TRAVESÍA EMPRENDEDORA
Volumen 8 No. 2
traves. emprend.
Jul-Dic 2024
e-ISSN: 2539-0376

# Análisis de tendencias y amenazas en la Internet de las Cosas (IoT)

**Jaider Jhoan Chamorro Córdoba**
Estudiante de Ingeniería de Sistemas
Universidad Mariana
Correo: jaiderjh.chamorro@umariana.edu.co

**Johan Javier Gonzales Cortez**
Estudiante de Ingeniería de Sistemas
Universidad Mariana
Correo: johanja.gonzalez@umariana.edu.co

**Juan Manuel Cáceres Paz**
Estudiante de Ingeniería de Sistemas
Universidad Mariana
Correo: cristianda.ortega@umariana.edu.co

## Introducción

En un mundo cada vez más conectado, la Internet de las Cosas (IoT, por sus siglas en inglés) ha experimentado un crecimiento exponencial y se ha convertido en una tecnología habilitada en múltiples sectores, desde la salud y la industria hasta la agricultura y la domótica. Sin embargo, este avance tecnológico no está a la altura de desafíos significativos, ya que la proliferación de dispositivos IoT también conlleva graves amenazas a la seguridad y la privacidad.

El problema central de esta investigación radica en la necesidad de comprender y abordar las tendencias emergentes en la IoT y, al mismo tiempo, analizar las amenazas a la seguridad y la privacidad asociadas a esta tecnología en constante evolución.

A medida que la IoT se integra cada vez más en nuestra vida cotidiana y en diversas aplicaciones industriales y comerciales, surge una pregunta fundamental: ¿Cómo se puede aprovechar las tendencias positivas en la IoT, al tiempo que se mitiga las amenazas que ponen en riesgo la seguridad de la información y la privacidad de los usuarios? Este estudio se enfoca en investigar las tendencias más recientes en la IoT, examinando su aplicación en distintos campos de la ingeniería y, analizando las principales amenazas relacionadas con la ciberseguridad, la integridad de los datos y la protección de la información personal.

El objetivo es proporcionar una visión integral de este campo en constante cambio y, contribuir a la identificación de estrategias efectivas para abordar estos desafíos, lo que es esencial para garantizar un uso seguro y eficaz de la IoT en el futuro.

## Desarrollo

La rápida evolución de la IoT ha transformado la forma como interactuamos con el mundo digital. La IoT es una red colectiva de dispositivos conectados y tecnología que facilita la comunicación entre ellos; se ha convertido en una de las tecnologías más importantes del siglo XXI y, su uso se ha generalizado en el mercado. Aunque la adopción generalizada de la IoT ha mejorado la eficiencia y la comodidad en una multitud de sectores, no se puede ignorar el creciente riesgo asociado con la seguridad y la privacidad de los datos en este entorno conectado. Es imperativo comprender y abordar estas amenazas emergentes para garantizar un desarrollo sostenible y seguro de la IoT en la vida cotidiana y en aplicaciones industriales.

Un ejemplo cotidiano de las implicaciones de la IoT es el uso de dispositivos de domótica en hogares inteligentes. Estos sistemas permiten a los usuarios controlar la iluminación, la temperatura, los electrodomésticos y la seguridad de sus hogares mediante la integración de dispositivos interconectados y sensores. Aunque este nivel de automatización y conectividad brinda comodidad y eficiencia, también plantea desafíos en términos de seguridad cibernética y privacidad de datos personales. La posibilidad de ataques cibernéticos a través de estos dispositivos, así como la recolección y el uso indebido de datos personales, resalta la necesidad urgente de comprender y abordar las amenazas asociadas con la IoT.

Por lo tanto, esta investigación busca proporcionar una visión exhaustiva de las tendencias y amenazas en la IoT, con el objetivo de destacar la importancia de implementar estrategias efectivas para garantizar la seguridad y la privacidad de los usuarios. Al comprender cómo las tendencias emergentes en la IoT impactan diversos campos de la ingeniería y evaluar las amenazas relacionadas con la ciberseguridad y la protección de datos, este estudio se propone proporcionar recomendaciones concretas para mitigar los riesgos y promover un uso seguro y eficaz de la IoT en el futuro.

## Metodología

Se ha adoptado un enfoque histórico-hermenéutico dentro del paradigma cualitativo para este estudio de caso. Este enfoque, basado en la comprensión profunda de los fenómenos sociales y tecnológicos tiene como objetivo, explorar las percepciones, experiencias y significados de las personas con relación a la IoT. La dimensión histórica de nuestra investigación se centra en rastrear la evolución temporal de la IoT en la domótica, mientras que la dimensión hermenéutica busca interpretar los significados subyacentes. Esta metodología facilita la construcción de una narrativa contextualizada, donde la historia se entrelaza con experiencias y valores.

### Unidad de análisis y unidad de trabajo

La unidad de análisis para este trabajo de grado son los estudiantes y profesores de la Facultad de Ingeniería de la Universidad Mariana, ubicada en la ciudad de Pasto, Nariño, Colombia, que cuentan con algún grado de conocimiento o experiencia práctica en el campo de la domótica. Dada la naturaleza específica de esta población, caracterizada por su interés y participación activa en el ámbito de la IoT aplicada a la domótica, se opta por un muestreo no probabilístico.

La unidad de trabajo se selecciona mediante muestreo intencionado con el cumplimiento de los siguientes criterios: población, caracterizada por su interés y participación activa en el ámbito de la IoT aplicada a la domótica; se opta por un muestreo no probabilístico.

La unidad de trabajo se selecciona mediante muestreo intencionado con el cumplimiento de los criterios establecidos en la Tabla 2:

**Tabla 1**

*Criterios*

| Criterios de inclusión | Criterios de exclusión |
|---|---|
| Estudiantes universitarios y docentes de la Universidad Mariana en la ciudad de Pasto, Nariño. | Estudiantes y docentes que no pertenezcan a la Universidad Mariana en la ciudad de Pasto, Nariño. |
| Estudiantes y docentes que hayan utilizado o estén utilizando dispositivos domóticos en sus residencias. | Estudiantes y docentes que no hayan utilizado dispositivos domóticos en sus residencias. |
| Estudiantes y docentes que posean un nivel mínimo de conocimiento o experiencia práctica en el campo de la domótica y la IoT. | Estudiantes y docentes que no estén dispuestos a participar voluntariamente en el estudio. |
| Estudiantes y docentes que estén dispuestos a compartir sus percepciones y experiencias relacionadas con la seguridad y la privacidad en el hogar conectado. | Estudiantes y docentes que no tengan ningún conocimiento o experiencia práctica en el campo de la domótica y la IoT. |

Se aclara que la unidad de trabajo no es inferior al 5 % de la unidad de trabajo.

El método de selección se lleva a cabo de manera intencionada, considerando la disponibilidad y disposición de los estudiantes y docentes para participar en el estudio. Se busca diversidad en términos de programas académicos y niveles de experiencia en domótica para obtener una representación integral de la población estudiantil y docente interesada en esta tecnología.

Este enfoque permite una selección estratégica de participantes que posean una comprensión significativa de la IoT en el contexto doméstico, lo que es fundamental para la profundización en las percepciones y experiencias relacionadas con la ciberseguridad y la privacidad del hogar conectado.

**Tabla 2**

*Procesos de investigación*

| Objetivos específicos | Fuente | Técnica de recolección | Instrumento | Técnica de Procesamiento | Resultados |
|---|---|---|---|---|---|
| Caracterizar las amenazas a la seguridad y privacidad de la IoT aplicada a la domótica, mediante revisión bibliográfica y análisis de casos. | Libros, artículos académicos, informes técnicos, documentos gubernamentales, estudios de casos de seguridad en domótica e IoT | Revisión: bibliográfica, documental, informes de seguridad y estudios de casos relevantes. | Fichas de lectura, matriz de categorización. | Análisis de contenido. | Lista de amenazas identificadas, clasificadas por tipo (por ejemplo, vulnerabilidades de software, ataques de red, violaciones de privacidad). |
| Proponer una estrategia de protocolos de seguridad para la implementación de la IoT en la domótica, asegurando la protección de datos y la integridad del sistema en entornos domésticos inteligentes. | Literatura especializada en seguridad informática y domótica, estándares y mejores prácticas de seguridad en IoT. | Revisión de libros, revistas, documentos técnicos y entrevistas. | Recopilación de opiniones y recomendaciones de expertos y plantilla de análisis para identificar patrones y tendencias en la literatura revisada. | Análisis comparativo e identificación de áreas entre las diferentes recomendaciones. | Propuesta de protocolos de seguridad, incluyendo medidas específicas para proteger datos y garantizar la integridad del sistema en entornos domésticos inteligentes. |

| | | | | | |
|---|---|---|---|---|---|
| Socializar los resultados del estudio con estudiantes y profesionales en domótica e IoT, con el fin de obtener retroalimentación y validar la viabilidad y efectividad de las soluciones propuestas. | Estudiantes, docentes y profesionales en domótica e IoT. | Talleres o seminarios y encuestas o cuestionarios. | Material de presentación (por ejemplo, diapositivas) y Cuestionario de retroalimentación. | Análisis de respuestas de encuestas o cuestionarios y registro de comentarios y sugerencias durante talleres o seminarios. | Evaluación de la aceptación y comprensión de los resultados presentados y retroalimentación sobre la viabilidad y efectividad de las soluciones propuestas. |

La Tabla 2 permite evidenciar el proceso de investigación de nuestros objetivos específicos.

## Conclusiones

Importancia de la IoT: la Internet de las Cosas ha revolucionado múltiples sectores, desde la salud hasta la educación, brindando eficiencia y comodidad, pero también, ha generado preocupaciones importantes sobre la seguridad y la privacidad.

Necesidad de abordar las amenazas: con la proliferación de dispositivos IoT, es crucial comprender y abordar las amenazas emergentes relacionadas con la ciberseguridad, la integridad de los datos y la protección de la información personal.

Relevancia en la ingeniería: la aplicación de la IoT en la ingeniería ha demostrado ser beneficiosa, pero también presenta desafíos en términos de seguridad y privacidad que deben ser abordados para garantizar su uso efectivo y seguro.

Impacto en la educación: la IoT ha transformado la educación universitaria al permitir campus inteligentes, mejorar la sostenibilidad, facilitar la investigación y personalizar la experiencia de aprendizaje, pero, asimismo plantea preocupaciones sobre la seguridad y la privacidad de los datos.

Enfoque metodológico: la investigación propuesta adopta un enfoque cualitativo y exploratorio para comprender las tendencias y amenazas en la IoT, así como el impacto en la educación universitaria. Esto permite una comprensión profunda de los fenómenos sociales y tecnológicos involucrados.

Mitigación de riesgos: se identifica estrategias de mitigación de riesgos, así como la identificación y evaluación de riesgos, la adopción de buenas prácticas de seguridad y, la implementación de soluciones específicas de IoT para proteger las implementaciones.