2 evaluación 30% 29/04/2024

- Presentación de su título para el artículo (el mismo será escogido de manera libre pero dentro de los principios de la informática, ingeniería en sistema, ingeniería de la computación)

- Definir y justificar el título (así como se hizo en la discusión en clases de la evaluación anterior)

- Escoger 4 artículos, publicaciones o bibliografía que se refieran a ese tema escogido y se le hará un resumen de lo que consideran que es de aporte importante a su artículo científico.

(Son 4 resúmenes descrito en 1 o 2 párrafo cada uno)

Se debe indicar:

- Autores

- título del artículo, revista científica, ponencia o investigación

- año

- universidad, revista o evento donde se presentó la ponencia

Titulo: "Exploración de Tendencias Emergentes en Ciberseguridad: Hacia un Futuro Más Seguro"

"Hacia la Inmunidad Digital: Innovaciones y Desafíos en Ciberseguridad"

1. **Claridad y Relevancia**: El título es claro y directo. Describe el enfoque del artículo: explorar las tendencias emergentes en ciberseguridad. Al incluir "futuro más seguro", se resalta la relevancia de las tecnologías que se abordarán.
2. **Inclusión de Palabras Clave**: Las palabras clave "ciberseguridad" y "tecnologías futuras" están presentes. Esto facilita la búsqueda y la indexación del artículo en bases de datos académicas.
3. **Perspectiva Positiva**: La frase "Hacia un Futuro Más Seguro" sugiere una perspectiva optimista. Los lectores pueden esperar descubrir soluciones y avances que contribuyan a la seguridad digital.
4. **Concisión y Estilo**: El título es breve y no contiene abreviaciones. Cumple con las recomendaciones de las **Normas APA** para títulos científicos .

Adaptive Blockchain Technology for a Cybersecurity Framework in IIoT

Publicado en: IEEE Revista Iberoamericana de Tecnologias del Aprendizaje (Volume: 17, Issue: 2, May 2022).

En este estudio, los autores exploran cómo la tecnología blockchain puede adaptarse para fortalecer los marcos de ciberseguridad en el Internet Industrial de las Cosas (IIoT). El IIoT se refiere a la interconexión de dispositivos y sistemas en entornos industriales, como fábricas, plantas de energía y redes de suministro.

El artículo propone una arquitectura basada en blockchain que aborda varios desafíos de seguridad en el IIoT. La tecnología blockchain permite verificar la integridad de los datos almacenados en dispositivos conectados. Cada transacción se registra en bloques enlazados criptográficamente, lo que dificulta la manipulación de datos mediante contratos inteligentes. Gracias a estos, se pueden establecer reglas de acceso y autorización para dispositivos y usuarios en la red. Esto mejora la seguridad y reduce los riesgos de acceso no autorizado.

La descentralización inherente de la tecnología blockchain dificulta los ataques dirigidos a un único punto de falla. Además, la inmutabilidad de los registros garantiza la trazabilidad y la auditoría.

Realizado por: Yeison Isaac LLanten Lucio; Katerine Márceles Villalba; Siler Amador Donado

Adaptive Blockchain Technology for a Cybersecurity Framework in IIoT | IEEE Journals & Magazine | IEEE Xplore

Servicio de navegación anónima basada en un Raspberry Pi

Publicado en: IEEE Revista Iberoamericana de Tecnologias del Aprendizaje

Los dispositivos Raspberry Pi que tiene instalado Tor y funciona como proxy anónimo. Al acceder a internet a través de Onion Pi como intermediario en lugar de hacerlo directamente desde el router, los usuarios pueden navegar con mayor libertad, evitando problemas de seguridad y privacidad. Por lo que crear un servicio de navegación anónima utilizando una Raspberry Pi y la red Tor, lo que proporciona una capa adicional de anonimato al tráfico de internet.

Realizado por: María Alejandra Zuñiga , Siler Amador Donado, Katerine Márceles Villalba

https://www.proquest.com/openview/5615fedd1bf08723cb42f214c4a7748e/1?pq-origsite=gscholar&cbl=1006393