6-1 Journal – Takeria Thompson

Part One:

1. Identification and Description of Each Technology

Zero Trust Architecture (ZTA) and Homomorphic Encryption:

Zero Trust Architecture (ZTA) is a cybersecurity framework built on the principle of “never

trust, always verify.” Unlike traditional security models that assume internal network traffic

is trustworthy, ZTA continuously authenticates users and verifies device integrity

regardless of their location. This model employs technologies such as multi-factor

authentication (MFA), identity and access management (IAM), and network segmentation to

ensure only authorized users access sensitive resources. Given the expansion of remote

work and cloud services, ZTA is a crucial defense mechanism against the growing

cybersecurity threat landscape (Chaudhary et al., 2021).

Homomorphic encryption allows computations to be performed directly on encrypted data

without requiring decryption. This ensures that sensitive information remains protected

even during processing. It is particularly valuable in environments like cloud computing,

healthcare, and finance, where data privacy is paramount. Organizations can securely

conduct machine learning and data analytics while safeguarding confidential information

(Rivest et al., 1978).

2. What are the likely impacts on computer science or your career?

The adoption of ZTA is expected to significantly increase demand for cybersecurity

professionals skilled in deploying and maintaining these systems. Knowledge of IAM,

network segmentation, and real-time monitoring will be essential for success in this field.

As cybersecurity threats continue to grow, expertise in ZTA will position me as a valuable

asset to any organization prioritizing data protection.

As data privacy becomes increasingly vital, proficiency in advanced encryption techniques

like homomorphic encryption will be highly sought after. Understanding how to apply and

optimize this method in real-world scenarios will be critical for roles in cybersecurity, data

science, and cloud infrastructure. This skillset will enable me to help organizations analyze

sensitive data securely, enhancing both my career opportunities and impact.

3. How might the two technologies impact humans, communities, or the world?

ZTA can significantly strengthen digital security for both organizations and individuals. By

verifying every access request, it reduces the likelihood of data breaches, thereby enhancing

trust in digital services. On a societal level, the adoption of ZTA can foster a culture of

cybersecurity awareness and resilience, leading to safer digital ecosystems.

This encryption technique has the potential to revolutionize how sensitive data is managed

across various sectors. In fields such as healthcare and finance, it allows organizations to

derive insights without compromising privacy. This promotes innovation while ensuring

compliance with data protection regulations. However, its implementation may also spark

debates about balancing data accessibility and privacy.

4.Which course outcomes have you achieved so far, and which ones remain?

Achieved:

- Acquired foundational knowledge of emerging security technologies and their relevance to

future computing trends.

- Evaluated the societal implications of disruptive technologies, especially concerning data

privacy and security

References:

Chaudhary, R., Zafar, A., & Peddinti, S. (2021). A comprehensive survey on Zero Trust Architecture: Principles,

frameworks, and security challenges.

Rivest, R. L., Adida, B., & Sipser, M. (1978).

https://luca-giuzzi.unibs.it/corsi/Support/papers-cryptography/RAD78.pdf

Part Two: