James Emery

CS 410

How Decentralized Computing impacts security and efficiency in IoT systems compared to Centralized Computing

Ch1: Introduction

In this modern era, the Internet of Things (IoT) has become a central function in our everyday lives. An IoT device is an object that specializes in connecting to the internet in order to send or process data. This includes smart watches, security cameras, or even smart light bulbs. The two most important aspects regarding the IoT are security and performance. Without one, the other is rendered unreliable. [1]

To expand on this topic, the following question will be used to conduct further research, as well as discussed in later chapters, and discussed:

How does decentralized computing affect the security and performance of IoT systems compared to centralized systems?

Given my experiences in cybersecurity and software engineering, my assumption is that decentralized computing will improve security. Eliminating the possibility of a single attack compromising the entire system will lead to improved data protection. However, I think

[1]

that performance in decentralized computing may be hindered due to the peer-to-peer communication system.

Ch 2: Decentralized and Centralized System Operations

As of today, most IoT systems rely on **centralized computing**. This means that all data is sent to a central server or host for processing. This way of data handling is efficient, but it comes with security risks, which will be discussed in the next chapter.[2]

To avoid reliability problems, many engineers have started experimenting with **decentralized computing**. Instead of one central server holding all the information, this way of system networking uses dozens of machines that copy, share, and process data. However, this way of data management can create complexity, making it more difficult for devices to send and receive information.[3]

Both of these systems have their respective advantages and disadvantages. Depending on the situation, there is reason to use one over the other. In chapters 3 and 4, these advantages and disadvantages will be scrutinized in more detail.

2

3

Ch 3: Security Comparison

While most systems today are never fully decentralized, many companies incorporate decentralized aspects into their mostly centralized systems. These companies use this method to integrate the strengths of both, while minimizing the drawbacks.[4]

Since centralized systems rely on a single system location to store data, an attack or outage on that server could be catastrophic. This is called a **central point of failure**, and it is one of the biggest weaknesses of centralized systems. In environments like healthcare, sensitive data must be as secure as possible.[5]

On the other hand, decentralized systems offer much better protection against attacks and server outages. The data being spread across many devices (called **nodes**) produces no central point of failure, offering much better protection against system failures. If one of these nodes fails via an outage or attack, only a segment of data is lost/compromised, improving system reliability and security.[6]

The technique of nearby nodes and local networks sharing data allows for **edge computing**. This procedure uses nearby nodes and local networks to reduce the distance data must travel. Shorter travel distance result in a lower probability of data interception by malicious third parties.[7]

4

5

6

7

Another key advantage of decentralized systems is that they are **scalable and distributed**. This means they can grow without putting too much pressure on a single component. They can also continue functioning even if part of the system fails or is hacked, making them more reliable in certain situations.[8]

Even with all of this in consideration, decentralized systems are still outclassed in many areas. Due to the number of nodes involved, coordinating them can be more difficult than in a centralized system. Data must be shared and synchronized across the network, which adds further complexity.[9]

Ch 4: Efficiency and Performance

Efficiency is another key factor when comparing centralized and decentralized systems. This is where centralized systems shine.

Centralized systems are generally more efficient than decentralized systems when network conditions are good. Most companies host powerful servers that can withstand large amounts of data quickly. Direct communication from a device to a central server is faster in most cases.[10]

8

9

10

Although, sometimes these systems can suffer from delays because data must travel long distances to reach the server. As more devices are added, this can create bottlenecks and slow down the system. [11]

This is an area where edge computing in decentralized systems would be superior. Reducing the travel distance of data improves latency and response times, especially in real-time applications. Edge computing increases scalability, allowing the number of users to grow without excessively hindering performance and efficiency. However, most companies today have the technology to improve scalability using centralized computing.[12]

Despite these benefits, there are tradeoffs. Coordinating multiple nodes requires additional communication, which can increase the amount of resources needed to run the system. At the same time, an overflow of requests to a central server can cause latency issues. Security features, such as encryption, can also slow down the system. [13]

Ch 5: Conclusion

Hardware Diagram:

Centralized System:

IoT Device -> Internet -> Central Server -> Database -> IoT Device

11

12

13

Decentralized System:

IoT Devices -> Node A -> Node B -> Node C -> IoT Device

In the article “Centralized vs. Decentralized Cloud Computing in Healthcare” a table is presented to discuss numerous proposed models of both centralized and decentralized systems, along with their strengths and weaknesses:[14]

1. One centralized model proposed a cloud-based centralized data repository for pediatric patient care. The model had many strengths like reduced latency and a user-friendly interface, but a pivotal setback was major security concerns due to the centralized nature of the system.

2. Another model proposed a decentralized system that uses a data management framework for digital health platforms while taking advantage of a NoSQL database. A large selling point of this model was its improved security and privacy, as well as performance and scalability, but it lacked simplicity.

3. For another centralized model, a cloud-based system for an emergency healthcare service that matches fingerprints to retrieve summarized data in time

14

sensitive situations offered quick, real-time access to patient data, but privacy concerns seemed to be the only issue.

4. In another decentralized system, a hybrid cloud infrastructure, termed "MedShare," organizes the utilization of medical resources across different devices. It had a couple of strengths, including being free to use and the ease of integration of its legacy systems, but a setback was the high response time and frequent timeouts when data was being exchanged between devices.

5. Lastly, this decentralized system model featured a personal cloud data model integrated into the Campus Health Information System (CHIS). The one strength was avoiding the bottleneck issue of excessive server requests slowing down the system. However, student devices may lack security protocols, making them much more vulnerable to attacks.

The strengths and weaknesses of the models shown above for the centralized and decentralized systems were largely similar to others proposed in the article.

After analyzing these models, centralized computing seemed to consistently excel, and there were no drawbacks to performance and efficiency in any of the frameworks. However, security issues seemed to be running rampant.

In the decentralized systems, a core strength was data protection, while a significant drawback was simplicity and performance, except for model #5.

#5 had high performance but poor security. This is proof that the performance, efficiency, and security of these two systems heavily depend on how they are set up. However, for most instances, centralized computing seemed to excel in performance and efficiency, while decentralized computing exceeded with security.

My initial assumption that decentralized systems improve security appears to be correct. By removing the single point of failure and distributing data across multiple nodes, these systems are more resistant to large-scale attacks and failures.

However, the impact on efficiency is less straightforward. While decentralized systems can reduce latency and improve scalability, they also introduce additional complexity. This means their performance can vary depending on the situation.

In the IoT, balancing the aspects of these two systems can produce a system that has both excellent performance and reliable security.

Footnotes

1. Niebla-Montero et al., 2022.
2. Abughazalah et al., 2024.
3. Abughazalah et al., 2024.
4. Abughazalah et al., 2024.
5. Abughazalah et al., 2024.
6. Abughazalah et al., 2024.
7. Niebla-Montero et al., 2022.

8. Niebla-Montero et al., 2022; Abughazalah et al., 2024.

9. Abughazalah et al., 2024.

10. Abughazalah et al., 2024.

11. Abughazalah et al., 2024.

12. Niebla-Montero et al., 2022.

13. Abughazalah et al., 2024; Niebla-Montero et al., 2022.

14. Abughazalah et al., 2024.

Bibliography

Abughazalah, M., Alsaggaf, W., Saifuddin, S., & Sarhan, S. (2024).

Centralized vs. decentralized cloud computing in healthcare. Applied Sciences, 14.

Niebla-Montero, Á., Froiz-Míguez, I., Fraga-Lamas, P., & Fernández-Caramés, T. M. (2022).

Practical latency analysis of a Bluetooth 5 decentralized IoT opportunistic edge computing system. Sensors, 22, 8360.