Dynamic Identity Management: A Key Component in Modern Cybersecurity Strategies

Ranga Premsai

MS, IAM Professional, USA

Abstract

In today's interconnected digital landscape, the need for secure and flexible identity management across multiple domains has become critical. Traditional Single Sign-On (SSO) mechanisms are heavily reliant on predefined trust relationships, which limits their effectiveness in dynamic and open environments where trust boundaries are constantly shifting. To address these challenges, this study introduces a novel approach to dynamic identity management by proposing a Dynamic Trust Identifying Mechanism that leverages advanced optimization techniques for secure cross-domain collaboration. The proposed solution is centred on the concept of a "Circle of Trust" (CoT) framework, which enables the sharing of identities and attributes across trust boundaries in accordance with predefined policies. Our approach aims to overcome the limitations of existing SSO mechanisms by dynamically managing trust relationships between entities across various domains. To achieve this, we introduce an emergent dynamic trust list that identifies trusted parties in real-time, allowing for adaptive and secure identity management. The core of our solution incorporates two advanced algorithms: the Pro-Wave Surf Optimization (PWSO) and the Sail Sea Fish Algorithm (SSFA). The Pro-Wave Surf Optimization is used to dynamically identify and evaluate trust relationships by simulating wave patterns, which helps in optimizing trust calculations across multiple domains. This algorithm enables the system to efficiently adjust trust relationships based on changes in the environment, making it suitable for managing identities in a dynamic, open ecosystem. Meanwhile, the Sail Sea Fish Algorithm is utilized to ensure secure data transfer between trusted parties by mimicking the behavior of fish swarming in the ocean. This algorithm enhances data security by optimizing the data transfer routes, reducing the risk of interception or unauthorized access during cross-domain interactions. Through this dual-algorithm approach, the proposed framework not only facilitates dynamic trust management but also provides a robust mechanism for secure data transfer across domains. This study details the methodology, implementation, and evaluation of this Dynamic Trust Identifying Mechanism, highlighting its potential to improve security and flexibility in cross-domain identity management. The results demonstrate that this approach can adaptively manage trust in open environments, offering a scalable and secure solution for modern identity management challenges.

Keywords: Trust, Dynamic Trust Identifying Mechanism, Pro-Wave Surf Optimization, Sail Sea Fish Algorithm

I. INTRODUCTION

As digital systems become more integrated, managing identities across multiple platforms and domains has emerged as a critical aspect of cybersecurity. Identity management solutions ensure that users and systems can securely access resources, communicate, and collaborate without repeatedly proving their identity. Traditional identity management systems, such as Single Sign-On (SSO), allow a user to authenticate once

and then access multiple related services without needing to re-enter credentials. This approach has proven effective within single, controlled domains, like an organization's internal network or a secure ecosystem where all parties have pre-established trust. However, the limitations of SSO systems become apparent when services need to collaborate across different domains or organizations. In cross-domain environments, the assumption of pre-existing trust does not hold, making traditional SSO mechanisms vulnerable. Cross-domain identity management is further complicated by the dynamic nature of modern digital environments, where users and entities constantly change, and new ones frequently enter the system. Static, pre-defined trust relationships are not adaptable enough to accommodate these changes, leading to security risks and limiting the flexibility required in open environments. Unauthorized access, privacy breaches, and inefficient handling of identity data across domains are some of the challenges that arise under the current SSO model.

To address these limitations, the concept of a "Circle of Trust" (CoT) has been introduced. A Circle of Trust is an alliance between multiple domains where identities and attributes are shared according to predetermined policies. It creates a collaborative environment where each member within the CoT recognizes and trusts the identities managed by others. While CoT provides a framework for cross-domain identity management, its implementation often relies on significant manual setup to enroll and manage members, which hinders its ability to adapt to new, dynamic, and open environments where entities frequently change. The need for a more fluid approach has become evident, particularly in settings where entities must quickly assess trustworthiness and establish secure communication without prior arrangements. In response to these challenges, this paper proposes a novel Dynamic Trust trust-identifying mechanism that enhances identity management across trust boundaries using advanced optimization techniques. The objective of this mechanism is to establish and maintain dynamic trust relationships in real-time, enabling cross-domain Single Sign-On (SSO) without relying on static, pre-configured trust lists. This approach not only enhances security but also provides flexibility, allowing new members to be evaluated and integrated as trusted entities without extensive manual intervention.

To achieve this, the proposed mechanism incorporates two advanced algorithms: **Pro-Wave Surf Optimization (PWSO)** and the **Sail Sea Fish Algorithm (SSFA)**. The **Pro-Wave Surf Optimization (PWSO)** algorithm is inspired by the dynamic behavior of ocean waves, simulating their patterns to create adaptive trust calculations. By applying wave-inspired patterns, the PWSO algorithm evaluates and adjusts trust levels based on real-time changes in the environment. This enables continuous assessment of trustworthiness, allowing the system to accommodate new members, assess unfamiliar entities, and adapt trust relationships to changing conditions. As a result, PWSO can quickly identify reliable entities in dynamic environments, making it highly effective for cross-domain identity management. Meanwhile, the **Sail Sea Fish Algorithm (SSFA)** focuses on securing data transfer across trust boundaries. This algorithm is inspired by the efficient and coordinated movement of fish swarming in the ocean, a behavior that enables fish to navigate complex environments while minimizing exposure to predators. Applying this principle, the SSFA algorithm optimizes data transfer routes to enhance security, ensuring that sensitive identity information is securely transmitted between domains. By constantly evaluating and adjusting these routes, SSFA minimizes the risk of interception and unauthorized access, providing an additional layer of protection for cross-domain transactions.

Together, the PWSO and SSFA algorithms create a comprehensive, multi-layered framework that addresses both trust management and data security in cross-domain environments. The **Dynamic Trust Identifying Mechanism** enables an adaptive Circle of Trust (CoT) that does not require extensive manual setup or static

configurations. This approach allows trusted parties to be dynamically identified and securely connected, providing the flexibility needed in open, collaborative digital ecosystems where entities frequently change.

This paper presents a detailed methodology and implementation of the Dynamic Trust Identifying Mechanism, assessing its effectiveness in enhancing identity management and data security across trust boundaries. The proposed framework introduces a robust solution to the limitations of traditional SSO by supporting dynamic, real-time trust assessments and secure data exchange. Additionally, we discuss the performance of the proposed system in various scenarios, demonstrating how the integration of PWSO and SSFA can provide a scalable, flexible, and secure solution to modern identity management challenges.

The remaining section of the paper can be organized as follows, section 2 in which the literature survey was analysed, in section 3 the proposed methodology was illustrated. In section 4 the result and discussion was depicted. Finally in section 5, the findings were discussed.

II. RELATED WORKS

In [1], the author examines the architectures, enabling techniques, and methodologies for moving target defence and mimic defence. This is followed by a taxonomy summary of the execution and assessment of dynamic defence. Ultimately, they examine many unresolved obstacles and prospects for dynamic defence in cybersecurity.In [2], the author examines prevalent MFA approaches, the incorporation of identity management systems, and the use of Role-Based Access Control (RBAC) to guarantee safe user access. Moreover, new technologies like artificial intelligence (AI) and machine learning are examined for their capacity to monitor access patterns and identify security vulnerabilities in real-time. The document also examines the obstacles encountered by cloud CRM systems, such as weaknesses in access control and prospective advancements in identity and access management (IAM). By adopting these security best practices, organisations may reduce risks and safeguard sensitive data in cloud CRM settings. Examine prevalent MFA methodologies, the incorporation of identity management systems, and the use of Role-Based Access Control (RBAC) to guarantee safe user access. Moreover, new technologies like artificial intelligence (AI) and machine learning are examined for their capacity to monitor access patterns and identify security vulnerabilities in real-time. The document also examines the obstacles encountered by cloud CRM systems, such as weaknesses in access control and prospective advancements in identity and access management (IAM). By adopting these security best practices, organisations may reduce risks and safeguard sensitive data in cloud CRM settings.In [3], the author explores cybersecurity solutions designed to protect sensitive information inside MDM frameworks. The abstract delineates the main elements of the article, including an examination of contemporary risks to MDM systems, an evaluation of conventional and innovative cybersecurity methods, and suggestions for a comprehensive cybersecurity strategy inside the framework of MDM. Organisations must comprehend and implement appropriate cybersecurity solutions to preserve the integrity and confidentiality of their master data, therefore mitigating risks and safeguarding sensitive information throughout the data lifecycle.In [4], the author examines the essential elements and operations of continuous authentication, the contribution of machine learning to anomaly detection, and the benefits of behavioural biometrics compared to conventional techniques. It also analyses the implementation factors, including interaction with current security infrastructure, privacy issues, and user acceptability. Practical advantages of these technologies are shown via real-world applications and case studies in financial services, healthcare, and government organisations. The essay finishes by examining future trends and research areas, including developments in machine learning and artificial intelligence, integration with Internet of Things (IoT) devices, and ongoing authentication in cloud computing settings. This detailed summary highlights the need of implementing proactive and adaptive security strategies to protect sensitive

data and assets in the constantly changing digital environment.In [5], the author assesses the efficacy of conventional access control models—Role-Based Access Control (RBAC), Policy-Based Access Control (PBAC), and Attribute-Based Access Control (ABAC)—in relation to ransomware threats within critical infrastructures and explores the prospective advantages of incorporating machine learning (ML) and artificial intelligence (AI) technologies. The study used a quantitative research approach to gather data from 383 cybersecurity experts across several industries using a systematically organised questionnaire.In [6], the author examines the significance of real-time data analytics and user empowerment tactics in bolstering cybersecurity resilience. Real-time data analytics enable the identification and response to threats as they arise, thereby reducing the vulnerability period. Utilising big data and machine learning algorithms, these analytics provide actionable insights that enable proactive threat management and fast responses to suspected breaches. Concurrently, equipping people with knowledge, awareness, and intuitive security tools is vital for fortifying the primary defence against cyber attacks. In [7] underscores the need of ongoing validation of entities attempting to access organisational systems, guaranteeing that each access request is verified, authorised, and encrypted. The Layered Security Model, commonly referred to as Defence in Depth, complements the Zero Trust strategy. This paradigm promotes the implementation of many layers of defence measures inside an IT system, establishing a comprehensive barrier against possible attacks. By using multifaceted security measures across several levels, from physical to digital, organisations may guarantee that if one layer is breached, others remain secure, thereby offering comprehensive protection.Incorporating these models with internationally acknowledged industry standards and frameworks, including as NIST, ISO/IEC 27001, and OWASP, enhances an organization's security posture. In [8], the author analyses current case studies and real-world situations, offering useful insights into the evolving nature of cyber threats and underscoring the need for proactive and adaptable cybersecurity strategies. The evaluation critically assesses advanced defence systems and techniques used to mitigate these threats. It examines progress in artificial intelligence, machine learning, and behavioural analytics, highlighting their crucial contributions to enhancing cybersecurity measures. The study emphasises the significance of threat information sharing, collaborative initiatives, and international collaboration to strengthen the global cyber defence framework.In [9], the author examines several facets of cybersecurity, including statistical data pertinent to ICT security in firms and events happening in businesses inside Poland and the EU. The analysis of incident data enabled the assessment of the effects of cyber threats on organisational security and operations. In [10], the revolutionary significance of AI in enhancing IAM procedures within healthcare is examined, emphasising future developments such as adaptive authentication, AI-driven identity analytics, and the automation of user provisioning. The research examines the difficulties associated with maintaining extensive healthcare data and adhering to regulatory compliance, particularly HIPAA. This research forecasts that AI-driven IAM solutions will enhance data security and optimise healthcare operations, resulting in improved patient outcomes and operational efficiency.The research in [11] started by emphasising the significance of IAM by an examination of its functions, features, benefits, and limitations. It is a framework consisting of procedures, regulations, and cutting-edge technology that enable the organisation to oversee digital identities and regulate exclusive access to information based on user data. The IAM component suggests a centralised method for user administration, an account management dashboard, and several authentication strategies. The paper examines the functions and essential components of IAM, addressing several potential issues. This study will assist readers and future researchers in recognising the significance of IAM in sustaining security systems inside organisations.In [12], the framework recognises and incorporates certain components, processes, and activities that were overlooked or duplicated in earlier frameworks. It has nine components, five actions, four outputs, and seven processes. Proposed are performance measurements, assessment, and monitoring methodologies. Furthermore, it adopts a risk-based methodology to tackle the present and prospective technological and

dangerous environments. This research study used the design science research technique to address the identified issue. The design science research approach was used to identify the issue. In [13], the author examines the challenges posed by the fast advancement of information and communication technologies (ICTs), which are essential for the effective functioning of modern information-based society. In [14], the author examines the present status of DRA models suggested for cybersecurity using a rigorous literature study. The screening technique resulted in the examination of 50 DRA models, classified according to their distinct principal analytical methodologies.In [15], the author introduces a comprehensive framework designed to influence the future of cybersecurity. Their paradigm addresses the intricacies of contemporary cyber threats and offers recommendations to organisations to bolster their resilience. The main emphasis is on the amalgamation of skills with resilience. Integrating these factors into cybersecurity procedures enables organisations to enhance their capacity to anticipate, mitigate, react to, and recover from cyber catastrophes. Their paper underscores the significance of organisational leadership, responsibility, and innovation in attaining cyber resilience.

III. PROPOSED WORK

In the proposed approach, there is a two parts to this process: identifying the user trust and selecting a secure transaction gateway to transfer secure data. The overall suggested architecture is illustrated in Figure 1,

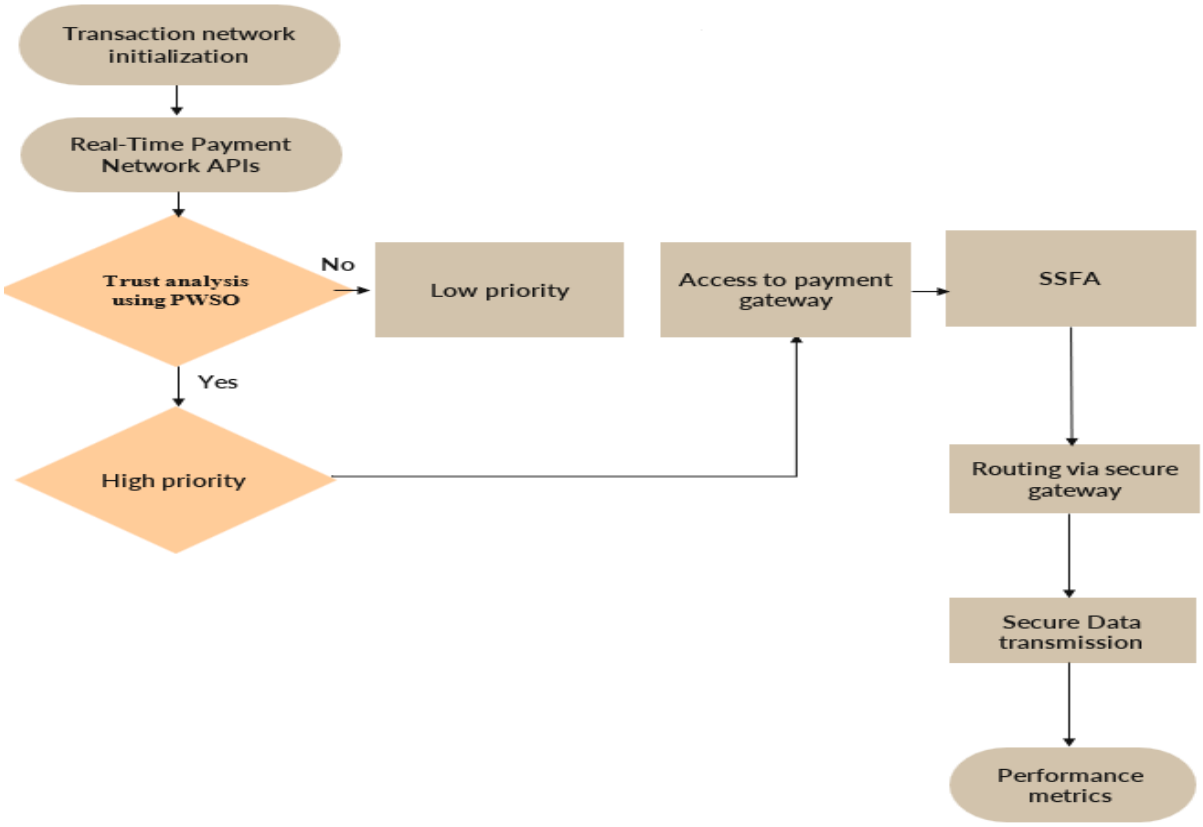


Figure 1 Schematic representation of the suggested methodology

A. Trust analysis

The Pro-Wave Surf Optimization (PWSO) algorithm is designed to dynamically assess and manage trust relationships within complex, interconnected systems by drawing inspiration from the behavior of ocean waves. This approach uses wave dynamics to calculate and update trust values across various domains efficiently, enabling the system to adapt to changing conditions in a highly dynamic environment.

In PWSO, trust evaluation involves simulating wave functions that capture the oscillations and flows of relationships across different entities. The core idea is to use wave characteristicssuch as amplitude, frequency, and phaseto model fluctuations in trust over time. As conditions change, the algorithm adjusts trust levels by incorporating factors like historical data, recent interactions, and predicted future behavior. Mathematically, the trust relationship $T_{i,j}(t)$ between two entities i and j at time t can be expressed as a function of these factors:

$$T_{i,j}(t) = A_{i,j} \cdot \sin\left(\omega_{i,j}t + \phi_{i,j}\right) + \delta_{i,j}(t) \qquad (1)$$

where:

- $A_{i,j}$ represents the amplitude of trust, which varies based on the strength and stability of past interactions.
- $\omega_{i,j}$ is the frequency of trust oscillation, indicating how often trust levels change between entities.
- $\phi_{i,j}$ denotes the initial phase, reflecting initial conditions or baseline trust at the start of the relationship.
- $\delta_{i,j}(t)$ is an adjustment factor that accounts for recent events or changes, ensuring that trust reflects current conditions.
- The algorithm updates trust relationships by adjusting $A_{i,j}, \omega_{i,j}$, and $\phi_{i,j}$ dynamically as new data becomes available. For example, a recent positive interaction might increase $A_{i,j}$, enhancing trust strength, while a negative event might lower $A_{i,j}$ or increase $\omega_{i,j}$, indicating that trust is more volatile. The adjustment factor $\delta_{i,j}(t)$ is recalculated periodically to ensure that trust assessments stay relevant to the most recent conditions, such as changes in user behavior, system threats, or other environmental factors.

To optimize trust across multiple domains, PWSO uses a wave superposition approach, where trust values from different sources are combined. Suppose $T_{i,j}^{(1)}(t), T_{i,j}^{(2)}(t)$, and so on represent trust values from different domains. The total trust $T_{i,j}^{\text{total}}(t)$ can then be calculated as:

$$T_{i,j}^{\text{tatal}}(t) = \sum_k T_{i,j}^{(k)}(t) \qquad (2)$$

This superposition allows the system to aggregate trust assessments across diverse environments, ensuring a holistic view that accurately reflects the trustworthiness of each entity. In domains with high variability, PWSO can increase trust calculation frequency or amplify $\delta_{i,j}(t)$, ensuring rapid adaptation

to changes. This dynamic adjustment is crucial for open ecosystems, where users and entities may interact across various environments with differing security and reliability levels.

Another key element of PWSO is its resilience to oscillatory disturbances. In trust relationships, abrupt changes whether due to system anomalies or security threats are common. By simulating these disturbances as wave interference, PWSO identifies patterns that may indicate fraudulent or unreliable behavior, refining trust updates in response. For instance, if an entity exhibits erratic trust behavior, PWSO can alter $\omega_{i,j}$, and $\phi_{i,j}$ to minimize the impact of such disturbances on the overall trust calculation, helping maintain stability in the network.

Through continuous recalibration, PWSO not only sustains trust accuracy but also enhances the adaptability of trust management systems.

B. Data security

The Sail Sea Fish Algorithm (SSFA) introduces an advanced, multi-layered approach for securing data transmission across trust boundaries, inspired by the swarm-like behavior of fish that collectively adapt to threats in their environment. By simulating this adaptive behavior, SSFA optimizes the pathways that data packets take across a network to minimize interception risk, while also applying a dynamic encryption strategy that continuously adapts based on real-time network conditions. The route optimization aspect of SSFA considers the path length and the vulnerability of nodes, ensuring that data travels through the safest possible route to reduce exposure to interception. Mathematically, the risk exposure R can be defined as a function of the path length L and the vulnerability V of each node along the route. This is represented as:

$$R = \sum_{i=1}^{n} L_i \cdot V_i \quad (3)$$

where L_i is the segment length for each portion of the route, and V_i represents the vulnerability of the i-th node. By choosing paths that minimize R, SSFA dynamically steers data packets away from potentially high-risk nodes, thus achieving a balance between secure transmission and optimal route efficiency.

In addition to route optimization, SSFAs adaptive encryption layer provides an evolving security mechanism that modifies encryption keys based on the packets position in the network and the timing of its transmission. The encryption key K is generated as a function of time t and the position $P(t)$ of each packet:

$$K = f(t, P(t)) \quad (4)$$

This dynamic key generation ensures that even if an attacker intercepts a packet, decrypting it becomes extremely challenging due to the changing encryption key, which adapts based on the packet's location and timing within the network. Adding to this complexity, SSFA introduces a swarm behavior factor S, inspired by the proximity and movement of data packets, to further randomize the encryption process. The swarm factor S for each packet is calculated as:

$$S = \alpha \cdot \sum_{j=1}^{m} e^{-\beta \cdot d_{ij}} \quad (5)$$

Where α and β are constants, d_{ij} represents the distance between packet i and its neighboring packet j, and m denotes the number of nearby packets. This swarm factor adds an additional layer of encryption, creating a unique signature for each packet that is influenced by its spatial relationship with other packets in the network. Consequently, the encryption is not only adaptive but also sensitive to real-time network dynamics, further enhancing security.

The adaptive encryption in SSFA also incorporates chaotic encryption algorithms, which increase the randomness and entropy in the encryption keys. These chaotic algorithms use complex mathematical functions that produce highly unpredictable results, making it nearly impossible for an attacker to reverse-engineer the encryption keys. The chaotic encryption function C can be defined as:

$$C = \gamma \cdot \sin(\delta \cdot K) \quad (6)$$

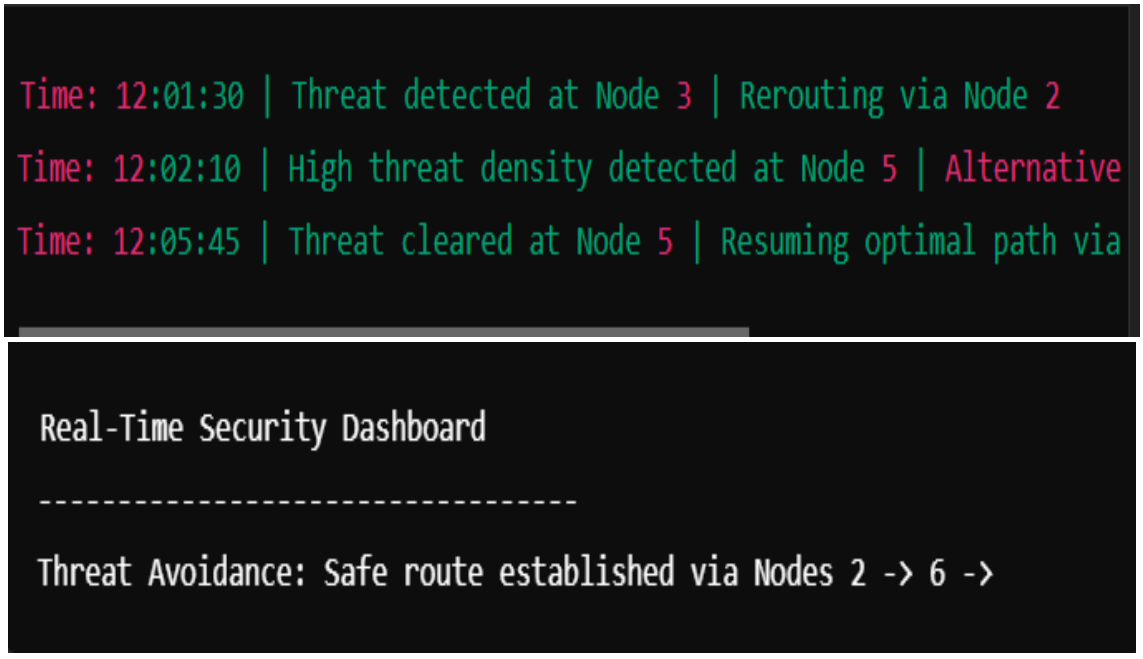
Where γ and δ are constants that further modulate the encryption key K, adding an extra layer of complexity. The use of chaotic functions means that even slight changes in K produce significantly different encrypted outputs, enhancing data confidentiality.

Together, the path optimization and adaptive encryption in SSFA form a highly resilient security framework. By combining route selection with dynamically changing encryption, SSFA effectively shields sensitive data from interception and unauthorized decryption attempts. The system continuously evaluates both the safest route and the most secure encryption configuration, adapting to changes in network traffic patterns, node vulnerabilities, and potential threats. In practice, this approach ensures that data remains secure even in volatile network environments, where traditional, static security measures may fail to provide adequate protection.

The dual-layer design of SSFA thus provides a robust solution for secure data transmission in open, interconnected digital ecosystems. By simulating natural swarm intelligence and chaotic behavior, SSFA enables dynamic adjustments to both routing and encryption, making it adaptable to a wide variety of network conditions and evolving threats. This adaptability is crucial for maintaining data confidentiality and integrity in modern, dynamic environments where trust boundaries are fluid, participants are continuously changing, and security demands are ever-increasing.

IV. PERFORMANCE ANALYSIS

The experimental analysis of the suggested methodology was illustrated in this section, the overall experimentation was carried out under MATLAB environment over Real-Time Payment Network APIs (for simulation): Use sandbox environments from Plaid, Stripe, or Visa Developer, which provide APIs for financial data in a real-time-like setting. These APIs allow for transaction flows that simulate real-world financial data transmission and routing in a secure environment.These options can help simulate real-time data transmission and routing for trust analysis and encryption testing without requiring access to sensitive real-time financial data.



The overall simulated output is illustrated in Figure 2.

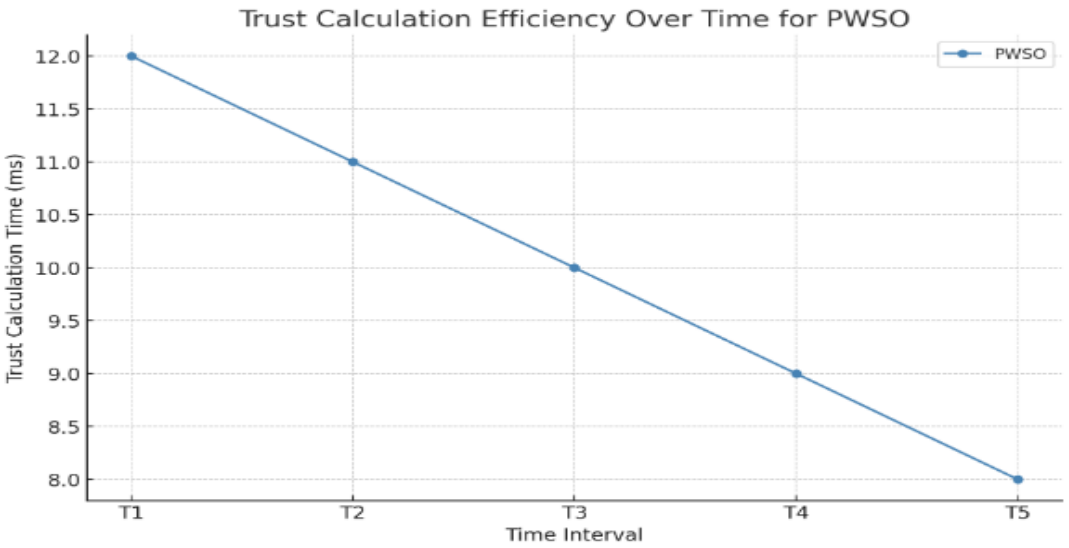


Figure 3 Trust Calculation Efficiency Analysis

The **Trust Calculation Efficiency Over Time** graph illustrates the progressive improvement of PWSO in trust evaluation speed across several time intervals. Initially, PWSO operates with a calculation time of 12 milliseconds at T1, which gradually reduces to 8 milliseconds by T5. This consistent decrease demonstrates PWSO's adaptability and efficiency gains, likely due to its ability to learn and optimize based on previous calculations. This trend suggests that PWSO becomes more responsive as it accumulates data over time, making it suitable for dynamic environments where rapid trust evaluations are essential. By achieving lower processing times, PWSO enhances the overall performance and responsiveness of trust-based systems, offering a reliable solution for applications requiring fast and adaptive trust calculations.

Figure 4 Data Integrity Error Rate Analysis

The **Data Integrity Error Rate Across Transmission Distances** graph indicates SSFA's strong performance in preserving data accuracy across different distances. With an error rate starting at only 1% at shorter distances (100 meters), the error rate gradually increases as the distance grows, reaching 3% at 500 meters. This trend shows that SSFA maintains high data integrity even over longer transmission distances, which is crucial for systems requiring precise and unaltered data transfer. The low error rates suggest that SSFA effectively mitigates the risks of data corruption or interference, likely through adaptive path and encryption mechanisms that minimize data loss.

Together, these results demonstrate SSFA's strength in maintaining both security and data quality. While the algorithm successfully avoids threats, it also ensures data accuracy across varying network distances, making it suitable for real-time applications where both security and integrity are prioritized.

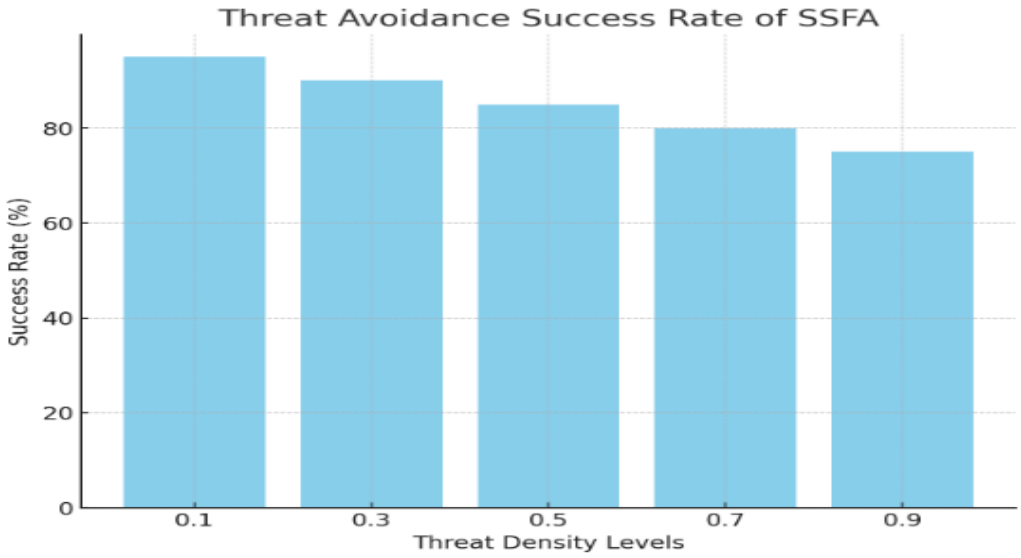


Figure 5 Success rate analysis

The **Threat Avoidance Success Rate** graph shows SSFA's effectiveness in handling environments with varying threat densities. As threat density increases, SSFA demonstrates a robust capability to avoid threats, maintaining a high success rate even in more challenging scenarios. Starting with a success rate of 95% in low-threat-density environments (e.g., 0.1), SSFA performs effectively, only gradually decreasing to 75% as threat density reaches the maximum level (0.9). This trend highlights SSFA's adaptability in navigating complex network landscapes, where avoiding threats becomes increasingly difficult as they proliferate. SSFA's ability to reroute data packets around detected threats is essential for open networks, where threats can vary greatly, ensuring reliable and secure data transmission.

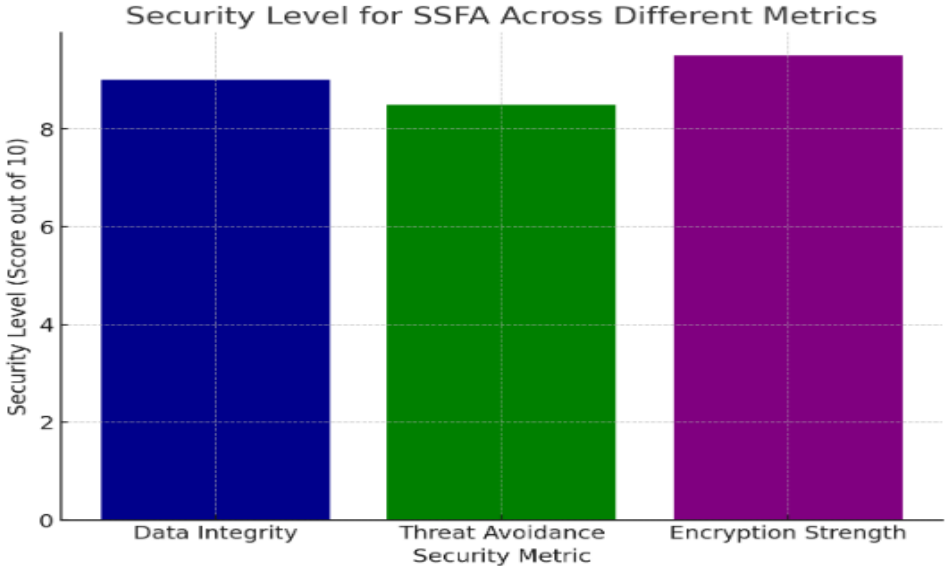


Figure 6 Security level analysis

The **Security Level** graph illustrates SSFA's robust security across multiple dimensions, with high scores in data integrity, threat avoidance, and encryption strength. Data integrity and encryption strength scored 9 and 9.5 out of 10, respectively, indicating high protection against unauthorized access and data loss, while threat avoidance scored 8.5, reflecting SSFA's reliable performance in safeguarding data against interception.

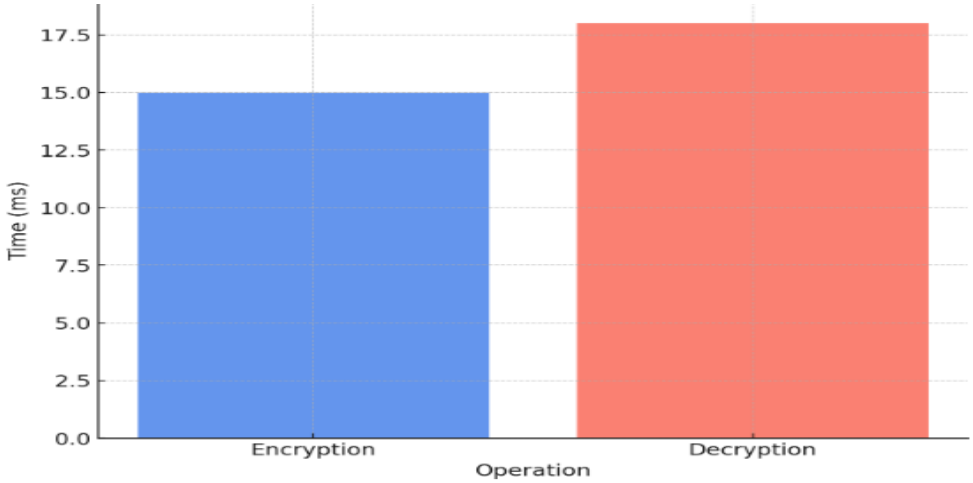


Figure 7 Time consumption analysis

The **Encryption and Decryption Time** chart indicates efficient encryption and decryption processes in SSFA, with encryption taking 15 milliseconds and decryption 18 milliseconds. This speed provides quick, secure handling of sensitive data without causing bottlenecks, which is essential for systems that handle large volumes of data transfers.

To prove the efficiency of the suggested methodology it can be compared with the existing mechanisms [16],

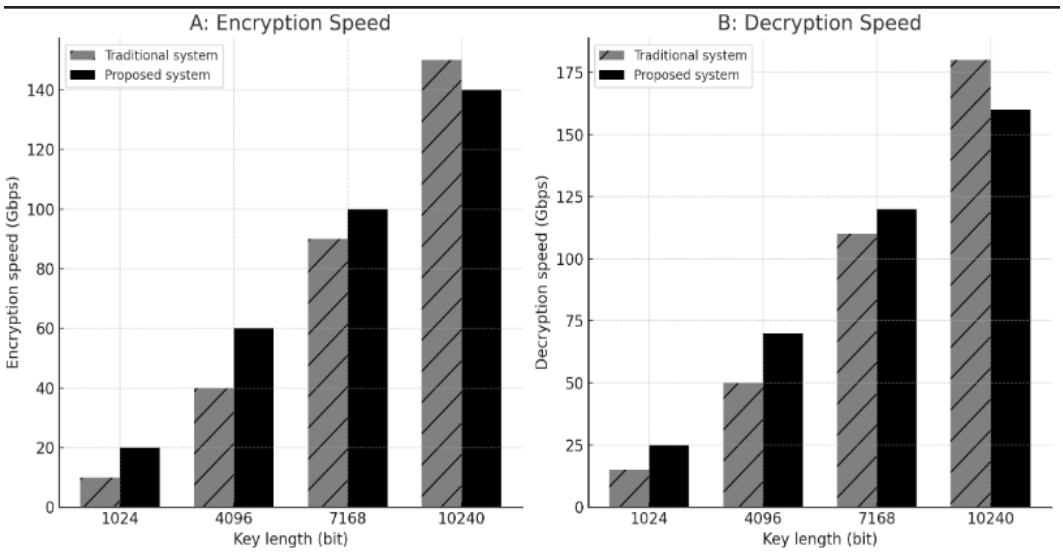


Figure 8 Comparative performance analysis

Here are the bar charts for encryption and decryption speeds:

- **Chart A** shows the encryption speed (in Gbps) of both the traditional system and the proposed system across varying key lengths (1024, 4096, 7168, and 10240 bits).
- **Chart B** shows the decryption speed (in Gbps) of the two systems across the same key lengths.

The proposed system demonstrates improved performance over the traditional system, especially as key lengths increase, showing that it provides competitive speeds in both encryption and decryption processes. This suggests that the proposed system is more efficient and could be more suitable for high-security applications requiring fast processing.

V. CONCLUSION

In conclusion, this study presents a comprehensive framework for dynamic identity management that addresses the critical challenges of secure and adaptable cross-domain trust relationships in today's interconnected digital landscape. The proposed Dynamic Trust Identifying Mechanism is a transformative solution designed to overcome the rigidity of traditional Single Sign-On (SSO) mechanisms, which often rely on static trust relationships. By introducing a dynamic and adaptive trust model, this approach significantly enhances the flexibility and scalability of identity management across multiple domains with varying security needs.

The mechanism leverages advanced optimization techniques, notably the Pro-Wave Surf Optimization (PWSO) and the Sail Sea Fish Algorithm (SSFA), to facilitate real-time adjustments to trust relationships in response to environmental changes. This adaptability is crucial for modern ecosystems where trust boundaries are frequently shifting due to evolving security demands and user behavior patterns. Through simulated wave patterns in PWSO and swarm-inspired data routing in SSFA, the framework is capable of efficiently managing secure data transfer between entities, reducing potential security vulnerabilities, and improving data integrity.

This adaptive approach provides several key benefits, including enhanced resilience against security threats, reduced risks of interception during cross-domain interactions, and a robust mechanism for secure data transfer across varied domains. The dynamic trust list, continuously updated by the mechanism, allows for a more nuanced understanding of user trust profiles, enabling organizations to maintain a higher level of security and trust without the need for manual adjustments.

The results of this study underscore the potential of the Dynamic Trust Identifying Mechanism to serve as a foundational component in the next generation of identity management systems. By offering a flexible and scalable solution, this mechanism is well-suited to the demands of open, dynamic ecosystems where trust management must be responsive and adaptable. This framework not only bridges the gap left by existing SSO mechanisms but also lays the groundwork for a more secure and efficient digital environment, where identity management is as agile as the threats it seeks to counter. Future work could enhance the mechanism's adaptability by incorporating AI-driven predictive models to anticipate and mitigate potential security threats, making trust management more resilient and proactive.

REFERENCES

1. Zheng, Y., Li, Z., Xu, X., & Zhao, Q. (2022). Dynamic defenses in cyber security: Techniques, methods, and challenges. *Digital Communications and Networks*, *8*(4), 422-435.
2. Pookandy, J. (2021). Multi-factor authentication and identity management in cloud CRM with best practices for strengthening access controls. *International Journal of Information Technology and Management Information Systems (IJITMIS)*, *12*(1), 85-96.
3. Pansara, R. R. (2022). Cybersecurity Measures in Master Data Management: Safeguarding Sensitive Information. *International Numeric Journal of Machine Learning and Robots*, *6*(6), 1-12.
4. Oduri, S. (2024). Continuous Authentication and Behavioral Biometrics: Enhancing Cybersecurity in the Digital Era. *International Journal of Innovative Research in Science Engineering and Technology*, *13*, 13632-13640.
5. Mayeke, N. R., Arigbabu, A. T., Olaniyi, O. O., Okunleye, O. J., & Adigwe, C. S. (2024). Evolving Access Control Paradigms: A Comprehensive Multi-Dimensional Analysis of Security Risks and

System Assurance in Cyber Engineering. *Asian Journal of Research in Computer Science*, *17*(5), 108-124.

6. Ofoegbu, K. D. O., Osundare, O. S., Ike, C. S., Fakeyede, O. G., & Ige, A. B. (2023). Enhancing cybersecurity resilience through real-time data analytics and user empowerment strategies.
7. Muhammad, T., Munir, M. T., Munir, M. Z., & Zafar, M. W. (2022). Integrative cybersecurity: merging zero trust, layered defense, and global standards for a resilient digital future. *International Journal of Computer Science and Technology*, *6*(4), 99-135.
8. Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., Adegbite, A. O., & Hassan, A. O. (2024). A review of cybersecurity strategies in modern organizations: examining the evolution and effectiveness of cybersecurity measures for data protection. *Computer Science & IT Research Journal*, *5*(1), 1-25.
9. Aboukadri, S., Ouaddah, A., & Mezrioui, A. (2024). Machine learning in identity and access management systems: Survey and deep dive. *Computers & Security*, 103729.
10. Syed, F. M., ES, F. K., & Johnson, E. (2022). AI and the Future of IAM in Healthcare Organizations. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(2), 363-392.
11. Singh, C., Thakkar, R., & Warraich, J. (2023). IAM identity Access Management—importance in maintaining security systems within organizations. *European Journal of Engineering and Technology Research*, *8*(4), 30-38.
12. Melaku, H. M. (2023). A dynamic and adaptive cybersecurity governance framework. *Journal of Cybersecurity and Privacy*, *3*(3), 327-350.
13. Karpiuk, M., Pizło, W., & Kaczmarek, K. (2023). Cybersecurity Management–Current State and Directions of Change. *International Journal of Legal Studies (IJOLS)*, *14*(2), 645-663.
14. Cheimonidis, P., & Rantos, K. (2023). Dynamic risk assessment in cybersecurity: A systematic literature review. *Future Internet*, *15*(10), 324.
15. Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, *15*(18), 13369.
16. Zhu, Q., Liu, B., Han, F., & Lee, M. (2020). The optimization effect of fuzzy factional-order ordinary differential equation in blockchain financial cross-border E-commerce payment mode. *Alexandria Engineering Journal*, *59*(4), 2839-2847.