Decentralized

Applications," *J. Grid Comput.*, 2020, doi: 10.1007/s10723-020-09527-x.

[61] M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras, "Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges," *IEEE Access*, vol. 8, pp. 32031–32053, 2020, doi: 10.1109/ACCESS.2020.2973178.

[62] D. L. Hernández-Rojas, T. M. Fernández-Caramés, P. Fraga-Lamas, and C. J. Escudero, *Design and practical evaluation of a family of lightweight protocols for heterogeneous sensing through BLE beacons in IoT telemetry applications*, vol. 18, no. 1. 2018.

[63] J. Hu, M. Reed, N. Thomos, M. F. AI-Naday, and K. Yang, "Securing SDN controlled IoT Networks Through Edge-Blockchain," *IEEE Internet Things J.*, vol. 14, no. 8, pp. 1–1, 2020, doi: 10.1109/jiot.2020.3017354.

[64] A. Kumari, R. Gupta, S. Tanwar, and N. Kumar, "A taxonomy of blockchain-enabled softwarization for secure UAV network," *Comput. Commun.*, vol. 161, no. August, pp. 304–323, 2020, doi: 10.1016/j.comcom.2020.07.042.

[65] P. Kruchten, "The 4+1 View Model of architecture," *IEEE Softw.*, vol. 12, no. 6, pp. 42–50, 1995.