PROYECTO DE AULA

JESUS MANUEL BERMUDEZ CASTRILLO
JERSON CAMILO TAPIAS CASTRO

DOCENTE: JUAN ANDRES YANETH
SEMINARIO DE INVESTIGACIÓN – GRUPO: 02

UNIVERSIDAD POPULAR DEL CESAR
FACULTAD DE INGENIERÍA DE SISTEMAS
VALLEDUPAR – CESAR
2023

Análisis de la computación cuántica en los sistemas de ciberseguridad en Medellín, Antioquia durante el periodo 2019-2023

Objetivo General: Examinar la implementación de la computación cuántica en los sistemas de ciberseguridad en Medellín, Antioquia.

Objetivos Específicos:

Examinar las aplicaciones prácticas de la computación cuántica en Ciberseguridad.

Analizar la Adopción de la computación cuántica en empresas de Ciberseguridad en Medellín.

Identificar las perspectivas futuras de la computación cuántica en Ciberseguridad en Medellín.

Variable: la variable es **"*la computación cuántica*"**, que es el concepto o aspecto específico que se está investigando. El problema o enfoque del estudio sería cómo esta variable se relaciona o impacta en los sistemas de ciberseguridad durante el período 2019-2023.

Planteamiento del problema

La ciberseguridad es un campo en constante cambio, desafiado por avances tecnológicos que amenazan la seguridad de la información. La computación cuántica, una innovación disruptiva, se perfila como un desafío crítico a nivel internacional.

Macro: La computación cuántica, con su capacidad para realizar cálculos más rápidos y la posibilidad de superar sistemas de seguridad actuales, plantea interrogantes sobre cómo afectará a la ciberseguridad; debido a esto, diversos países están invirtiendo en investigaciones y desarrollos en ciberseguridad, con un enfoque creciente en la computación cuántica, llevando a cabo iniciativas para comprender y enfrentar este desafío, ya que se necesita un análisis profundo para comprender su impacto y cómo se están adaptando las estrategias de protección.

Meso: En la Universidad del Valle (Cali, Valle del Cauca), Los físicos colombianos John Reina, Cristian Susa y Andrés Ducuara, hablaron a cerca de los qubits. “un procesamiento masivo de información, en paralelo, porque todo se hace simultáneamente, a diferencia de los computadores clásicos” dándonos a entender el potencial de estas computadoras cuánticas en cuanto a la aceleración de actividades de procesamiento de datos, ligando esto directamente con la ciberseguridad y como cambiara con esta nueva tecnología.

Este estudio busca entender cómo la computación cuántica está cambiando el panorama de la ciberseguridad y cómo se puede garantizar la seguridad en este nuevo entorno tecnológico.

Control

La computación cuántica, puede mejorar mucho la ciberseguridad, pero también puede mejorar los ataques y amenazas, para poder mitigar estas amenazas, se puede brindar educación y capacitación en seguridad y para personas con mayor conocimiento del tema, capacitación en seguridad cuántica.

Además, la implementación de algoritmos cuánticos resistentes y la implementación de criptografía cuántica. A través de protocolos como el "BB84 Quantum key Distribution", mejoraría la seguridad en la comunicación de dos partes. De igual manera la adopción de pruebas de Post-Quantum, garantizaría la resistencia futura de los sistemas criptográficos.

Pronostico

Se espera una continua mejora en el desarrollo de hardware cuántico, con la aparición de computadoras cuánticas más potentes y accesibles para la investigación y algunas aplicaciones comerciales especializadas. Aunque no reemplazarán a las computadoras clásicas, proporcionarán un entorno de prueba para algoritmos cuánticos y técnicas de ciberseguridad cuántica. De igual forma, se prevé un crecimiento en la cantidad y complejidad de algoritmos cuánticos prácticos y su aplicación en áreas como optimización, simulación molecular y aprendizaje automático. Esto aumentará la necesidad de soluciones de seguridad cuántica para proteger estos algoritmos y sus aplicaciones. Por ende, se anticipa una mayor conciencia sobre la amenaza que la computación cuántica representa para los algoritmos de criptografía clásica. La necesidad de migrar a algoritmos postcuánticos será más evidente, especialmente en sectores con datos sensibles.

Dicho todo esto se espera una mayor integración de tecnologías cuánticas en la ciberseguridad empresarial, especialmente en organizaciones con un enfoque en investigación, desarrollo e innovación, para fortalecer la protección de datos y sistemas críticos.