



Participation Report: IoT Forum Discussion

González Matuk Said Jesús

Fecha de entrega: 27/08/2025

1 Introduction

The Internet of Things (IoT) represents a paradigm shift in modern technology, creating an interconnected ecosystem of devices that permeate everyday life, from smart homes to industrial sensors. While offering unprecedented convenience, efficiency, and data-driven insights, this hyper-connectivity introduces significant and complex challenges in security, privacy, and ethical data management.

This report provides a detailed analysis of an individual student's participation in a course forum titled "Effects of the Internet of Things (IoT) in Daily Life." The purpose is to document and evaluate the contributions made, focusing on a primary post about IoT security and privacy, and the subsequent critical commentary provided on the posts of other students. The analysis is based solely on the content visible in the provided screenshots, ensuring an objective review of the depth, relevance, and constructiveness of the participation.

2 Analysis of Primary Post

Title: "Security and privacy in the Internet of Things (IoT)"

Content Summary:

 SAID JESUS GONZALEZ MATUK 11/08 08:31 a.m.

Seguridad y privacidad en el Internet de las Cosas (IoT)

El crecimiento del Internet de las Cosas (IoT) ha impulsado una revolución tecnológica que conecta todo tipo de dispositivos a la red: desde electrodomésticos y cámaras hasta relojes inteligentes y sensores industriales. Sin embargo, esta conectividad masiva ha traído consigo nuevas amenazas en materia de seguridad y privacidad que no pueden pasarse por alto. Cada dispositivo inteligente puede convertirse en un punto de entrada a toda la red si no cuenta con medidas de protección adecuadas.

En muchos casos, los fabricantes priorizan la funcionalidad y el bajo costo sobre la ciberseguridad, lo que expone al usuario a posibles ataques. Además, una gran cantidad de dispositivos IoT carece de actualizaciones de seguridad periódicas o automáticas, lo que permite que vulnerabilidades conocidas permanezcan sin corregirse durante largos períodos de tiempo. Uno de los riesgos más relevantes es la recolección masiva y continua de datos personales, como ubicación, hábitos de [ver más](#)



 MIRIAM ORTEGA CRESCENCIO viernes 07:53 p.m.

Desde mi punto de vista tu aportación es sumamente interesante ya que dejas claro como participa el internet de las cosas en el ámbito de la seguridad, de igual manera como es su consumo de recursos y la forma en que nos beneficia aplicarlo en el hogar desde obtener comodidad, servicios mas completos y mayor seguridad.



 ESTEBAN GONZALEZ GARCIA Ayer 04:54 p.m.

Ilustración 1



The primary post established a critical tone by acknowledging the technological revolution brought by IoT while immediately highlighting its accompanying threats. The argument was structured around several key vulnerabilities:

- Expanded Attack Surface: It was argued that every connected smart device, from appliances to industrial sensors, represents a potential entry point into a larger network if not properly secured.
- Manufacturer Priorities: A critical view was presented, suggesting that manufacturers often prioritize functionality and low cost over robust cybersecurity measures, leaving end-users vulnerable.
- Lack of Updates: A crucial technical challenge was identified: many IoT devices do not receive regular, automated security updates, allowing known vulnerabilities and bugs to remain unpatched for extended periods.
- Mass Data Collection: The post identified the constant and massive collection of personal data (e.g., location, habits) as one of the most concerning risks, often conducted without clear user consent or transparency.

Alignment with Forum Themes:

This post directly addressed the forum's theme of "Security and Privacy," providing a well-structured initial analysis supported by concrete examples of risks and manufacturer practices.

3 Analysis of Comments to Peers

The responses to other participants demonstrated an advanced ability to engage critically, offering not just agreement but substantive additions that deepened the discussion.

Comment for Esteban González García ("IoT in the Home"):

- Nature of Feedback: Constructive and additive.
- Key Contributions:
- Agreement and Reinforcement: The comment praised the original post for clearly exposing both the benefits of home IoT and its associated security risks, specifically highlighting mentions of unauthorized access and botnets.
- Introduction of a Key Concept: A significant technical perspective was added by stressing that security must be integrated from the design stage ("security by design") and not only during implementation, ensuring a more reliable lifecycle for the technology.

Expanded Perspective: The response broadened the discussion by introducing the critical role of the end-user. It pointed out that many vulnerabilities persist due to poor user practices, such as failing to change default settings or a lack of digital literacy, concluding that IoT security is a shared responsibility between manufacturers and users.



Monitoreo y análisis continuo del tráfico para detectar comportamientos anómalos
[ver menos](#)



GABRIEL SANCHEZ HERNANDEZ 05:12 p.m.

Aquí muestras de forma clara cómo el IoT ha transformado los hogares en espacios más cómodos y automatizados, pero también adviertes sobre los riesgos de seguridad que acompañan esta innovación ya que mencionas que cada dispositivo conectado representa un potencial punto de vulnerabilidad, lo cual hace indispensable integrar la

[ver más](#)

SAID JESUS GONZALEZ MATUK 06:35 p.m.

El aporte del compañero Esteban resulta muy relevante al exponer tanto los beneficios del IoT en el hogar como los riesgos de seguridad que este conlleva. La mención de amenazas como el acceso no autorizado o el uso de botnets resalta la necesidad de adoptar un enfoque integral en la protección de estos dispositivos. Considero especialmente acertada la idea de que la seguridad debe incorporarse desde la etapa de diseño y no solo en la implementación, pues esto garantiza un ciclo de vida más confiable para la tecnología.

Un punto que podría complementarse es la reflexión sobre el papel de los usuarios finales: muchas vulnerabilidades persisten por la falta de cambios en configuraciones básicas o por desconocimiento de buenas prácticas digitales. De esta manera, la seguridad en el IoT no solo depende del fabricante o de la infraestructura, sino también de la responsabilidad de los usuarios al gestionar sus dispositivos.

[ver menos](#)

Ilustración 2

Comment for Miguel Monroy López ("IoT in Everyday Life..."):

- Nature of Feedback: Constructive and suggestive.
- Key Contributions:
- Recognition of Technical Merit: The comment praised the original post for clearly highlighting the essential role of IoT and the central technical challenge of achieving interoperability between devices with different protocols.
- Ethical and Privacy Expansion: It suggested valuably expanding the reflection beyond technical interoperability to include the ethical challenges and privacy implications that accompany mass interconnection, arguing that a more connected world also implies greater risks of data exposure.

Universidad Autónoma del Estado de México

Centro Universitario UAEM Atlacomulco



Abrir 4 respuestas de usted, GABRIEL SANCHEZ HERNANDEZ, ALEJANDRO MARTINEZ FAUSTINO y 1 persona más

ALEJANDRO MARTINEZ FAUSTINO 11/08 08:26 a.m.

Tu texto tiene una base muy sólida. Capturas muy bien la idea central del IoT y su principal desafío técnico, que es la comunicación entre diferentes dispositivos. Mi principal sugerencia sería enfocar el párrafo únicamente en ser una introducción al tema, ya que ahora mismo parece mezclar esa presentación general con la justificación de una

[ver más](#)

GABRIEL SANCHEZ HERNANDEZ 05:05 p.m.

El compañero menciona que el IoT se ha convertido en un eje fundamental para la conectividad y la comodidad en la vida diaria y resulta interesante que no solo se destaque la integración de dispositivos comunes sino también el reto técnico de lograr que equipos con distintos protocolos y tecnologías logren comunicarse de manera fluida, porque si

[ver más](#)

SAID JESUS GONZALEZ MATUK 06:37 p.m.

El aporte del compañero Miguel resalta con claridad cómo el IoT se ha convertido en un elemento esencial para la vida cotidiana, ofreciendo conectividad y comodidad en distintos ámbitos. La idea de una arquitectura integrada que permita la interoperabilidad entre dispositivos con diferentes protocolos es clave, ya que justamente la fragmentación tecnológica constituye uno de los mayores retos para la evolución de un ecosistema IoT eficiente.

Me parece interesante también que se haya empleado una metodología cualitativa, pues no solo se centra en los aspectos técnicos, sino en cómo esta tecnología transforma la experiencia humana. Sin embargo, considero que sería valioso ampliar la reflexión hacia los desafíos éticos y de privacidad que acompañan esta interconexión masiva, ya que un mundo más conectado también implica mayores riesgos de exposición de datos.

[ver menos](#)

Ilustración 3

Comment for José Luis Guadarrama Martínez ("Security and privacy"):

- Nature of Feedback: Complementary and affirming.
- Key Contributions:
 - Agreement with Analysis: The comment agreed that the analysis was comprehensive and addressed one of the most sensitive issues within IoT.
 - Emphasis on User Awareness: It emphasized a crucial nuance: the privacy problem is exacerbated because users are often unaware of the extent of the information they are sharing and lack control over it, adding a layer of critical analysis regarding user consent and autonomy.



Abrir 5 respuestas de usted, JESUS MALDONADO CRUZ, DIEGO SEBASTIAN DAVILA GARCIA y 2 personas más

DIEGO SEBASTIAN DAVILA GARCIA 11/08 08:30 a.m.

El texto de mi compañero jose, presenta de forma clara y bien estructurada los desafíos actuales en torno a la seguridad y privacidad en el contexto del Internet de las Cosas. Me parece muy acertado cómo se equilibra el reconocimiento de los beneficios del IoT con una reflexión crítica sobre los riesgos asociados. La mención de la falta [ver más](#)

JESUS MALDONADO CRUZ 11/08 08:35 a.m.

Tu texto en base al Internet de las Cosas, en tu texto se dice que como es que se ofrece la comodidad y la eficiencia, pero también implica riesgos importantes como las vulnerabilidades de seguridad, la falta de actualizaciones y la recolección masiva de datos personales y vigilancia lo que se hace muchas veces sin un consentimiento claro

SAID JESUS GONZALEZ MATUK 06:38 p.m.

El análisis del compañero José Luis es muy completo, ya que aborda uno de los temas más sensibles dentro del IoT: la seguridad y la privacidad. Coincido en que la recolección masiva de datos personales es uno de los mayores riesgos, sobre todo porque los usuarios muchas veces desconocen el alcance de la información que comparten y carecen de [ver más](#)

Ilustración 4

4 Conclusion

The student's participation in the forum was outstanding and exemplary. The contributions demonstrated a deep understanding of the technical and ethical dimensions of IoT.

The primary post was a solid, well-structured critical analysis that perfectly addressed the core theme of security and privacy.

The comments to peers were the highlight of the participation. They consistently added high-value perspectives, introducing advanced concepts like "security by design," "shared responsibility," and "ethical challenges," which significantly enriched the forum's discourse.

All interventions maintained a respectful, academic, and constructive tone, fostering deeper debate and demonstrating strong capacity for critical thinking and collaborative dialogue.