electronics

MDPI

Article

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

Clement Daah *, Amna Qureshi, Irfan Awan and Savas Konur

School of Computer Science, Artificial Intelligence and Electronics, Faculty of Engineering and Digital Technologies, University of Bradford, Bradford BD7 1DP, UK; a.qureshi19@bradford.ac.uk (A.Q.); i.u.awan@bradford.ac.uk (I.A.); s.konur@bradford.ac.uk (S.K.)

* Correspondence: c.daah@bradford.ac.uk

Abstract: As financial institutions navigate an increasingly complex cyber threat landscape and regulatory ecosystem, there is a pressing need for a robust and adaptive security architecture. This paper introduces a comprehensive, Zero Trust model-based framework specifically tailored for the finance industry. It encompasses identity and access management (IAM), data protection, and device and network security and introduces trust through blockchain technology. This study provides a literature review of existing Zero Trust paradigms and contrasts them with cybersecurity solutions currently relevant to financial settings. The research adopts a mixed methods approach, combining extensive qualitative analysis through a literature review and assessment of security assumptions, threat modelling, and implementation strategies with quantitative evaluation using a prototype banking application for vulnerability scanning, security testing, and performance testing. The IAM component ensures robust authentication and authorisation processes, while device and network security measures protect against both internal and external threats. Data protection mechanisms maintain the confidentiality and integrity of sensitive information. Additionally, the blockchain-based trust component serves as an innovative layer to enhance security measures, offering both tamper-proof verification and increased integrity. Through analysis of potential threats and experimental evaluation of the Zero Trust model's performance, the proposed framework offers financial institutions a comprehensive security architecture capable of effectively mitigating cyber threats and fostering enhanced consumer trust.

Keywords: Zero Trust; identity and access management; device and network security; data protection; blockchain

Citation: Daah, C.; Qureshi, A.; Awan, I.; Konur, S. Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: A Proposed Framework. *Electronics* **2024**, *13*, 865. https://doi.org/10.3390/electronics13050865

Academic Editor: Mehdi Sookhak

Received: 31 January 2024
Revised: 18 February 2024
Accepted: 20 February 2024
Published: 23 February 2024

1. Introduction

Banks, credit unions, and insurance companies bear the responsibility of protecting vast amounts of sensitive information and critical infrastructure. While perimeter-based security measures are still necessary and should be built upon, they still need to be improved to sufficiently safeguard these assets against increasingly complex and robust cyber threats. Financial institutions' challenges in securing their networks have been further intensified by the increasing interconnectedness of systems, the popularity of cloud computing, and the widespread use of mobile and Internet-of-Things (IoT) devices.

The financial impact of cyberattacks on financial institutions can be substantial, leading to significant financial losses and reputational damage. For instance, a study by [1] revealed that a cyberattack can increase cash holdings from a base level of 23% of assets to 26.87%. This increase in cash holdings is a sign that businesses are taking precautions to lessen the financial impact of potential cyberattacks.

Additionally, decreased firm value, weaker stock market performance, lower operating performance, decreased merger and acquisition activity, customer loss, and an increased cost of capital are some of the effects of reputational damage that a study by [2] has

documented. This highlights the substantial financial and reputational consequences that financial institutions may face following a cyberattack.

Traditional perimeter-based defences and the Defence-in-Depth approach, while providing layered security, have shown limitations in addressing sophisticated internal and external threats. These models often struggle to adapt dynamically to changing threat environments and may not effectively handle threats that have penetrated network perimeters.

The Zero Trust model has become a possible security framework that could help solve these problems by shifting the focus from traditional perimeter-based security to a more all-encompassing and granular approach [3]. The Zero Trust model is based on the principle "never trust, always verify," and it calls for the continuous verification of users, devices, and applications before providing them access to confidential data and resources [4]. Financial institutions are moving towards this model due to its potential to prevent advanced persistent threat (APT) attacks or significantly mitigate them. APT attacks are particularly concerning for financial institutions due to the potential for substantial financial losses and reputational damage. Incorporating the Zero Trust model can help reduce the risk of such attacks, thereby safeguarding the financial institution's assets and maintaining customer trust. The ever-changing nature of today's threats makes this model's more dynamic and adaptable security stance crucial.

Blockchain is one such technology that can provide a secure and transparent platform for information sharing in a Zero Trust context [5]. It can prevent unauthenticated participants from sharing information and filter out forged information through smart contracts and consensus mechanisms [6]. It guarantees anonymity yet entity authentication, data privacy yet data trustworthiness, and participant stimulation yet fairness [5]. Additionally, blockchain can ensure access management, user authentication, and transaction security in a Zero Trust architecture [7].

Blockchain technology has been increasingly applied in the financial industry, particularly in startup financing, supply chain finance, and banking services. It has been shown to streamline institutional functions, reduce operational risks, and improve business income [8–10]. In recent years, several financial firms like Goldman Sachs, J.P. Morgan, and other banking giants have established their blockchain laboratories, collaborating closely with blockchain platforms [10]. Additionally, blockchain technology has been applied in areas such as sustainable supply chain finance, central bank digital currencies, and transaction systems using smart contracts [11]. The technology's impact on the financial industry is significant, with its characteristics, performance, and advantages dramatically influencing various aspects of the industry.

Recent studies, such as those by [12], proposed a framework based on the Zero Trust concept and blockchain technology with the focus of making the banking sector safe from cyber attacks and data breaches. In addition to the framework, an algorithm for blockchain-based online transactions was designed to make use of practical implementation in the future. The use of blockchain technology in the finance industry has been shown to decrease banks' stock market volatility and facilitate price stabilisation [13]. Additionally, the application of blockchain in finance can accelerate the system to a stable state, ensuring compliance with contracts and enhancing automatic monitoring capabilities [14].

However, current implementations of Zero Trust in the banking sector, as discussed by [12], reveal limitations in scalability and adaptability. Responding to these challenges, this paper introduces a novel framework that integrates blockchain technology within the Zero Trust model, inspired by advancements in other sectors, such as e-health, where [7] have effectively employed a similar integration for secure medical image sharing. The proposed framework in our study is designed to enhance identity and access management, device and network security, and data protection in financial institutions, addressing the limitations of traditional models like Defence in Depth and the existing Zero Trust models and elevating their scalability and adaptability.

The primary objective of this research is to propose a comprehensive, Zero Trust model-based framework enhanced with blockchain technology and tailored for the finance

industry. This framework aims to address the limitations of traditional cybersecurity models by offering significant improvements in defences against cyber attacks. Additionally, the research examines the framework's influence on the operational efficacy of banking applications, specifically regarding its impact on transaction processing efficiency, system throughput, scalability, and resilience to cyber threats. By doing so, this study aims to address the following research questions:

- How does the integration of blockchain technology within a Zero Trust model framework improve cybersecurity measures in financial institutions?
- What cyber threats and vulnerabilities are effectively mitigated by the proposed blockchain-enhanced Zero Trust framework, and through what mechanisms?
- How does the proposed framework balance enhanced security measures with operational efficiency, particularly in terms of transaction latency, system throughput, and scalability?
- How does the proposed framework compare with established cybersecurity frameworks in the financial industry, particularly in terms of adherence to Zero Trust principles, regulatory compliance (including AML and KYC), data protection, and operational efficiency?

The framework incorporates strong authentication and authorisation processes, robust device and network security mechanisms, and advanced data protection techniques to mitigate cyber threats effectively and maintain the confidentiality, integrity, and availability of critical financial data, ultimately increasing consumer confidence in the institution's services. This study demonstrates the framework's effectiveness through practical examples and insights gained from implementing a prototype bank app. A comprehensive evaluation of the framework's performance against existing cybersecurity frameworks was conducted, including compliance and regulatory adherence, implementation complexity, performance efficiency, and adaptability to evolving cyber threats. Additionally, this paper provides a detailed summary of Zero Trust, its evolution, and how it is reshaping the future of the finance industry. At the time of writing this paper, no study had proposed a Zero Trust model-based framework for financial institutions.

The remaining part of this paper is organised as follows: Section 2 discusses the Zero Trust framework, cybersecurity frameworks for the finance industry, cybersecurity challenges in the finance industry, real-world Zero Trust approaches, and security models in the finance industry. Section 3 details the proposed framework and its components with and without Zero Trust implementation. Section 4 provides implementation details and evaluation methodology. Section 5 analyses the results and discusses the benefits. Finally, Section 6 concludes this paper and provides future research directions.

2. Background and Related Work

This section examines and summarises current research relevant to applying the Zero Trust model in financial organisations. The aim is to offer a detailed look at the Zero Trust approach, existing cybersecurity challenges in the finance industry, existing cybersecurity frameworks and solutions in the financial sector, real-world Zero Trust approaches, and the current security models used in the finance industry. Given the growing complexity and sophistication of cyber threats targeting financial institutions and the legal requirements that these organisations face, the review emphasises the necessity for a comprehensive and adaptive security architecture for the finance sector.

2.1. Zero Trust

Zero Trust is a strategic initiative for cybersecurity that can keep an organisation safe [15]. It does this by getting rid of blind trust and continuously validating each step of digital interaction. Zero Trust is based on the principle "never trust, always verify". Its goal is to protect today's technological environment while making digital transformation easier. It uses multi-factor authentication, network segmentation, elimination of lateral movement, layer 7 threat prevention, and streamlining granular "least access" policies.

The concept of "Zero Trust" arose from the realisation that conventional security models are based on the out-of-date idea that everything within an organisation's network can be trusted without further investigation [4]. Because there are not enough fine-grained security controls, users (including threat actors and malicious insiders) can freely move around the network, access sensitive data, and send it out because the network trusts them.

Principles of Zero Trust

Zero Trust is based on three core principles, as outlined in the NIST Special Publication 800-207.

- The first principle is "continuous verification", which means that trust should never be assumed and that every access request should be verified [16]. This principle aligns with the idea of not trusting any entity by default, whether inside or outside the security perimeter;
- The second principle is to limit the "blast radius", which involves restricting the breadth of credentials or access pathways an attacker can use. By implementing Zero Trust, organisations can minimise the potential damage caused by a breach and buy time to respond and mitigate the attack [17];
- The third principle is to "automate context collection and response", which emphasizes the importance of collecting and analysing data from various sources to make effective and accurate security decisions in real time.

2.2. Zero Trust Architecture

The Zero Trust model encompasses several pillars that form the foundation of its implementation, as shown in Figure 1. These pillars include Zero Trust data, networks, workloads, people, devices, applications, visibility and analytics, and automated orchestration. Zero Trust data focuses on protecting data as the primary objective and implementing controls to detect and prevent unauthorised access [17]. Zero Trust networks involve separating, isolating, and limiting network access, making it difficult for attackers to move laterally within the network. Zero Trust workloads encompass securing all applications and back-end software to prevent unauthorised access and interference. Zero Trust people emphasise the need to limit and monitor user access to resources and to trust but verify all user actions.

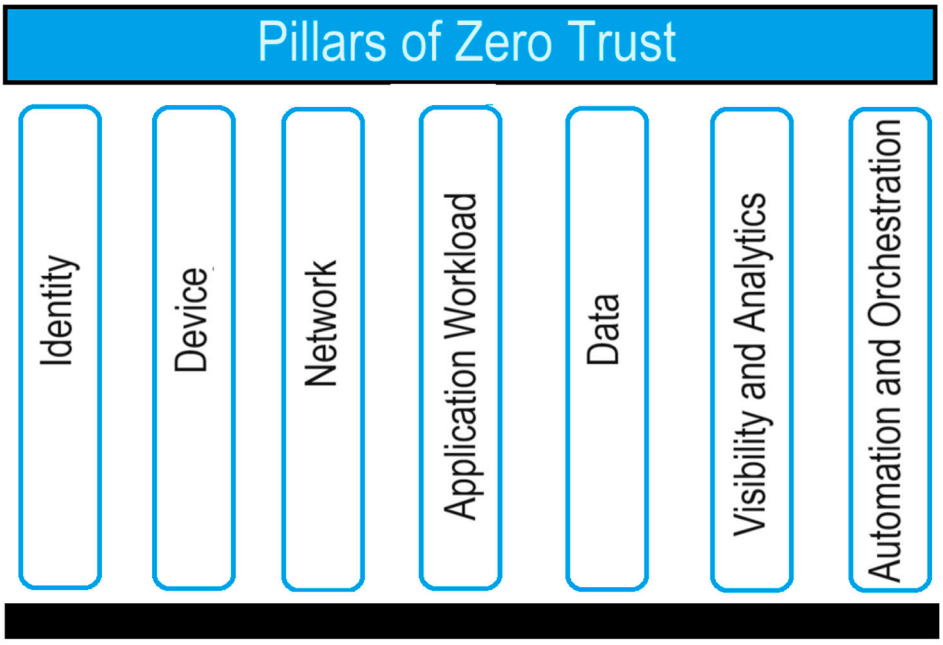

Figure 1. Pillars of the Zero Trust security framework [18].

Zero Trust devices involve securing and controlling every device connected to the network to prevent potential access points for attackers. Zero Trust applications focus on securing access at the application layer by connecting user, device, and data components. Visibility and analytics enable organisations to have complete visibility into their IT environment and use analytics to detect and respond to suspicious activities in real time. Automated orchestration involves continuously enforcing Zero Trust rules and automating security systems to keep up with the increasing number of monitoring events.

In the last decade, businesses have begun to spread their DAAS (data, assets, applications, and services) across different servers and cloud storage options. Due to this decentralisation, it is no longer possible to secure a network by isolating it within a single location, group of devices, or group of users. The Zero Trust framework was made in this distributed, cloud-native environment to help businesses protect their most valuable assets.

Based on the idea that there is no secure network perimeter, Zero Trust requires designing a system in which every user and service is treated as a possible security risk, no matter how deeply they are embedded in the network. Access requests must be constantly checked to ensure that the system can connect to the applications and services [19]. Users and devices would undergo continuous authentication of their identities and privileges, and logins, connections, and API tokens would have a finite lifespan. User DAAS access can be closely monitored with this "never trust, always verify" strategy. Access control, constant evaluation, and maximum observability are essential in the cloud-native world, where consumers may be geographically dispersed, using various devices, and actively trying to access DAAS via secure and unsecured networks [20].

The Zero Trust model treats every request as if it came from the public Internet rather than trusting that anything behind the company firewall is secure. Zero Trust teaches us to "never trust, always verify," regardless of the source or target of a request [21]. Each request is checked for authentication, authorisation, and encryption before access is given, as shown in Figure 2. The principles of micro-segmentation and least-privileged access are used to restrict communication between nodes. Anomalies are identified and dealt with instantly by employing sophisticated intelligence and analytics.

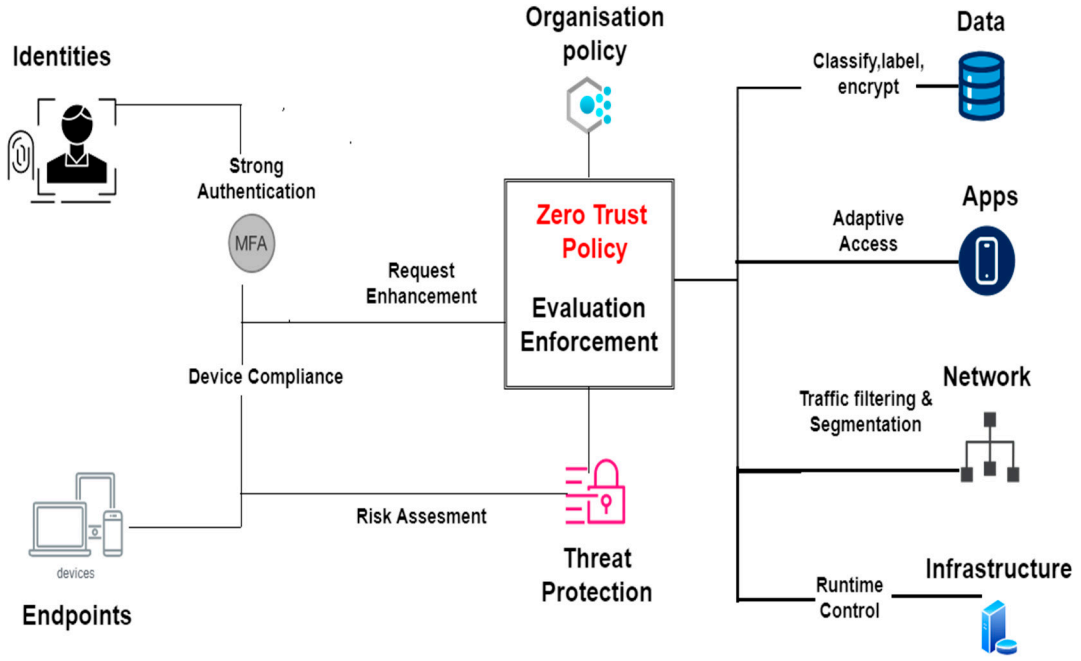

Figure 2. Zero Trust security architecture [22].

2.3. Existing Cybersecurity Challenges in the Finance Industry

The finance industry, particularly banks, faces a diverse range of security challenges due to the dynamic digital landscape and the sensitive nature of its operations [23]. These challenges are multifaceted, interconnected, and continually evolving, necessitating robust and adaptive security measures.

The prevalence of cyber threats, including sophisticated malware, ransomware attacks, phishing, and social engineering campaigns, has escalated in recent years, demanding advanced cybersecurity strategies to combat the complexity and variety of these attacks [24]. Data breaches in the finance sector not only led to financial losses but also undermined customer trust, emphasising the critical need for effective data protection measures. The growing concern for privacy, compounded by regulations such as the General Data Protection Regulation (GDPR), places additional pressure on financial institutions to safeguard customer data and ensure compliance with data privacy laws.

The banking industry faces increased risks from cyber threats, primarily through mobile applications, web portals, and other communication channels [25]. Furthermore, the efficient management of cyber risk in IT-based banking systems is stressed by managers, regulators, and international organisations, as cyber risk can adversely affect banks and financial institutions [26]. One of the critical challenges faced by banks is the behaviour of their employees, which can lead to cybersecurity threats. It has been noted that cybersecurity threats originating from employees' incorrect behaviour remain a significant challenge in the banking sector [27]. A recent example that highlights the persistent threat of phishing and social engineering in the financial sector is the 2021 phishing attack on Banco de España. This attack involved a sophisticated phishing campaign that targeted the bank's customers, employing fraudulent emails and websites that closely mimicked the bank's official communications. This incident not only resulted in financial losses but also raised serious concerns about the security of customer information, demonstrating the ongoing challenge that financial institutions face in protecting against these types of cyber threats.

Additionally, until banking staff are appropriately trained to operate and behave in a cyber-resilient manner, banks will continue to be exposed to a wide variety of cyber threats. Weak security controls in the banking sector have led to difficulties in detecting and preventing fraud. The recent credit crisis has exposed considerable weaknesses in risk management across the financial services industry, necessitating a critical review of governance mechanisms.

The banking sector is also exposed to various types of cybercrimes, including underground attack technologies, which have been examined in the context of the Nigerian banking sector [28]. Furthermore, the paper "Cyber Security Challenges through the Lens of the Financial Industry" draws attention to the increased concern among European and international authorities regarding cybersecurity risks faced by the financial industry, emphasising the need for proper prevention, identification, assessment, and management of these risks [29].

Moreover, the economic cost of publicly announced information security breaches has been studied, with limited evidence of an overall negative stock market reaction to such breaches. However, the financial costs associated with data breaches are growing, and data breach disclosure laws have been found to impact the cash policies of corporations in the United States [30]. This underscores the financial implications of cybersecurity challenges for banks and financial institutions.

In addressing these challenges, financial institutions must adopt a holistic and layered approach to security. The Zero Trust model, with its principle of "never trust, always verify," offers a promising framework to counter these threats by fundamentally rethinking how security is implemented.

2.4. Existing Cybersecurity Frameworks for the Finance Industry

Financial institutions prioritise robust cybersecurity measures to protect against cyber-attacks and secure sensitive financial data. Existing cybersecurity frameworks guide them in implementing best practices and ensuring the confidentiality, integrity, and availability of critical data and information. This section delves into some of the popular existing cybersecurity frameworks used in the finance industry.

2.4.1. NIST Cybersecurity Framework

One widely accepted cybersecurity framework in the banking sector is the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Organisations widely recognise and utilise the NIST Cybersecurity Framework to facilitate cybersecurity risk management [31]. This framework provides a comprehensive approach to identifying, protecting, detecting, responding to, and recovering from cybersecurity incidents. It emphasises the importance of risk assessment, continuous monitoring, and incident response planning [32]. The NIST Cybersecurity Framework also promotes collaboration and information sharing among stakeholders to enhance cybersecurity resilience [33].

As illustrated in Figure 3, the NIST Cybersecurity Framework consists of five core functions: Identify, Protect, Detect, Respond, and Recover.

- Identify function: This involves understanding the organisation's cybersecurity risks, establishing governance, and managing assets and access controls;
- Protect function: It focuses on implementing safeguards against potential threats and vulnerabilities. This includes activities such as access control, awareness training, and data protection measures;
- Detect function: This involves continuous monitoring and timely detection of cybersecurity events. This includes activities such as anomaly detection, security event monitoring, and incident detection;
- Respond function: It focuses on taking appropriate actions to mitigate the impact of a cybersecurity incident. This includes activities such as incident response planning, communication, and coordination;
- Recover function: This involves restoring normal operations and services after a cybersecurity incident. This includes activities such as recovery planning, improvements, and lessons learned [34].

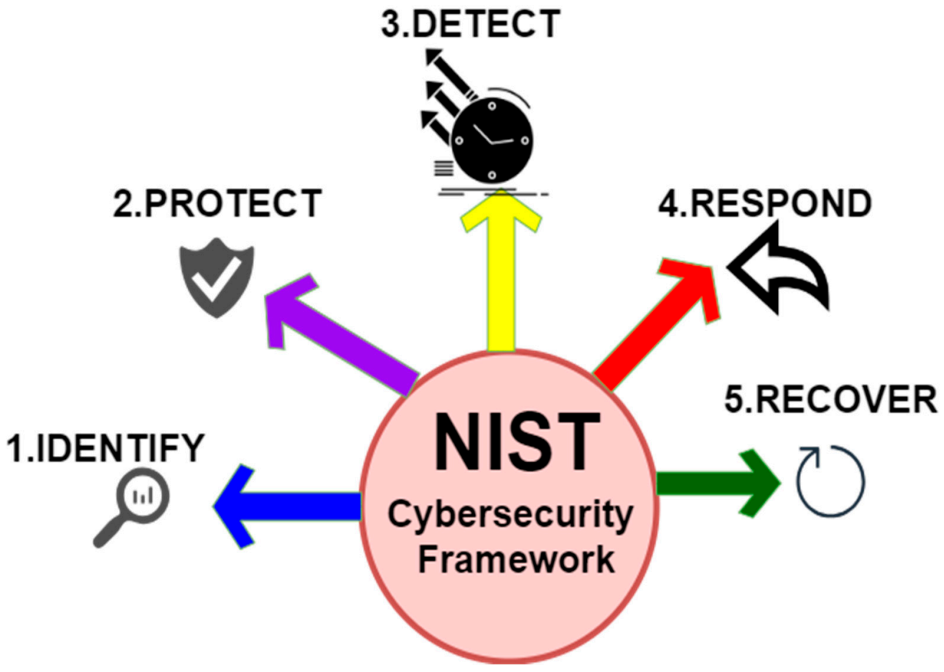

Figure 3. NIST Cybersecurity Framework [35].

The NIST Cybersecurity Framework provides the finance industry with a flexible and customisable approach to managing cybersecurity risks. It can be tailored to an organisation's specific needs and risk profile. The framework encourages organisations to assess their current cybersecurity posture, set goals, and prioritise actions based on their risk assessment. It also emphasises the importance of continuous improvement and adaptation to evolving cyber threats [36]. However, it is important to note that the NIST Cybersecurity Framework has some limitations: the framework does not provide specific technical implementation details or prescribe specific security controls. It provides high-level guidance and principles, leaving the implementation details to the organisation's discretion [37].

2.4.2. Centre for Internet (CIS) Critical Security Controls

Another significant cybersecurity framework widely used in the finance industry is the CIS Critical Security Controls [38]. These controls offer a prioritised set of actions organisations can implement to enhance their cybersecurity posture. The controls encompass various areas, including inventory and control of hardware and software assets, continuous vulnerability management, secure configuration for hardware and software, and controlled use of administrative privileges, as shown in Figure 4.

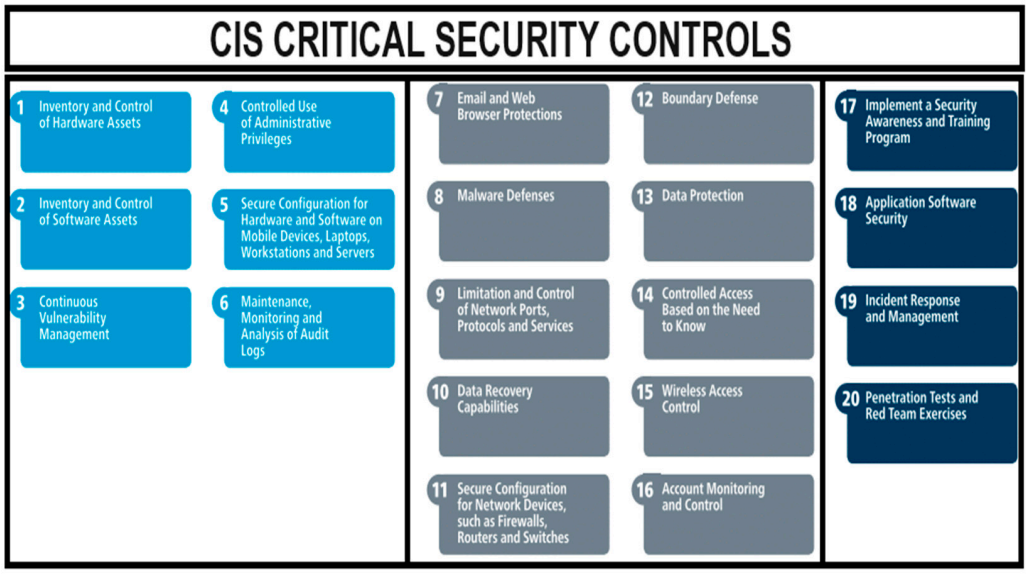

Figure 4. CIS Critical Security Controls [35].

The CIS Critical Security Controls are specifically designed to address common cybersecurity risks and provide organisations with a roadmap for implementing effective security measures. By adhering to these controls, organisations can improve their ability to detect and respond to cyber threats, reduce vulnerabilities, and safeguard sensitive financial information.

- Inventory and Control of Hardware and Software Assets: This control focuses on maintaining an up-to-date inventory of all hardware and software assets within the organisation. It aids in identifying and managing potential vulnerabilities and ensuring that only authorised devices and software are utilised;
- Continuous Vulnerability Management: This control emphasises the importance of regularly scanning and assessing systems for vulnerabilities. By implementing vulnerability management processes, organisations can promptly identify and remediate vulnerabilities, thereby reducing the risk of exploitation by attackers;

- Secure Configuration for Hardware and Software: It is a critical control that emphasises the implementation of secure configurations for all hardware and software assets. This control ensures that systems are configured securely, following industry best practices and minimising potential security breaches;
- Controlled Use of Administrative Privileges: It is another important control that aims to limit and monitor the use of administrative privileges within the organisation.

These controls, along with others included in the CIS Critical Security Controls framework, provide stakeholders with a comprehensive approach to managing cybersecurity risks in the finance industry. By addressing areas such as inventory and control of assets, vulnerability management, secure configuration, and controlled use of administrative privileges, organisations can enhance their ability to detect, respond to, and mitigate cyber threats in the finance industry. However, one limitation of the CIS Critical Security Controls is that they are not updated as frequently as other frameworks. Cyber threats and attack techniques constantly evolve, and new vulnerabilities and risks emerge regularly [39].

2.4.3. ISO 27001/27002

ISO 27001/27002 [40] is an international standard for information security management systems (ISMS) that banks and financial institutions widely adopt to ensure the confidentiality, integrity, and availability of their information. This standard provides a systematic approach to managing sensitive company information, including financial data. It outlines a risk management process and provides a set of controls that organisations can implement to protect their information assets [41].

The ISO 27001 standard focuses on establishing, implementing, maintaining, and continually improving an ISMS within the organisation. It provides a framework for organisations to identify and assess information security risks, define security objectives and controls, and monitor and review the effectiveness of the implemented controls as shown in Figure 5 [42]. The standard emphasises the importance of a risk-based approach to information security management, ensuring that controls are implemented based on the identified risks and the organisation's risk appetite [43].

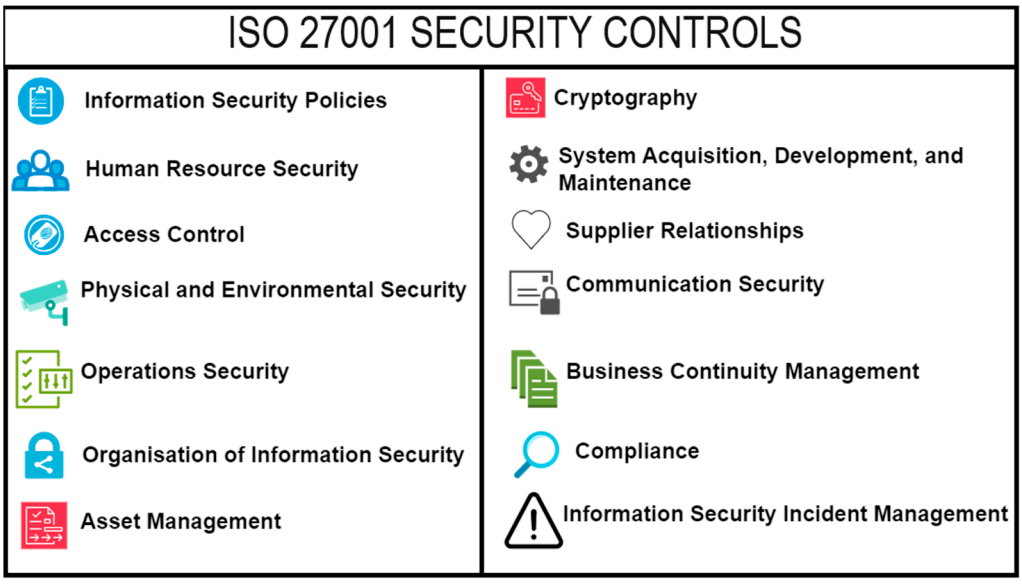

Figure 5. ISO 27001 security controls [35].

ISO 27002, on the other hand, provides a code of practice for information security controls. It offers a comprehensive set of security controls that organisations can select and implement based on their specific needs and risk profiles. These controls cover various areas, such as access control, cryptography, physical and environmental security, and inci-

dent management [44]. By implementing the controls outlined in ISO 27001/27002, banks and financial institutions can establish a robust information security management system.

This helps them protect sensitive financial data, prevent unauthorised access, and mitigate the risk of security breaches. The standard provides a structured and systematic approach to managing information security risks, ensuring appropriate controls are in place to safeguard critical information assets [45]. However, it is important to note that implementing ISO 27001/27002 requires significant effort and resources. Organisations need to conduct a thorough risk assessment, develop and implement security policies and procedures, and regularly monitor and review the effectiveness of the implemented controls. This can be a complex and time-consuming process, requiring the involvement and commitment of various stakeholders within the organisation [46].

2.4.4. PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a global standard specifically designed to secure cardholder data in credit card transactions. It is essential for financial institutions involved in payment card transactions and aims to protect sensitive financial information. The PCI DSS standard outlines a set of requirements that organisations must comply with to ensure cardholder data security. These requirements cover various aspects of information security, including network security, access control, encryption, and vulnerability management, as shown in Figure 6. By adhering to these requirements, organisations can mitigate the risk of data breaches and unauthorised access to cardholder information [47]. One of the key aspects of PCI DSS is the requirement for organisations to maintain a secure network infrastructure. This includes implementing firewalls, regularly updating security patches, and restricting access to cardholder data. By maintaining a secure network, organisations can prevent unauthorised access and protect cardholder information from potential threats [48].

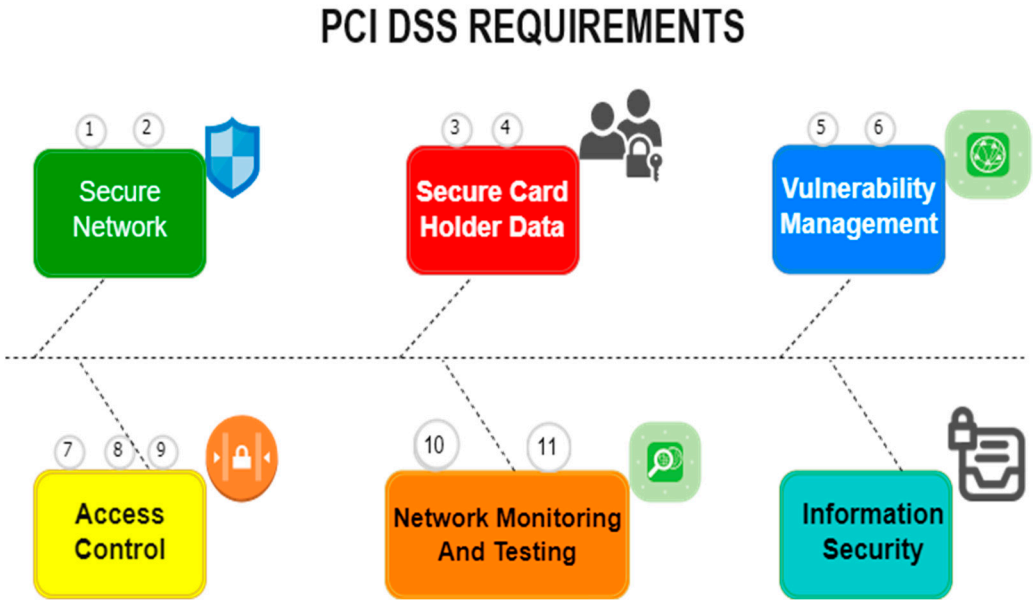

Figure 6. Requirements of PCI DSS [49].

Another important requirement of PCI DSS is the implementation of strong access control measures. This involves assigning unique user IDs, implementing strong authentication mechanisms, and regularly reviewing user access privileges. By enforcing strict access controls, organisations can ensure that only authorised individuals have access to cardholder data [50]. Encryption is also a crucial component of PCI DSS. The standard requires organisations to encrypt cardholder data during transmission and storage. Encryp-

tion helps protect sensitive information from being intercepted or accessed by unauthorised parties, thereby reducing the risk of data breaches [51].

Furthermore, PCI DSS emphasises the importance of regular vulnerability scanning and penetration testing. Organisations are required to conduct regular scans to identify and address vulnerabilities in their systems. By proactively identifying and addressing vulnerabilities, organisations can reduce the risk of exploitation by attackers [52]. However, it is important to note that PCI DSS has a limited scope and may require supplementary security measures to ensure comprehensive protection of cardholder information [53].

The finance industry, including the banking sector, has recognised the critical importance of cybersecurity. The above-mentioned cybersecurity frameworks have been developed to guide the finance industry in managing cybersecurity risks and protecting sensitive financial information. These frameworks provide a structured approach to identify, protect, detect, respond to, and recover from cyber threats. However, it is crucial for the finance industry to continuously monitor and improve their cybersecurity measures to stay resilient against evolving cyber threats.

2.5. Real-World Zero Trust Approaches

The rising number of cyber threats targeting financial institutions necessitates shifting from traditional perimeter-based security models to more robust and adaptive frameworks. The Zero Trust model has emerged as a feasible paradigm, with several real-world implementations manifesting its principles in practical settings. This section delves into some of the prominent real-world implementations of the Zero Trust model, including Google's BeyondCorp, Forrester NGFW/ZTX, the Software-Defined Perimeter (SDP), and VMWare NSX, exploring their architectures, functionalities, and the context of their applicability.

2.5.1. BeyondCorp

BeyondCorp, developed by Google, represents an updated version of the Zero Trust model, using both their extensive expertise and community feedback. By shifting access rules away from network boundaries and focusing on individual users, BeyondCorp eliminates the need for VPNs. This approach aligns with the NIST Zero Trust guidelines for device agent/gateway-based deployment [54]. The complete structure of BeyondCorp includes key components such as Single Sign-On (SSO), access proxy, control engine, lists of users and devices, security rules, and a trusted database. This creates a strong system for protecting modern applications and services [55].

BeyondCorp questions the idea that separating network areas is sufficient for protecting sensitive data. Instead, it introduces a user- and device-focused process for authentication and permission when accessing applications. Although promising, this paradigm shift presents challenges in transitioning without disrupting user experiences. The advent of BeyondProd as a cloud-native security service exemplifies the continuous evolution to accommodate varying organisational needs [7]. BeyondCorp represents an updated version of the Zero Trust model that focuses on individual users and devices rather than network boundaries, as shown in Figure 7. It eliminates the need for VPNs and introduces a user- and device-focused process for authentication and permission. While promising, the transition to BeyondCorp may present challenges in terms of the user experience. Nonetheless, the continuous evolution of BeyondCorp, such as the introduction of BeyondProd, demonstrates its adaptability to meet the evolving needs of organisations.

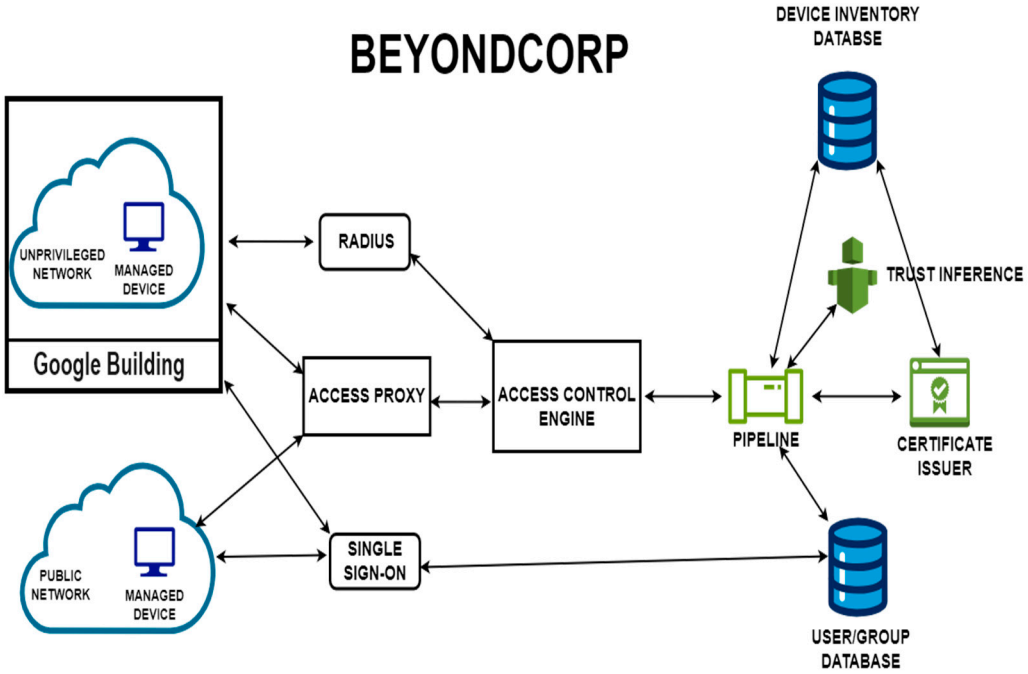

Figure 7. Google BeyondCorp components and access flow [56].

2.5.2. Forrester NGFW/ZTX

The Forrester NGFW/ZTX model, proposed by Kindervag in 2010, advocates for a centralised engine to segregate the corporate network into micro-core and perimeter (MCAP) segments, as shown in Figure 8. This model aligns with NIST's resource portal-Based deployment model and provides a simplistic yet effective framework, particularly suitable for organisations with a large number of IoT devices.

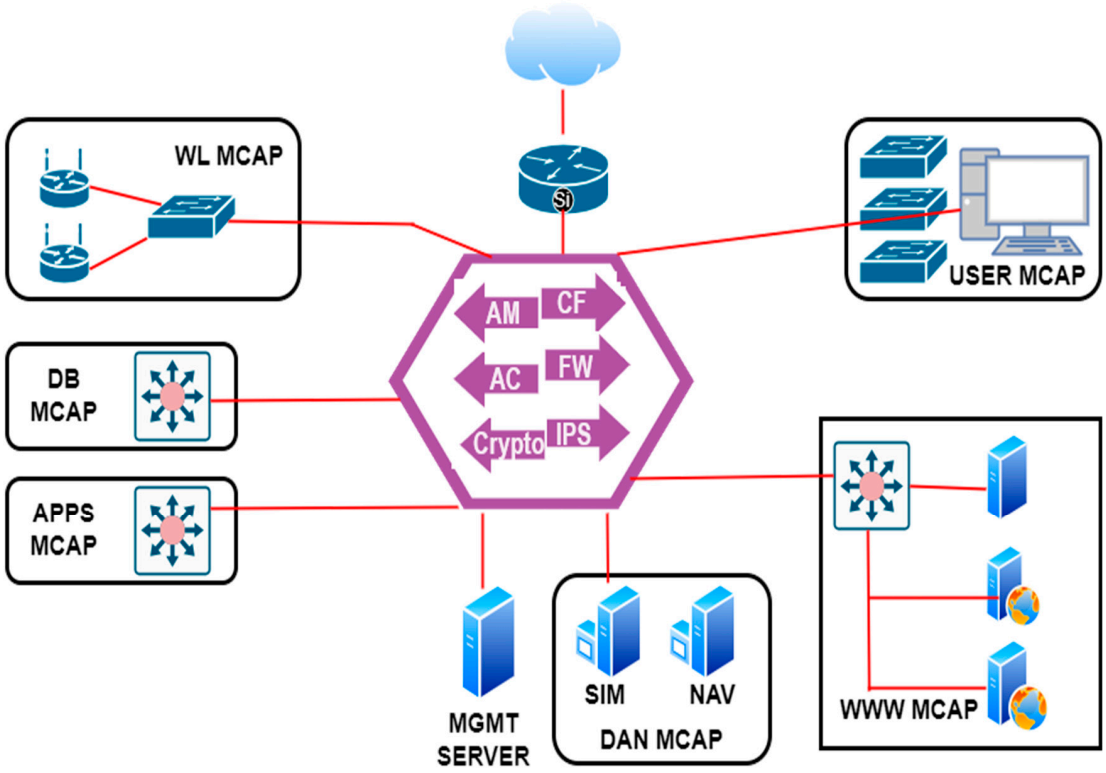

Figure 8. The Forrester/NGFW model [57].

The Forrester Zero Trust eXtended (ZTX) framework expands beyond network segmentation and encompasses seven crucial dimensions where Zero Trust principles apply: networks, data, people, workloads, devices, visibility and analytics, automation, and orchestration. This comprehensive framework enables security personnel to understand how different technologies contribute to network isolation, segmentation, security, data categorisation, encryption, and control principles. It also facilitates the implementation of policies to secure human users, network infrastructure resources, and application workloads in both public and private cloud environments. However, a notable drawback of the Forrester NGFW/ZTX model is the firewall's inability to authenticate users due to limitations in the segmentation engine [58]. The model's limitations in user authentication highlight the need for additional technologies like IAM and VPNs to address this challenge.

2.5.3. Cloud Security Alliance's (CSA) Software-Defined Perimeter

The Software-Defined Perimeter (SDP) model, originating from the U.S. Department of Defence, emphasises network access micro-segmentation and creates on-the-fly one-to-one connections between users and the required resources. Unlike traditional models, SDP focuses on protecting both the user and the application, employing a unique session initiation protocol to enable precise access control [59].

The SDP framework consists of two essential components: the SDP controller and the SDP host or gateway, as shown in Figure 9. These components work together to establish a secure communication channel between authorised entities. This framework offers a more granular and dynamic approach to network security. The SDP model aligns with the principles of Zero Trust, as it emphasises the need for strict access control and verification of both users and devices. By implementing SDP, organisations can achieve a higher level of security by reducing the attack surface and ensuring that only authorised entities can access specific resources. However, the implementation process may pose challenges, requiring careful consideration and setup on both the resource and endpoint.

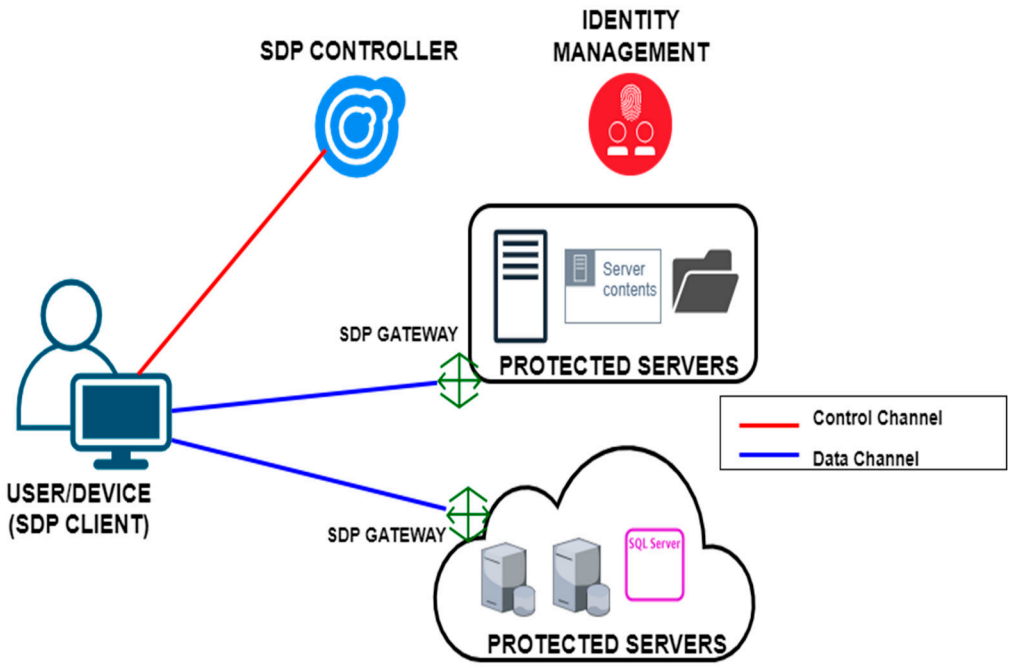

Figure 9. Software-Defined Perimeter framework [60].

2.5.4. VMware NSX

The VMware NSX model, based on Zero Trust principles, offers network virtualisation technology that includes various components for the development, security, and management of virtual networks, as shown in Figure 10. The core principle of the NSX Data Centre

is micro-segmentation, which allows for precise control over traffic flow across different operational environments.

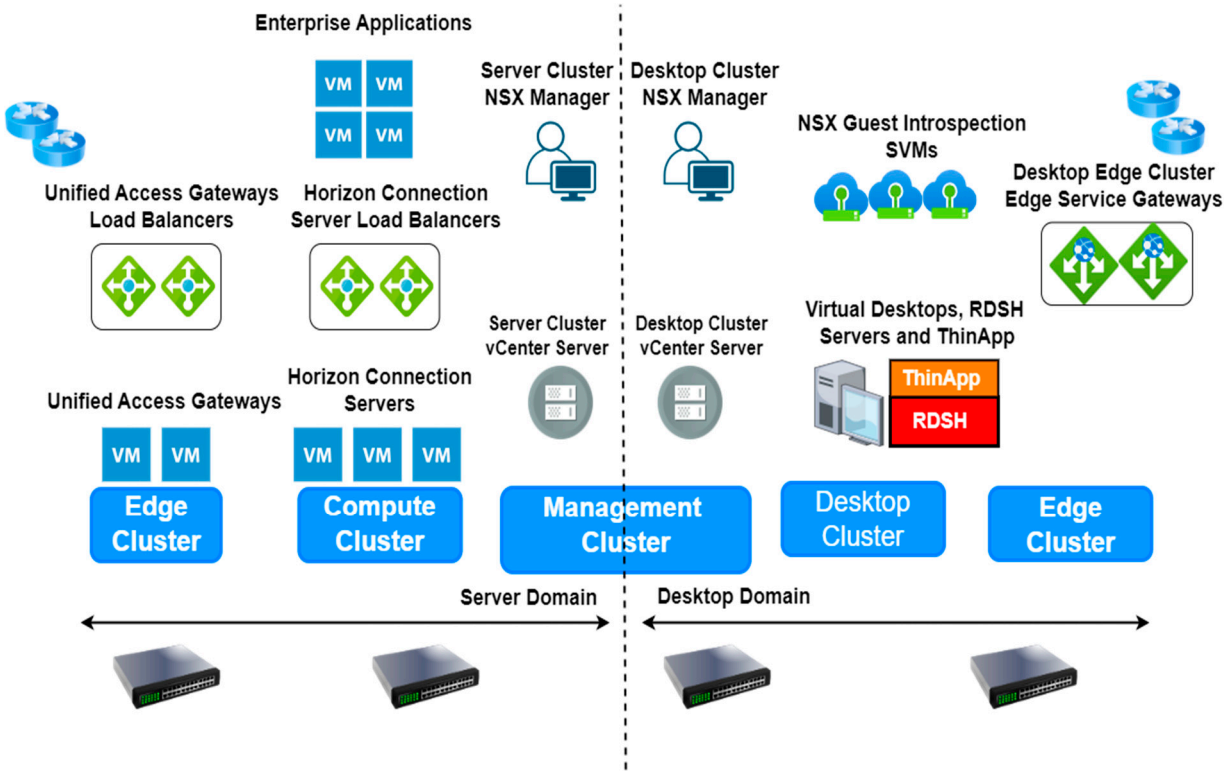

Figure 10. VMware NSX model [61].

The VMware NSX model demonstrates a virtualised desktop approach that effectively thwarts attackers' attempts to establish a persistent presence within the network. The network virtualisation technology and focus on micro-segmentation align with Zero Trust principles and provide organisations with a robust framework for network security. However, the requirement for virtualisation in the model can present challenges, particularly in IoT systems where virtualisation may be necessary for sensors and operational technology [62].

2.5.5. Comparative Analysis of the Real-World Zero Trust Model Implementations

Table 1 effectively aligns practical implementations of the Zero Trust model with the main pillars of the Zero Trust model, offering a comprehensive view of the performance, benefits, and limitations of each implementation. This comparative analysis provides a solid base for identifying the most fitting Zero Trust strategy across different organisational scenarios, with a focus on the financial sector.

It is evident from Table 1 that BeyondCorp excels in network segmentation and strong user and device verification processes, making it suitable for cloud-hosted applications. VMware NSX shows proficiency in micro-segmentation and transport encryption alongside virtualised desktop solutions, but it can be costly. The SDP model stands out for its cost-effective application integration and strong access control mechanisms, though it requires a significant initial setup effort. Forrester's NGFW/ZTX framework, while offering simplified deployment in BYOD environments, faces challenges in direct user authentication with its segmentation engine.

Table 1. The real-world Zero Trust model implementations mapped to the main pillars of the Zero Trust security model in terms of performance, advantages, and limitations.

Pillars	BeyondCorp	VMWare NSX	SDP	Forrester NGFW/ZTX
Network	Dispelled network segmentation	Micro-segmentation and transport encryption	Network micro-segmentation	Network micro-segmentation
Data	Encryption at rest and in transit	Data protection at rest	Data encryption and authentication	Data classification, encryption at rest and in transit
People	Multi-factor authentication (MFA)	Passwordless and MFA	Multi-factor/step-up authentication	Authentication and access control policies
Workload	Secure apps and Google Cloud network	Secure apps and SDKs	Secure apps and cloud-based resources	Secure sensitive apps and services
Devices	MFA	Device authentication	(MFA)	Device identification and MFA
Visibility and Analytics	Continuous traffic inspection	Log collection, monitoring dashboards	Identity-centric logging, SIEM integration	Security process monitoring
Application Trust	Single Sign-On (SSO)	SSO, any device access	Single-packet authorisation (SPA)	N/A
Advantages	Suitable for cloud-hosted applications	Virtualised Desktop	Cost-effective application integration	Simplified deployment in BYOD
Limitations	Applicability is limited to Google Cloud infrastructure	Costly	High initial setup effort	Direct user authentication challenge with NGFW segmentation engine

2.6. Real-World Applications of Blockchain Technology in Financial Institutions

Blockchain technology has been increasingly adopted in the banking and finance industries, transforming established practices. It has decentralised and streamlined vital institutional functions, including supply chain management, marketing, and finance [8]. Financial institutions globally are increasingly adopting blockchain to transform conventional operations, streamline processes, and offer innovative services. This section explores the real-world uses of blockchain in the finance industry, highlighting innovators and the advantages and challenges of adopting blockchain technology.

Blockchain technology has found significant success in direct financing, bank credit, and supply chain finance, offering transparency and financial data security [63]. Blockchain has become the focus of global attention, presenting unprecedented opportunities and challenges for traditional credit businesses in commercial banks [64].

Among the pioneers, Santander Bank has significantly marked its presence by leveraging blockchain for international payments. In 2018, Santander unveiled the Santander One Pay FX service, utilising Ripple's blockchain technology to facilitate faster, more transparent, and cost-efficient cross-border transactions, setting a benchmark in the industry [65]. Similarly, HSBC's venture into blockchain for trade finance transactions in 2018 stands as a testament to the technology's potential to condense the traditional processing timeline from days to mere hours, thereby enhancing operational efficiency and reducing risks [66].

The application of blockchain extends beyond payments and trade finance. Institutions such as Barclays and Deutsche Bank are exploring blockchain for identity verification and Know-Your-Customer (KYC) processes. These efforts aim to establish a shared, immutable ledger for KYC, potentially reducing redundancy and costs while improving the customer onboarding experience and compliance with regulatory mandates [67,68]. Furthermore, JPMorgan Chase's initiation of the Interbank Information Network (IIN), rebranded as Liink, showcases blockchain's capability to refine interbank communications and settlements. By employing a blockchain-based network, Liink facilitates quicker and more secure payment

validations among participating banks, illustrating the efficiency gains achievable through blockchain adoption [69].

Blockchain technology has extended the traditional functions of banking applications and infrastructure, offering more convenient and efficient financial management. Therefore, the adoption of blockchain technology in the banking and finance industry has brought about significant advancements, offering transparency, security, and efficiency in various financial applications.

Despite the clear benefits, including enhanced security, reduced transaction times, and increased transparency, the journey towards widespread blockchain adoption in finance is not devoid of challenges. Scalability concerns, integration complexities with legacy banking systems, and strict regulatory requirements persist, emphasising the need for continued innovation and regulatory engagement.

2.7. Current Security Models in the Finance Industry

The security infrastructure of the finance industry plays a crucial role in protecting sensitive data and financial assets. Over time, various security models have been developed and implemented to address these challenges. This section discusses the Castle-and-Moat model, Layered Security model, Defence in Depth, Bell–LaPadula model, and Biba Integrity model, each offering unique mechanisms for protecting financial institutions.

2.7.1. Castle-and-Moat Model

The Castle-and-Moat model in the finance industry is a traditional security paradigm that emphasises strong perimeter defence to protect resources within. Similar to how mediaeval castles were safeguarded by surrounding moats, this model aims to create a formidable barrier against external threats. However, it operates under the assumption that once inside the perimeter, entities are trusted, which, in modern cybersecurity landscapes, can be a significant vulnerability.

This model focuses primarily on establishing robust perimeter defences such as firewalls, intrusion detection systems, and boundary routers. The goal is to scrutinise and control incoming and outgoing network traffic, thereby preventing unauthorised access to the institution's internal networks and systems [70].

One of the critical aspects of the Castle-and-Moat model is its emphasis on external threats. It is built on the premise that attacks are likely to originate from outside the organisation. Consequently, considerable resources are allocated to fortifying external defences. While effective against direct external attacks, this model often overlooks the potential for internal threats or breaches that occur due to compromised credentials.

In the context of financial institutions, where the protection of sensitive data and financial assets is crucial, the Castle-and-Moat model has been a longstanding approach. It provides a fundamental level of security by creating a well-defined boundary around the institution's digital assets. However, the increasing sophistication of cyber threats and the rise of insider threats have exposed limitations to this model. The Castle-and-Moat approach is less effective in a landscape where attackers can bypass perimeter defences through social engineering, phishing attacks, or by exploiting insiders. Once inside the perimeter, attackers can move laterally with little resistance, as internal security is often less stringent [71].

2.7.2. Layered Security Model

The Layered Security model, distinct from the Defence-in-Depth strategy, is a specific approach to cybersecurity focusing on implementing multiple layers of protection across different aspects of the IT infrastructure. In the finance industry, the Layered Security model is essential for protecting sensitive data and systems against a range of cyber threats. This model operates on the premise that no single defence measure is sufficient to thwart all types of cyber threats. Instead, security is enhanced by integrating various protective

measures at different layers within the IT environment. The key components of the Layered Security model typically include the following:

- Perimeter Security: This is the outermost layer, involving technologies such as firewalls and intrusion detection systems to monitor and control incoming and outgoing network traffic, acting as a barrier to external threats;
- Network Security: Within the network, measures such as secure VPNs, network segmentation, and intrusion prevention systems are used to safeguard data in transit and to limit the spread of attacks within the network [72];
- Endpoint Security: At the device level, endpoint security solutions like antivirus software, anti-malware programs, and personal firewalls are employed to protect individual devices that access the network;
- Application Security: This layer focuses on protecting software applications from threats. It involves secure coding practices, regular vulnerability scanning, and application firewalls to defend against application-level attacks [73];
- Data Security: The innermost layer focuses on safeguarding the data itself, irrespective of where it is stored or how it is transmitted. This involves encryption, access controls, and data loss prevention strategies to ensure data confidentiality, integrity, and availability;
- Physical security: The outermost layer involves measures such as access control systems, surveillance cameras, and secure facilities, aiming to prevent unauthorised physical access to critical systems and data centres.

In the financial sector, the Layered Security model is particularly effective due to its comprehensive nature. It ensures that if a threat bypasses one layer of security, additional layers are in place to mitigate the risk. This model is crucial for protecting against a variety of threats, ranging from external hacking attempts to internal data leaks. While this model addresses some limitations of the Castle-and-Moat model by implementing multiple defence layers across the IT infrastructure, it is still not inadequate for dynamically responding to the evolving and sophisticated nature of modern cyber threats.

2.7.3. Defence in Depth

The Defence-in-Depth approach is crucial in the finance industry to protect against a wide range of threats. The authors in [74] argue that the legal environment, particularly as constructed by the enforcement activities of regulators, significantly influences the likelihood that organisations will effectively implement self-regulatory commitments, highlighting the importance of legal and regulatory layers in the Defence-in-Depth strategy for financial security. Furthermore, the authors in [75] propose a 16-component model of financial security management, emphasising the systemic nature of financial security. This comprehensive model aligns with the concept of Defence in Depth by incorporating multiple layers of security parameters, including organisational culture, sustainable development, and systemic optimisation, to fortify the financial infrastructure against potential threats.

This model is based on the concept that no single defence mechanism is sufficient against the variety of threats faced in the financial sector. For example, if there was a physical theft, how could information be guarded against a forensic data recovery? Among other concerns are threat delay, rapid notification, and response when attacks and disasters are underway. The key components of the Defence-in-Depth strategy include the following:

- Layered Security Components: Incorporating the elements of the Layered Security model, such as perimeter, network, endpoint, application, and data security;
- Monitoring and Alerting: Continuously surveilling systems to detect and alert suspicious activities, an essential component for early threat detection;
- Emergency Response: Readiness for immediate action during security incidents, ensuring rapid containment and mitigation;
- Authorised Personnel Activity: Managing and monitoring actions of authorised users to prevent insider threats and unauthorised access;

- Disaster Recovery: Developing robust processes to ensure business continuity and data integrity in the event of significant disruptions or disasters;
- Criminal Activity Reporting: Implementing procedures for the reporting and handling of criminal activities essential for legal compliance and threat intelligence;
- Forensic Analysis: Conducting detailed investigations post-breach, including scenarios like physical theft, to understand attack vectors and prevent future incidents.

Although this model offers a more comprehensive defence through a multi-layered strategy, there are still gaps in addressing real-time threats and ensuring seamless integration of various security components.

2.7.4. Bell–LaPadula Model

In the finance sector, the Bell–LaPadula model's principles are particularly relevant. Financial institutions often handle sensitive client data across various levels of confidentiality. The model maintains data confidentiality by categorising both users (subjects) and data files (objects) in a non-discretionary manner [76]. This approach aligns with the industry's need for a robust framework to handle multiple data categorisations securely. Developed by physicists David Elliot Bell and Leonard J. LaPadula, the model is recognised as the first mathematical framework aimed at restricting unauthorised access to confidential information. Its core features include an access matrix for discretionary access control (ds-property), the "simple security" or "no read-up" rule (ss-property), and the "star property" or "no write-down" rule. These properties ensure that a system adheres to strict confidentiality protocols.

The primary benefit of using this security model is that subjects and objects cannot change their security levels after they have been created. Another advantage is that subjects and objects cannot degrade information [77]. Despite its theoretical soundness, the Bell–LaPadula model has seen limited practical implementation, with Honeywell Multics being a notable but ultimately unsuccessful case. The model's primary focus on maintaining confidentiality, without addressing other aspects like access control or covert channels, presents certain challenges. Additionally, the model does not prevent the creation of higher-categorisation objects by any user, posing a risk in environments like finance where data integrity is crucial.

2.7.5. Biba Integrity Model

The Biba model, named after its creator, scientist Kenneth J. Biba, is a critical framework in the realm of information security, particularly focusing on the aspect of integrity. In the finance industry, where the accuracy and consistency of data are paramount, the Biba model's principles are highly relevant. In financial settings, the stringent approach to maintaining the data integrity of the Biba model is crucial. It categorises users (subjects) and data files (objects) without discretion, ensuring that integrity levels are strictly adhered to. This model is a response to the limitations of the Bell–LaPadula model, which primarily addresses data confidentiality but lacks the ability to ensure complete system integrity.

The Biba model operates on fundamental principles distinct from the Bell–LaPadula model. It enforces "no read-down" and "no write-up" policies, meaning higher integrity levels cannot read data from lower integrity levels, and subjects cannot transmit data from lower to higher security environments [77]. This approach is especially pertinent in the finance industry, where the integrity of transactional data and financial records is critical.

Currently, some high-assurance systems in production are utilising a combination of the Biba and Bell–LaPadula models. This synergy creates a robust security framework capable of ensuring both the integrity and confidentiality of data, a requirement increasingly significant in the finance sector's move towards models like Zero Trust [78]. The Biba Model's primary advantages are its simplicity and its compatibility with the Bell–LaPadula model, which forms a comprehensive security framework. However, one significant limitation is its lack of mechanisms for authorisation control and confidentiality provision.

This drawback requires financial institutions to supplement the Biba model with other security measures to achieve a holistic security posture.

2.8. Comparative Analysis of the Current Security Models Used in the Finance Industry

Table 2 compares the existing security models used in the finance industry based on their strengths, weaknesses, and applications in the finance industry. It provides insights into which security model or combination of models best aligns with specific institutional needs, considering factors like the nature of data, threat landscape, and compliance requirements.

Table 2. Comparative analysis of the existing security models used in the finance industry.

Model	Strengths	Weaknesses	Application in Finance
Castle-and-Moat	Simple and effective against basic threats.	Vulnerable to advanced attacks, weak against internal threats and data integrity issues.	Primarily for basic perimeter security at smaller institutions.
Layered Security	More robust than Castle-and-Moat, Wider threat coverage.	Complex to manage, requires ongoing maintenance.	Widely used for protecting critical systems and data.
Defence in Depth	Highly resilient, deters attackers even if they breach one layer.	Requires comprehensive threat analysis, potential for redundancy.	Essential for protecting high-value assets and mitigating complex threats.
Bell–LaPadula (BLP)	Guarantees data confidentiality and integrity, suitable for classified information.	Complex, restrictive for collaboration, not suitable for dynamic environments.	Limited use for handling classified information.
Biba Integrity	Strong data integrity, prevents unauthorised modification.	Complex, limited practical application.	Limited use for specific scenarios requiring high data integrity, often in conjunction with BLP.

Each of these models plays a significant role in the overarching security strategy of financial institutions. The Layered Security and Castle-and-Moat models provide robust perimeter defences, while Defence in Depth offers a more comprehensive, multi-layered approach. The Bell–LaPadula and Biba models, on the other hand, focus on specific aspects of security: confidentiality and integrity, respectively. The effectiveness of these models in the finance industry lies in their strategic implementation and integration into a cohesive security architecture.

3. Banking Application without Zero Trust Security

This section offers a comprehensive overview of a banking application that lacks Zero Trust security measures, highlighting potential vulnerabilities and emphasising the need for incorporating Zero Trust principles to safeguard sensitive financial data.

3.1. Identity and Access Management (IAM)

Prior to the adoption of Zero Trust principles, the IAM framework was founded on traditional security models that emphasise perimeter defence. The process begins with the authentication phase, where bank customers enter their credentials to be verified against the internal user database. If the credentials are confirmed as valid, the system issues session tokens, thereby granting access to the bank application. Should the verification fail, access is consequently denied.

Following authentication, the authorisation phase commences. The policy enforcement point (PEP) handles the customer's access request and sends it to the policy decision point (PDP). The PDP evaluates the request against a set of predefined roles and access control policies managed by the policy administrator. If the request complies with the access control policy, the customer is granted access to protected resources. However, if the request is non-compliant, the customer is denied access to these resources.

This IAM framework operates under the assumption that the network's interior is secure once access is granted, demonstrating a notable lack of continuous validation, as shown in Figure 11. It relies on static Role-Based Access Controls (RBAC), where user roles are fixed and do not dynamically adapt to evolving contexts or security threats. Therefore, it may not be equipped to handle the current digital landscape, highlighting the need for an adaptive approach, such as Zero Trust frameworks.

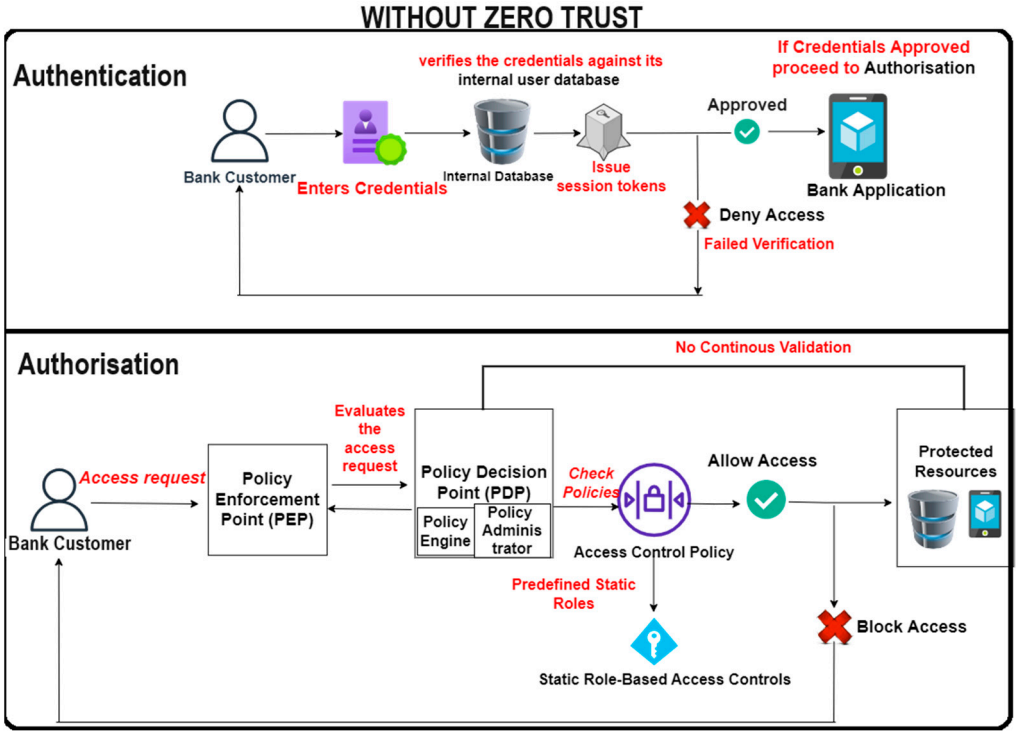

Figure 11. Identity and access management (IAM) without Zero Trust.

3.2. Device and Network Security

The device and network security framework prior to the implementation of Zero Trust principles relied on a perimeter-based defence strategy, as shown in Figure 12. This model is characterised by its emphasis on securing the boundaries of the network rather than focusing on the security within the network itself. In the traditional setup, the DMZ serves as a buffer zone between the untrusted public internet and the internal network. It hosts public-facing servers such as the Web server and the Application server, which are exposed to internet traffic but isolated from the internal network to mitigate risk. Perimeter defences, such as firewalls, are deployed to scrutinise incoming and outgoing traffic. The firewalls operate based on predefined security rules to block or allow data packets, acting as the first line of defence against external threats. Endpoint protection (antivirus) software is also used on devices to protect against malware and other cybersecurity threats.

The IDS complements the firewall by monitoring network traffic for suspicious patterns that may indicate a security breach. It serves as a watchdog, alerting administrators to potential intrusions. The network is segmented according to departmental functions, such as the Finance and Credit Card departments, each with its own bank systems and databases, but it does not have its own end-point protections, internal firewalls, or IDS to monitor for unauthorised data transmissions or infiltration attempts and also to prevent cross-segment breaches.

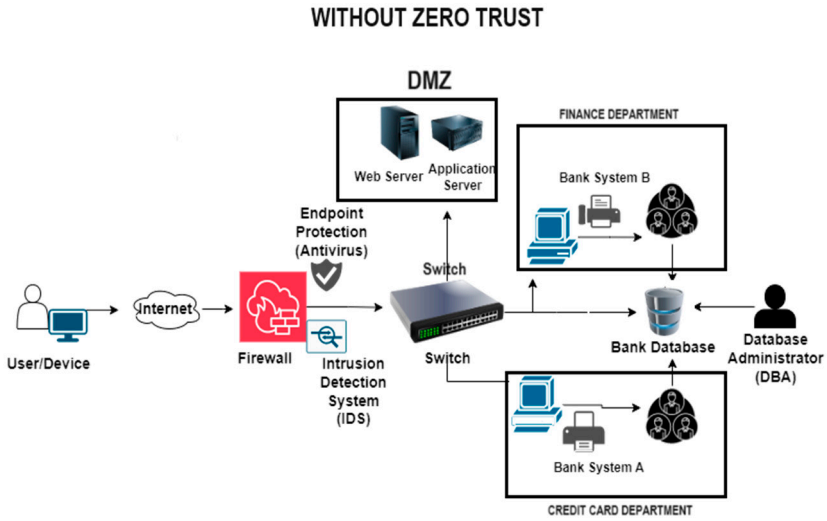

Figure 12. Device and network security without Zero Trust.

Databases, which store sensitive financial information, are secured and managed by database administrators (DBAs). The DBAs are responsible for maintaining the integrity and confidentiality of the data stored within these databases. In this pre-Zero Trust device and network security framework, trust is implicitly granted to users and devices within the network perimeter, which has been identified as a vulnerability. The assumption that the internal network is secure once access is granted through the perimeter defences does not account for the lateral movement of threats that bypass the initial barriers.

The outlined framework serves as a foundation upon which the more dynamic and granular Zero Trust approach is built. The Zero Trust model assumes that threats may exist both outside and inside the network perimeter, leading to a more thorough and continuous verification process for devices and users, regardless of their location relative to the network infrastructure.

3.3. Data Protection

The data protection strategy in place prior to the adoption of Zero Trust principles was built on a foundation of perimeter defence and static security measures. The key components of this strategy involved less centralised key management and a basic level of data loss prevention (DLP). Staff from various departments, such as Accounting and Credit Card, would initiate data transactions by sending files or emails to their managers. This process was not governed by real-time security checks or dynamic policy enforcement. The central server played a vital role in receiving data and conducting basic security checks. However, these checks were relatively simple and not designed to adapt to the constantly evolving threat landscape.

The pre-Zero Trust approach utilised a DLP system to monitor and control data transfer based on static rules. Figure 13 shows how the system worked, with the ability to log activities for compliance and auditing purposes. The key management service was less centralised and largely manual. Encryption applies to only sensitive files without the aid of automated systems to ensure consistency and reduce human error. Managers were responsible for the decryption of only sensitive files using keys. This manual intervention added a layer of security but also introduced potential delays and inefficiencies in the data handling process. The enterprise security manager (ESM) oversaw the security policies and tools. While providing a level of oversight, the ESM in a pre-Zero Trust framework was not equipped with the tools necessary for continuous monitoring or enforcement of adaptive security policies.

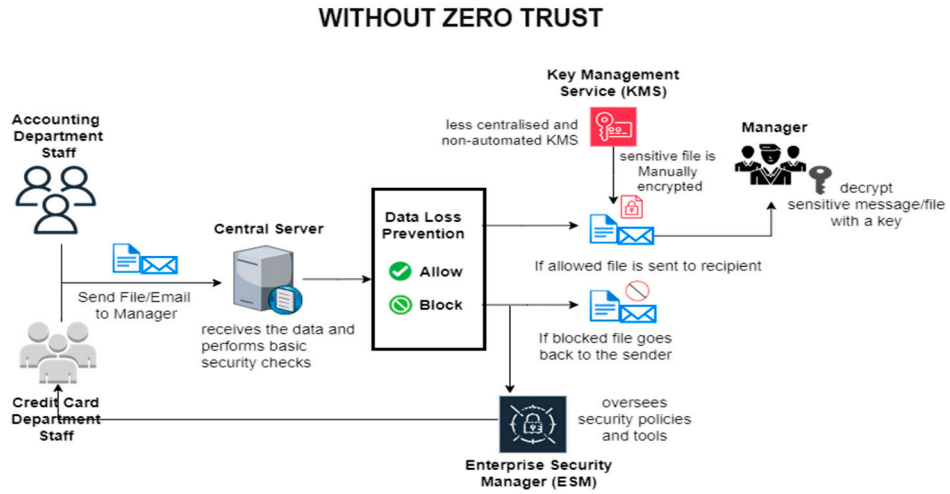

Figure 13. Data protection without Zero Trust.

In summary, the pre-Zero Trust data protection model was characterised by its reliance on fixed roles and static security measures. This model lacked the flexibility to respond to sophisticated cyber threats effectively, as it did not incorporate the granular controls or the principle of least privilege inherent in Zero Trust frameworks. The transition to a Zero Trust model was driven by the need for a more resilient and dynamic approach to data protection capable of countering the threats within an ever-changing cyber environment.

4. Proposed Zero Trust Framework

This section presents a Zero Trust framework for financial institutions, encompassing three key areas: identity and access management (IAM) with blockchain, device and network security, and data protection. This proposed framework is designed to address the limitations inherent in traditional cybersecurity models like Bell–LaPadula and Biba, including Castle-and-Moat, Layered Security, and even Defence-in-Depth approaches, which are commonly employed in the finance industry.

4.1. Security Assumptions

In implementing this framework, several security assumptions are made:

- Continuous Verification: It is assumed that continuous verification of all users and devices within the network can significantly mitigate the risk of internal and external threats associated with unauthorised access, such as phishing attacks. This assumption underlies the application of the Zero Trust model;
- Immutable Record with Ethereum: The framework utilises Ethereum blockchain technology to establish a secure, immutable record for IAM processes. This enhancement is predicated on Ethereum's capability to enforce the integrity of user authentication and authorisation, thereby fortifying the trust layer essential to the Zero Trust model;
- Comprehensive Threat Detection: The framework assumes that the integration of various security components like IDS, firewalls, and DLP tools will effectively detect and mitigate a wide range of cyber threats, including XSS and CSRF attacks;
- Adaptive Security Posture: The framework is based on the assumption that an adaptive security posture, responsive to evolving threats such as brute-force and MiTM attacks, is critical in the dynamic landscape of financial cybersecurity;
- Data Integrity and Confidentiality: The assumption is that through data classification and encryption, the integrity and confidentiality of sensitive data can be maintained effectively, reducing the risk of data breaches and unauthorised access.

4.2. Threat Model

Following the security assumptions, our proposed framework addresses multiple threats that could compromise various components of financial institutions' cybersecurity landscapes. Each threat is analysed for its potential impact.

- Man-in-the-Middle Attack: It could compromise the integrity of data in transit between users and services, particularly affecting the network security component;
- Phishing Attack: It directly targets user authentication processes, jeopardising the IAM component by attempting to steal credentials;
- SQL Injection: It threatens the data protection component by potentially allowing unauthorised access to or manipulation of the database;
- Cross-Site Scripting (XSS): It endangers client-side data and can lead to unauthorised actions, impacting the data protection and network security modules;
- Cross-Site Request Forgery (CSRF): It could manipulate authenticated sessions, affecting transaction processing within IAM;
- Brute-force Attack: It targets the robustness of user authentication, putting the IAM system at risk;
- Insider Threat: It puts at risk all components by potentially bypassing internal security measures due to authorised access.

Our framework includes specific security measures to address each threat, ensuring complete protection across IAM, data protection, and network security.

4.3. Security Implementation/Mitigation Strategies

After identifying potential threats to financial institutions' cybersecurity, our proposed framework implements a robust set of security measures tailored to safeguard critical components and ensure data integrity and confidentiality.

- IAM: We integrate strict access control mechanisms, including role-based access controls and dynamic permissions, to mitigate the risk of unauthorised access and insider threats. Using blockchain technology, which offers an unchangeable and verifiable record of user activity and access patterns, authentication processes are enhanced;
- Device and Network Security: To protect against external breaches and internal vulnerabilities, our framework employs advanced encryption standards, intrusion detection systems, and continuous network monitoring. These measures are designed to detect and prevent man-in-the-middle and brute-force attacks, ensuring secure communication channels and device integrity;
- Data Protection: Sensitive data are protected through end-to-end encryption, both at rest and in transit. SQL injection and XSS threats are mitigated by implementing stringent input validation, parameterised queries, and content security policies. Additionally, regular security audits are conducted to identify and rectify potential vulnerabilities, ensuring the resilience of data protection measures;
- Adaptive Threat Response: The framework is engineered to adapt dynamically to emerging threats. By continuously analysing threat intelligence, the system can apply real-time updates to security configurations, ensuring a state of preparedness against evolving cyber threats.

When a threat is detected, our framework engages a predefined mitigation strategy based on a set of criteria that include the type of threat, its severity, the system's current state, and the potential impact on operations. This decision-making process involves an automated evaluation using threat intelligence and real-time system monitoring to determine the most effective response. For example, if the system saw an attempt to get in without permission, it would tighten access controls and start an immediate audit trail review through the blockchain's immutable records. This would effectively find and stop the threat vector. This protocol ensures a rapid and precise security response, minimising risk exposure and system vulnerability.

Each of these strategies is systematically illustrated in Figures 14–16, which depict the Zero Trust mechanisms across IAM, data protection, and network security, demonstrating the practical application of our security measures.

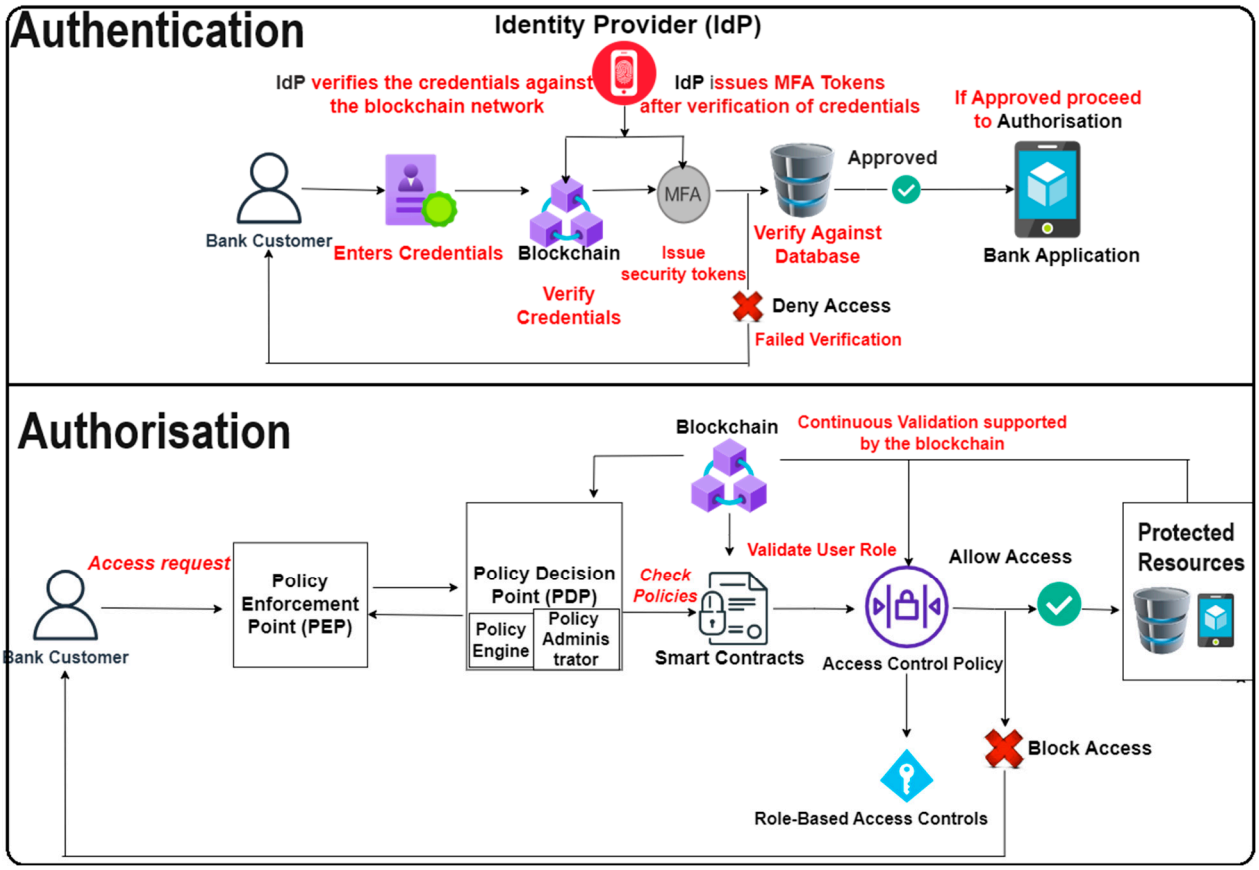

Figure 14. Identity and access management (IAM) with blockchain.

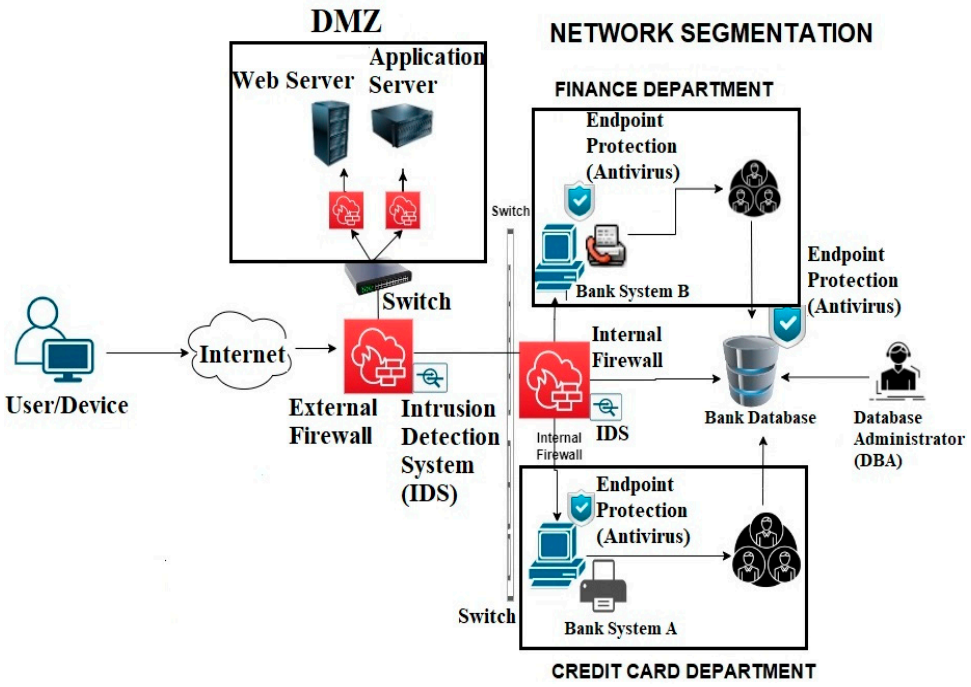

Figure 15. Device and network security.

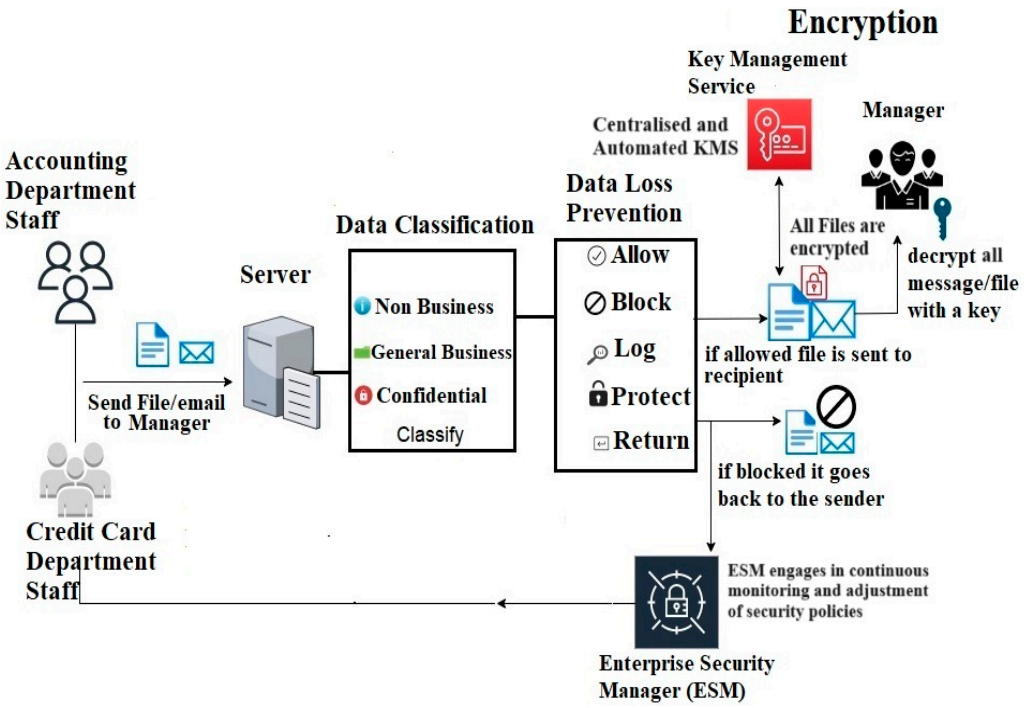

Figure 16. Data protection.

4.4. Identity and Access Management with Blockchain

The IAM component is crucial in ensuring that only authorised users are granted access to an organisation's resources, particularly in financial institutions where sensitive data and transactions are involved. It is important to implement robust authentication and authorisation mechanisms such as Multi-factor authentication (MFA), Role-Based Access Controls (RBACs), and access control policies. Integrating blockchain technology as a trust layer is also essential in maintaining security.

Figure 14 illustrates the proposed IAM process, in which users first enter their credentials, which are then verified by the authentication server or identity provider (IdP), potentially using a blockchain to check the validity of the credentials in a secure and tamper-proof manner. Blockchain's distributed ledger technology ensures that user credentials are not centrally stored, thus mitigating the risk of a single point of failure. Upon successfully verifying the user's credentials, the IdP issues MFA tokens, which may include blockchain-based security tokens that provide cryptographic proof of the user's identity.

The MFA phase ensures an added layer of security by requiring proof of identity that is verifiable via blockchain, making the authentication process more resistant to fraud and unauthorised access. After verifying the MFA token, the system moves to the authorisation phase, where the PEP intercepts the user's request and forwards it to the PDP for evaluation against the defined access control policies. These policies, underpinned by the trust layer, ensure that the rights and credentials exchanged during the process are immutable and verifiable through blockchain records.

The PDP defines access rules for different roles, such as customers and employees, specifying which endpoints these roles can access. For instance, customers may only access their dashboard and transaction history, while employees can manage accounts or generate reports. These policies are encoded as smart contracts within a blockchain platform, ensuring tamper-proof, immutable, and enforceable rules that reflect the organisation's access control structure. The PEP acts as a middleware that checks if a user's role, fetched from the session and verified against the blockchain, permits access to the requested resource. If a role does not have access, it denies the request.

RBAC is applied at this stage, granting customers and employees access to the resources and actions they are authorised to perform based on their assigned roles. These

roles are recorded on the blockchain, ensuring they cannot be altered without consensus, adding an additional layer of security. Finally, the system provides access to the resources and continuously monitors and audits user activities to ensure compliance with security policies and detect potential threats or anomalies. This constant monitoring makes it possible to find and fix security risks in real-time, which makes the financial institution even safer overall.

In conclusion, integrating a trust layer using blockchain technology into the IAM systems aligns with financial regulations and data protection laws, such as the General Data Protection Regulation (GDPR) for data privacy, the Payment Card Industry Data Security Standard (PCI DSS) for transaction security, and other relevant financial industry standards. By using blockchain, the financial institution ensures that access logs are immutable and traceable, which is paramount for audits and regulatory compliance. Furthermore, the decentralised nature of blockchain addresses the concentration risk, where a central repository of sensitive data might present a lucrative target for cyberattacks.

The IAM system integrated with blockchain technology offers a robust and adaptive solution to the challenges identified in the pre-Zero Trust model IAM shown in Figure 11, establishing a forward-thinking security stance that aligns with the evolving demands of the financial sector's cybersecurity needs.

4.5. Device and Network Security

Device and network security are integral to the Zero Trust model, designed to protect against internal and external threats. This is achieved by incorporating various security components such as firewalls, IDS, DMZ, and network segmentation.

Financial institutions are highly susceptible to security threats due to the sensitive data they manage and the value of their transactions. To mitigate such risks, the implementation of robust security measures is essential. For instance, IDS can detect and stop advanced threats that target organisations.

Figure 15 illustrates the proposed device and network security mechanism, in which all user and device traffic is treated as untrusted and verified before accessing any network resources. The framework begins by implementing an external firewall, which regulates incoming and outgoing traffic to allow legitimate traffic while blocking unauthorised traffic. IDS is also deployed to detect and prevent intrusion attempts into the network, providing a reactive security posture to complement the firewall's preventative measures.

Network segmentation is implemented by dividing the network into separate segments based on functionality and security requirements. For instance, the finance department would be cordoned off, possessing its own internal firewalls and IDS to monitor for unauthorised data transmissions or infiltration attempts, while the credit card department would have similar but separate defences to prevent cross-segment breaches. Each segment incorporates endpoint protection to defend against malware and other malicious activities. This layer of security operates at the device level, ensuring that all terminals, whether they are workstations or servers within the segment, maintain integrity against compromise.

A DMZ is created to act as a segregated network buffer, containing and controlling access to public-facing services such as web and application servers. Each server is scrutinised and monitored continuously, ensuring that any communication with these servers, whether entering or leaving, is authenticated and authorised in real time. This isolation from the core internal network is critical, as it limits the exposure of sensitive internal resources to external vulnerabilities and attacks.

The database component is crucial for financial institutions, and its security is maintained through endpoint protection and database administration. Endpoint protection ensures database servers are immune to malware, while DBAs manage access controls, monitor database activity, and enforce policies to defend against unauthorised access or data exfiltration. The vulnerability scanning is conducted using automated scanning tools such as Nessus and OpenVAS. These tools scan the network infrastructure to de-

tect and remediate potential security vulnerabilities, thereby enabling timely remediation before exploitation.

The device and network security component of our proposed Zero Trust framework in Figure 15 represents a strategic shift from the pre-Zero Trust static, perimeter-oriented defences in Figure 12 to dynamic, context-aware, and adaptive security mechanisms. This ensures that the finance industry's network infrastructure remains secure and resilient against cyber threats.

4.6. Data Protection

Data protection is critical to the Zero Trust model, particularly for financial institutions that handle sensitive customer data and financial transactions. Implementing effective data protection measures ensures that sensitive information is secure from potential data breaches and unauthorised access. The framework is designed to address vulnerabilities inherent in the pre-Zero trust data protection strategies shown in Figure 13 by incorporating automated processes and continuous validation.

Figure 16 shows the proposed data protection method, which includes data classification, DLP, encryption, and ESM. The first step in data protection is to classify the data based on its sensitivity level. This can range from non-business data to confidential data, requiring the highest protection level. Non-business data, which are less sensitive, might include everyday internal communications. General business data include operational information that might be sensitive but is not critical. Confidential data, which could include customer financial details, require the highest level of security. Data classification helps organisations identify the types of data they hold and prioritise security measures accordingly.

DLP is a set of technologies and policies that help prevent data from leaving an organisation's network. These tools work by setting rules that can block, log, or allow the transfer of data based on its classification. For example, if an employee tries to send confidential data outside the network, the DLP tool can block the transfer and notify the security team. This not only prevents data breaches but also provides a traceable log for audits and compliance checks.

Encryption is another essential data protection technique used to secure data and information. This protects all data at rest, in transit, and in use, ensuring that it remains confidential even if intercepted or accessed by unauthorised parties. Key management services and managers play a crucial role in the encryption process, helping to ensure that encryption keys are generated, stored, and managed securely. The right encryption and key management can make data almost useless to attackers. The encryption–decryption process is streamlined and automated to minimise errors and reduce the administrative burden.

The ESM is a centralised management platform that provides visibility and control over an organisation's security infrastructure, unlike the static policies of the past. This includes monitoring and managing security events, policies, and configurations; analysing security data; and generating reports. It is like the command centre for data protection, where all the monitoring, management, and analysis happen. The ESM helps financial institutions proactively identify and respond to security threats and vulnerabilities. This ensures that sensitive data remain secure and confidential, reducing the risk of data breaches and ensuring compliance with data protection regulations.

By implementing these data protection measures, the finance industry moves away from the perimeter defence and static security measures in Figure 13 towards a framework where trust levels are continuously evaluated. No entity within or outside the network is inherently trusted, and verification is a constant process. This approach significantly enhances the security posture, ensuring that data protection measures are resilient, responsive, and capable of defending against sophisticated cyber threats in a proactive manner.

By addressing the security assumptions and integrating the key components effectively, the proposed framework offers a robust approach to implementing the Zero Trust model in financial institutions, ensuring a secure and compliant environment for handling sensitive financial data.

5. Implementation and Evaluation

To validate the proposed framework, we developed a prototype bank application using JavaScript (version 1.8.5), HTML5, and CSS3 for the front-end development, Node.js (version 14.17.0) as the runtime environment, and Express.js (version 4.17.1) served as the web application framework, together enabling efficient processing and routing of server-side requests. Data storage and management were handled using MySQL (version 8.0.23), a robust relational database management system that ensures secure and scalable storage of sensitive customer and transaction data. Additionally, the application integrated the AWS KMS for cryptographic key management and the AWS SDK for interfacing with AWS services. Web3.js was used for interactions with the Ethereum blockchain, particularly for smart contract functionalities associated with user authentication. Ethereum-Ganache (v. 2.7.1), part of the Truffle Suite, provided a local blockchain environment for Ethereum development, facilitating the testing and development of smart contract functionalities. Truffle was employed as a comprehensive environment for the development, testing, and deployment of Ethereum smart contracts.

Security measures were a paramount consideration, with the application incorporating client sessions for secure session management, bcrypt (v. 5.0.1) for robust password hashing, Helmet for setting secure HTTP headers, express rate limit for mitigating brute-force attacks, and XSS filters and Bleach for sanitising user inputs to prevent cross-site scripting attacks. The HTTPS module was used to establish a secure server, encrypting data exchanged between the client and the server, thus reinforcing the application's adherence to the Zero Trust model principles.

We then evaluated the bank application's performance against prevalent attacks such as SQL injection, brute-force, CSRF, XSS, and man-in-the-middle attacks, utilising tools like Burp Suite (v. 2023.10), OWASP ZAP (v. 2.14.0), and Wireshark (v. 4.0.2) for comprehensive vulnerability scanning and security testing. Additionally, we assessed the application's transaction processing efficiency and performance, where tools like Ethereum-Ganache v2.7.1 and Apache JMeter v5.6.3 played a crucial role in measuring transaction latency, throughput, and scalability, respectively. Lastly, we conducted a comparative analysis of our framework against established cybersecurity frameworks, ensuring the Zero Trust model's robustness and applicability in safeguarding financial institutions.

5.1. Framework Implementation

5.1.1. Identity and Access Management with Blockchain

Our prototype application enhances security by incorporating blockchain technology into the identity and access management (IAM) processes, which is crucial for financial institutions dealing with sensitive data and information.

At the authentication layer, we leverage the Web3.js library to interface with the Ethereum blockchain set up through Ganache, where our custom smart contract, BankAppAuth, resides. This smart contract is written in Solidity, as shown in Figure 17, and is pivotal in the verification of user credentials and roles, providing a decentralised and tamper-proof ledger that enhances the integrity of the proposed IAM processes.

Upon user login attempts, credentials are sanitised and verified against hashed passwords stored in a MySQL database, utilising the bcrypt library for hash comparison. This not only secures password storage but also anchors our authentication process on a tried-and-tested cryptographic foundation.

Upon successful credential matching, the application transitions to the blockchain layer for additional validation. The smart contract's authenticateUser function is called, passing a hash of the user's password for verification against the blockchain-recorded hash. This double-layer verification fortifies the security posture by ensuring that the user's credentials are valid both within our database and on the blockchain.

```
Define contract BankAppAuth

Define structure User with properties:
  username (string)
  passwordHash (bytes32)
  role (string)
  isRegistered (boolean)

Define a mapping 'users' mapping address to User

Define events:
  UserRegistered with parameters (userAddress, username, role)
  UserAuthenticated with parameter (userAddress)

Define function registerUser with parameters (_userAddress, _username, _passwordHash, _role)
  Check if user is already registered
  Create new User and add to 'users' mapping
  Emit UserRegistered event

Define function authenticateUser with parameters (_userAddress, _passwordHash)
  Check if user is registered and password hash matches
  Emit UserAuthenticated event
  Return true

Define function getUserRole with parameter (_userAddress)
  Check if user is registered
  Return user's role

End contract
```

Figure 17. Pseudocode for the smart contract written in Solidity.

Simultaneously, MFA further solidifies the authentication process. A custom generateMfaCode function creates a 6-digit random code. This code is then sent to the user's phone number for additional verification, as shown in Figure 18, effectively strengthening the authentication process. This step is crucial for safeguarding access, as it ties the user's identity to a physical device, significantly reducing the likelihood of unauthorised access.

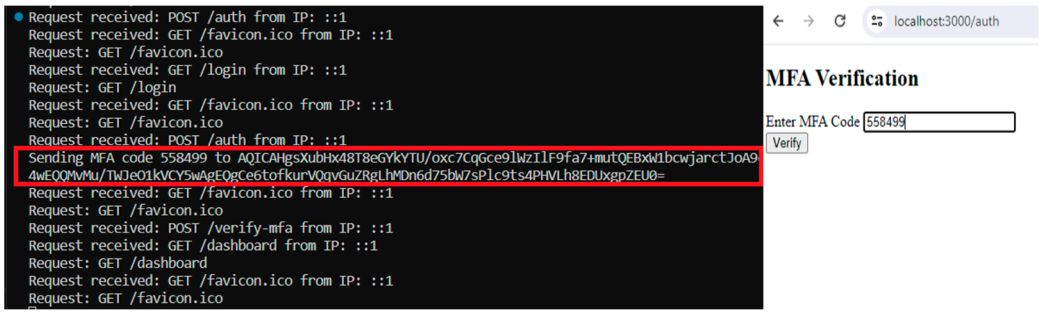

Figure 18. Confirmed MFA after successful login by user, which shows encrypted phone number.

Following authentication, the authorisation phase commences, guided by RBAC protocols. A middleware function, policyEnforcementPoint, was implemented to serve as the PEP in the application, as shown in Figure 19. This function retrieves the username from the session and the requested resource from the request path. It then queries the database to find the roles associated with the username. Once the roles are fetched, the policyDecisionPoint function is called with these roles and the requested resource as arguments. If the policyDecisionPoint function returns true, the middleware allows the request to proceed by calling next (). If it returns false, access is denied, and a '403 Access Denied' response is sent to the user.

This middleware is used in the application routes to enforce access control. By applying this middleware, each request is checked against the defined RBAC policies before granting access to any protected resource. RBAC is implemented through a combination of the PDP and PEP functions. The RBAC logic is encapsulated within the policyDecisionPoint function, where roles are mapped to permitted resources. This mechanism ensures that users can only access the parts of the application that their roles permit, adhering to the principle of least privilege.

```
Define function policyDecisionPoint with parameters (userRoles, requestedResource)
  Define accessRules as a constant with rules:
    'Customer' can access ['/customer/dashboard', '/balance', '/transactions']
    'Employee' can access ['/employee/dashboard', '/manage', '/reports']

  Return true if any of the userRoles is allowed to access requestedResource as per accessRules
end function

Define function policyEnforcementPoint as middleware with parameters (req, res, next)
  Retrieve username from req.session.username
  Define requestedResource as req.path
```

Figure 19. Pseudocode for the policyEnforcementPoint and policyDecisionPoint functions.

User activities are continuously monitored and logged, which aligns with the Zero Trust model's requirement for dynamic and real-time security measures. These logs are essential for compliance and provide an audit trail that is crucial for detecting potential threats. By integrating blockchain as a trust layer within our IAM system, we ensure that access logs are immutable, roles are verified, and user authentication is strengthened, as shown in Figure 20. This integration not only enhances security but also aligns with financial regulations and data protection laws, such as GDPR and PCI DSS. The decentralised nature of blockchain addresses concentration risk and presents a robust approach to preventing unauthorised access and cyberattacks.

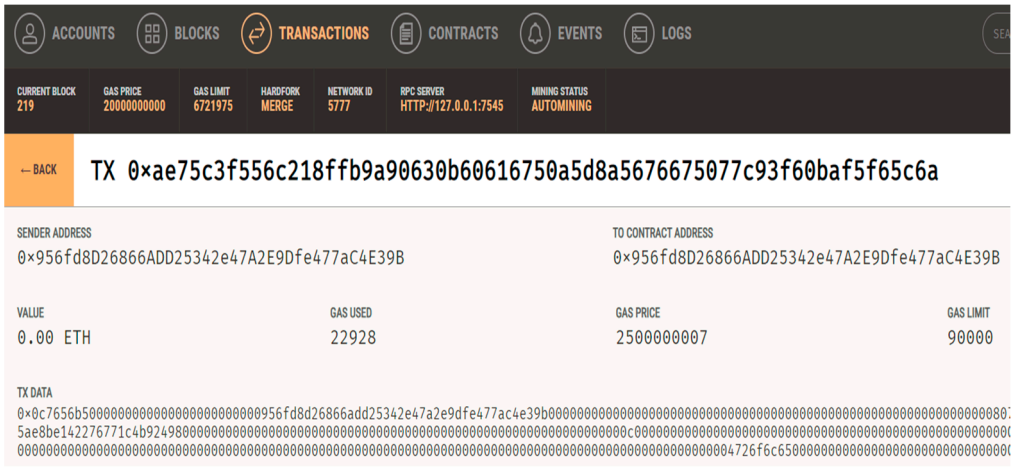

Figure 20. Blockchain transaction verification in Ganache.

5.1.2. Device and Network Security

In our prototype bank application, we have meticulously implemented robust device and network security measures, which are foundational to the Zero Trust model. This comprehensive approach was achieved using an array of technologies and tools, each tailored to address specific aspects of cyber threats and safeguard the application.

Secure communication between the client and the server was ensured using HTTPS, utilising TLS encryption to secure data in transit. SSL certificates are used to establish a secure connection, protecting against data interception and man-in-the-middle attacks. To combat brute-force attacks, we integrated rate-limiting using the express-rate-limit package. This middleware effectively limits the number of requests from a single IP address within a 15 min window, providing a strong defence against rapid, automated attack attempts. The implementation of a content security policy (CSP) further enhances our security posture. Utilising the Helmet library, we established a policy that restricts the sources from which scripts, styles, and fonts can be loaded. This CSP is crucial in reducing the risk of cross-site scripting (XSS) attacks, ensuring that only scripts from trusted sources are executed within the application.

Our proposed IDS plays a significant role in identifying and mitigating potential security threats. Custom middleware in Express.js, guided by threatDetectionRules, monitors for patterns in network requests indicative of security threats, such as repeated attempts from the same IP or access to sensitive URLs, as shown in Figure 21. Upon detecting such patterns, the IDS effectively blocks these requests, reinforcing the security of our application, as shown in Figure 22.

```
Define function threatDetectionRules with parameter (req)
  Define suspiciousPatterns as ['/dashboard', '/login']
  Define nonSuspiciousIps as ['127.0.0.1', '::1']
  Return true if req.url contains any pattern in suspiciousPatterns and req.ip is not in nonSuspiciousIps
End function

Define function ipRangeCheck with parameters (ipAddress, range)
  Return true if ipAddress is within the specified range
End function

Use middleware for app
  If threatDetectionRules(req) returns true
    Log warning about suspicious request
    Respond with status 403 and message 'Access Denied'
  Else
    Call next middleware
End middleware
```

Figure 21. Pseudocode for detecting potentially suspicious web requests based on URL patterns and IP addresses.

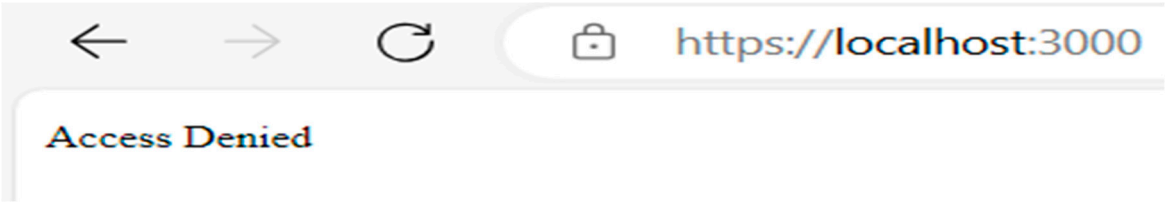

Figure 22. Access denied message due to the IDS middleware and the threatDetectionRules.

For user activity logging, a middleware function, logUserActivity, captures and logs each user activity, including usernames, request methods, URLs, and timestamps. These logs are stored in the MySQL database and are vital for tracking user actions, auditing, and analysing security incidents.

Network traffic monitoring is conducted through middleware functions that log each request's details, such as the HTTP method and URL, as shown in Figure 23. This monitoring is essential for understanding the app's security posture and identifying potential suspicious activities. As shown in Figure 23, additional middleware analyses requests for suspicious activity, taking decisive actions like logging or blocking these requests to prevent potential security breaches.

Device authentication middleware was implemented to verify the identity and integrity of connecting devices. The deviceAuthenticationMiddleware function ensures that only authenticated devices are granted access to the application, as shown in Figure 23. It validates the 'user-agent' header of incoming requests, allowing access solely to devices that pass these authentication checks.

Network segmentation was enforced through a custom function called isRequestFromAllowedSegment. This function checks if a request originates from an IP address within approved network segments, such as '192.168.1.0/24' or '192.168.2.0/24'. Requests from outside these segments are denied access, ensuring that only authorised network segments can communicate with the application.

```
Define middleware deviceAuthenticationMiddleware with parameters (req, res, next)
  Call function performDeviceAuthentication with req.headers['user-agent']
  If device is authorized
    Proceed to next middleware
  Else
    Respond with status 401 and message 'Device authentication failed'
End middleware

Define a protected route '/api/protected'
  Use deviceAuthenticationMiddleware
  On successful authentication, respond with status 200 and message 'Access granted to protected resource'
End route definition

Define network traffic monitoring middleware
  Log the request method and url
  Proceed to next middleware
End middleware

Define middleware for monitoring suspicious network activity
  If request is suspicious
    Log the suspicious request details
    Respond with status 403 and message 'Forbidden'
  Else
    Proceed to next middleware
End middleware
```

Figure 23. Pseudocode for middleware functions for device authentication, network traffic logging, and monitoring of suspicious network activities in the bank application.

Through the integration of these security components, our application adheres to the Zero Trust principle of "never trust, always verify". Each security measure, from rate-limiting to secure transmission, contributes to a comprehensive defence strategy, ensuring that the network infrastructure is resilient against the array of cyber threats faced by financial institutions.

5.1.3. Data Protection

Data protection is an important aspect of the implementation of Zero Trust in our prototype bank application. We have adopted a multifaceted approach to secure sensitive customer data, employing various technologies and applying rigorous methodologies at every stage of data handling.

Firstly, data classification is handled by the classifyData function, as shown in Figure 24. This function categorises data into 'Confidential', 'Internal', or 'Public' based on its content. This classification is critical for applying the appropriate protection levels and is utilised throughout the data handling process to ensure each data type receives the necessary security measures.

To prevent unauthorised data exfiltration, data loss prevention mechanisms were implemented by the isDataLossPreventionEnabled and isDataExfiltrationDetected functions. The app incorporated data loss prevention rules and checks to detect and respond to potential data breaches or unauthorised data access. When data are received through a POST request to the "/api/data" endpoint, the data loss prevention mechanism applies data loss prevention rules to verify if the data exfiltration is detected, as shown in Figure 24. If the data pass the checks and are deemed secure, they are saved to the database.

Encryption is a critical step following classification and DLP checks. Encryption techniques were employed using cryptographic algorithms and keys. We utilised the "encryptData" and "decryptData" functions, leveraging the cryptographic capabilities of the "crypto" module in Node.js. These functions, as shown in Figure 25, securely transformed the data into an unreadable format and ensured its confidentiality. The encrypted data are then stored in the database to maintain its confidentiality.

```
Define function classifyData with parameter (data)
  If data contains 'confidential'
    Return 'Confidential'
  Else if data contains 'internal'
    Return 'Internal'
  Else
    Return 'Public'
End function

Define route '/api/data' for POST requests
  Retrieve data from request body
  Retrieve username from session or default to 'Guest'
  Classify data using classifyData function
  Log data access with data submission details
  If Data Loss Prevention is enabled and no data exfiltration is detected
    Encrypt the data
    Save encrypted data to database
    Respond with status 200 and message 'Data saved successfully'
  Else
    Respond with status 403 and message 'Data loss prevention triggered'
End route definition
```

Figure 24. Pseudocode showing the function for classifying data based on its content and a route that uses this classification to implement DLP measures.

```
Function encryptData with parameter (data)
  Read public key from file "MyCertificate.crt"
  Encrypt data using the public key
  Return encrypted data in Base64 format
End Function

Function decryptData with parameter (encryptedData)
  Read private key from file "MyKey.key"
  Decrypt encrypted data using the private key
  Return decrypted data in UTF-8 format
End Function
```

Figure 25. Pseudocode showing public and private key encryption and decryption functions.

ESM functionalities are reflected in our approach to data access event logging. Each data submission is recorded with detailed information such as a timestamp, the user's action, the data classification, and a preview of the data. This practice enables the monitoring and analysis of data access patterns and is instrumental in detecting and responding to security incidents.

Moreover, the logDataAccess function embodies a broader security monitoring strategy where every data transaction is logged for auditability. These logs create a trail essential for compliance purposes and post-incident investigations, ensuring transparency and accountability in all data interactions within the application.

In summary, our banking application's data protection measures represent a comprehensive approach encompassing data classification, loss prevention, encryption, and enterprise-level security management. These measures are seamlessly integrated into the application's workflows, ensuring that sensitive data are classified, protected from unauthorised access or exfiltration, encrypted for security, and continuously monitored for compliance and auditing purposes.

5.2. Evaluation Methodology and Results

5.2.1. Evaluation Methodology

The evaluation of the proposed Zero Trust framework and its implementation in a prototype banking application was methodically structured to ensure comprehensive testing. The environment setup replicated a typical banking application infrastructure with simulated user interaction points, such as login, registration, and transaction interfaces, as shown in Figure 26. This simulated environment was hosted on a local server, mirroring the operational settings of an online banking platform.

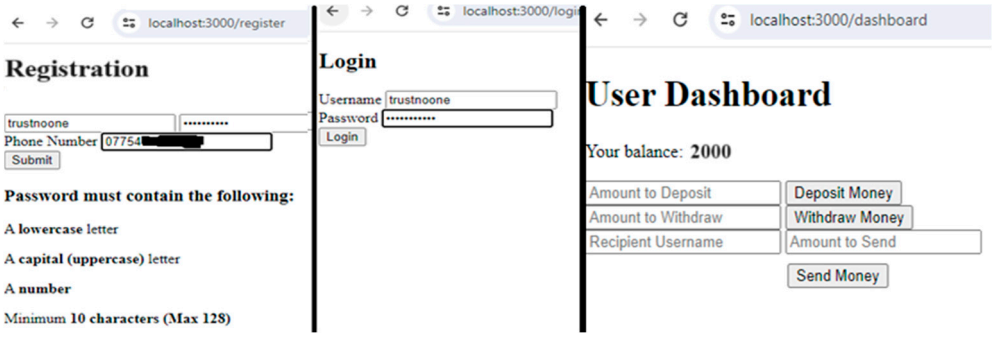

Figure 26. Proof of concept registration, login, and user dashboard pages of the prototype application.

5.2.2. Tools and Techniques

- Burp Suite v10.3.7: This integrated platform was selected for its ability to perform security testing of applications. It provided a range of functionalities, from initial mapping to analysis of the application's attack surface, including the identification of security loopholes;
- OWASP ZAP v2.14.0: As an open-source web application security scanner, OWASP ZAP was instrumental in performing both manual and automated scans to quickly identify a wide range of vulnerabilities, from surface-level issues to deep-rooted security flaws;
- Wireshark v4.0.05.: Network packets were captured and analysed using Wireshark to ensure that the application's data transmissions were encrypted and conformed to expected security protocols;
- Ganache v2.7.1: A pivotal tool in simulating Ethereum blockchain environments, which allowed us to monitor and measure transaction latency and gas usage. Ganache provided a controlled setting to assess the time complexity of blockchain operations, contributing to our comprehensive evaluation of system performance under various load scenarios;
- Apache JMeter v5.6.3: A versatile tool used to perform load testing and measure the performance of the application, including throughput and latency. JMeter was pivotal in simulating user traffic to evaluate how the application scales and maintains responsiveness under varied loads.

5.2.3. Vulnerability Scanning Processes

- Automated Scanning: We employed Burp Suite's scanner for a thorough analysis, initially crawling the application for content and functionality, followed by an in-depth audit for vulnerabilities. We specifically chose a lightweight scan mode to balance thoroughness with efficiency. The scan was launched from a pre-determined URL to ensure targeted coverage. Throughout the scanning process, we closely monitored the application's responses to various test scenarios, analysing them for indications of security issues;
- Manual Scanning: Using OWASP ZAP, we conducted targeted tests to probe for vulnerabilities that automated scanners might overlook, particularly those that exploit the business logic or require complex, multi-step processes to uncover.

5.2.4. Security and Performance Testing Processes

A. Security Testing Processes

In our comprehensive security testing process, we performed a series of targeted tests, each focusing on specific aspects of the application's security infrastructure, to ensure that it can withstand the potential threats mentioned in our threat model in Section 4.2. Our methodology not only tested the application's defences against common vulnerabilities but also validated the effectiveness of the integrated security measures in a real-world scenario. In total, we conducted the following detailed tests:

- SQL Injection: Deliberate attempts were made using Burp Suites's intruder tool to inject a series of malicious SQL queries into the application's input fields to assess the effectiveness of input sanitisation. The queries tested ranged from simple authentication bypasses like ' OR '1'='1 to more complex injections aimed at unauthorised data manipulation, such as ' OR '1'='1' --, and potentially destructive commands intended to test data integrity, including '; DROP TABLE users; --. These tests were critical for identifying and mitigating risks associated with improper data handling and potential security breaches;
- Brute-Force Attacks: An in-depth brute-force attack test was conducted on the demo bank application to evaluate the strength of its authentication system, especially given the presence of MFA. Using Burp Suite's Intruder tool, we initiated a series of automated password submissions against the application's login form. The process began with capturing a legitimate login request, which was then replicated with varying passwords, cycling through a list of commonly used passwords and algorithmically generated permutations;
- Cross-Site Request Forgery (CSRF): Our CSRF testing methodology was rigorously designed to assess the resilience of our application against CSRF attacks, a critical aspect of application security. Firstly, we identified a request within the application that could be susceptible to CSRF attacks. Next, we used Burp Suite to generate a proof of concept (PoC) for CSRF. We crafted a request that would allow unauthorised actions to be performed on behalf of a logged-in user if the application was vulnerable. The generated PoC was modified to alter the MFA value, which was then tested in various browser environments under different user sessions. Each test was meticulously monitored, with a particular focus on how the application processed and responded to the modified requests;
- Cross-Site Scripting (XSS): The application was tested for vulnerabilities that would allow the injection and execution of malicious scripts in the user's browser, potentially leading to unauthorised access to user sessions or personal data. The process entailed a series of carefully planned steps, leveraging the capabilities of Burp Suite.

We initiated the process by systematically capturing HTTP requests within the application, pinpointing areas where user inputs were accepted and later rendered by the browser. Targeted fields were identified for potential vulnerability exploitation. Using Burp Suite's Repeater functionality, we meticulously injected various XSS payloads. Each payload was crafted to test the application's response to different types of script injections, ranging from simple alert dialogues to more complex script executions. The application's responses to these injections were closely monitored. Notably, we paid attention to how the application processed and displayed these inputs in subsequent HTTP responses.

- Man-in-the-Middle Attack Testing: To assess the prototype banking application's resilience against man-in-the-middle attacks, we conducted a thorough network traffic analysis using Wireshark. This involved capturing and analysing data packets transmitted between the client and server during typical user interactions with the application. The primary focus was on identifying any instances of unencrypted or poorly encrypted data transmissions. This testing was critical to verify the application's adherence to the Zero Trust model, ensuring that all data in transit were

securely encrypted, thus preventing potential interception and unauthorised access by middle entities.

B. Performance Testing Processes

Our performance testing approach was multifaceted, comprising the evaluation of latency, throughput, and scalability in the prototype application. Initially, we focused on transaction latency. Using Ganache, we were able to simulate the Ethereum blockchain environment and measure the average gas used per transaction, which provided us with insights into the time complexity of operations. This analysis is critical to understanding the efficiency of our security measures and their impact on the application's performance. The average transaction time was monitored to ensure that the security processes did not adversely affect the system's responsiveness.

To extend our analysis, we incorporated Apache JMeter, which allowed us to simulate varying user loads to measure throughput and general system latency. We methodically configured Thread Groups in JMeter, determining the number of users, ramp-up period, and loop count to mimic realistic usage scenarios, as shown in Figure 27. This setup enabled us to observe the system's behaviour under different stress levels and analyse its capability to handle increasing transactions.

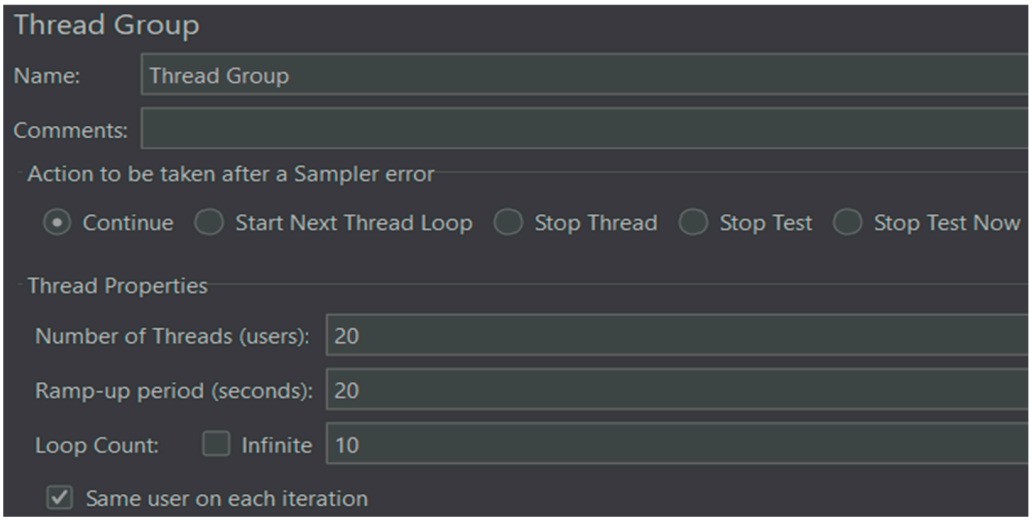

Figure 27. Thread Group in JMeter.

Additionally, we conducted a scalability analysis. By plotting scalability curves using the data from JMeter, we visualised the relationship between the number of threads, throughput, and latency. This analysis was vital in assessing the system's ability to maintain performance levels as user loads increased.

This testing process ensured a robust evaluation of the application's efficiency, security, and scalability within a blockchain-integrated environment, which is crucial for its deployment in financial institutions.

5.3. Results

The results of our comprehensive evaluation are crucial in assessing the effectiveness of the Zero Trust model within the prototype banking application.

5.3.1. Vulnerability Scans Findings

Our vulnerability scans, conducted using Burp Suite and OWASP ZAP, yielded no detectable vulnerabilities, as shown in Figures 28 and 29. This outcome is significant as it suggests that the fundamental aspects of the prototype, such as input validation, session management, and security configurations, are well secured against common web application vulnerabilities. The absence of detected vulnerabilities is particularly telling of

the application's strong IAM framework, effective data protection measures, and resilient network security protocols. The entire process, from the initial setup to the final analysis, was thoroughly documented.

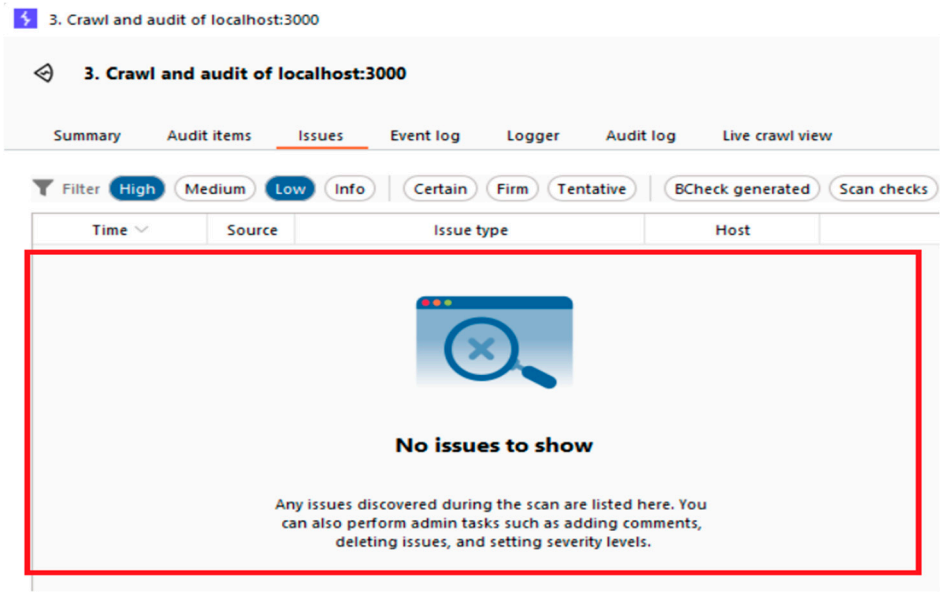

Figure 28. Automated vulnerability scanning results from Burp Suite show no vulnerability.

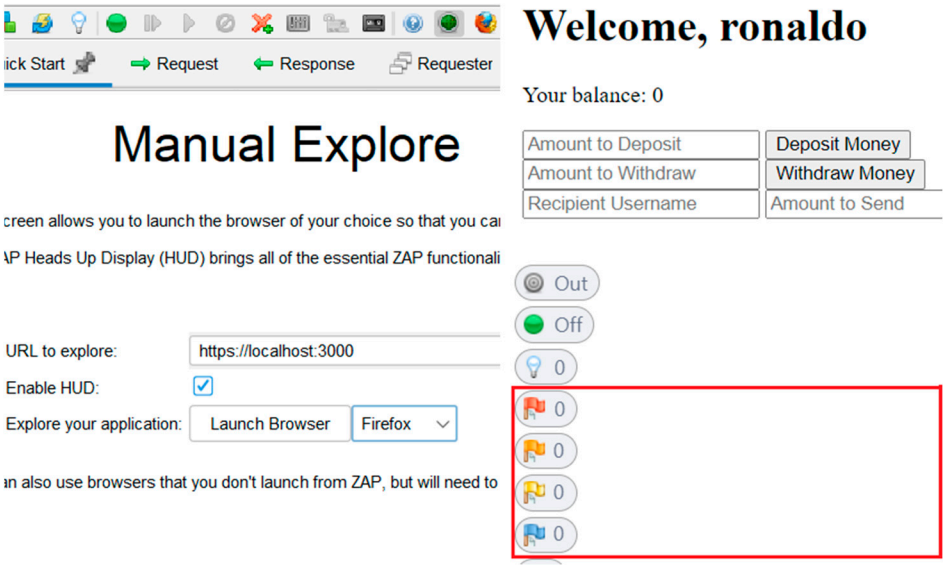

Figure 29. Manual vulnerability scanning results from OWASP ZAP show no vulnerability.

5.3.2. Security Testing Results

The security testing performed through both manual and automated means demonstrated the prototype bank app's resilience to various attacks. For SQL injection, prepared statements and parameterised queries thwarted our attempts to manipulate database queries. Notably, the server issued '403 Forbidden' and '429 Too Many Requests' HTTP status codes in reaction to the test SQL injections, as shown in Figure 30. These responses are indicative of the application's defensive mechanisms effectively recognising and mitigating potentially malicious requests. The '429' responses shown in Figure 31, in particular, suggest a rate-limiting control designed to prevent brute-force attacks, further demonstrating the robustness of the application's security posture.

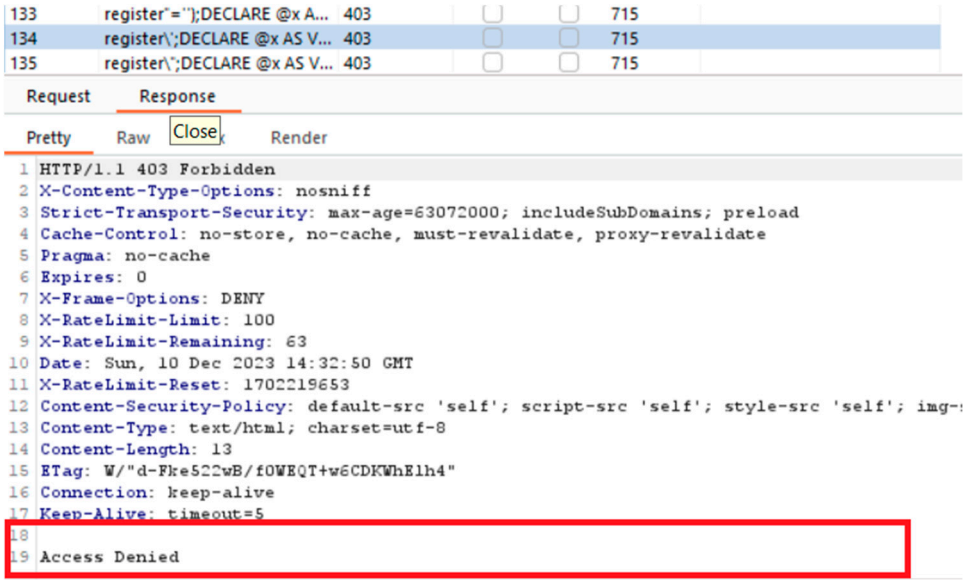

Figure 30. Forbidden response to SQL injection attempt showing access denial.

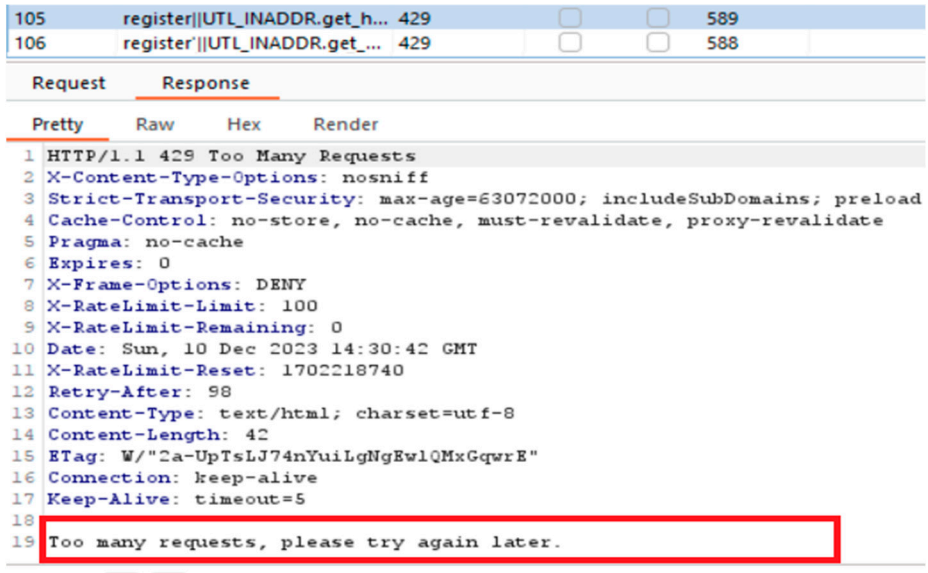

Figure 31. Rate-limiting response to SQL injection attack showing too many request messages.

Brute-force attacks were mitigated by account lockout mechanisms and robust password complexity requirements. The application initially responded with HTTP 200 OK status codes for all the login attempts, alongside a standard "Wrong Username or Password" message, as shown in Figure 32. A few minutes into the brute-force attack, the application began to return HTTP 429 Too Many Requests status codes, indicative of a rate-limiting mechanism responding to the high frequency of login attempts. After the temporary period during which the 429 status code was issued, the application resumed returning 200 OK status codes, which suggests that the rate-limiting mechanism was designed to temporarily halt the attack before allowing attempts again.

Figure 32. Response to repeated login attempts during a brute-force attack showing wrong username or password message.

In our CSRF attacks, instead of typical vulnerability exploits, the application steadfastly displayed messages of "invalid or expired MFA code" upon each test request, as shown in Figure 33. This consistent outcome showcases not only the application's rigorous check against CSRF attacks but also its effectiveness in proactively invalidating any unauthorised or altered requests that could compromise user sessions or data integrity.

Figure 33. CSRF test result indicating invalid or expired MFA code.

The application's response to stored XSS attempts was equally robust. Despite various payloads being injected, not a single one resulted in script execution. The browser's responses were scrutinised, and only legitimate user data were displayed, as shown in Figure 34, illustrating the strength of the input sanitisation and output encoding practices employed by the application. This demonstrates a solid defensive posture against XSS attacks, ensuring the preservation of the integrity and confidentiality of user data.

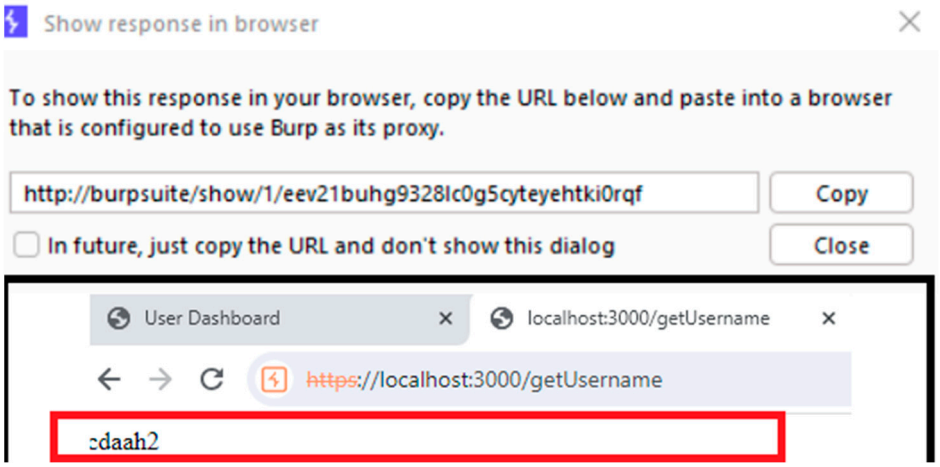

Figure 34. Non-execution of injected scripts during stored XSS test displaying only legitimate user data.

Wireshark played a vital role in our man-in-the-middle attack security testing process. Through meticulous analysis of data transmission, it was confirmed that all client–server traffic was securely encrypted using TLS v1.3, as shown in Figure 35. This level of encryption is crucial for ensuring that data in transit, including sensitive authentication tokens, financial transactions, and personal customer information, remain confidential and integral. The effective use of cryptographic protocols in our application is a testament to its resilience against potential interception or deciphering by unauthorised entities.

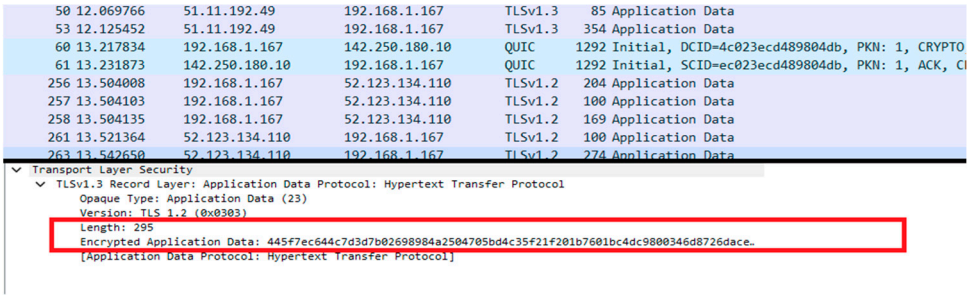

Figure 35. Wireshark encryption verification for MITM attack resilience.

5.3.3. Performance Testing Results

Our performance testing focused on a multifaceted analysis of the system's capabilities, including transaction latency, throughput and latency, and scalability.

A. Transaction Latency

During our performance testing, particular attention was given to the system's performance in terms of transaction latency, which is crucial for maintaining a seamless user experience in a secure banking environment. Our testing, conducted using the Ganache platform, also provided valuable data on the transaction processing time and associated costs.

The latency was measured by the time taken for a transaction to be processed and included in a block, which was recorded at an average of 40 s. This metric is crucial for real-time applications and reflects the responsiveness of the Zero Trust model implementation on a blockchain network. Specifically, transactions consumed an average of approximately 22,844 gas units, as shown in Figure 36, reflecting a balance between computational thoroughness and time efficiency. The associated gas price, set at 20 Gwei (0.00000002 ETH), and the absence of ETH value transfer for these specific transactions ensure that operation costs are maintained at a minimal level, reflecting a cost-efficient design.

Figure 36. Transaction gas usage overview.

B. Throughput and General system latency

The system's throughput and latency were examined closely under simulated conditions using Apache JMeter. Throughput demonstrated a positive correlation with increased load, rising from 3.7 transactions per second (tps) at 20 threads to 4.4 tps at 100 threads, with the average throughput shown as a dashed line in Figure 37 Latency, denoted as the average response time, was consistently low at 2 milliseconds up to 60 threads before a moderate increase to 3 milliseconds, as observed at 80 and 100 threads, as depicted in Figure 38. This balance between throughput and latency underlines the system's capability to handle increased transaction volumes while maintaining responsiveness.

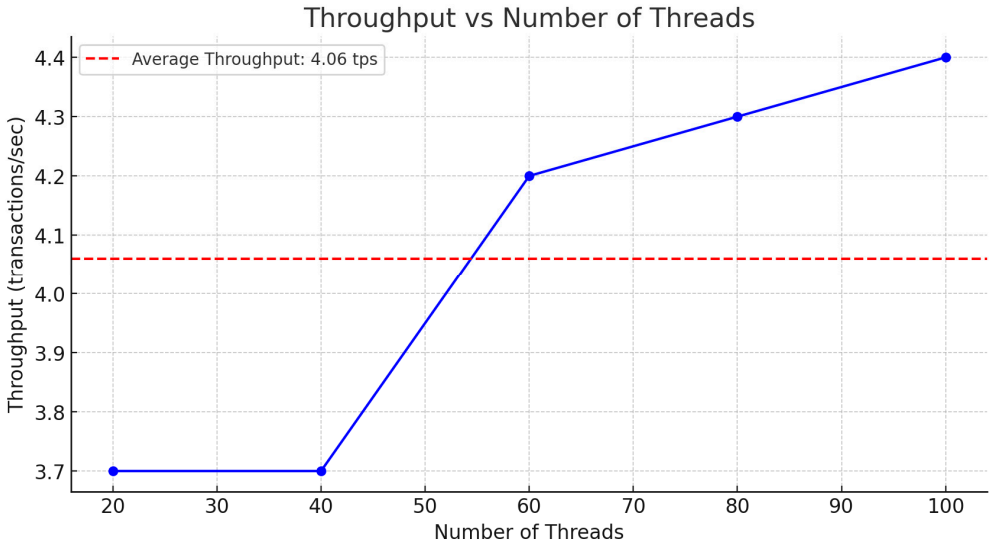

Figure 37. Average throughput. The blue line in the graph represents the actual throughput (transactions per second) as a function of the number of threads. It shows how the throughput changes when the number of threads increases.

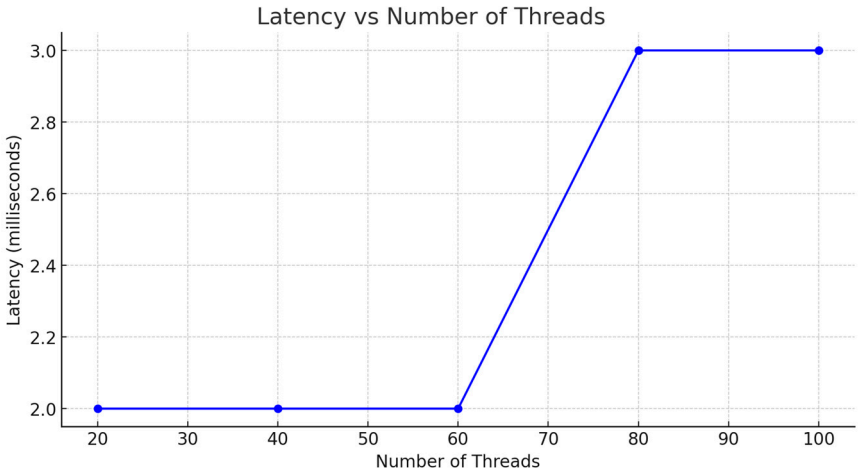

Figure 38. Average latency.

C. Scalability

The scalability analysis, conducted using JMeter data, revealed that while the system maintains a consistent response time for up to 60 users, a slight increase in latency was observed at higher user counts (80 and 100 threads). These data were visualised in the scalability curve in Figure 39, illustrating the relationship between the number of threads, throughput, and latency. The curve reflects a system effective at scaling, with a steady increase in throughput and a marginal rise in latency at elevated thread counts, indicating a resilient framework capable of handling increased demand while maintaining service quality.

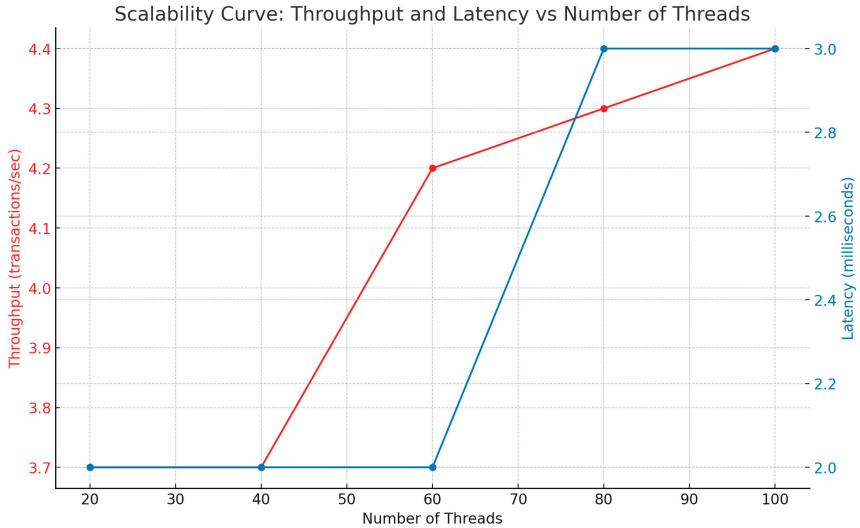

Figure 39. Scalability curve.

These preliminary findings provide insight into the operational efficiency of the system under test conditions. However, it is imperative to note that comprehensive performance evaluation, particularly in terms of time complexity, latency, and throughput under varied network loads, will be conducted as part of future work. This will involve simulations in a real network environment to further validate the robustness and scalability of the implemented framework.

5.4. Discussion

This section discusses the results of the evaluation within the context of the established threat model, examining the effectiveness of the Zero Trust model and blockchain implementation in mitigating the risks identified during security testing. The comprehensive testing procedure, carefully designed to probe for weaknesses highlighted by our threat model, revealed no substantive vulnerabilities. We were able to successfully defend against sophisticated external attacks such as SQL injection, man-in-the-middle attacks, and brute-force attempts, which were identified as high-probability events. The system's response to SQL injection attempts with '403 Forbidden' and '429 Too Many Requests' HTTP status codes reflects the model's proactive defensive mechanisms. The mitigation of brute-force attacks through account lockout mechanisms and password complexity requirements aligns with the Zero Trust approach of stringent access controls. The consistent application of rate-limiting in response to potential brute-force attacks underlines the robustness of the IAM system. It demonstrates the application's effectiveness in safeguarding user credentials and preventing unauthorised access.

The security testing against man-in-the-middle attacks further validates the model's efficacy. The use of Wireshark confirmed that all data transmissions, including sensitive exchanges, were securely encrypted using TLS v1.3. This encryption ensures data integrity and confidentiality, aligning with the Zero Trust model's commitment to secure communication channels.

The effective handling of CSRF attacks demonstrates robust measures in user session and authentication management, a cornerstone of IAM, and underscores the application's strengths in data protection and network security. By successfully mitigating the CSRF attacks, the application ensures the integrity and confidentiality of user transactions and interactions, safeguarding against unauthorised actions.

The failure of XSS attack attempts further confirms the model's robustness. The lack of payload execution suggests robust input validation and encoding mechanisms within the application. These findings are particularly relevant to the IAM component of our proposed model, demonstrating an effective barrier against common XSS exploits. By preventing stored XSS attacks, the application mitigates the risk of client-side attacks that could compromise user sessions or propagate across the network.

This demonstrates that our framework is capable of protecting critical data against external threats and preserving its integrity. Similarly, internal threats, including potential insider attacks and privilege exploitation, were contemplated within the model. The robust access control and monitoring measures integral to our Zero Trust approach were confirmed to be effectively operational, as evidenced by the failure of these attacks during our testing. The absence of unauthorised lateral movements within the system or any indication of internal data breaches during the security tests further validates the threat model's predictive accuracy and the effectiveness of the implemented security controls.

Moreover, blockchain technology's role in IAM provided an additional layer of security. The immutable nature of blockchain complemented the Zero Trust model's continuous verification requirement, ensuring that the verification processes were not just rigorous but also transparent and tamper-proof. This integration was pivotal in reinforcing the IAM component, as it was subjected to and withstood various simulated attacks as part of our evaluation process.

Our framework has demonstrated not only robust security measures but also impressive operational efficiency, validated by thorough performance testing. Latency measurements have shown that the system maintains swift transaction processing times even as the load increases, a critical factor for maintaining an optimal user experience in financial services. At the same time, the throughput performance scales admirably with increased loads, which is evidence of the system's capacity to handle a high volume of transactions. The scalability analysis, as reflected in the scalability curve in Figure 39, further underscores the framework's ability to efficiently manage growing transaction loads without a corresponding compromise in performance. These findings validate the model's efficacy in

providing secure yet efficient transactional environments. Alongside the robust defences against various cyber threats, the system's performance metrics further affirm its real-world applicability, ensuring that enhanced security does not come at the expense of performance.

In conclusion, the defence measures, as per the threat model's guidance, have been proven effective. This confirms the model's alignment with real-world cyber threats and demonstrates the practical application and effectiveness of the security controls deployed in the prototype. The defence measures are thus proven to be comprehensive, leaving no avenue for threat actors to compromise the system's critical assets.

5.5. Comparative Analysis

This section presents a detailed comparison of the proposed Zero Trust model framework, integrated with blockchain, against established cybersecurity frameworks used in the finance industry, as shown in Table 3. Our proposed framework demonstrates a strong alignment with Zero Trust principles, particularly through continuous verification and least privilege access control. It stands out with its strong blockchain integration, which significantly enhances security and data integrity.

Table 3. Comparative analysis of cybersecurity frameworks in the financial industry against the proposed framework.

Criteria	ISO/IEC 27001	NIST CSF	PCI DSS	CIS Controls	Proposed Framework
Alignment with Zero Trust Principles	Moderate	Moderate	Limited (focuses on cardholder data)	Good (focuses on critical controls)	Strong, with a focus on continuous verification and trust assessment
Blockchain Integration	Limited	Limited	Limited	Limited	High, leveraging blockchain for enhanced security and data integrity
Compliance and Regulatory Adherence	Strong (e.g., GDPR, HIPAA)	Moderate (flexible compliance approach)	Very high (mandatory for card payments)	Moderate (supports specific compliance)	Moderate (adaptable to various standards)
Scope and Coverage	Broad security foundation	Prioritised security controls	Data security for the payments industry	Mitigating common cyber threats	Broadly, addressing multiple aspects of cybersecurity in finance
Implementation Complexity	High (requires expertise)	Moderate	Moderate	Low (actionable controls)	Moderate (due to advanced technology integration)
Adaptability to Evolving Threats	Moderate (adaptable through risk assessments)	High (encourages continuous improvement)	Low (specific but focused scope)	High (prioritises rapid implementation)	High (responsive to new challenges and technological advancements)
Performance Efficiency	High (structured processes for efficiency)	Moderate (flexible customisation for optimisation)	Moderate (prescriptive requirements ensure adequate cardholder data protection)	High (prioritised controls deliver high impact with lower resource burden)	High (designed for minimal latency, scalability, and quick response times)
Data Protection	Strong focus on data security with controls for encryption, access control, and incident response.	Moderate (flexible approach allows for customisation of data protection controls based on needs)	Moderate (primarily focused on cardholder data security, but can be adapted for broader data protection)	Strong (includes controls for data encryption, access control, and data loss prevention)	Strong (implements data encryption, least privilege access, and real-time monitoring to prevent unauthorised access)
Anti-Money Laundering (AML)	Moderate (it can be adapted to meet AML requirements through risk assessments, transaction monitoring, and suspicious activity reporting)	Moderate (includes controls for customer identification, transaction monitoring, and suspicious activity reporting)	Not directly applicable to AML but can support compliance through data security controls	Moderate (includes controls for customer identification, transaction monitoring, and suspicious activity reporting)	High (incorporates blockchain to ensure traceability and transparency of transactions, enhancing behaviour analysis and anomaly detection for AML compliance)

Table 3. *Cont.*

Criteria	ISO/IEC 27001	NIST CSF	PCI DSS	CIS Controls	Proposed Framework
Know Your Customer (KYC)	Moderate (it can support KYC compliance through customer identification and verification controls)	High (flexible approach allows for customisation of KYC processes based on risk)	Not directly applicable to KYC but can support compliance through data security controls	Moderate (includes controls for customer identification and verification)	High (employs blockchain for immutable audit trails in identity verification, enhancing KYC accuracy and reliability)
Secure Transactions	Strong (it supports secure transactions with encryption, access control, and intrusion detection controls)	High (it can be adapted to secure transactions through various controls based on needs)	Very high (requires strong authentication and secure communication protocols for cardholder data transactions)	High (includes controls for secure communication protocols, transaction integrity, and fraud prevention)	Very high (utilises blockchain for immutable transaction records and employs strict encryption and access controls for maximum security)

The framework's adaptability to various compliance and regulatory standards is considerable, supporting a dynamic response to regulatory changes. The scope and coverage of the framework are broad, addressing multiple aspects of cybersecurity in finance with an emphasis on performance efficiency. Designed for minimal latency, it ensures scalability and quick response times, which are essential for real-time financial transactions. The implementation complexity remains moderate, taking into account the sophisticated technology integration, yet the framework is highly adaptable to evolving threats, owing to its responsive design to new challenges and technological advancements. In terms of data protection, it implements strong encryption and access control measures reinforced by blockchain's capabilities for secure, auditable data management.

Blockchain strengthens the framework's AML provisions by ensuring transaction traceability and enhancing behavioural analysis for compliance. KYC processes are strengthened by blockchain's immutable audit trails, thereby enhancing accuracy and reliability. Furthermore, the framework provides very high security for transactions, utilising blockchain for immutable records and strong encryption, showcasing its robust defence against fraud. This comprehensive analysis underlines the proposed framework's advantages in operational efficiency, economic benefits, and adherence to security standards, making it a strategic cybersecurity solution for the financial industry.

6. Conclusions and Future Work

This paper presents research that highlights significant advancements in cybersecurity within financial institutions using the proposed Zero Trust model framework integrated with blockchain technology. This innovative approach, which includes the development and comprehensive testing of a prototype banking application, is a crucial step towards safeguarding financial data against various cyber threats. The framework's primary strengths lie in its ability to provide continuous verification, decentralised authentication, and immutable data integrity, which establish a robust defence mechanism against both internal and external security breaches. Additionally, it shows operational excellence by maintaining high throughput, low latency, and scalability, which are crucial for financial services' real-time operations. Its successful implementation and security evaluation outcomes pave the way for further research and development, potentially leading to more secure and resilient financial systems in the face of evolving cyber threats.

The practical implications of this research extend to enhancing the security posture of financial institutions by mitigating risks associated with cyber threats, thereby fostering a secure environment for conducting transactions and managing data. The integration of blockchain technology with the Zero Trust model provides a comprehensive approach to identity verification, data protection, and transaction security, offering financial institutions a pathway to not only comply with strict regulatory requirements but also to gain a competitive advantage through improved trust and customer satisfaction.

The research makes significant theoretical contributions to the field of cybersecurity through the integration of blockchain technology and the Zero Trust model. This integration not only enhances security mechanisms but also introduces a novel approach to financial institutions' transaction security, data integrity, and identity and access management. This work represents a significant shift in cybersecurity strategies for the financial sector by demonstrating the practical application of blockchain to strengthen Zero Trust architectures while providing insights into the scalability, adaptability, and effectiveness of such integrated frameworks in combating cyber threats. Furthermore, it lays the foundation for future research into the convergence of these technologies, indicating a significant shift in cybersecurity strategies for the financial sector.

Moving forward, the research highlights multiple pathways for future work to enhance and expand the capabilities and applicability of the framework. It is crucial to come up with strategies that enable smooth integration of this framework with existing financial IT infrastructures, ensuring that the transition is efficient. Further studies could also examine the scalability of the framework in real-world settings, evaluating its performance and security in large-scale deployments. Additionally, incorporating more advanced machine learning algorithms for better threat prediction and real-time response systems could greatly improve the framework's usefulness. Another critical area for future exploration is the application of this framework beyond the financial sector, particularly in industries that manage sensitive information and face similar cybersecurity challenges. Additionally, it is important to adapt and improve the cybersecurity framework to keep up with evolving threats and leverage new technologies. Adhering to global cybersecurity regulations is crucial for legal compliance and maintaining stakeholder trust.

Author Contributions: C.D.: Conceptualization, Methodology, Prototype Development, Security Validation, and Writing—Original Draft Preparation. A.Q.: Methodology, Writing—Review and Editing, and Supervision. I.A.: Methodology, Writing—Review and Editing, and Supervision. S.K.: Methodology, Writing—Review and Editing, and Supervision. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The complete implementation codes and screenshots will be made available on GitHub [79] upon publication.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Garg, P. Cybersecurity breaches and cash holdings: Spillover effect. *Financ. Manag.* **2019**, *49*, 503–519. [CrossRef]
2. Blank, B.; Hadley, B.; Unsal, O. Financial consequences of reputational damage: Evidence from government economic incentives. *Financ. Rev.* **2021**, *56*, 693–719. [CrossRef]
3. Kindervag, J. *Build Security into Your Network's DNA: The Zero Trust Network Architecture*; Forrester Research: Cambridge, MA, USA, 2010.
4. Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S. *Zero Trust Architecture. NIST Special Publication (SP) 800-207*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020.
5. Liu, Y.; Hao, X.; Ren, W.; Xiong, R.; Zhu, T.; Choo, K.; Min, G. A blockchain-based decentralized, fair and authenticated information sharing scheme in zero trust internet-of-things. *IEEE Trans. Comput.* **2023**, *72*, 501–512. [CrossRef]
6. Wang, J.; Xiong, N.; Alfarraj, O.; Tolba, A.; Ren, Y. S-bds: An effective blockchain-based data storage scheme in zero-trust IoT. *ACM Trans. Internet Technol.* **2023**, *23*, 1–23. [CrossRef]
7. Sultana, M.; Hossain, A.; Laila, F.; Taher, K.; Islam, M.N. Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology. *BMC Med. Inform. Decis. Mak.* **2020**, *20*, 256. [CrossRef]
8. Ahluwalia, S.; Mahto, R.V.; Guerrero, M. Blockchain Technology and Startup Financing: A Transaction Cost Economics Perspective. *Technol. Forecast. Soc. Chang.* **2020**, *151*, 119854. [CrossRef]
9. Rijanto, A. Blockchain Technology Adoption in Supply Chain Finance. *J. Theor. Appl. Electron. Commer. Res.* **2021**, *16*, 3078–3098. [CrossRef]
10. Osmani, M.; El-Haddadeh, R.; Hindi, N.; Janssen, M.; Weerakkody, V. Blockchain for Next Generation Services in Banking and Finance: Cost, Benefit, Risk, and Opportunity Analysis. *J. Enterp. Inf. Manag.* **2020**, *34*, 884–899. [CrossRef]

11. Sethaput, V.; Innet, S. Blockchain Application for Central Bank Digital Currencies (CBDC). *Cluster Comput.* **2023**, *26*, 2183–2197. [CrossRef]
12. Chaudhry, U.B.; Hydros, A.K.M. Zero-Trust-Based Security Model against Data Breaches in the Banking Sector: A Blockchain Consensus Algorithm. *IET Blockchain* **2023**, *3*, 98–115. [CrossRef]
13. Othman, A.H.A.; Alshami, M.; Abdullah, A. The linear and non-linear interactions between blockchain technology index and the stock market indices: A case study of the uae banking sector. *J. Financ. Econ. Policy* **2022**, *14*, 745–761. [CrossRef]
14. Li, J.; Li, S.; Zhang, Y.; Tang, X. Evolutionary Game Analysis of Rent Seeking in Inventory Financing Based on Blockchain Technology. *Manag. Decis. Econ.* **2023**, *44*, 4278–4294. [CrossRef]
15. Shore, M.; Zeadally, S.; Keshariya, A. Zero trust: The what, how, why, and when. *Computer* **2021**, *54*, 26–35. [CrossRef]
16. Tyler, D.; Viana, T. Trust no one? A framework for assisting healthcare organizations in transitioning to a zero-trust network architecture. *Appl. Sci.* **2021**, *11*, 7499. [CrossRef]
17. Campbell, M. Beyond zero trust: Trust is a vulnerability. *Computer* **2020**, *53*, 110–113. [CrossRef]
18. Taylor, P.R. Unveiling Zero Trust Pillars: Constructing an Impregnable Cyber Defense within Today's Threat Landscape. Medium. 28 August 2023. Available online: https://medium.com/@patricertaylorusa/unveiling-zero-trust-pillars-constructing-an-impregnable-cyber-defense-within-todays-threat-ee4dba074bd9 (accessed on 4 January 2024).
19. Chen, B.; Qiao, S.; Zhao, J.; Liu, D.; Shi, X.; Lyu, M.; Chen, H.; Lu, H.; Zhai, Y. A security awareness and protection system for 5G smart healthcare based on zero-trust architecture. *IEEE Internet Things J.* **2020**, *8*, 10248–10263. [CrossRef]
20. D'Silva, D.; Ambawade, D.D. Building a zero trust architecture using Kubernetes. In Proceedings of the 2021 6th International Conference for Convergence in Technology (I2CT), Mumbai, India, 2–4 April 2021; pp. 1–9.
21. Papakonstantinou, N.; Van Bossuyt, D.L.; Linnosmaa, J.; Hale, B.; O'Halloran, B. A zero trust hybrid security and safety risk analysis method. *J. Comput. Inf. Sci. Eng.* **2021**, *21*, 050907. [CrossRef]
22. Microsoft Security. Zero Trust Model—Modern Security Architecture. Available online: https://www.microsoft.com/en-us/security/business/zero-trust (accessed on 4 January 2024).
23. Buchak, G.; Matvos, G.; Piskorski, T.; Seru, A. Fintech, regulatory arbitrage, and the rise of shadow banks. *J. Financ. Econ.* **2018**, *130*, 453–483. [CrossRef]
24. Meng, X. Risk assessment and analysis in supply chain finance based on blockchain technology. *J. Sensors* **2022**, *2022*, 1985803. [CrossRef]
25. Jakovljević, N. Analysis of cyber threats as a risk factor in the banking sector. *Bankarstvo* **2022**, *51*, 32–65. [CrossRef]
26. Khan, A.; Mubarik, M.S.; Naghavi, N. What matters for financial inclusions? Evidence from emerging economy. *Int. J. Financ. Econ.* **2021**, *28*, 821–838. [CrossRef]
27. Nakato, R.; Kituyi, M.G.; Kaggwa, F. Establishing the influences of cardinal virtues on employees' cyber security ethical behavior in the banking sector in Uganda. *Eur. J. Technol.* **2022**, *6*, 1–13. [CrossRef]
28. Alade, O.; Amusan, E.A.; Adedeji, O.T.; Adebayo, S. Cybercrime and underground attack technologies: Perspectives from the Nigerian banking sector. In Proceedings of the 27th iSTEAMS Multidisciplinary & Inter-Tertiary Research Conference, Accra, Ghana, 1–2 June 2021.
29. Boitan, I.A. Cyber security challenges through the lens of the financial industry. In Proceedings of the 2nd International Conference on Advanced Research in Management, Business and Finance, Milan, Italy, 30 October–1 November 2019.
30. Boasiako, K.A.; Keefe, M.O. Data breaches and corporate liquidity management. *Eur. Financ. Manag.* **2020**, *27*, 528–551. [CrossRef]
31. Moreira, F.; Filho, D.; Nze, G.; Sousa, R.; Nunes, R. Evaluating the performance of NIST's framework cybersecurity controls through a constructivist multicriteria methodology. *IEEE Access* **2021**, *9*, 129605–129618. [CrossRef]
32. Sulistyowati, D.; Handayani, F.; Suryanto, Y. Comparative analysis and design of cybersecurity maturity assessment methodology using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. *JOIV Int. J. Inform. Vis.* **2020**, *4*, 225. [CrossRef]
33. Malatji, M.; Solms, S. Cybersecurity capabilities for critical infrastructure resilience. *Inf. Comput. Secur.* **2021**, *30*, 255–279. [CrossRef]
34. Scholl, M.; Suloway, T. Introduction to Cybersecurity for Commercial Satellite Operations. 2022. Available online: https://csrc.nist.gov/pubs/ir/8270/final (accessed on 22 February 2024).
35. Cippollone, F. Defining a Security Strategy—WHY. Secjuice. 24 December 2018. Available online: https://www.secjuice.com/defining-a-security-strategy-part-1-why/ (accessed on 4 January 2024).
36. Stine, K.; Quinn, S.; Ivy, N.; Feldman, L.; Witte, G.A.; Gardner, R.H. *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management (ERM)*; NIST: Gaithersburg, MD, USA, 2021.
37. Fleming, C.; Reith, M.; Henry, W. Securing commercial satellites for military operations: A cybersecurity supply chain framework. In Proceedings of the International Conference on Cyber Warfare and Security, Towson, ML, USA, 9–10 March 2023; Volume 18, pp. 85–92.
38. Lallie, H.S.; Debattista, K.; Bal, J. A review of attack graph and attack tree visual syntax in cybersecurity. *Comput. Sci. Rev.* **2020**, *35*, 100219. [CrossRef]
39. Ahmadu, B.; Hussin, A.R.C.; Bahari, M. Identification of key predicting factors affecting classified information assurance in institutions of higher learning. *Int. J. Acad. Res. Bus. Soc. Sci.* **2022**, *12*, 1–11. [CrossRef] [PubMed]

40. International Organization for Standardization. ISO/IEC 27001:2022, Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements. Available online: https://www.iso.org/standard/27001 (accessed on 22 February 2024).
41. Fenz, S.; Plieschnegger, S.; Hobel, H. Mapping information security standard ISO 27002 to an ontological structure. *Inf. Comput. Secur.* **2016**, *24*, 452–473. [CrossRef]
42. Topa, I.; Karyda, M. From theory to practice: Guidelines for enhancing information security management. *Inf. Comput. Secur.* **2019**, *27*, 326–342. [CrossRef]
43. Kurii, Y.; Opirskyy, I. ISO 27001: Analysis of changes and compliance features of the new version of the standard. *Cybersec. Educ. Sci. Tech.* **2023**, *3*, 46–55. [CrossRef]
44. Fenz, S.; Neubauer, T. Ontology-based information security compliance determination and control selection on the example of ISO 27002. *Inf. Comput. Secur.* **2018**, *26*, 551–567. [CrossRef]
45. Ribas, C.; Burattini, M.; Massad, E.; Yamamoto, J. Information security management system—A case study in a Brazilian healthcare organization. In Proceedings of the International Conference on Health Informatics, Jakarta, Indonesia, 20–21 October 2012.
46. Beckers, K.; Heisel, M.; Solhaug, B.; Stølen, K. ISMS-Coras: A structured method for establishing an ISO 27001 compliant information security management system. In *Engineering Secure Future Internet Services and Systems*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 315–344.
47. Elluri, L.; Nagar, A.; Joshi, K. An integrated knowledge graph to automate GDPR and PCI DSS compliance. In Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 10–13 December 2018.
48. Robinson, P. Can PCI DSS 4.0 reverse the decline in compliance? *Comput. Fraud Secur.* **2022**, *2022*, 6. [CrossRef]
49. QRC Solutionz. PCI DSS Compliance and Certification. Available online: https://www.qrcsolutionz.com/certification/pci-dss (accessed on 4 January 2024).
50. Süzen, A.; Duman, B. Blockchain-based secure credit card storage system for e-commerce. *Sakarya Univ. J. Comput. Inf. Sci.* **2021**, *4*, 204–215. [CrossRef]
51. Taherdoost, H. Understanding cybersecurity frameworks and information security standards—A review and comprehensive overview. *Electronics* **2022**, *11*, 2181. [CrossRef]
52. Rahaman, S.; Wang, G.; Yao, D. Security Certification in Payment Card Industry: Testbeds, Measurements, and Recommendations. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, London, UK, 11–15 November 2019; pp. 481–498.
53. Lessa, L.; Gebrehawariat, D. Effectiveness of banking card security in the Ethiopian financial sector: PCI-DSS security standard as a lens. *Int. J. Ind. Eng. Oper. Manag.* **2023**, *5*, 135–147. [CrossRef]
54. He, Y.; Huang, D.; Chen, L.; Ni, Y.; Ma, X. A survey on zero trust architecture: Challenges and future trends. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 6476274. [CrossRef]
55. Collier, Z.; Sarkis, J. The zero trust supply chain: Managing supply chain risk in the absence of trust. *Int. J. Prod. Res.* **2021**, *59*, 3430–3445. [CrossRef]
56. BeyondCorp. A New Approach to Enterprise Security. Available online: https://www.beyondcorp.com/ (accessed on 4 January 2024).
57. Piya, K.; Au, Q.; Shrestha, S.; Singh, A.; Khan Mohd, T. IoT in Health Care Industry: A Promising Prospect. In Proceedings of the 2021 IEEE UEMCON, New York, NY, USA, 1–4 December 2021; pp. 466–474.
58. Vang, T.; Lind, M.L. Factors Influencing Cloud Computing Adoption in a Zero-Trust Environment. Preprint Version 1. Research Square, 2023. Available online: https://www.researchsquare.com/article/rs-3152878/v1 (accessed on 4 January 2024).
59. Moubayed, A.; Refaey, A.; Shami, A. Software-defined perimeter (SDP): State of the art secure solution for modern networks. *IEEE Netw.* **2019**, *33*, 226–233. [CrossRef]
60. ProcureAdvisor. The Definitive Guide to Software-Defined Perimeter. Available online: https://procureadvisor.com/the-definitive-guide-to-software-defined-perimeter/ (accessed on 4 January 2024).
61. VMware. 4 VMware NSX Webcasts for the Curious Network and Security Professional. Available online: https://blogs.vmware.com/vmtn/2020/02/4-vmware-nsx-webcasts-for-the-curious-network-and-security-professional.html (accessed on 4 January 2024).
62. Alsaedi, A.; Moustafa, N.; Tari, Z.; Mahmood, A.; Anwar, A. Ton_iot telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems. *IEEE Access* **2020**, *8*, 165130–165150. [CrossRef]
63. Hua, S.; Yu-dong, Y.; Tao, Z. Application of Blockchain in Enterprise Financing: Literature Review and Knowledge Framework. *Nankai Bus. Rev. Int.* **2023**, *14*, 373–399.
64. Wang, R. Blockchain and Bank Lending Behavior: A Theoretical Analysis. *SAGE Open* **2023**, *13*, 215824402311645. [CrossRef]
65. Browne, R. Santander Launches a Blockchain-Based Foreign Exchange Service That Uses Ripple's Technology. CNBC. 2018. Available online: https://www.cnbc.com/2018/04/12/santander-launches-blockchain-based-foreign-exchange-using-ripple-tech.html (accessed on 14 February 2024).
66. Browne, R. HSBC Says It's Made the World's First Trade Finance Transaction Using Blockchain. CNBC. 2018. Available online: https://www.cnbc.com/2018/05/14/hsbc-makes-worlds-first-trade-finance-transaction-using-blockchain.html (accessed on 14 February 2024).

67. Deutsche Bank. Deutsche Bank Partners with IBM for Blockchain-Based Shared KYC Platform. 2017. Available online: https://www.db.com/news/detail/20171117-deutsche-bank-partners-with-ibm-for-block-chain-based-shared-kyc-platform?language_id=1 (accessed on 14 February 2024).
68. Puleston Jones, S. Blockchain and Barclays: A Structured Approach. FIA Market Voice. 2017. Available online: https://www.fia.org/marketvoice/articles/blockchain-and-barclays-structured-approach (accessed on 14 February 2024).
69. Finextra. JPMorgan Builds on Blockchain-Based Payment Network. Finextra. 28 October 2020. Available online: https://www.finextra.com/newsarticle/36836/jpmorgan-builds-on-blockchain-based-payment-network (accessed on 14 February 2024).
70. Cheswick, W.R.; Bellovin, S.M.; Rubin, A.D. *Firewalls and Internet Security: Repelling the Wily Hacker*; Addison-Wesley Professional: Boston, MA, USA, 2003.
71. Amoroso, E.G. *Cyber Attacks: Protecting National Infrastructure*; Elsevier: Amsterdam, The Netherlands, 2012.
72. Scarfone, K.; Mell, P. *Guide to Intrusion Detection and Prevention Systems (IDPS)*; NIST Special Publication 800-94; NIST: Gaithersburg, MD, USA, 2007.
73. Howard, M.; LeBlanc, D. *Writing Secure Code*; Microsoft Press: Redmond, WA, USA, 2003.
74. Short, J.L.; Toffel, M.W. Making self-regulation more than merely symbolic: The critical role of the legal environment. *Adm. Sci. Q.* **2010**, *55*, 361–396. [CrossRef]
75. Nosan, N.; Nazarenko, S. Financial security management in economic security systems at different levels of management systems: Methodological problems. *Financ. Credit Act. Probl. Theory Pract.* **2022**, *6*, 138–146.
76. Suresh, V. Introduction to Classic Security Models. Available online: https://www.geeksforgeeks.org/introduction-to-classic-security-models/ (accessed on 4 January 2023).
77. Justiniano, I. Security Models: Integrity, Confidentiality and Protection of the Data. Available online: https://www.linkedin.com/pulse/security-models-integrity-confidentiality-protection-data-justiniano (accessed on 28 December 2023).
78. Toapanta, M.; Nazareno, J.; Tingo, R.; Mendoza, F.; Orizaga, A.; Mafla, E. *Analysis of the Appropriate Security Models to Apply in a Distributed Architecture*; IOP Publishing Ltd.: Bristol, UK, 2018.
79. ZeroTrustBankApp. Available online: https://github.com/daahclem/Zero-Trust-Bank-App (accessed on 21 January 2024).