Course Code: CSE707

Name: Mosa. Rabeya

I'd: 23266013

Section: 01

Review: Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: A Proposed Framework

URL: https://doi.org/10.3390/electronics13050865

1. Summary:

Daah et al. (2024) This article was conducted on Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration.

1.1 Motivation:

The paper is motivated by the need to enhance cybersecurity in financial institutions, particularly within the context of evolving cyber threats and vulnerabilities. Sophisticated attacks like SQL injection, man-in-the-middle, insider threats, and brute-force attacks cannot be adequately addressed by traditional cybersecurity techniques. The authors' proposal integrates blockchain technology with a Zero Trust framework to overcome these issues and provide enhanced security for transactions involving sensitive financial data.

1.2 Contribution:

This paper proposes a new framework that integrates Blockchain into the Zero Trust security model. The framework focuses on identity and access management, device and network security, and data protection with Blockchain providing enhanced integrity and verification. It offers a solution specifically tailored to the financial industry's needs, addressing scalability, adaptability, and protection from cyber threats.

1.3 Methodology:

The Zero Trust model incorporates Blockchain to secure IAM, device and network security, and data protection. The purpose of this suggested framework is to address the drawbacks of conventional cybersecurity models such as Bell-LaPadula and Biba, ranging from Layered Security to Castle-and-Moat to Defense-in-Depth strategies, which are frequently used in the financial sector.

Security assumptions and threat models are defined, with the framework integrated into a prototype banking application. The prototype is evaluated using security testing (e.g., SQL injection, brute-force, and CSRF attacks) and performance testing (e.g., transaction latency and system throughput). Tools like Burp Suite, Wireshark, and Apache JMeter are used for testing.

1.4 Conclusion:

The proposed Zero Trust framework demonstrated robust protection against various cyber threats in the prototype banking application. Security tests confirmed the effectiveness of the framework against common vulnerabilities, while performance testing highlighted that the security measures did not compromise

system efficiency. The integration of Blockchain adds transparency, ensuring immutable access logs and tamper-proof credentials, which are crucial for regulatory compliance and auditing in the financial sector.

2. Limitations:

2.1 First Limitation: The current implementations of Zero Trust in the financial sector face challenges related to scalability, particularly when integrated with Blockchain.

2.2 Second Limitation: Implementing Blockchain into the Zero Trust model adds complexity to the security infrastructure.

2.3 Third Limitation: Ensuring the framework meets all financial regulations like AML (Anti-Money Laundering) and KYC (Know Your Customer) remains a challenge.

3. Synthesis:

In the future, the research can be including-

3.1 First Potential: Integration with other emerging technologies such as AI or machine learning to improve threat detection and response mechanisms.

3.2 Second Potential: Future iterations should focus on optimizing the framework for better performance, particularly in high-throughput environments like global financial institutions.