**Zero Trust Infrastructure Utilizing Network Segmentation and Microservices in a Financial System**

Yilake Mengstie

Department of Computer Technology: Bowie State University

CTEC445:

Fall 2024

September 03, 2024

Contents

[I. Abstract 3](#_Toc178967028)

[II. Introduction 3](#_Toc178967029)

[III. Literature Review 3](#_Toc178967030)

[A. Title: Emerging Technologies Driving Zero Trust Maturity Across Industries 3](#_Toc178967031)

[B. Title: Zero Trust Maturity Model 4](#_Toc178967032)

[C. Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: A Proposed Framework 5](#_Toc178967033)

[D. Zero-trust-based security model against data breaches in the banking sector: A blockchain consensus algorithm 5](#_Toc178967034)

[IV. Methodologies 6](#_Toc178967035)

[A. Blockchain-Integrated Zero Trust Architecture: 6](#_Toc178967036)

[B. Microservices and Network Segmentation: 6](#_Toc178967037)

[C. Multi-Factor Authentication (MFA) and Identity Management: 6](#_Toc178967038)

[D. Privacy-Enhancing Technologies (PETs) and Encryption: 6](#_Toc178967039)

[E. Continuous Monitoring and Threat Intelligence: 6](#_Toc178967040)

[V. Comprehensive Experiment and Results 6](#_Toc178967041)

[A. Source 1: Joshi (2024) 6](#_Toc178967042)

[B. Source 2: Cybersecurity and Infrastructure Security Agency (CISA) (2023) 6](#_Toc178967043)

[C. Source 3: Daah et al. (2024) 7](#_Toc178967044)

[D. Source 4: Chaudhry & Hydros (2023). 7](#_Toc178967045)

[VI. Comprehensive Conclusion 7](#_Toc178967046)

[VII. References 7](#_Toc178967047)

Zero Trust Infrastructure Utilizing Network Segmentation and Microservices in a Financial System

Yilake Mengstie  
Department of Computer Technology and Security

Bowie State University

14000 Jericho Park Rd, Bowie, MD 20715

[Mengstiey0518@student.bowiestate.edu](mailto:Mengstiey0518@student.bowiestate.edu)

# Abstract

Zero Trust Infrastructure (ZTI) is a security framework that, by default, does not trust any person or system inside or outside the network. It does this by implementing strict access limits. Financial systems that handle sensitive data and transactions that are prime targets for hackers are finding greater and greater importance in this approach. This paper explores the integration of ZTI, microservices, and network segmentation in a financial system. The technique of splitting a network into distinct pieces is known as network segmentation, and it helps to reduce the attack surface and limit an attacker's movement within the network. On the other hand, microservices simplify administration by breaking up applications into more manageable, secure communication components.

The infrastructure can monitor all connections, interactions, and data flow by combining network segmentation and microservices into a zero-trust model. This technique improves data security, and only approved and authenticated connections between various network components are made. The recommended ZTI emphasizes implementing security mechanisms like encryption, live monitoring, and identity verification.

This study demonstrates how implementing zero trust can increase overall system resilience, prevent unwanted access, and minimize potential harm in the event of a breach. According to the study, financial systems can be placed in a flexible, scalable, and secure environment that guarantees the security of sensitive information and compliance with regulations by integrating network segmentation and microservices within a zero-trust framework.

Keywords—Trust Infrastructure (ZTI)

# Introduction

Financial institutions' growing use of online services and cloud technologies presents them with cybersecurity challenges in today's quickly changing digital environment. Growing interest in Zero Trust Architecture (ZTA) as a more reliable alternative to traditional security models that rely on perimeter defenses has resulted from these models' inability to handle sophisticated cyber threats (CISA, 2023). Under the tenet of "never trust, always verify," ZTA enforces stringent access controls, ongoing verification, and dynamic user activity monitoring.

In order to improve data integrity and transaction security in the financial sector, recent research highlights incorporating cutting-edge technology, such as blockchain, into zero-trust models (Daah et al., 2024). Blockchain's decentralized nature allows tamper-proof verification and secure data sharing, offering a suitable platform for ZTA in financial systems (Joshi, 2024). Even with these developments, there are still issues with scalability, regulatory compliance, and interoperability with legacy systems when integrating ZTA into intricate financial infrastructures. This study investigates how to combine network segmentation, microservices, and Zero Trust Infrastructure to create a complete security framework specifically for financial institutions.

# Literature Review

## Title: Emerging Technologies Driving Zero Trust Maturity Across Industries

Zero Trust Infrastructure (ZTI) is gaining traction as a strong cybersecurity concept, replacing the conventional "trust but verify" strategy. Joshi (2024) highlights that the traditional strategy cannot safeguard distributed IT environments entirely and does not reduce the effect of security breaches. In contrast, the Zero Trust approach relies on concepts that offer a more robust security posture, such as stringent authentication, least privilege access, and continuous verification. The development of Zero Trust models in recent years has been inspired by the exponential expansion of network-connected endpoints, such as Internet of Things (IoT) devices, as well as advances in blockchain, machine learning, and artificial intelligence (AI). In complex cybersecurity contexts, these developments are essential for enhancing dynamic access control and trust evaluation procedures [1].

Improving cybersecurity now requires integrating emerging technologies into Zero Trust frameworks. Joshi (2024) talks about how AI and ML make it possible to create increasingly complex threat detection systems that can gradually adjust to new threats and patterns. Assessing the reliability of individuals, devices, and network traffic is greatly enhanced by using graph-based trust propagation methods, machine learning models, and Bayesian networks. However, incorporating cutting-edge technologies brings additional difficulties, including worries about data privacy, algorithm biases, and difficulty sustaining verification across cloud settings [1].

Joshi (2024) delves into the function of Privacy-Enhancing Technologies (PETs) in the context of the Zero Trust framework, including homomorphic encryption, secure multi-party computation, differential privacy, and zero-knowledge proofs. By balancing security and data protection standards, these PETs enable the computation of encrypted data while maintaining individuals' privacy. For example, homomorphic encryption improves data security in cloud environments by allowing enterprises to study encrypted data without decoding it [1].Diagram of a diagram of a system

Description automatically generated

.

Figure 1: Trust Algorithms in Zero Trust Architecture

(Source: Adapted from Joshi, 2024, as cited in [original source, GAO, n.d.])

This figure illustrates the continuous authentication process in Zero Trust Architecture, where trust algorithms make real-time access decisions based on multiple information sources.

## Title: Zero Trust Maturity Model

A developing security paradigm, the "Zero Trust model," prioritizes ongoing verification and assumes that no user, device, or network can be trusted by default. CISA (2023)'s "Zero Trust Maturity Model Version 2.0" provides a thorough method for reaching Zero Trust specifically designed for government agencies but can also be used by other businesses, such as financial institutions. Along with three cross-cutting capabilities—Visibility and Analytics, Automation and Orchestration, and Governance—the paradigm is organized into five central pillars: Identity, Devices, Networks, Applications and Workloads, and Data

The CISA model highlights that achieving Zero Trust is a phased process that moves through four distinct maturation stages: Traditional, Initial, Advanced, and Optimal. Primary perimeter defenses and restricted visibility are the first features of the Traditional model, which develops into a fully automated, dynamic system that offers complete visibility and policy enforcement (Optimal). Organizations are encouraged by the maturity phases to evaluate their security posture, make plans for minor, incremental improvements, and invest in the resources needed to strengthen their Zero Trust architecture.A diagram of a building with columns

Description automatically generated

Figure 2:Zero Trust Maturity Model Pillars( source: CISA.gov[2]

Figure 2 depicts the five critical pillars of the Zero Trust Maturity Model (ZTMM) outlined by CISA. The pillars include Identity, Devices, Networks, Applications and workloads, and Data.

According to cisa.gov, this model reflects the seven tenets of zero trust as outlined in NIST SP 800-207:

1. Data sources and computer services are examples of resources.
2. Corporate resources are allotted to each individual on a per-session basis.
3. All communication is secure and independent of the network's location.
4. . Flexible policies govern resource access.
5. Al-owned and associated assets are monitored, and the organization measures its security posture and integrity.
6. . Authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The business collects much information on the state of its assets, network infrastructure, and communications to improve its security posture.

The paper also covers issues related to implementing Zero Trust, like moving away from outdated systems that depend on implicit trust. The Identity pillar, for instance, emphasizes risk assessments, access control, and robust authentication to guarantee that people and entities have access at the right moment. Similarly, the Network pillar emphasizes how crucial it is to segregate networks and encrypt communications to prevent lateral movement during possible intrusions. Organizations can create a comprehensive zero-trust plan that improves security posture by methodically addressing each pillar.

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

Zero Trust security models specifically designed for the financial industry are examined in the paper "Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: A Proposed Framework" by Clement Daah et al. (2024). The authors stress the need for a robust security architecture since financial institutions are subject to more sophisticated cyber threats. Identity and access management (IAM), data security, network and device security, and blockchain technology are the main focus areas for the proposed Zero Trust framework to improve trust mechanisms [3].

A diagram of a blockchain system

Description automatically generated

Figure 3: Identity and access management (IAM) with blockchain (Source: Daah et al., 2024)

This figure depicts how blockchain technology is helpful to the identity and access management processes. It visually represents how blockchain enhanced user authentication with components like multi-factor authentication (MFA) and the issuance of security tokens for user identity verification.

The literature review compares cybersecurity solutions pertinent to financial contexts with the current zero-trust paradigms. The ability to adapt to complex internal and external threats has been demonstrated to be limited by traditional models such as defense-in-depth and perimeter-based defenses. The Zero Trust approach is based on "never trust, always verify," as the authors explain. It prioritizes ongoing user, device, and application verification before allowing access to critical information and resources. They also talk about how financial institutions increasingly implement blockchain technology, which offers a safe and decentralized platform for information exchange. Through consensus mechanisms and smart contracts, blockchain can improve trust algorithms in Zero Trust models [3].

## Zero-trust-based security model against data breaches in the banking sector: A blockchain consensus algorithm

The report highlights the growing cybersecurity risks that the banking sector is experiencing by presenting a Zero-Trust-Based Security Model that uses blockchain consensus techniques. The literature analysis of the study looks at how traditional security techniques fall short against new forms of cyberattacks, such as denial-of-service attacks, ransomware, and phishing. Strong and consistent cybersecurity measures are necessary because banks are increasingly targeted due to their transition to online services, cloud storage, and outsourcing of IT operations [1].

Stringent access controls, continuous user identity verification, and strong defense against insider and outside threats are some of the core principles of the zero-trust strategy the research talked about. The research also explained how ZTA might profit from utilizing blockchain technology, making the case that financial transactions would be more secure and reliable due to blockchain's decentralized structure. The author also covers the benefits of online transaction verification using consensus algorithms based on blockchain technology, which ensures the immutability and decentralization of financial processes [1].

# Methodologies

## Blockchain-Integrated Zero Trust Architecture:

Including blockchain technology in Zero Trust models is one of the main approaches covered in a recent study (Daah et al., 2024). The procedure leverages the blockchain's decentralized ledger to securely handle financial systems' identities, access controls, and data transactions. Blockchain offers a visible, unchangeable record of all access requests by utilizing consensus techniques like Proof of Work (PoW) and Proof of Stake (PoS). This guarantees ongoing verification and prevents unwanted access.

## Microservices and Network Segmentation:

Securing financial systems requires both microservices and network segmentation. It restricts possible attackers' ability to travel laterally by segmenting the network into separate areas (Joshi, 2024). Applications are divided into smaller, autonomous components with their security controls by the microservices architecture. Because of its modular design, Zero Trust principles may be enforced, reducing the attack surface by requiring all microservices to communicate exclusively over encrypted, authorized channels.

## Multi-Factor Authentication (MFA) and Identity Management:

Using strong Identity and Access Management (IAM) in conjunction with MFA is crucial to ZTA. Research (CISA, 2023) strongly emphasizes continuous verification, which authenticates users through risk-based authentication, biometric verification, and dynamic access controls. This technology requires numerous verification processes, such as passwords, biometric data, or security tokens, reducing the danger of unauthorized access even if one protection layer is compromised.

## Privacy-Enhancing Technologies (PETs) and Encryption:

Encryption is a cutting-edge approach to protecting data in transit and at rest. Joshi (2024) brings up homomorphic encryption, which guarantees secrecy by enabling operations on encrypted data without decryption. Differential privacy and zero-knowledge proofs are two examples of privacy-enhancing technologies (PETs) that allow secure data processing while protecting sensitive financial data.

## Continuous Monitoring and Threat Intelligence:

The methodology of integrating continuous monitoring with real-time threat intelligence is vital for Zero Trust deployment (Prakash, 2024). Sophisticated machine learning algorithms examine network traffic patterns, identify irregularities, and implement automated reactions to possible hazards. By limiting access to network resources to only authorized users and devices, this real-time monitoring technique helps to reduce risks.

# Comprehensive Experiment and Results

## Source 1: Joshi (2024)

Joshi's study centered on how cutting-edge technologies, including blockchain, quantum computing, artificial intelligence (AI), and machine learning, improve Zero Trust Architecture (ZTA). According to the report, artificial intelligence (AI) and machine learning allow for dynamic trust evaluation, real-time access limits, and adaptation to changing threats. Although this integration strengthens zero-trust models, it must be improved to protect privacy and guarantee impartial decision-making. Microservices and network segmentation were also crucial for establishing Zero Trust in financial systems. Organizations can gain precise control over network interactions and improve their cybersecurity posture by segmenting programs into smaller, more secure components.

## Source 2: Cybersecurity and Infrastructure Security Agency (CISA) (2023)

A roadmap for implementing Zero Trust principles in phases, from traditional perimeter-focused security to a more advanced, context-aware approach, is provided by the CISA Zero Trust Maturity Model. One of the study's main conclusions was the need for automation and analytics in real-time threat identification and response, which is essential for the successful deployment of Zero Trust. To effectively respond to dynamic threats, the paradigm prioritizes continual improvement across its pillars, including Identity, Devices, Networks, Applications and workloads, and Data. By implementing this maturity model, financial institutions can increase system resilience overall, restrict unwanted access, and improve data protection.

## Source 3: Daah et al. (2024)

This study conducted extensive security testing on a blockchain-integrated zero-trust model for financial institutions. The results indicated a strong defense against common web application vulnerabilities, as confirmed through vulnerability scans using tools like Burp Suite and OWASP ZAP. Security tests demonstrated the system's ability to handle attacks such as SQL injection, Cross-Site Request Forgery (CSRF), and Cross-Site Scripting (XSS). Additionally, communications were securely encrypted using TLS v1.3. Performance testing highlighted an average transaction processing time of 40 seconds on the Ethereum blockchain, achieving a throughput of 3.7 transactions per second (tps) at 20 threads, increasing to 4.4 tps at 100 threads. Scalability analysis showed consistent response times for up to 60 users, with a slight increase in latency beyond 80 users, demonstrating the model's efficiency in handling increased demand

## Source 4: Chaudhry & Hydros (2023).

To overcome data breaches in the banking industry, Chaudhry and Hydros presented a Zero-Trust-Based Security Model in this study. In order to protect online transactions, the study used a blockchain consensus algorithm, highlighting the significance of decentralized administration and immutable data. Adopting the "never trust, always verify" philosophy, multi-factor authentication, ongoing surveillance, and stringent access control methods were implemented to bolster security. Incorporating Proof of Work (PoW) and Proof of Elapsed Time (PoET) into a blockchain-based consensus algorithm improved transaction verification and reduced the risk of man-in-the-middle attacks. The study results show that this kind of integration can significantly improve the security framework for confidential financial informationandactivities,emphasizing the role blockchain plays in bolstering zero-trust practices in the banking industry

# Comprehensive Conclusion

Integrating Zero Trust Architecture (ZTA) into financial systems has become a crucial cybersecurity tactic in response to cyber threats' increasingly complex and dynamic nature. This study has demonstrated how ZTA's dynamic trust evaluation techniques, ongoing monitoring, and stringent access constraints protect sensitive financial data and transactions. It is clear from a thorough analysis of the literature—which includes studies by Joshi (2024), CISA (2023), Daah et al. (2024), and Chaudhry & Hydros (2023)—that the Zero Trust model provides the financial sector with a proactive and flexible security framework**.**

Joshi (2024) highlighted how cutting-edge technologies like blockchain, AI, and machine learning might improve the effectiveness of Zero Trust models. According to the research, microservices, and network segmentation are essential elements that provide fine-grained control over network interactions and lower the attack surface. CISA's Zero Trust Maturity Model (2023) offered a more organized implementation roadmap for Zero Trust principles, which outlined the requirements for automation, real-time analytics, and continuous improvement across several security pillars. Financial organizations can switch from conventional perimeter-focused security to a more advanced, context-aware strategy with the help of this model.

Daah et al. (2024) showed the effectiveness of a blockchain-integrated zero-trust framework in financial systems in the assessed practical implementations. According to their findings, the model was able to tackle a variety of cyberattacks effectively, encrypt data communications, and maintain transaction efficiency even under high demand. Likeways, Chaudhry and Hydros (2023) stressed the significance of immutability, decentralized management, and stringent access control mechanisms in their proposal for a Zero-Trust-Based Security Model that uses blockchain consensus algorithms to safeguard online banking transactions. Their conclusions emphasized how crucial blockchain is to upholding zero-trust guidelines and reducing the risk of security lapses in banking systems.

Despite ZTA's benefits, problems like scalability, backward compatibility, and the need for objective, explicable decision-making in AI and machine learning models still need to be fixed. However, current advancements in privacy-enhancing technologies (PETs)—such as zero-knowledge proofs and homomorphic encryption—indicate a feasible future for strengthening data security and privacy in Zero Trust settings.

In conclusion, a thorough and reliable security architecture for the financial sector is presented by combining Zero Trust Infrastructure, network segmentation, microservices, and blockchain technology. Financial organizations may strengthen their cybersecurity posture against new threats by putting advanced encryption techniques, continuous monitoring, and dynamic access controls into place. In an increasingly digital environment, financial systems must embrace a flexible, adaptive Zero Trust strategy, as described by CISA (2023) and supported by numerous research studies, to ensure improved data security, integrity, and compliance.

# References

1. Chaudhry, U. B., & Hydros, A. K. M. (2023, March 23). *Zero‐trust‐based security model against data breaches in the ...* Zero-trust-based security model against data breaches in the banking sector: A blockchain consensus algorithm. <https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/blc2.12028>
2. **Cybersecurity and Infrastructure Security Agency.** (2023, April). *Zero Trust Maturity Model Version 2.0.* <https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf>.
3. Daah, C., Qureshi, A., Awan, I., & Konur, S. (2024). *Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: A Proposed Framework.* Electronics, 13, 865. <https://doi.org/10.3390/electronics13050865>
4. Joshi, H. (2024, September 10). *Emerging Technologies Driving Zero Trust Maturity Across Industries* [Preprint]. TechRxiv. <https://d197for5662m48.cloudfront.net/documents/publicationstatus/223293/preprint_pdf/bd4586940bae3e5d8c654e0f1b27a54f.pdf>.