Análisis de la seguridad de los datos en Internet de las Cosas usando tecnología Blockchain

Mg. Jorge Eterovic; Esp. Marcelo Cipriano; Lic. Luis Torres

Instituto de Investigación en Ciencia y Tecnología
Dirección de Investigación Vicerrectorado de Investigación y Desarrollo.
Universidad del Salvador.
Lavalle 1854 – C1051AAB -Ciudad Autónoma de Buenos Aires - Argentina

jorge.eterovic@gmail.com; cipriano1.618@gmail.com; torreslu@ar.ibm.com

RESUMEN.

El mayor reto al que se enfrenta la seguridad de IoT (Internet of Things, Internet de las Cosas) procede de la propia arquitectura del ecosistema actual, que se basa por completo en un modelo centralizado conocido como cliente/servidor. Todos los dispositivos se identifican, autentican y conectan a través de servidores en la nube.

La conexión entre los dispositivos tiene que realizarse a través de la nube, aunque se encuentren separados por tan solo unos pocos metros. Aunque este modelo ha interconectado dispositivos informáticos durante décadas, no podrá responder a las crecientes necesidades de los enormes ecosistemas de IoT del futuro.

La seguridad de este modelo se basa en la existencia de terceras entidades de confianza que emiten certificados digitales a un determinado costo.

El Blockchain es una de las tecnologías más innovadoras de nuestro tiempo y su uso viene ganando interés desde su aparición, gracias a su capacidad para asegurar la integridad de las transacciones y la autenticidad entre cualquier entidad conectada a Internet, de manera descentralizada, lo que significa que no hay un servidor maestro que albergue toda la cadena de transacciones. En su lugar, los nodos participantes tienen una copia de la cadena.

La gran ventaja de Blockchain es que es público. Todos los que participan pueden ver los bloques y las transacciones almacenadas en ellos. La aplicación de esta tecnología en el campo de IoT busca garantizar la seguridad y la privacidad de los datos en la interconexión digital de dispositivos físicos a través de Internet, ya que la cadena de bloques (Blockchain) es descentralizada, por lo que no hay una única autoridad que apruebe las transacciones o defina reglas específicas para la aceptación de transacciones.

Palabras Clave:
Seguridad en Internet de las Cosas. Blockchain. Convergencia IoT-Blockchain.

CONTEXTO

El Vicerrectorado de Investigación y Desarrollo (VRID), perteneciente a la Universidad Nacional del Salvador (USAL), dicta las políticas referidas a la investigación, concibiéndola como un servicio a la comunidad, entendiendo que los nuevos conocimientos son la base de los cambios sociales y productivos. Con el impulso de las propias Unidades Académicas se han venido desarrollando acciones conducentes a concretar proyectos de investigación uni/multidisciplinarios, asociándolos a la docencia de grado y postgrado y vinculando este accionar, para potenciarlo, con otras instituciones académicas del ámbito nacional e internacional.

La Dirección de Investigación, dependiente del VRID, brinda soporte a las distintas Unidades de Investigación de la y a sus investigadores para el desarrollo de Proyectos y Programas de Investigación, nacionales e internacionales,

como así también, apoyo y orientación de recursos para la investigación.

A ella pertenece el Instituto de Investigación en Ciencia y Tecnología (RR 576/12) en el cual se enmarca este proyecto, con una duración de 2 años (2019-2020).

1. INTRODUCCIÓN.

Durante la última década, el IoT (Internet of Things) se ha ido introduciendo gradualmente en nuestras vidas gracias a la disponibilidad de sistemas de comunicación inalámbricos [1].

El paradigma de IoT abarca muchos conceptos; dispositivos inteligentes que recopilan datos del entorno, muchas tecnologías diferentes para permitir su conexión, servicios y estándares, y todos los elementos que participan [2], [3].

IoT puede traer muchos beneficios a la sociedad de muchas maneras diferentes, pero es muy importante estar atento para que se encuentre la mejor solución para proteger la privacidad de los datos [4] [5].

El gran desafío del IoT es encontrar un entorno de comunicación confiable que garantice la seguridad de los datos transmitidos entre todos los dispositivos conectados [6].

Una de las posibles soluciones podría ser la convergencia entre la tecnología IoT y Blockchain. Esta hipótesis se analizará en este proyecto de investigación [7].

Hay tres elementos principales a los que se hace referencia en una arquitectura de IoT [8] [10]:

1. Cosas: Dispositivos que tienen un medio de conectarse a una red más amplia.
2. Red: Conecta los múltiples dispositivos a la nube.
3. Nube: Los servidores remotos en un centro de datos cuya función es consolidar y almacenar los datos de forma segura.

La tecnología Blockchain tiene el potencial de asegurar este entorno, gracias a la criptografía, que todos los usuarios tengan una clave secreta y única a través de la cual acceden a sus datos [9].

Los protocolos abiertos basados en Blockchain pueden estandarizar el uso de los protocolos de comunicaciones y geolocalización de todos los tipos de sensores, tan comunes por ejemplo, en las líneas de montaje del sector industrial para automatizar los datos de forma segura (Industria 4.0) [11].

Muchos sectores se beneficiarán de esta tecnología, como el del cuidado de la salud o los sectores de transporte y logística, que también podrán obtener grandes beneficios de su uso para integrar las ventajas del IoT [8].

Las ventajas que ofrece incluyen la descentralización y la transparencia de la información, ya que todos los actores están en el mismo nivel jerárquico, evitando que un organizador principal use incorrectamente los datos [3].

Aunque actualmente no se puede garantizar el entorno deseado de una manera completamente segura, muchas empresas y organizaciones trabajan para mejorar cada vez más esta cobertura de Internet de las cosas. No es imposible evitar los ataques, pero los hace mucho más difíciles de producir.

Muchos estudios se centran actualmente en el uso de cifrado homomórfico. En el pasado, ya se ha demostrado que este cifrado era factible, pero requiere mucho más tiempo que los procesos convencionales, y hay que seguir investigando para mejorarlo.

Por el momento no existe un desarrollo sólido para mantener la seguridad deseada en este entorno y los ataques a los dispositivos son el principal desafío que tenemos por delante [4].

Este proyecto de investigación se centra en la necesidad de revisar y estudiar toda la información a través de diversas investigaciones llevadas a cabo en el campo de IoT, Blockchain y su convergencia, y analizar cuáles son las mejores soluciones para minimizar las amenazas y vulnerabilidades de las principales tecnologías que forman parte de Internet de cosas.

El resultado esperado es reunir la información clave del paradigma de IoT relacionado con la seguridad y los mejores mecanismos para garantizar la integridad y la privacidad de los datos en IoT.

Otro objetivo es permitir que otras personas interesadas en este campo accedan fácilmente a la información y el conocimiento recogidos en este proyecto.

Finalmente, se propondrán algunos escenarios donde podría converger la tecnología IoT y Blockchain en el futuro.

2. LÍNEAS DE INVESTIGACIÓN y DESARROLLO.

La metodología para llevar a cabo este proyecto es buscar información en artículos de investigación y publicaciones para estudiar las amenazas y vulnerabilidades más importantes que se han presentado hasta el momento en el paradigma de IoT.

También se estudiará como aporta a la seguridad la tecnología Blockchain.

Luego, se analizará la convergencia de ambas tecnologías y como se puede resolver el problema de garantizar la privacidad y seguridad de los datos en IoT usando Blockchain para generar entornos de confianza que pueden prevenir futuros ataques.

Finalmente se redactará un informe con los resultados obtenidos.

3. RESULTADOS OBTENIDOS/ ESPERADOS.

Los objetivos de este proyecto de investigación son:

- Exponer en detalle los conceptos de IoT (Internet de las cosas) y Blockchain y hacer un estudio de su impacto en la sociedad y sus perspectivas de futuro como posibles aplicaciones.
- Hacer un estudio de los artículos de investigación y publicaciones que relacionen estos conceptos, destacando las contribuciones más importantes.
- Analizar la privacidad en el intercambio de datos en las principales tecnologías de IoT y cuáles son las mejores contramedidas para evitar las posibles amenazas.
- Analizar los desafíos y oportunidades de la convergencia entre IoT y la tecnología Blockchain.
- Proponer la convergencia de las tecnologías IoT y Blockchain para aplicaciones seguras.

4. FORMACIÓN DE RECURSOS HUMANOS.

El equipo de investigadores pertenece al cuerpo docente de Tecnologías Aplicadas de la Facultad de Ingeniería, específicamente al área de la Seguridad Informática, de la Universidad del Salvador.

A este proyecto, que recién inicia, se incorporarán próximamente un docente investigador con amplia experiencia en la industria y 2 alumnos que se encuentran promediando la carrera de Ingeniería en Informática.

Esto redundará en un aumento del activo académico e investigativo representado por su cuerpo de docentes investigadores, como así también sembrará las bases para la investigación a futuro, a través de la participación de alumnos de la Facultad de Ingeniería.

5. BIBLIOGRAFÍA.

[1] F. Mattern and C. Floerkemeier; "From the Internet of Computers to the Internet of Things"; ACM Digital Library; From Active Data Management to Event-Based Systems and More; 2010. http://www.vs.inf.ethz.ch /publ/papers/Internet-of-things.pdf.

[2] R. Minerva, A Biru, D. Rotondi; "Towards a definition of the Internet of Things (IoT)"; IEEE Xplore Digital Library; 2015. https://iot.ieee.org/images/files/pdf/

IEEE_IoT_Towards_Definition_Internet_of_Things_ Revision1_27MAY15.pdf

[3] Shaddad Abdul-Qawy, P. P. J, E. Magesh, T. Srinivasulu; "The Internet of Things (IoT): An Overview"; Directory of Open Access Journals; International Journal of Engineering Research and Applications; V.5, N. 12; 2015.

[4] D.Mendez, I. Papapanagiotou, B Yang; "Internet of Things: Survey on Security and Privacy"; Cornell University Library; 2017. https://arxiv.org/abs/1707.01879

[5] J. Granjal, E. Monteiro, J. Sá Silva; "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues"; IEEE Xplore Digital Library; IEEE Communications Surveys & Tutorials, 2015, Volume 17, Number 3; http://0-ieeexplore.ieee.org.cataleg.uoc.edu/ document/7005393

[6] A. Bahga, V. K. Madisetti, "Blockchain Platform for Industrial Internet of Things"; Scientific Research; Vol.9, No.10, October 2016. https://www.scirp.org/Journal/Paper Information.aspx?PaperID=71596

[7] E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A Margheri, and V. Sassone; "Blockchain-based Database to Ensure Data Integrity in Cloud Computing Environments"; First Italian Conference on Cybersecurity (ITASEC17); Venice, Italy; 2017. http://ceur-ws.org/Vol-1816/paper-15.pdf

[8] G.Zyskind, O. Nathan, A. Sandy Pentland; "Decentralizing Privacy: Using Blockchain to Protect Personal Data"; IEEE Xplore Digital Library; Security and Privacy Workshops (SPW); 2015. http://ieeexplore.ieee.org/ document/ 7163223/

[9] T. Tuan Anh Dinh, R. Liu; "Untangling Blockchain: A Data Processing View of Blockchain Systems"; Cornell University Library; 2017. http://www.comp.nus.edu.sg/ ~ooibc/blockchainsurvey.pdf

[10] K. Christidis, "Blockchains and Smart Contracts for the Internet of Things" IEEE Xplore Digital Library, IEEE Access, Volume 4; 2016. http://0-ieeexplore.ieee.org.cataleg.uoc.edu/document/7467408/

[11] J.L. del Val Román, "Industria 4.0: la transformación digital de la industria" Informe CODDii, Conferencia de Directores y Decanos de Ingeniería Informática, Facultad de Ingeniería de la Universidad de Deusto. Bilbao, España. 2016.