Mecanismo de seguridad para sistemas IoT mediante blockchain

Director de Tesis: Dra. Erica Cecilia Ruiz Ibarra

Codirector: Dr. Adolfo Espinoza Ruiz

Problema a resolver:

El IoT es la tecnología que consiste en objetos con capacidad para conectarse a internet, interactuar entre sí y compartir información al estar conectados a la red de redes. Los dispositivos IoT generan grandes cantidades de información valiosa para las empresas, la cual utilizan para analizar y generar nuevas ideas, productos e investigaciones [1]. Sin embargo, por ser una tecnología que no se encuentra en una fase de madurez, tiende a sufrir vulnerabilidades, esto se ve reflejado al momento de su implementación en algunos sectores debido a la falta de seguridad en los dispositivos y la falta de conocimiento por parte del usuario, quienes tienden a dejar las claves de acceso por defecto en los dispositivos IoT, permitiendo a los cibercriminales realizar ataques a través de estos dispositivos. Según estudios realizados por Symantec, los mayores ataques se realizan haciendo uso de los dispositivos IoT, aprovechando su fácil acceso y control de los dispositivos de forma remota con ataques ransomware [2].

Concretamente, la revolución IoT está causando un crecimiento masivo en el número de dispositivos conectados a Internet. Se estima que en 2020 se alcanzarán cifras próximas a los 50 mil millones. Esto plantea serios problemas a las arquitecturas en la nube, que siguen un paradigma centralizado, ya que serían incapaces de procesar cantidades de datos tan grandes. Por ello, técnicas descentralizadas como el Edge Computing [3], mejor preparadas para la distribución de carga, van a ocupar un rol fundamental en un futuro próximo. Otro problema que se presenta, causado por claras limitaciones de diseño, es la incapacidad para utilizar mecanismos de seguridad tradicionales por parte de los dispositivos IoT [4], convirtiéndolos en posibles objetivos vulnerables [5, 6]. Estos, por su baja potencia y restricciones de consumo, necesitan soluciones más ligeras o el uso de tecnologías que sigan un planteamiento distinto.

Productos académicos comprometidos:

1 artículo de revista indizada

Estancia del estudiante (en caso de ser posible):

Estancia corta en el Universidad de Mérida Yucatán con Dr. Javier Velázquez (SNI 1)

Conferencia del estudiante:

IoT Solutions World Congress (2021) **https://www.iotsworldcongress.com/**

Referencias

[1] J. E. Salvatore et al., “Tecnologías de la información y las comunicaciones mediante IoT para la solución de problemas en el medio socio productivo”.http://sedici.unlp.edu.ar/bitstream/handle/109

[2] ŸSymantec, “ISTR Internet Security Threat Report” https://www.symantec.com/content/dam/sym antec/docs/reports/istr-24-2019-en.pdf

[3] S. Madakam, R. Ramaswamy and S. Tripathi, “Internet of Things (IoT): A Literature Review,” 2015. [Online]. Available: https://file.scirp.org/pdf/JCC_2015052516013923.pdf

[4] W. Shi, “Edge computing: Vision and challenges,” IEEE Internet of Things Journal 3.5, 2016.

[5] J. Pan and J. McElhannon, “Future Edge Cloud and Edge Computing for Internet of Things Applications,” IEEE nternet of Things Journal, Special Issue on Fog Computing in IoT, 2018.

[6] A. Mosenia and N. K. Jha, “A comprehensive study of security of internet-of-things,” IEEE Transactions on Emerging Topics in Computing, 2017