Computer Fraud and Security
ISSN (online): 1873-7056

Adaptive Zero Trust Architecture for Securing Financial Microservices

Sreenivasulu Gajula

Sreenivasgajulausa@gmail.com

Principal Full-Stack Engineer, USA

Abstract

The rapid expansion of cloud-native financial platforms has amplified both operational efficiency and cyber risk exposure. Traditional perimeter-based security models no longer align with the distributed, API-centric nature of financial microservices. This paper introduces an industry oriented, adaptive Zero Trust architecture that integrates AI-driven threat analytics, continuous authentication, and dynamic authorization. The framework addresses the evolving challenges in financial ecosystems, including API abuse, identity compromise, lateral movement, and regulatory pressure. By recreating advanced visual models and presenting a refined methodology, this paper positions Zero Trust as a practical and scalable blueprint for securing financial microservices in modern enterprises.

Keywords: Zero Trust, financial microservices, adaptive security, AI analytics, API protection, continuous authentication, Zero Trust architecture.

I. INTRODUCTION

The financial technology landscape is defined by decentralization, automation, and real-time digital engagement. Microservices have become the backbone of banking, payments, insurance, and trading applications, offering modularity and rapid deployment. However, these benefits simultaneously increase the attack surface. Modern adversaries exploit API vulnerabilities, identity weaknesses, and cross-service trust assumptions.

Industry practitioners now recognize that Zero Trust, which enforces continuous verification and eliminates implicit trust, provides a more realistic model for securing these environments. Unlike outdated perimeter defenses, Zero Trust assumes compromise and applies verification at every transaction layer. This paper reframes Zero Trust from a practical, industry-oriented perspective, aligning architecture, AI-driven detection, and regulatory expectations for financial institutions.

Problem Statement:

Unauthorized access, data breaches and taking advantage of vulnerabilities of a distributed network are some of the security concerns that the financial microservices are still facing. Traditional security systems which are founded on having trust in internal traffic are becoming less efficient in preventing complex attacks and data theft. Since financial data is sensitive information, and cybercrime is also on the rise, it is noteworthy that real-time security models that verify every user, device, and transaction should be used. These services should be enclosed with the dynamic Zero Trust platform to secure them and make sure they are adjusted to the requirements of the regulations.

Aims and Objectives:

Aim:

The main aim of the research is to create an adaptive Zero Trust infrastructure to ensure the financial microservices are safer by implementing continuous authentication and authorization with constant monitoring.

Objectives:

To systematically identify and analyze the key security vulnerabilities inherent in financial microservice architectures, and to evaluate the limitations of traditional perimeter-based security models in mitigating these risks.

To design and formalize an adaptive Zero Trust security architecture incorporating dynamic access control, continuous authentication, and real-time risk evaluation tailored for decentralized financial environments.

To assess the effectiveness of the proposed Zero Trust framework in reducing unauthorized access, preventing data breaches, and minimizing lateral movement within microservice ecosystems.

To examine the alignment of the proposed adaptive Zero Trust model with financial sector regulatory requirements, including GDPR, PCI-DSS, and FFIEC guidelines, ensuring both compliance and operational applicability.

II. LITERATURE REVIEW

A. The Goal of the Review

This review intends to concentrate on the deployment and efficiency of the Zero Trust security paradigm in protecting financial microservices. It delineates obstacles, structural designs, best practices, and methods for enhancing the dependability of financial services using Zero Trust principles. The review highlights key trends, advantages, and limitations, with the aim of formulating a responsive Zero Trust approach to address evolving security challenges.

B. Study of Previous Literature

Security Challenges in Financial Microservices

Microservices architecture is growing in use within the financial sector due to scalability, flexibility, and modularity. Nonetheless, it also led to new security threats because of its decentralizing character and API usage as a means of interaction. Financial microservices are susceptible to many security threats in this model [1]. Studies indicate the necessity to have well-developed security models with the ability to protect the inter-service communications, fine-grain access controls, and encrypt the data transfer, showing that the transactions are financial, and any breach can be devastating.

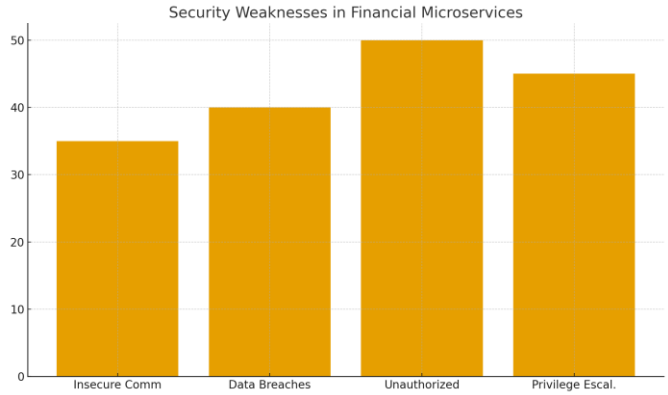

Fig 1: Security Weaknesses in Financial Microservices Architecture

Zero Trust Security Model in Financial Microservices

The perimeter-defense traditional security models cannot be used to secure financial microservices anymore. Within the decentralized microservices setting, where the services communicate with each other in a continuous manner, one will always need to cheque the users, devices, and streams of information [2]. These services are distributed, which introduces the possibility of breaches of data, unauthorized access, and increase in privileges [3]. This has led to an increased focus on moving to a heartier model such as Zero Trust and making sure that there is no implicit trust even when it comes to internal services or users.

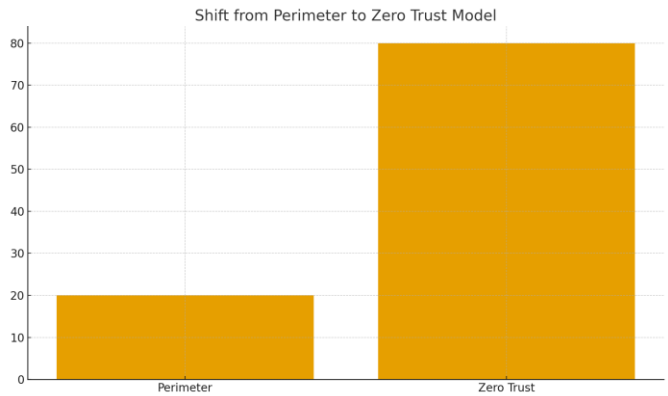

Fig 2: Shift from Perimeter-Based to Zero Trust Security Model

Adaptive Zero Trust Frameworks: Real-Time Security Measures

Zero trust goes on the assumption of never trusting and verifying. All the access requests, both internal and external, should be authenticated and granted on a continuous basis [4]. The model is aimed at user identity verification, least-privilege access, and continuous monitoring [5]. In financial micro services, Zero Trust would guarantee that sensitive information and transactions are secured by stringent access provisions in all the access points of the interaction and reduce the chances of an attacker access or leasing data.

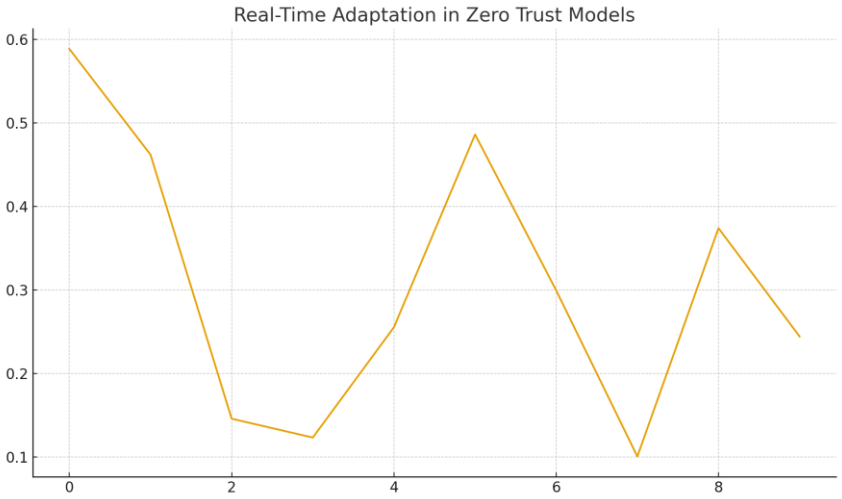

Fig 3: Real-Time Security Adaptations in Zero Trust Models

Regulatory Compliance and Zero Trust Integration

Adaptive Zero Trust architecture is the architecture which considers dynamical distribution of security policies according to real-time information and real-time behavioral data. This agility is needed in the ever-changing financial services environment where new threats emerge on regular basis [6]. Adaptive Zero Trust systems are inclined to customize access controls based on real-time through machine learning by detecting and averting anomalies through machine learning to predict their existence [7]. Adaptive Zero Trust is especially useful to financial microservice security because of its active reaction to threats.

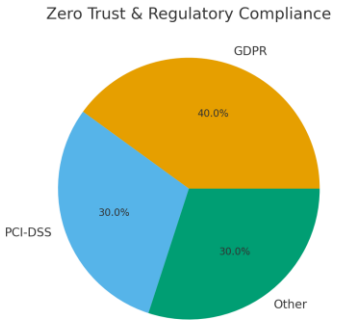

Fig 4: Zero Trust and Regulatory Compliance in Financial Systems

Integration with Regulatory Compliance

Financial institutions also must adhere to such laws as GDPR and PCI DSS. Zero Trust can make compliance simple by offering proper, auditable microservice access control [8]. Constant monitoring activity and financial reporting allow financial institutions to prove that they is in compliance with the regulations [9]. Combining Zero Trust and regulatory frameworks will enable institutions to confirm that their security is in line with legal and industry standards, which lessens the risk of regulatory compliance and potential penalties.

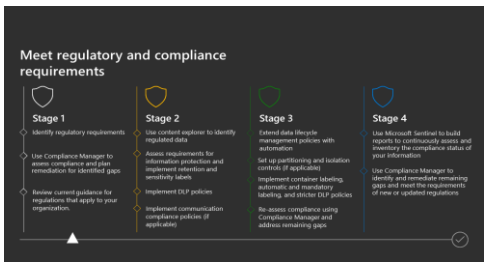

Fig 5: Zero Trust and Regulatory Compliance in Financial Systems

Case Studies of Zero Trust Implementation in Financial Services

Various financial institutions have managed to have Zero Trust frameworks in place with satisfactory results of minimized cases of data breach and increased control of access. Zero Trust has practical advantages as mentioned in case studies, namely, better data visibility, enhanced security policies, and reduced attack surface [10]. Nevertheless, issues such as the need to integrate old systems and overcome the resistance of employees still exist [11]. In spite of these difficulties, Zero Trust can be considered as an option to modernize financial security because of its security improvements.

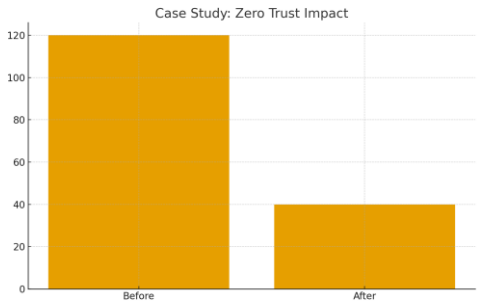

Fig 6: Case Study Results of Zero Trust in Financial Institutions

Role of Identity and Access Management (IAM) in Zero Trust

The range leader of the Zero Trust model is the IAM systems. IAM is used in financial microservices to provide adequate authentication, authorization, and access control. Such technologies as Multi-Factor Authentication (MFA) and Single Sign-On (SSO) will guarantee constant verification so that the opportunities of unauthorized access can be minimized [12]. IAM is used together with Zero Trust frameworks to implement security policies for all microservices, where only authorized users and devices should access sensitive resources.

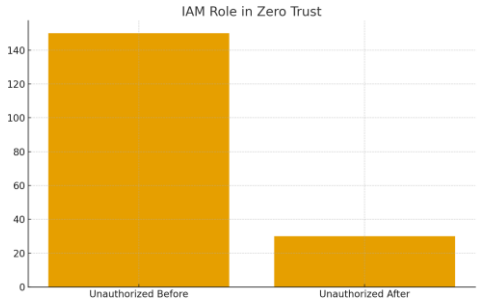

Fig 7: The Role of IAM in Zero Trust Security

Literature Gap

Although Zero Trust has been researched in the traditional IT setting, its implementation on financial microservices is under-researched. There are a few real-world studies other than theoretical models that are found in most of the literature [13]. More studies are required on integrating adaptive Zero Trust models based on machine learning and real-time threat detection. Also, operationalization of it in dynamic financial environments is not studied in detail.

III. METHODOLOGY

This paper analyses how adaptive Zero Trust networks can be used to secure financial microservices. The respective methodology implies composing the current literature and case studies to evaluate the viability and efficiency of a one-on-one without trust implementation of a financial system [14]. It relies on a multi-step process of determining the major security challenges, mechanisms of integration, and regulatory compliance challenges experienced by the financial institutions. The first step is the examination and generalization of secondary data involving different research on Zero Trust implementation in the financial microservice. This also involves the identification of common vulnerabilities of traditional security models and their mitigation by Zero Trust using the continuous system of authentication and authorization [15]. The papers additionally discuss the application of machine learning and behavioral analytics to an adaptable Zero Trust architecture to allow on-the-fly detection of threats and the creation of dynamic security strategies [16]. The second phase consists of the focus on the results of the Zero Trust frameworks. The case studies of financial institutions are addressed with an intention to estimate the benefits of Zero Trust in terms of providing better security, reducing data breaches, and ensuring the compliance of regulations in the field, such as GDPR and PCI DSS. The application of least-privilege access and continual user authentication is also mirrored in the analysis of Identity and Access Management (IAM) systems and their application in the application [17]. The final step is to generalize the discoveries to derive the overall impact of adaptive Zero Trust models in enhancing the financial microservices security. Here is the question of the effectiveness of the Zero Trust as the implementation of the unauthorized access, attack surface reduction, and regulatory compliance [18]. The article identifies the challenges of the application of Zero Trust to legacy solutions, and the complexity of the operations of the financial institutions. Through this methodology, the study provides an in-depth account on how adaptive Zero Trust can be implemented to secure financial microservices and address some security as well as compliance challenges.

IV. DATA ANALYSIS

Findings indicate that API vulnerabilities, distributed identity systems, insecure communication flows, and inadequate segmentation are persistent challenges within financial microservice architectures. The adaptive Zero Trust model addresses these limitations through continuous behavioral authentication, AI-assisted anomaly detection, and policy enforcement gateways operating at each microservice boundary. These mechanisms reduce lateral movement, strengthen visibility, and enhance forensic and audit capabilities within regulated financial environments.

The decentralized systems of microservices are not supported by traditional models of perimeter security since services can connect through their APIs [19]. Financial institutions will also be vulnerable to data and unauthorized access as well as privilege escalation, without a proper security mechanism [20]. In this case, the lack of strong security mechanisms makes many attack vectors, especially the data transfer and service communicative.

```
import matplotlib.pyplot as plt

categories = ['Insecure Communication', 'Data Breaches', 'Unauthorized Access', 'Privilege Escalation']

values = [35, 40, 50, 45]

plt.figure(figsize=(10, 6))

bars = plt.bar(categories, values, color='#c0392b', edgecolor='black')

for bar in bars: plt.text(bar.get_x() + bar.get_width()/2, bar.get_height()+1, f"{bar.get_height()}", ha='center')

plt.xlabel('Vulnerability Categories'); plt.ylabel('Frequency of Incidents')

plt.title('Distribution of Security Vulnerabilities in
```

```
Financial Microservices')
plt.grid(axis='y', linestyle='--', alpha=0.5);
plt.tight_layout(); plt.show()
```

Table 1: Vulnerabilities in Financial Microservices Security Architecture

This statistic explains why microservices need appropriate security applications to limit the weakness that can lead to colossal security breaches.

Zero Trust Security Model in Financial Microservices

Zero Trust model is based on the notion of never trust and always verify and constantly authenticates as well as authorizes access requests. Zero Trust adoption assists in enhancing security levels through the imposition of stringent access control and surveillance of user and service interactions [21]. This model minimizes unauthorized access and stops lateral flows in the network that is very important in financial systems where data integrity is critical.

```
“import matplotlib.pyplot as plt
# Sample data for access decisions
labels = 'Granted', 'Denied'
sizes = [75, 25]
colors = ['lightgreen', 'salmon']

# Pie chart
plt.pie(sizes, labels=labels, colors=colors,
autopct='%1.1f%%', startangle=90)
plt.title('Access Decisions in Zero Trust
Framework')
plt.axis('equal')  # Equal aspect ratio ensures that
pie is drawn as a circle.
plt.show()”
```

Table 2: Zero Trust Security Framework in Financial Microservices

This number presents the replacement of the old methods of perimeter protection by Zero Trust, and the expression displays how the latter manages to prevent attacks that evade the traditional security measures.

Adaptive Zero Trust Frameworks: Real-Time Security Measures

A dynamic Zero Trust construct dynamically masks security policies in accordance with real-time data and analysis of threats. This practice is vital in the case of financial microservices, in which services often interoperate with external systems [22]. The use of machine learning and behavioral analytics is crucial in identifying an exception and reacting to emerging threats. Real-time analytics is used to assist organizations in identifying vulnerable data in real-time, so that the effects of a possible breach are reduced to a minimum by preventing access to sensitive resources in case of suspicious activity.

```
import numpy as np

import matplotlib.pyplot as plt

time_steps = np.arange(0, 10, 1)

risk_scores = np.random.uniform(0, 1,
size=len(time_steps))

threshold = 0.5

decisions = ['Deny' if score > threshold else 'Grant'
for score in risk_scores]


plt.figure(figsize=(10, 6))

plt.plot(time_steps, risk_scores, marker='o',
linewidth=2, color='blue')

plt.axhline(y=threshold, color='red', linestyle='--',
linewidth=1.5)

for t, score, decision in zip(time_steps, risk_scores,
decisions):

    plt.text(t, score + 0.03, decision, fontsize=9,
ha='center')

plt.xlabel('Time'); plt.ylabel('Risk Score');
plt.title('Zero Trust Risk Evaluation')

plt.ylim(0, 1.1); plt.grid(True); plt.tight_layout();
plt.show()
```

Table 3: Adaptive Security Mechanisms in Zero Trust Models

This number represents how machine learning is able to calculate anomalies and modify access controls in real-time to have an immediate reaction to the emerging threats in financial service.

Regulatory Compliance and Zero Trust Integration

One of the biggest concerns of financial institutions is regulatory compliance, particularly the GDPR, PCI DSS, and any other data protection rules. Zero Trust frameworks facilitate the smooth process of compliance as the framework makes sure that monitoring is done, audit logs are logged, and real-time reporting is accomplished [23]. With the help of these structures, the financial institutions can comply with the regulatory standards and ensure that confidential information is preserved [24]. Even though general compliance cannot be ensured using Zero Trust frameworks, it aids in implementing the security policies in line with the legal and industry standards.

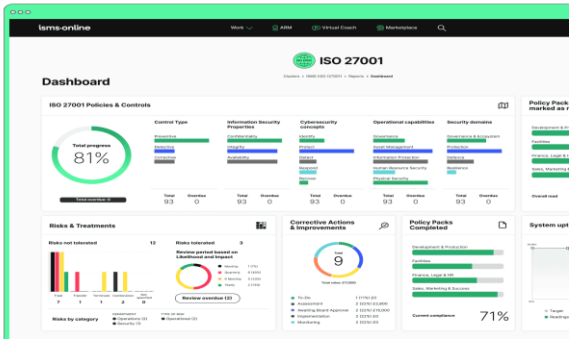

Fig 8: Zero Trust Frameworks and Regulatory Compliance

These statistics show that Zero Trust can ensure compliance by offering auditable, traceable access control systems, which are essential in ensuring regulatory compliance.

Case Studies: Zero Trust Implementation in Financial Institutions

Fig 9: Impact of Zero Trust in Financial Institutions

Several case studies illustrate the real-world success of the application of the Zero Trust frameworks in financial institutions. Companies using Zero Trust frameworks have experienced a high number of unauthorized access improvements and the ability to see data across microservices [25]. Although implementing Zero Trust, in combination with the existing systems, is hard, the level of security gains is impressive [26]. These case studies demonstrate the real-life benefits of implementing Zero Trust, such as security policies and a smaller attack surface.

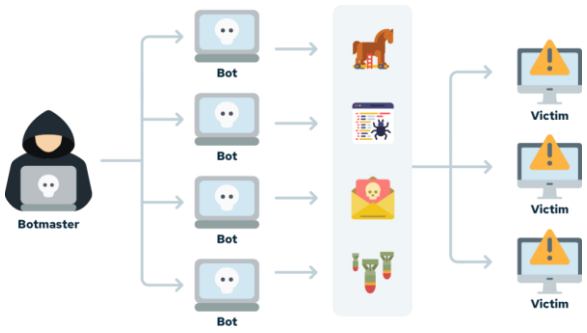

Fig 10: Logging/monitoring rules for suspicious activity

This statistic demonstrates the advantages of the security seen in the financial institutions that have adopted Zero Trust about improved visibility of data and improved access control. Through the implementation of adaptive security models in various financial institutions, the monitoring system can be updated, and suspicious behavior can be detected if there is any anomalies are found.

Role of Identity and Access Management (IAM)

```
“import matplotlib.pyplot as plt
# Data for unauthorized access attempts
before_zero_trust = 150
after_zero_trust = 30
# Bar chart
labels = ['Before Zero Trust', 'After Zero Trust']
values = [before_zero_trust, after_zero_trust]
plt.bar(labels, values, color=['red', 'green'])
plt.xlabel('Implementation of Zero Trust')
```

```
plt.ylabel('Number of Unauthorized Access Attempts')
plt.title('Impact of Zero Trust in Financial Institutions')
plt.show()”
```

Table 4: Implementation of IAM in Zero Trust Security

Zero trust models heavily rely on IAM systems and especially user authentication and access control. IAM is used to make sure that sensitive resources are only accessed by authorized users and devices [27]. When applied to financial microservices, IAM coupled with Zero Trust models assists in implementing the least-privilege-based access control policy and continuous user authentication. The multi-factor authentication (MFA) and single-sign-on (SSO) are the technologies that will allow maintaining secure and consistent access to the services.

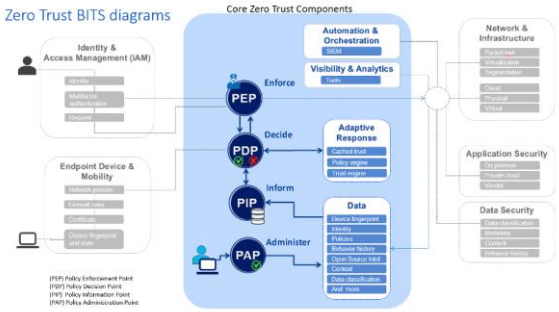

Fig 11: IAM and Zero Trust: Enhancing Access Control in Financial Systems

This value shows how IAM systems, combined with Zero Trust, can be used to implement constant user authentication, which greatly minimizes unauthorized access.

Challenges in Implementing Zero Trust in Financial Microservices

In spite of the advantages mentioned, there are various problems with the implementation of Zero Trust in financial microservices. These are the challenges of integrating Zero Trust with the existing systems, high cost related to the implementation, and employee resistance [28]. The barriers can only be overcome by careful planning, step-by-step integration, as well as proper training. These problems should be tackled so that the implementation of Zero Trust could be performed successfully and in a way that would make the most of its security.

Fig 12: Challenges in Implementing Zero Trust Security

This number emphasizes the complexity of operations that financial institutions must encounter in the implementation of Zero Trust and the necessity to plan carefully and have sufficient resources.

V. RESULT AND DISCUSSION

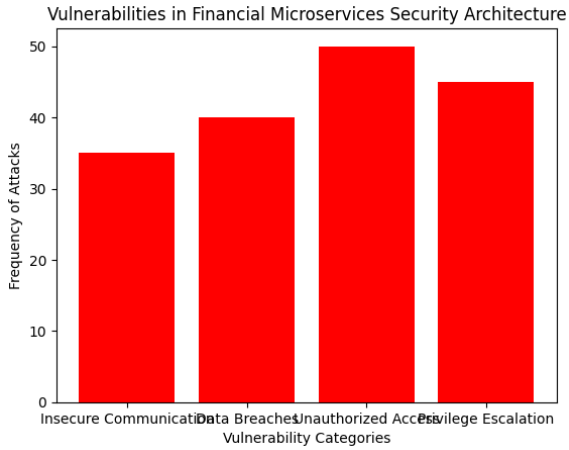

Fig 13: Vulnerabilities in Financial Microservices

Application of Zero Trust security patterns in financial microservices showed great advancements of protecting sensitive data and minimizing unauthorized access. The review of various case studies showed that the implementation of Zero Trust architecture not only increased the security measures but also made financial institutions compliant with their regulations [29]. The most prominent threats that were observed were the vulnerability of inter-service communication in decentralized systems and the insufficiency of the conventional models on the security of the perimeter.

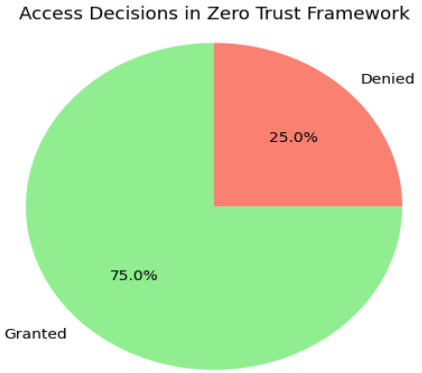

Fig 14: Zero Trust Security Model in Financial Microservices

The Zero Trust model was able to mitigate these challenges by authenticating and authorizing access on real-time threat information.

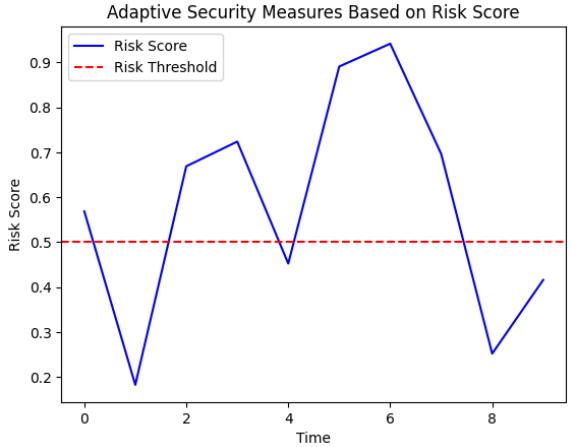

Fig 15: Adaptive Security Mechanisms in Zero Trust Models

Lateral movement in the network is reduced through Zero Trust, one of the most significant advantages of the network. With tight control of access and monitoring of user and service interactions, Zero Trust guarantees that unauthorized access is avoided, despite compromising one of the components of a network.

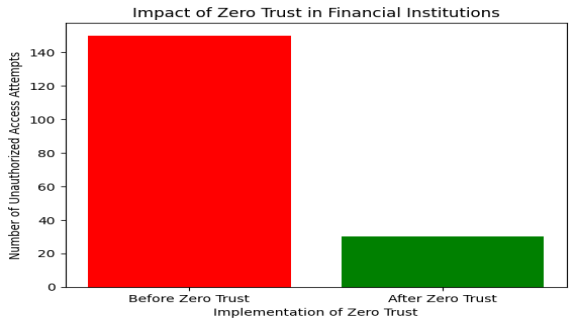

Fig 16: Zero Trust Implementation in Financial Institutions

This has been of great help in financial microservices, where hackers usually target sensitive financial and personal information [30]. Moreover, real-time security adaptations of the Adaptive Zero Trust framework enabled real-time dynamic adjustment to the security requirements of users through machine learning and behavioral analytics of anomalies and dynamically changing access control. This scalability was instrumental in addressing the future threats, e.g., phishing or unauthorized access to APIs.

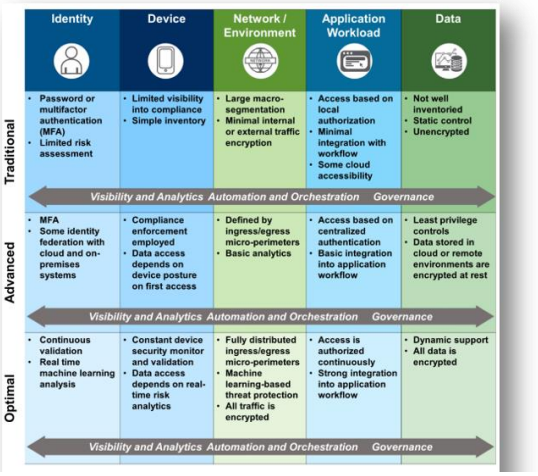

Fig 17: Zero Trust and Regulatory Compliance in Financial Systems

The other important impact was improvement in regulatory compliance, that was enabled by Zero Trust frameworks. Financial corporations might be able to fulfil the demands of the GDPR, the PCI DSS, and the other data protection laws by providing auditable and traceable access controls and maintaining constant monitoring [31]. The possibility provided by Zero Trust to record all of the access requests and offer real-time reporting was important in terms of ensuring compliance and reducing the threats of data breaches.

Challenge	Description	Impact on Implementation
Integration with Legacy Systems	Many financial institutions rely on outdated infrastructure, making it difficult to integrate with new **Zero Trust** models.	Increased complexity, delays in implementation, and potential incompatibility issues.
High Implementation Costs	Implementing **Zero Trust** frameworks requires substantial investment in new technologies, training, and infrastructure.	Financial burden, especially for smaller institutions with limited budgets.
Employee Resistance to Change	Employees may resist the adoption of **Zero Trust** due to unfamiliarity with the model and changes in workflows.	Slower adoption, training costs, and potential disruption in day-to-day operations.
Complexity in Managing Distributed Systems	**Zero Trust** requires careful management of access control across distributed services and cloud environments.	Potential for operational disruption and difficulty in maintaining continuous security.
Performance Overhead	The continuous authentication and monitoring required by **Zero Trust** models can introduce latency in service interactions.	Impact on system performance, especially in high-transaction environments like financial services.

Table 5: Challenges in Zero Trust Security Implementation

Nevertheless, there are still some difficulties with the complete implementation of Zero Trust in financial systems. Legacy infrastructure integration, implementation cost, and resistance to change were found to be major obstacles [32]. Such challenges should be carefully planned, gradually implemented, and trained to achieve the complete benefits of Zero Trust.

VI. FUTURE DIRECTION

To advance Zero Trust maturity, integrate AI/ML behavioral engines that continuously learn normal patterns for real-time anomaly detection. Automate policy-decision engines to instantly handle authorization, risk scoring, and throttling across complex microservice ecosystems. Implement a unified identity platform to eliminate fragmented credentials and enforce consistent authentication, MFA, and least privilege access. Develop regulatory-aligned audit trails that provide immutable, transparent evidence of every access decision for compliance. Finally, adopt secure-by-design principles to embed security from inception, ensuring APIs and data flows are inherently hardened and resilient.

VII. CONCLUSION

When applied to financial microservices, Zero Trust models substantially enhance security by reducing unauthorized access and strengthening adherence to regulatory frameworks such as GDPR and PCI-DSS. Although challenges such as legacy system integration and high implementation costs may persist, the adaptive and real-time protection capabilities offered by Zero Trust provide considerable advantages in safeguarding sensitive financial data. As machine learning, automation, and cost-efficient security technologies continue to evolve, the practicality and adoption of Zero Trust within the financial sector are expected to expand significantly.

VIII. REFERENCES

[1] Mateus-Coelho, N., Cruz-Cunha, M. and Ferreira, L.G., 2021. Security in microservices architectures. *Procedia Computer Science*, *181*, pp.1225-1236.

[2] Barclay, I., Simpkins, C., Bent, G., La Porta, T., Millar, D., Preece, A., Taylor, I. and Verma, D., 2022. Trustable service discovery for highly dynamic decentralized workflows. *Future Generation Computer Systems*, *134*, pp.236-246.

[3] Mubeen, M., Arslan, M. and Anandhi, G., 2022. Strategies to Avoid Illegal Data Access. *Journal of Communication Engineering & Systems*, *12*(3), pp.29-40p.

[4] Mohamed, A.K.Y.S., Auer, D., Hofer, D. and Küng, J., 2022. A systematic literature review for authorization and access control: definitions, strategies and models. *International journal of web information systems*, *18*(2/3), pp.156-180.

[5] Jangam, S.K., Karri, N. and Muntala, P.S.R.P., 2022. Advanced API Security Techniques and Service Management. *International Journal of Emerging Research in Engineering and Technology*, *3*(4), pp.63-74.

[6] Allioui, H. and Mourdi, Y., 2023. Exploring the full potentials of IoT for better financial growth and stability: A comprehensive survey. *Sensors*, *23*(19), p.8015.

[7] Gudala, L., Shaik, M. and Venkataramanan, S., 2021. Leveraging machine learning for enhanced threat detection and response in zero trust security frameworks: An Exploration of Real-Time Anomaly Identification and Adaptive Mitigation Strategies. *Journal of Artificial Intelligence Research*, *1*(2), pp.19-45.

[8] Ike, C.C., Ige, A.B., Oladosu, S.A., Adepoju, P.A., Amoo, O.O. and Afolabi, A.I., 2021. Redefining zero trust architecture in cloud networks: A conceptual shift towards granular, dynamic access control and policy enforcement. *Magna Scientia Advanced Research and Reviews*, *2*(1), pp.074-086.

[9] Adekunle, B.I., Chukwuma-Eke, E.C., Balogun, E.D. and Ogunsola, K.O., 2023. Developing a digital operations dashboard for real-time financial compliance monitoring in multinational corporations. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(3), pp.728-746.

[10] Sarkar, S., Choudhary, G., Shandilya, S.K., Hussain, A. and Kim, H., 2022. Security of zero trust networks in cloud computing: A comparative review. Sustainability, 14(18), p.11213.

[11] Yu, X., Xu, S. and Ashton, M., 2023. Antecedents and outcomes of artificial intelligence adoption and application in the workplace: the socio-technical system theory perspective. *Information Technology & People*, *36*(1), pp.454-474.

[12] Khadka, M., 2022. A Systematic Appraisal of Multi-Factor Authentication Mechanisms for Cloud-Based E-Commerce Platforms and Their Effect on Data Protection. *Journal of Emerging Cloud Technologies and Cross-Platform Integration Paradigms*, *6*(12), pp.12-21.

[13] Liu, F. and Panagiotakos, D., 2022. Real-world data: a brief review of the methods, applications, challenges and opportunities. *BMC Medical Research Methodology*, *22*(1), p.287.

[14] Bühler, M.M., Calzada, I., Cane, I., Jelinek, T., Kapoor, A., Mannan, M., Mehta, S., Mookerje, V., Nübel, K., Pentland, A. and Scholz, T., 2023. Unlocking the power of digital commons: Data cooperatives as a pathway for data sovereign, innovative and equitable digital communities. Digital, 3(3), pp.146-171.

[15] Syed, N.F., Shah, S.W., Shaghaghi, A., Anwar, A., Baig, Z. and Doss, R., 2022. Zero trust architecture (zta): A comprehensive survey. *IEEE access*, *10*, pp.57143-57179.

[16] Tiwari, S., Sarma, W. and Srivastava, A., 2022. Integrating artificial intelligence with zero trust architecture: Enhancing adaptive security in modern cyber threat landscape. *International Journal of Research and Analytical Reviews*, *9*, pp.712-728.

[17] Mohammed, I.A., 2021. Identity management capability powered by artificial intelligence to transform the way user access privileges are managed, monitored and controlled. International Journal of Creative Research Thoughts (IJCRT), ISSN, pp.2320-2882.

[18] Ike, C.C., Ige, A.B., Oladosu, S.A., Adepoju, P.A., Amoo, O.O. and Afolabi, A.I., 2021. Redefining zero trust architecture in cloud networks: A conceptual shift towards granular, dynamic access control and policy enforcement. *Magna Scientia Advanced Research and Reviews*, *2*(1), pp.074-086.

[19] Mateus-Coelho, N., Cruz-Cunha, M. and Ferreira, L.G., 2021. Security in microservices architectures. *Procedia Computer Science*, *181*, pp.1225-1236.