ANEXO

FUNDAMENTACIÓN:

La Criptografía y los Sistemas Distribuidos son áreas de rápido desarrollo y vital importancia no solamente para el mundo actual, sino también para futuras aplicaciones. La criptografía moderna ha permitido el desarrollo de los sistemas de comunicación y comercio electrónicos, a partir de la postulación de los fundamentos y esquemas prácticos de criptografía de clave pública. Esto permitió no solamente desarrollar métodos eficientes de intercambio de clave en canales inseguros, sino también métodos de autenticación basados en firmas digitales. Posteriormente, el desarrollo de pruebas de integridad criptográfica permitió asegurar la integridad de un cómputo, de un modo que es eficiente en términos de tiempo de verificación y costo de comunicación. Estos métodos resultan cruciales para el escalamiento de block chains, donde la validez de los cómputos está basado en la re-ejecución de los mismos.

El rápido desarrollo de la inteligencia artificial también presenta desafíos desde el punto de vista de la criptografía. El uso de cloud computing presenta vulnerabilidades a los datos, ya que, si bien estos son encriptados cuando se transmiten a los servidores que los procesarán, nada impide que quienes operen los servidores tengan acceso a los datos o que atacantes puedan comprometer a dichos servidores. La encriptación totalmente homomórfica permite el cálculo sobre datos encriptados, sin la necesidad de desencriptarlos primero, mitigando estos riesgos.

Dentro de las aplicaciones de la criptografía, podemos mencionar:

1. Crecientes amenazas a la ciberseguridad

A medida que proliferan los sistemas digitales y los servicios en línea, también lo hacen las amenazas que plantean los ciberdelincuentes. Los métodos criptográficos avanzados son esenciales para proteger datos confidenciales, proteger las comunicaciones y garantizar la integridad y confidencialidad de las transacciones digitales.

2. Proliferación de la tecnología Blockchain

La tecnología Blockchain está revolucionando diversas industrias, desde las finanzas (por ejemplo, las criptomonedas) hasta la gestión de la cadena de suministro, la atención médica y más. La naturaleza descentralizada e inmutable de blockchain requiere técnicas criptográficas sofisticadas para garantizar su seguridad, escalabilidad y eficiencia.

3. Problemas de privacidad y robo de identidad

Con la creciente cantidad de datos personales que se comparten y almacenan en línea, el robo de identidad y las violaciones de la privacidad se han convertido en preocupaciones importantes. Se necesitan mecanismos de identidad eficaces y tecnologías que preserven la privacidad para proteger las identidades y la información personal de las personas.

4. Avances en Computación Cuántica

La computación cuántica plantea una amenaza potencial a los algoritmos criptográficos tradicionales. A medida que las computadoras cuánticas se vuelven más capaces, existe una necesidad apremiante de desarrollar métodos criptográficos resistentes a las computadoras cuánticas para salvaguardar los datos contra futuros ataques cuánticos.

5. Finanzas Descentralizadas (DeFi) y Web 3.0

El auge de las finanzas descentralizadas y el desarrollo de la Web 3.0 se basan en sistemas seguros y descentralizados. La criptografía y los sistemas distribuidos son fundamentales para permitir interacciones seguras, transparentes y sin confianza en estos nuevos paradigmas digitales.

6. Seguridad del Internet de las cosas (IoT)

El ecosistema de IoT se está expandiendo rápidamente y conecta miles de millones de dispositivos. Proteger estos dispositivos y sus comunicaciones requiere protocolos criptográficos sólidos para evitar vulnerabilidades y garantizar un funcionamiento confiable.

7. Transformación Digital y Ciudades Inteligentes

A medida que las sociedades avanzan hacia la transformación digital y el desarrollo de ciudades inteligentes, la necesidad de infraestructuras digitales seguras, confiables y escalables se vuelve primordial. La criptografía y los sistemas distribuidos son esenciales para respaldar estos avances, garantizando un intercambio de datos seguro, una conectividad confiable e infraestructuras resilientes.

8. Sistemas de identidad digital mejorados

Los futuros sistemas de identidad digital deberán ser más seguros, estar centrados en el usuario y preservar la privacidad. Las innovaciones en marcos de identidad descentralizados, respaldados por técnicas criptográficas avanzadas, permitirán a las personas controlar sus identidades y datos personales.

OBJETO:

El Centro de Criptografía y Sistemas Distribuidos de la UBA tendrá por objeto el estudio de áreas de tecnología e informática vinculadas a la criptografía, los sistemas distribuidos, compiladores y programación de sistemas (*system programming*) generando nuevo acervo de conocimiento para la academia, la vinculación tecnológica y la producción de insumos que tiendan a la innovación científica y tecnológica.

FUNCIONES

1. Realizar estudios sobre criptografía, programación concurrente, sistemas distribuidos y compiladores y temas vinculados.
2. Publicitar resultados y hallazgos, a través de publicaciones, eventos y conferencias en razón de su competencia.
3. Promover la vinculación y transferencia tecnológica, así como también, el asesoramiento de las áreas específicas en todos sus ámbitos de aplicación posibles (empresas privadas, organismos públicos, etc.).
4. Desarrollar material didáctico y realizar tareas de enseñanza tanto en ámbitos públicos como privados.

1821 Universidad de Buenos Aires

Anexo Resolución Consejo Superior

Hoja Adicional de Firmas

Número: ACS-2024-175-E-UBA-SG#REC

CIUDAD DE BUENOS AIRES
Miércoles 14 de Agosto de 2024

Referencia: EX-2023-02854072- -UBA-DME#REC - Centro de Criptografía y Sistemas Distribuidos de la UBA

El documento fue importado por el sistema GEDO con un total de 3 pagina/s.

Digitally signed by ALFONSIN Juan
Date: 2024.08.14 14:15:46 ART
Location: Ciudad Autónoma de Buenos Aires

Juan Alfonsin
Secretario General
Secretaría General
Rectorado

Digitally signed by GDE UBA
Date: 2024.08.14 14:15:47 -03:00