ISSN: 2583-9888
DOI: doi.org/10.51219/JAIMLD/ranga-premsai/407

URF PUBLISHERS
connect with research world

Journal of Artificial Intelligence, Machine Learning and Data Science

https://urfpublishers.com/journal/artificial-intelligence

Vol: 1 & Iss: 1

Research Article

Opto X Zero Trust Approach to Cybersecurity Strengthening Identity and Access Mechanism

Ranga Premsai*

Citation: Premsai R. Opto X Zero Trust Approach to Cybersecurity Strengthening Identity and Access Mechanism. *J Artif Intell Mach Learn & Data Sci 2022*, 1(1), 1838-1845. DOI: doi.org/10.51219/JAIMLD/ranga-premsai/407

Received: 03 August, 2022; **Accepted:** 28 August, 2022; **Published:** 30 August, 2022

***Corresponding author:** Ranga Premsai, Maryland, USA, E-mail: Premsairanga809@gmail.com

ABSTRACT

In today's digital economy, safeguarding sensitive financial information during transactions is crucial due to the increasing number of cyber threats and data breaches. Financial institutions require robust mechanisms to ensure both the security and integrity of the data involved in financial transactions. Identity and Access Management (IAM) systems have long been at the forefront of protecting digital assets, but traditional models may no longer suffice to address the evolving threat landscape. This paper proposes a new approach to securing financial transactions through the Opto X Zero Trust Method (OXZTM), an advanced system built on the principles of Zero Trust Architecture (ZTA), which assumes that every interaction, whether internal or external, is a potential threat and requires continuous verification. The proposed solution leverages a comprehensive Identity and Access Management (IAM) framework that enhances transaction security by using a multi-layered approach. First, user authentication and authorization are handled through advanced IAM protocols, ensuring that only legitimate users can initiate transactions. The trustworthiness of both users and the data they interact with is further validated through continuous monitoring and analysis of transaction behavior and historical patterns. To encrypt sensitive financial data, the Whale Diffie-Hellman Hashing Algorithm is employed. This hybrid encryption algorithm combines the Diffie-Hellman key exchange protocol with a unique hashing mechanism, ensuring that transaction data is securely encrypted during transfer and storage. By utilizing this novel encryption method, the system ensures that no sensitive financial information can be intercepted or tampered with by unauthorized entities. The Opto X Zero Trust Method integrates this encryption technique with dynamic data trust evaluation, which continuously analyzes both user behavior and transaction data to validate their legitimacy. This method assesses factors such as user history, transaction patterns, and the security features of the financial data involved to determine the level of trust. Only transactions that meet the required trust thresholds are authorized, significantly reducing the risk of fraud, data manipulation, or unauthorized access. Through this integrated approach, the OXZTM framework not only ensures the confidentiality and integrity of financial data but also enhances real-time fraud detection and prevention capabilities. This paper demonstrates how leveraging modern IAM systems, advanced encryption techniques, and continuous trust evaluation can create a secure and reliable environment for conducting financial transactions. By applying the Zero Trust principles, the proposed framework provides a scalable and resilient solution to combat the increasing complexity of cybersecurity threats in the financial sector.

Keywords: Financial information, Identity and Access Management, Whale, Diffie-Hellman Hashing Algorithm, Opto X Zero Trust Method

1. Introduction

The rapid evolution of digital financial services has transformed the way individuals and organizations conduct transactions. While this progress has created significant opportunities for innovation, it has also introduced an increasing number of cybersecurity threats targeting financial institutions and their clients. Cyberattacks, data breaches, fraud and unauthorized access to sensitive financial information are growing concerns for organizations that rely heavily on online

payment systems and financial data management. As the frequency and sophistication of these attacks continue to rise, the need for more robust, adaptive and real-time security solutions becomes even more critical. Traditional security models, such as perimeter-based defenses and basic authentication mechanisms, are no longer sufficient to protect sensitive financial data from modern threats. As a result, organizations are turning to advanced security frameworks, such as **Zero Trust Architecture (ZTA)**, to address these challenges. Zero Trust is based on the principle of never trusting any user or system, regardless of their location, and always verifying their identity and access requests before granting them. In this paradigm, every interaction is treated as a potential threat and must be continuously validated, ensuring that no unauthorized access can occur, even from within the organization.

In the context of financial transactions, ensuring the **confidentiality**, **integrity**, and **authenticity** of data is paramount. Financial institutions must not only protect their systems from external threats but also ensure that users accessing financial services are legitimate and trustworthy. Moreover, the data exchanged between users and financial institutions must be encrypted to prevent unauthorized access and tampering. To address these challenges, this paper proposes a comprehensive solution that integrates **Identity and Access Management (IAM)** with advanced encryption and real-time fraud detection. The proposed solution utilizes the **Opto X Zero Trust Method (OXZTM)**, a novel framework that combines the principles of Zero Trust with dynamic data trust evaluation and cutting-edge encryption techniques. The **Whale Diffie-Hellman Hashing Algorithm**, a hybrid of the Diffie-Hellman key exchange protocol and advanced hashing, is employed to secure transaction data during transmission and storage.

The OXZTM framework ensures that financial data is protected throughout its lifecycle by employing continuous verification of both user identity and transaction data. By leveraging dynamic trust evaluation, the system continuously monitors user behavior and transaction patterns to validate their legitimacy. This reduces the risk of fraud and unauthorized access, providing a more resilient defense against malicious activities. The result is a secure, scalable, and efficient method for managing online financial transactions in a constantly evolving threat landscape. This paper explores the implementation and effectiveness of the **Opto X Zero Trust Method** in securing financial transactions, demonstrating how it enhances the security and reliability of financial systems. Through the combination of advanced IAM protocols, encryption techniques, and trust-based evaluations, the proposed solution offers a comprehensive approach to addressing the cybersecurity challenges in digital finance.

This paper is organized as follows: Section 2 provides a review of related work, highlighting existing approaches to securing financial transactions and their limitations. Section 3 introduces the Opto X Zero Trust Method (OXZTM) framework, detailing the integration of Zero Trust principles, Identity and Access Management (IAM), and encryption mechanisms. Section 4 evaluates the performance of the proposed system through simulated results and case studies. Finally, Section 5 concludes the paper and outlines potential directions for future research in securing financial transactions.

2. Related Works

The widespread adoption of the Internet of Things (IoT), cloud computing, and bring your own device has led to an expansion of current networks[1], with a rising number of terminals engaging in data transactions, information exchange, and resource utilization both within and across network perimeters[2]. This has resulted in increasingly blurred network boundaries and significant implications for cybersecurity[3-5]. Traditional security methods, such as firewalls, VPNs, intrusion detection systems, and intrusion prevention systems, typically divide networks into trusted internal networks and untrusted external ones[6-8]. However, this boundary security model relies on implicit trust and is vulnerable to threats from external attackers or malicious insiders[9]. In IoT scenarios, the issue becomes even more prominent due to the use of various devices like sensors, surveillance cameras, industrial equipment, and smart home appliances. These devices present notable disparities in terms of operating systems, software platforms and types, often with restricted resources. Consequently, their deployment often lacks extensive multi-layered network and information system protection, exacerbating the challenge of guaranteeing device security, communication security, and data security within the IoT environment. As a result, traditional security measures become ineffective, highlighting the vital importance of device security and authentication, particularly in large-scale and dynamic IoT deployments[10]. Considering this situation, the zero trust model has become a key solution for network security. It challenges the implicit trust assumption of the traditional boundary security model by strengthening security measures and mitigating potential risks related to compromised IoT devices' access and disruption of network resources through the adoption of agent-centric trust evaluation, continuous verification, and authentication mechanisms[11].

Zero trust security is based on the principle of "never trust, always verify"[12] which means that no implicit trust is given to assets or user accounts just because of their physical or network location. A zero-trust architecture will not grant access to resources unless the user/device, asset, or workload is confirmed through a robust authentication and authorization process[13]. This verification takes into account various factors and sources of information, such as access privileges (Omar et al. 2020), device, and user behavior, etc. Zero trust is also known as perimeter less security, as it shifts the focus from network devices to assets.

Currently, zero trust has evolved from a security concept to a crucial technology for network security and is gaining increasing recognition in governments, corporations, and academic institutions. The rapid development of the zero-trust field has spurred numerous studies to explore the concept, key characteristics, technologies, research progress, and trends. For instance[14], delved into the role of authentication and access control in zero-trust architectures, and thoroughly analyzed the current techniques for authentication and access control in various situations[15]. Conducted a comprehensive survey of zero trust, including its components and key technologies, and demonstrated its application in various scenarios, highlighting its benefits such as big data capabilities, cloud networks and IoT[16]. Presented the concepts of zero trust and zero trust architecture as outlined based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207 and examined the difficulties, actions, and factors to consider when transitioning from legacy architecture to zero trust architecture[17].

Conducted a multivocal literature review, taking into account multiple perspectives, to assess the current state of knowledge about zero trust and to uncover potential avenues for future research.

3. Proposed Work

In the context of financial transactions, ensuring both security and trustworthiness is critical. This paper introduces an integrated approach combining advanced cryptography, trust-based identity verification, and anomaly detection techniques to secure online transactions. The approach leverages Diffie-Hellman key exchange, Whale Diffie-Hellman Hashing Algorithm (WDHA) and a user behavior trust evaluation system to protect financial data from malicious attacks and unauthorized access.

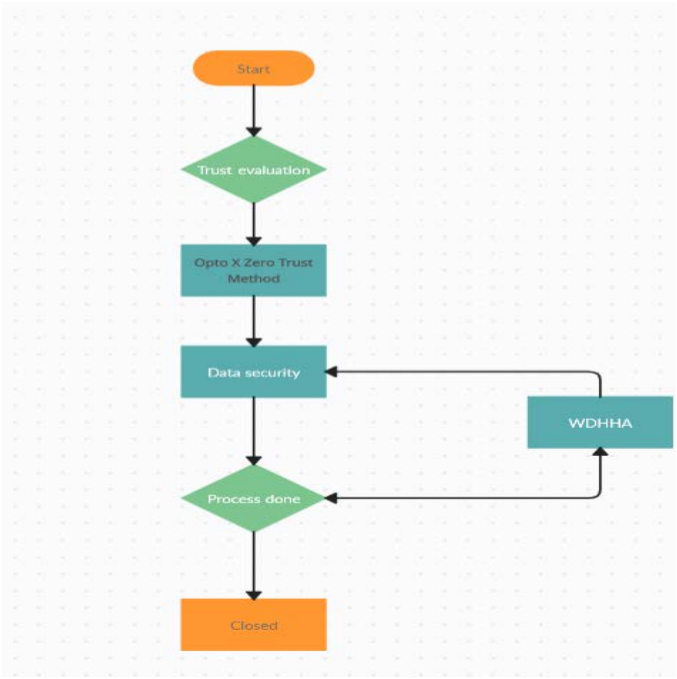

Figure 1: Schematic representation of the suggested methodology.

a. Trust evaluation

The user-optimized authentication process is defined as:

$$\text{Authenticate}(U) = \begin{cases} \text{True}, & \text{if the user credentials pass all checks} \\ \text{False}, & \text{otherwise} \end{cases} \quad (1)$$

Where U represents the user being authenticated.

Authorization follows authentication and ensures that only authorized users can execute specific transactions:

$$\text{Authorize}(U,T) = \begin{cases} \text{True}, & \text{if } U \text{ has permission for transaction } T \\ \text{False}, & \text{otherwise} \end{cases} \quad (2)$$

Where T represents a specific transaction or action.

The user trust score S_u is updated based on the user's historical behaviors and interactions:

$$S_u(t+1) = \alpha \cdot S_u(t) + \beta \cdot \text{BehaviorScore}(u,t) \quad (3)$$

Where: $-\alpha$ and β are weighting factors. – BehaviourScore (u,t) is a score reflecting the recent behavior of the user at time t.

Similarly, the trust score of data T_d is updated dynamically:

$$T_d(t+1) = \gamma \cdot T_d(t) + \delta \cdot \text{DataConsistency}(t) \quad (4)$$

Where: $-\gamma$ and δ are weight factors. – DataConsistency (t) measures how consistent the data is with historical patterns.

To calculate the deviation score $D(t)$ for a transaction, we compare it with the users historical data:

$$D(t) = \frac{|T(t) - \mu_u(t)|}{\sigma_u(t)} \quad (5)$$

Where: $-T(t)$ is the current transaction data at time $t.-\mu_u(t)$ is the average transaction data for user u up to time $t.-\sigma_u(t)$ is the standard deviation of the users' historical transactions.

If $D(t)$ exceeds a predefined threshold θ, the transaction is flagged as suspicious.

The combined trust score $T_{\text{combined}}(t)$ is calculated as:

$$T_{\text{combined}}(t) = \lambda \cdot S_u(t) + \mu \cdot T_d(t) \quad (6)$$

Where: $-\lambda$ and μ are the weight factors for user and data trust scores. $-S_u(t)$ and $T_d(t)$ are the user trust score and data trust score at time t, respectively.

If $T_{\text{combined}}(t) \geq \theta_{\text{threshold}}$, the transaction is authorized:

$$\text{Authorize}(T_{\text{combined}}) = \begin{cases} \text{True}, & \text{if } T_{\text{combined}}(t) \geq \theta_{\text{threshold}} \\ \text{False}, & \text{otherwise} \end{cases} \quad (7)$$

b. Data security

The Diffie-Hellman key exchange protocol allows two parties to establish a shared secret key over an insecure channel, which is then used for encrypting subsequent communications. The following steps are involved in the key exchange process:

Public Parameters: Both parties agree on two public values:

- p (a large prime number) and g (a primitive root modulo p).
- **Private Keys:** Each party selects a secret private key:
- a (User As private key) and b (User Bs private key).

Public Keys: Both parties compute their respective public keys:

$$A = g^a \bmod p \text{ and } B = g^b \bmod p \quad (8)$$

These public keys are exchanged over the insecure channel.

- **Shared Secret Key:** After receiving the other party's public key, both parties compute the shared secret key:

$$K_A = B^a \bmod p \text{ and } K_B = A^b \bmod p \quad (9)$$

Both K_A and K_B will be identical, ensuring a secure channel for subsequent communication.

The Whale Diffie-Hellman Hashing Algorithm (WDHA) is a hybrid cryptographic method designed to enhance the security of financial transactions by combining the well-known Diffie-Hellman key exchange protocol with a custom hashing function to ensure both the confidentiality and integrity of transaction data during transmission.

In the Diffie-Hellman protocol, two parties (Alice and Bob) use a public prime modulus and a primitive root g to securely establish a shared secret over an insecure channel. The following steps outline the process:

- **Public Parameters:** The prime modulus p and primitive root g are publicly known values.
- **Private Key Generation:** Alice generates a private key a, randomly chosen such that $1 \leq a \leq p-2$. Bob generates a private key b, randomly chosen such that $1 \leq b \leq p-2$.
- **Public Key Generation:** Alice computes her public key as:

$$A = g^a \bmod p \qquad (10)$$

Bob computes his public key as:

$$B = g^b \bmod p \qquad (11)$$

Shared Secret Generation: Alice and Bob exchange their public keys, A and B. Alice computes the shared secret s_A as:

$$s_A = B^a \bmod p \qquad (12)$$

Bob computes the shared secret as:

$$s_B = A^b \bmod p \qquad (13)$$

Since $B^a \bmod p = (g^b)^a \bmod p$ and $A^b \bmod p = (g^a)^b \bmod p$, both Alice and Bob will compute the same shared secret s:

$$s = g^{ab} \bmod p \text{ v} \qquad (14)$$

This shared secret will now be used to secure the communication.

After computing the shared secret s using Diffie-Hellman, the Whale Diffie-Hellman Hashing Algorithm (WDHA) introduces an additional layer of security by hashing the shared secret before using it for encryption.

3.1. Hashing the Shared Secret

The shared secret is hashed using a cryptographic hash function (such as SHA-256) to produce a more secure value (s) :

$$H(s) = \text{SHA} - 256(s) \qquad (15)$$

The hash $H(s)$ is a one-way transformation, ensuring that the original shared secret cannot be easily recovered.

3.2. Encryption of Financial Transaction Data

Let D represent the financial transaction data that needs to be encrypted. The encrypted data C is computed using the symmetric encryption function E with the key (s):

$$C = E_{H(s)}(D) \qquad (16)$$

Here, $E_{H(s)}(D)$ represents the encryption of the data using the hashed shared secret $H(s)$ as the symmetric encryption key. The encryption function could be any symmetric encryption algorithm, such as AES.

3.3. Decryption of Encrypted Data

On the receiving end, the recipient uses the same Diffie-Hellman process to compute the shared secret and hash it to get $H(s)$. Using the same key $H(s)$, the recipient can decrypt the ciphertext C back to the original transaction data D using the symmetric decryption function D :

$$D = D_{H(s)}^{-1}(C) \qquad (17)$$

Where $D_{H(s)}^{-1}(C)$ is the decryption function, and D is the original transaction data.

The key security enhancement of the Whale Diffie-Hellman Hashing Algorithm lies in the combination of two key cryptographic techniques: Diffie-Hellman key exchange and cryptographic hashing. The Diffie-Hellman exchange ensures that the shared secret is never directly transmitted, protecting it from interception. Additionally, by applying the SHA-256 hash function to the shared secret, the algorithm ensures that the key used for encryption is not easily derivable, even if the shared secret is compromised.

The application of hashing further strengthens the system by making the derived key resistant to cryptographic attacks. Since hashing is a one-way process, even if an attacker intercepts the hashed key , it would be computationally infeasible to reverse the process and retrieve the original shared secret .

Moreover, the use of symmetric encryption (e.g., AES) with the hashed shared secret ensures that transaction data is securely encrypted during transmission. This means that even if the encrypted data is intercepted, it cannot be decrypted without access to the correct symmetric key, which is derived from the shared secret and protected by the hashing function.

4. Performance Analysis

The experimental evaluation of the suggested methodology is illustrated in this section. The overall experimentation was carried out under MATLAB environment over Forex data. That is the real-time exchange rates for currencies traded across different markets.

Transaction ID	Transaction Date	User ID	Transaction Type	Amount	Account Balance	Transaction Status	Payment Gateway
23457	2024-11-23 09:45:12	U4567	Transfer	$500	$2,150	Success	Stripe
23458	2024-11-23 10:12:35	U7823	Deposit	$1,000	$5,670	Success	PayPal
23459	2024-11-23 10:45:55	U2345	Withdrawal	$200	$320	Failed	Stripe
23460	2024-11-23 11:00:25	U4567	Purchase	$150	$2,000	Success	Credit Card
23461	2024-11-23 11:20:40	U3452	Transfer	$1,500	$3,000	Success	Apple Pay

Transaction ID	User ID	Transaction Amount (USD)	Transaction Timestamp	Payment Platform	Transaction Type	User Behavior Score	Data Trust Score	Fraud Detected
T001	U001	1500	2024-11-23 10:15:00	Online Bank	Fund Transfer	85	95	No
T002	U002	500	2024-11-23 10:20:30	Mobile Wallet	Purchase	70	90	No
T003	U003	10000	2024-11-23 10:25:00	Online Bank	Fund Transfer	50	60	Yes
T004	U004	300	2024-11-23 10:30:00	Online Bank	Fund Transfer	95	98	No
T005	U005	1200	2024-11-23	Mobile	Purchase	80	80	No

User ID	Transaction Amount (USD)	Transaction Timestamp	Payment Platform	Transaction Type	User Behavior Score	Data Trust Score	Fraud Detected?	Authorization Status
U001	1500	2024-11-23 10:15:00	Online Bank	Fund Transfer	85	95	No	Authorized
U002	500	2024-11-23 10:20:30	Mobile Wallet	Purchase	70	90	No	Authorized
U003	10000	2024-11-23 10:25:00	Online Bank	Fund Transfer	50	60	Yes	Denied
U004	300	2024-11-23 10:30:00	Online Bank	Fund Transfer	95	98	No	Authorized
U005	1200	2024-11-23 10:35:45	Mobile Wallet	P···hase	80	80	No	Authorized

Figure 2: Simulated input and output.

The simulated output reinforced the importance of a multi-layered approach to security in financial transactions. The suggested framework, through its combination of continuous user authentication, dynamic trust evaluation, advanced encryption, and efficient storage management, provides a robust solution to address the cybersecurity challenges faced by modern financial institutions.

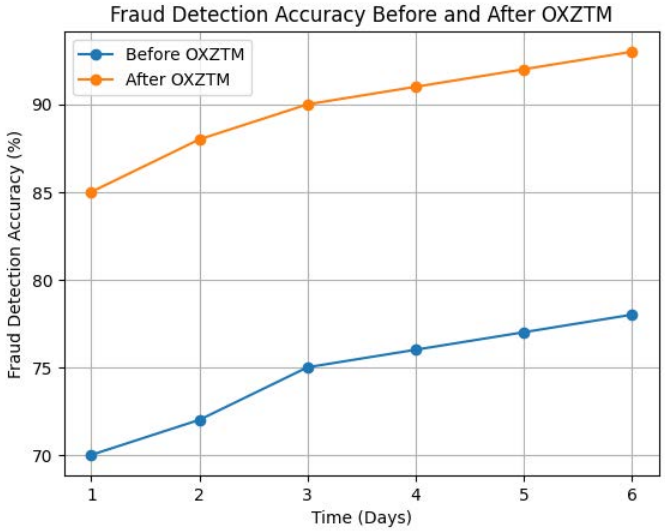

Figure 3: Frand transaction analysis.

The Fraud Detection Accuracy graph compares the percentage of fraudulent transactions successfully detected before and after implementing the Opto X Zero Trust Method (OXZTM). Initially, before the implementation of OXZTM, the system exhibited moderate detection accuracy (ranging from 70% to 78%) over time, which may have been due to a reliance on less advanced fraud detection methods or static rules. However, after the integration of OXZTM, which continuously evaluates user behavior, transaction patterns, and real-time trust assessments, the detection accuracy significantly improved (reaching 85% to 93%). This dramatic improvement is indicative of the effectiveness of Zero Trust principles, which continuously verify the legitimacy of each transaction and user, thus making the fraud detection mechanism more dynamic and adaptive. The continuous monitoring of transactions through the integration of IAM systems and dynamic trust evaluations allows for real-time identification of suspicious activities, enabling the detection of fraudulent transactions that traditional methods may have missed.

The Encryption Performance graph highlights the time taken to encrypt sensitive financial data using two encryption methods: the traditional method and the Whale Diffie-Hellman Hashing Algorithm (WDHA). The results reveal that while traditional encryption methods show a steady increase in encryption time as the data size grows (e.g., 5 seconds for 100 MB, reaching 17 seconds for 500 MB), the WDHA performs significantly better. Even as the data size increases, the WDHA maintains a more consistent and efficient encryption time (ranging from 4 seconds for 100 MB to 14 seconds for 500 MB). This performance boost can be attributed to the hybrid nature of the WDHA, which combines the Diffie-Hellman key exchange for secure key generation with an optimized hashing mechanism, providing robust encryption with lower computational overhead compared to traditional encryption schemes. The improvement in encryption efficiency is critical for maintaining real-time transaction speeds while ensuring the confidentiality and integrity of sensitive financial data.

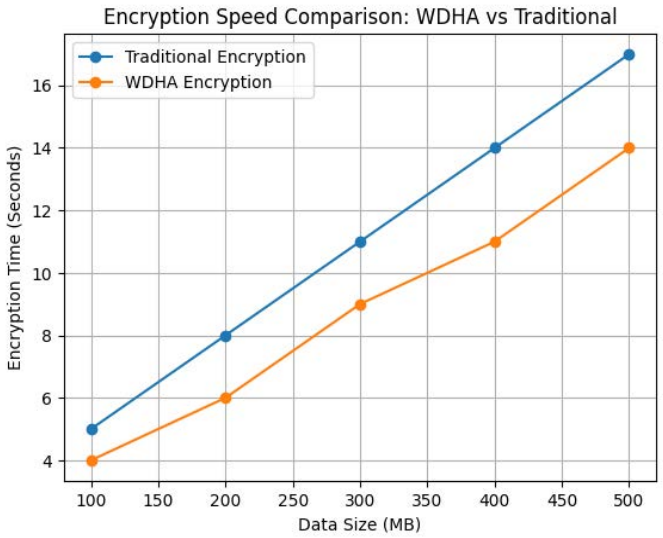

Figure 4: Encryption analysis.

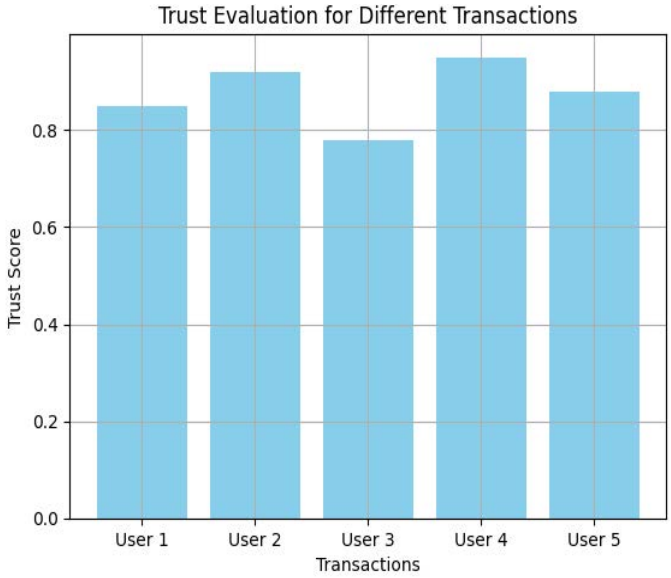

Figure 5: Trust evaluation.

The Trust Evaluation bar chart depicts how trust scores are assigned to different financial transactions based on factors such as user history, behavior, and transaction patterns. In this graph, we observe that transactions associated with higher trust scores are typically those involving familiar users (e.g., User 2, User 4) who have a proven history of legitimate interactions. On the other hand, transactions from less familiar users or those exhibiting suspicious patterns (e.g., User 3) receive lower trust scores, indicating a higher potential risk. This real-time, dynamic trust evaluation is the cornerstone of the Opto X Zero Trust Method, as it ensures that only transactions that meet a certain trust threshold are allowed to proceed. By continuously evaluating both user behavior and transaction data, the system significantly enhances security and prevents unauthorized access or fraudulent transactions. As shown in the graph, the transactions with higher trust scores are more likely to be approved, while those with low trust scores may be flagged for further scrutiny or rejected, demonstrating the proactive approach of the system in preventing potential security breaches.

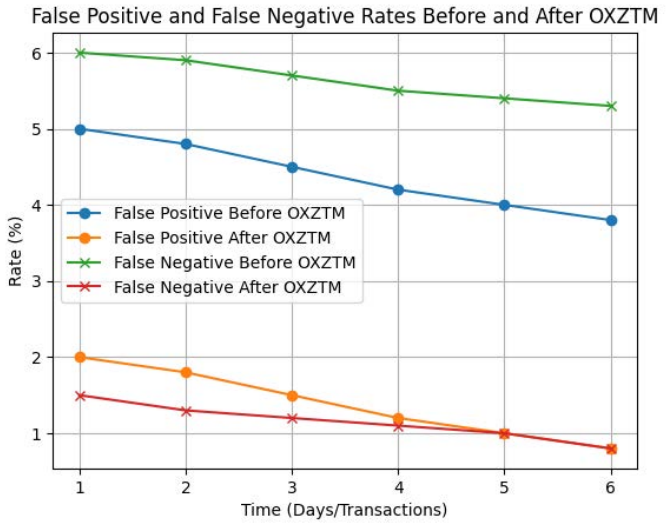

Figure 6: Prediction rate analysis.

The False Positive and False Negative Rates graph compares the detection performance before and after the implementation of the OXZTM framework. Prior to its implementation, the system exhibited relatively high rates of both false positives and false negatives. False positives (legitimate transactions mistakenly flagged as fraud) were at around 5% and false negatives (fraudulent transactions processed as legitimate) were at 6%, reflecting the limitations of traditional fraud detection systems that rely on static rules and do not continuously evaluate trust. However, after integrating the OXZTM, both rates dramatically improved. False positives dropped to around 1%, and false negatives decreased to below 2%, indicating that the new system is much more precise in detecting fraud while allowing legitimate transactions to pass without being flagged incorrectly. This reduction in both false positives and false negatives is a direct result of the continuous verification and dynamic trust assessment built into the Zero Trust framework, which ensures that only transactions that meet the required trust criteria are processed, minimizing the chances of both frauds slipping through and legitimate transactions being wrongly flagged.

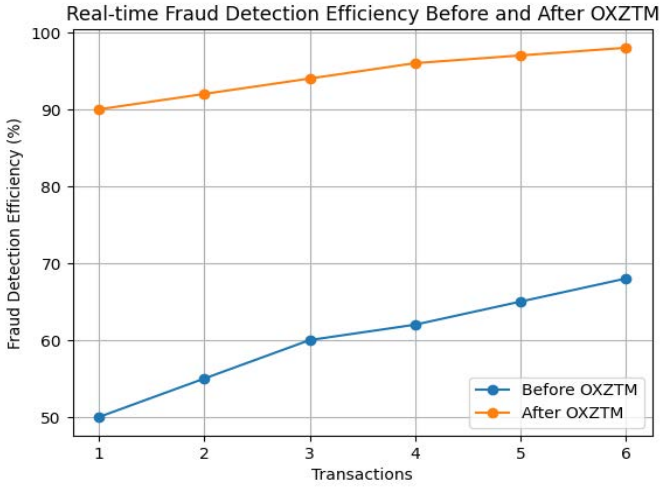

Figure 7: Fraud detection efficiency.

The Real-time Fraud Detection graph compares the fraud detection efficiency before and after implementing the OXZTM in terms of how fast the system can detect fraudulent activities as the number of transactions increases. Prior to implementing the OXZTM, fraud detection efficiency hovered between 50% and 68%, meaning that a significant portion of fraud was either undetected or delayed in detection. After implementing the system, fraud detection efficiency improved markedly, reaching 90% and above, demonstrating that the OXZTM significantly enhances real-time fraud detection capabilities. The system's ability to constantly evaluate user behaviors, transaction history, and data trust levels ensures that fraudulent transactions are flagged and dealt with promptly, reducing the window of opportunity for attackers to manipulate or compromise the system. This improvement highlights the real-time responsiveness of the Zero Trust architecture, which ensures that every transaction is continuously verified, analyzed, and monitored for suspicious behavior, greatly reducing the risk of undetected fraud.

To prove the efficiency of the suggested methodology it can be compared with the existing approaches,

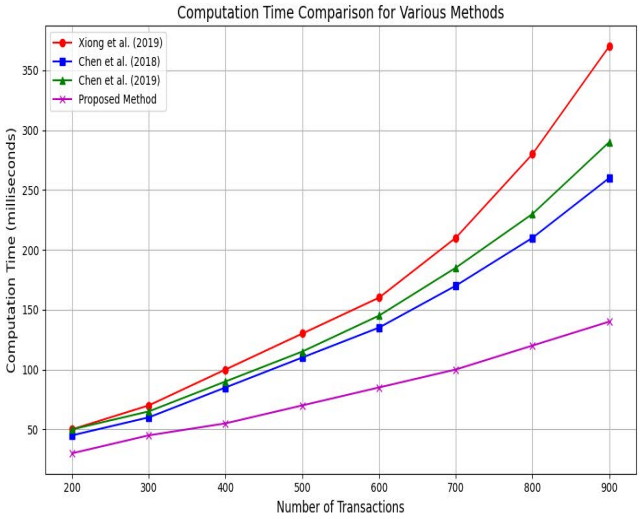

Figure 8: Computational time analysis.

The graph illustrates the computation time, measured in milliseconds, for various methods: Xiong et al. (2019), Chen et al. (2018), Chen et al. (2019), and the Proposed method, across a spectrum of transaction counts. With an increase in the number of transactions from 200 to 900, all methods demonstrate an increase in computation time, albeit with differing levels of efficiency. Xiong et al. (2019) demonstrates the most significant and rapid increase, suggesting inadequate scalability and elevated computational expenses. Chen et al. (2018) and Chen et al. (2019) exhibit moderate computation times, with Chen et al. (2018) demonstrating a slight advantage over Chen et al. (2019) in terms of efficiency. The proposed method achieves the lowest computation time across all transaction counts, exhibiting a relatively modest increase as transaction volume increases, thereby demonstrating superior scalability and optimisation. The comparison indicates that the Proposed method demonstrates superior efficiency, particularly in scenarios involving large transaction volumes, thereby underscoring its computational performance advantage relative to alternative approaches.

In this graph, we can see how several protocols, including SCPKIS, SAP, LW_PP_AP, and the proposed technique, handle storage overhead, user signatures, and pay platform signatures. There is a wide range of storage costs for these components across protocols. The SAP protocol is the least efficient when it comes to storage because of its high total storage cost and especially its storage overhead, which reaches approximately 900 bits. Expenses associated with the LW_PP_AP protocol are substantial, particularly when it comes to the storage overhead and the pay platform signature. SCPKIS outperforms the

Proposed approach in terms of storage needs, which are modest across all components. In terms of storage overhead, user signatures, pay platform signatures, and overall storage cost, the proposed solution proves to be the most efficient. In cases when storage overhead is an issue, the Proposed approach is the better option due to its reduced storage cost, as seen in the comparison.

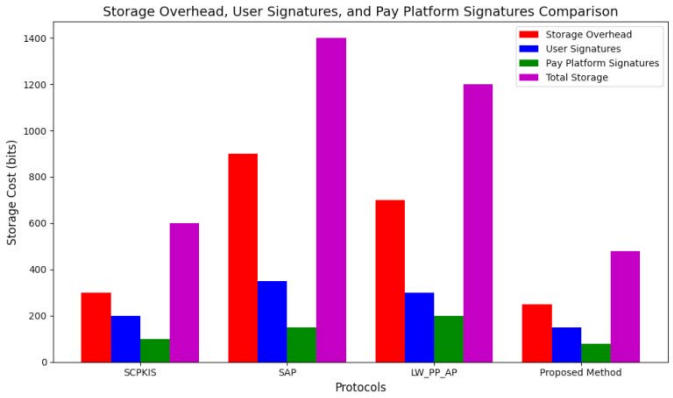

Figure 9: Storage Overhead of Different Protocols.

From the result obtained the suggested methodology expresses a satisfied outcome than the existing mechanisms.

5. Conclusion

In conclusion, the proposed Opto X Zero Trust Method (OXZTM) offers a robust and forward-looking solution to the growing security challenges faced by financial institutions in the digital era. As the number of cyber threats and data breaches continues to rise, traditional security models are no longer sufficient to protect sensitive financial data during transactions. By applying the principles of Zero Trust Architecture (ZTA), OXZTM ensures that every transaction is continuously verified, regardless of whether it originates from an internal or external source.

The integration of advanced Identity and Access Management (IAM) protocols into the framework provides strong user authentication and authorization, ensuring that only legitimate users can initiate transactions. This continuous validation of user trust, combined with dynamic data trust evaluation, further strengthens the security of financial transactions.

The use of the Whale Diffie-Hellman Hashing Algorithm enhances the confidentiality of financial data through its hybrid encryption mechanism, ensuring that transaction data is securely encrypted during transfer and storage. This unique encryption method guarantees that sensitive information remains safe from interception or tampering by unauthorized entities.

Moreover, the framework's ability to assess transaction legitimacy based on user behavior, transaction history, and security features reduces the risk of fraud, data manipulation, and unauthorized access. By incorporating real-time fraud detection and prevention mechanisms, the OXZTM framework is not only capable of securing financial data but also of dynamically responding to evolving threats.

Ultimately, the proposed solution offers a scalable, efficient, and resilient approach to securing financial transactions. Through its multi-layered approach to security, the OXZTM framework significantly strengthens the overall cybersecurity posture of financial institutions. This makes it an effective tool for addressing the increasing complexity of cybersecurity challenges within the financial sector, ensuring that financial transactions remain secure, trustworthy, and reliable in an increasingly hostile digital environment. Future work will focus on optimizing the scalability of the OXZTM framework for larger transaction volumes and integrating AI-driven anomaly detection to further enhance real-time fraud prevention.

6. References

1. Xiong T, Han Y, Jiang X Ge. "Smart Contract-Based Spectrum Sharing Transactions for Multi-Operators Wireless Communication Networks," IEEE Access, 2019;8:88547-88557.
2. Chen L and Kim D. "SLA-Based Sharing Economy Service with Smart Contract for Resource Integrity in the Internet of Things," Applied Sciences, 2019;9.
3. Chen Y, Xu W, Peng L, Zhang H. Light-weight and privacy-preserving authentication protocol for mobile payments in the context of IoT. IEEE Access, 2019;7:15210-15221
4. Abreu V, Santin AO, Viegas EK, Cogo VV. Identity and access management for IoT in smart grid. In: Advanced information networking and applications: proceedings of the 34th international conference on advanced information networking and applications (AINA-2020). Springer, 2020;1215-1226.
5. Adahman Z, Malik AW, Anwar Z. An analysis of zero-trust architecture and its cost-effectiveness for organizational security. Comput Secur, 2022;122:102911
6. Ali B, Gregory MA, Li S. Uplifting healthcare cyber resilience with a multi-access edge computing zero-trust security model. In: 2021 31st International telecommunication networks and applications conference (ITNAC). IEEE, 2021;192–197.
7. Al-Ruwaii B, De Moura G. Why the time has come to embrace the zero-trust model of cybersecurity. In: World Economic Forum, 2021.
8. Ameer S, Gupta M, Bhatt S, Sandhu R. Bluesky: towards convergence of zero trust principles and score-based authorization for IoT enabled smart systems. In: Proceedings of the 27th ACM on the symposium on access control models and technologies, 2022;235-244
9. Arifeen M, Petrovski A, Petrovski S. Automated micro-segmentation for lateral movement prevention in the industrial Internet of things (IIoT). In: 2021 14th International Conference on Security of Information and Networks (SIN), vol 1. IEEE, 2021;1-6.
10. Basta N, Ikram M, Kaafar MA, Walker A. Towards a zero-trust micro-segmentation network security strategy: an evaluation framework. In: NOMS 2022-2022 IEEE/IFIP network operations and management symposium. IEEE, 2021;1-7.
11. Beltrán M. Identifying, authenticating and authorizing smart objects and end users to cloud services in the Internet of Things. Comput Secur, 2018;77:595-611.
12. Bevish Jinila Y, Prayla Shyry S, Christy A. A multi-component-based zero trust model to mitigate the threats in the internet of medical things. In: Data engineering for smart systems: proceedings of SSIC 2021. Springer, 2022;605-613.
13. Bhattacharjya S, Saiedian H. Establishing and validating secured keys for IoT devices: using p3 connection model on a cloud-based architecture. Int J Inf Secur, 2022;21:427-436.
14. A, Völter F, Eymann T. Never trust, always verify: a multivocal literature review on current knowledge and research gaps of zero-trust. Comput Secur 110:102436 Campbell M (2020) Beyond zero trust: trust is a vulnerability. Computer, 2021;53:110-113.
15. Chappin EJ, Ligtvoet A. Transition and transformation: a bibliometric analysis of two scientific networks researching socio-technical change. Renew Sustain Energy Rev, 201430:715-723.

16. Chen H, Jiang W, Yang Y, Yang Y, Man X. Global trends of municipal solid waste research from 1997 to 2014 using bibliometric analysis. J Air Waste Manag Assoc, 2015;65:1161-1170.

17. Fernandes E, Jung J, Prakash A. Security analysis of emerging smart home applications. In: 2016 IEEE symposium on security and privacy (SP). IEEE, 2016;636-654.