COLLABORATIVE DISCUSSION 1: THE DATA COLLECTION PROCESS

PEER RESPONSES

Mahir Hashimov
12695120
Unit 1-3
Deciphering Big Data
University of Essex Online
24 May 2024

CONTENTS

MY PEER RESPONSES TO OTHERS

Peer Response: To Aneta Worku (2024)

Hi Aneta,

I appreciate you sharing your Internet of Things (IoT)-related work. Your work is thorough and educational. These are some strong elements that I thought were worth mentioning. I would want to ask a few questions.

Strength:

1. You demonstrated the adaptability of IoT by skilfully describing a range of applications.

2. Offering prospects and obstacles in equal measure provides a well-rounded viewpoint.

3. Your views are effectively shown by using real-world examples, such as linked automobiles and smart household appliances.

Questions:

1. How can the flaws in the present IoT security measures be addressed?

2. Could you give a particular example of how the Internet of Things is enhancing safety in the transportation or healthcare industries?

Overall, your assignment is well done.

Best regards,

Mahir Hashimov

Peer Response: To Panagiotis Mourtas (2024)

Hello, Panagiotis

I appreciate your thoughtful writing about IoT (Internet of Things).

You present a fair assessment while acknowledging the dangers and difficulties connected to IoT. How can IoT systems be strengthened to guard against data breaches and illegal access?

And what do you think, how can businesses balance the advantages of IoT infrastructure against its implementation and maintenance costs?

Best regards,

Mahir Hashimov

PEER RESPONSES TO ME

Peer Response: From Panagiotis Mourtas (2024)

Hello Mahir and thank you for your comment.

As for your first question, specific measures have to be taken. Firstly, IoT systems need to be implemented with authentication features to prevent unauthorized access from malicious users. Other than that, they have to use encrypted methods and secured firmware in order to strengthen their mechanisms even more. In addition, they should create a monitoring system to track the overall activity of the connected devices in order to easily manage them, even remotely. Lastly, updating their software and conducting regular security audits will be beneficial and more appropriate for the efficiency of all the previous measures (1).

As for your second question, investing in IoT security can be cost-efficient because, with that in your pocket, you can avoid possible costs of data breaches and regulatory fines in the near future. Other than that, nowadays there are a lot of platforms and systems available on the market for you to choose from. Cloud-based platforms are less costly and they provide many significant built-in features. However, the overall cost of these systems depends on your business needs, so you have to choose carefully which is more appropriate (2). As an alternative, you can choose a third-party provider who handles a bunch of IoT systems at a good price too (3). With the latest, you will not have the need for additional staff.

References:

1) Fortinet (2024) What Is IoT Security? Challenges and Requirements. Available at: https://www.fortinet.com/resources/cyberglossary/iot-security

2) FasterCapital (2024) Cost Estimation Internet of Things: How to Use IoT Devices to Collect and Transmit Cost Data. Available at: https://fastercapital.com/content/Cost-Estimation-Internet-of-Things--How-to-Use-IoT-Devices-to-Collect-and-Transmit-Cost-Data.html

3) Medium (2023) Cost-Effective IoT Development: How Outsourcing Can Reduce Your Budget. Available at: https://medium.com/@sparkleotech/cost-effective-iot-development-how-outsourcing-can-reduce-your-budget-8d78d7bff8e5