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

Data security analysis on the Internet of Things, using Blockchain technology

Investigadores USAL:
Eterovic, Jorge (jorge.eterovic@usal.edu.ar); Cipriano, Marcelo; Torres, Luis

Alumnos practicantes USAL:
Madeo, Juan; Fernández, Nicolás

Palabras clave: Seguridad en IoT; Cadena de bloque; Convergencia IoT.
Keywords: *IoT Security; Blockchain; Convergence IoT.*

Resumen

El mayor reto al que se enfrenta la seguridad de la comunicación de los datos en 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 se realiza a través de Internet, sin importar la distancia. Este modelo ha interconectado dispositivos informáticos durante décadas, pero no podrá responder a las crecientes necesidades de los ecosistemas de IoT del futuro. Actualmente la seguridad se basa en la existencia de terceras entidades de confianza que emiten certificados digitales a un determinado costo, pero esta solución no es aplicable a los dispositivos que tienen baja capacidad de almacenamiento y procesamiento.

A partir de esta realidad, este trabajo se centró en la búsqueda y análisis de distintos estudios e investigaciones llevadas a cabo en el campo de IoT y Blockchain y cómo la convergencia de ambas tecnologías pueden aportar a la seguridad a los datos que se trasmiten en la nube. El IoT puede brindar muchos beneficios a la sociedad de diferentes maneras, pero es muy importante investigar y trabajar buscando la mejor solución para proteger la seguridad en la comunicación de los datos entre todos los dispositivos conectados. 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, logrando descentralizar y transparentar la información, ya que todos los actores están en el mismo nivel jerárquico, evitando que un organizador principal pueda manipular los datos.

En el sector industrial, los protocolos de comunicación y geolocalización de los sensores son comunes en las líneas de montaje para automatizar los procesos. También en ámbitos tales como el del cuidado de la salud, el transporte y la logística, entre otros. Actualmente no se pueden garantizar que

las comunicaciones se realicen de una manera segura, sin embargo muchas empresas y organizaciones trabajan para mejorar este aspecto de Internet de las Cosas, partiendo de la premisa que no es imposible evitar los ataques, pero si aportar soluciones que los hagan mucho más difíciles de producir. Gran cantidad de estudios se centran actualmente en el uso de cifrado convencional. En el pasado, ya se ha demostrado que este cifrado era factible, pero requiere mucha capacidad de procesamiento y almacenamiento, que no todos los dispositivos poseen. Por el momento no existe un desarrollo sólido para mantener la seguridad deseada en este entorno y los ataques a la seguridad de los datos son el principal desafío que tenemos por delante.

Este proyecto de investigación se centró en la búsqueda y análisis de la información de diversos estudios e investigaciones llevadas a cabo en el campo de IoT, Blockchain y su convergencia para dar seguridad, destacando los beneficios y desafíos a resolver, donde los nodos no confiables pueden interactuar entre sí sin un intermediario confiable, de manera verificable.

Como conclusión de este trabajo de investigación se puede asegurar que los mecanismos de consenso y criptografía de clave pública de la tecnología Blockchain permiten resolver los problemas de seguridad, privacidad y confianza en las comunicaciones entre todas las partes que conforman el sistema de Internet de las Cosas.

Abstract:

The greatest challenge that the security of data communication in IoT (Internet of Thing) faces comes from the architecture of the current ecosystem itself, which is completely based on a centralized model known as client/server. All devices are identified, authenticated, and connected through servers in the cloud.

The connection between the devices is made through the Internet, regardless of distance. This model has interconnected computing devices for decades, but it will not be able to respond to the growing needs of the IoT ecosystems of the future. Currently, security is based on the existence of trusted third parties that issue digital certificates at a certain cost, but this solution is not applicable to devices that have low storage and processing capacity. Based on this reality, this work focused on the search and analysis of different studies and research carried out in the field of IoT and Blockchain, and how the convergence of both technologies can contribute to the security of the data transmitted in the Cloud.

The IoT can bring many benefits to society in different ways, but it is very important to research and work towards the best solution to protect the security of data communication between all connected devices. Blockchain is one of the most innovative technologies of our time and its use has been gaining interest since its appearance, thanks to its ability to ensure the integrity of transactions and authenticity between any entity connected to the Internet in a decentralized way, which means that there is no master server hosting the entire chain of transactions. Instead, the participating nodes have a copy of the chain, achieving decentralization and making the information transparent, since all the participants are at the same hierarchical level, preventing a main organizer from manipulating the data.

In the industrial sector, communication protocols and geolocation of sensors are common in assembly lines to automate processes. They are also common in areas such as health care, transportation, and logistics, among others. Currently, communications cannot be guaranteed to be made in a secure manner; nevertheless, many companies and organizations are working to improve this aspect of the Internet of Things, starting from the premise that it is not possible to prevent attacks, but it is to provide solutions that make them much more difficult to occur.

Many studies are currently focused on the use of conventional encryption. In the past, this encryption has already been shown to be feasible, but it requires a lot of processing and storage

power, which not all devices have. At the time, there is no solid development that ensures the desired security in this environment. Attacks on data security are the main challenge ahead.

That is why this research project focused on searching and analysing the information from various studies and research carried out in the field of IoT, Blockchain and their convergence to provide security, highlighting the benefits and challenges to be solved, in which the untrusted nodes can interact with each other without a trusted intermediary in a verifiable way.

As a conclusion, it can be assured that the consensus mechanisms and public key cryptography of Blockchain technology allow the solving of security, privacy, and trust issues in communications between all the parties that make up the Internet of Things system.