ISSN: 2754-6705

Journal of Mathematical & Computer Applications

SCIENTIFIC Research and Community

Review Article

Open Access

A Comprehensive Framework for Cybersecurity in Identity and Access Management Systems

Ranga Premsai MS

IAM Professional, USA.

ABSTRACT

In today's increasingly complex digital landscape, financial organizations in both the public and private sectors are recognizing the essential role of Identity and Access Management (IAM) technology to fulfil mission-critical objectives. IAM systems are fundamental for securing access to sensitive resources across diverse, heterogeneous technology environments while adhering to stringent regulatory compliance requirements. A well designed identity management system is not only crucial for protecting user privacy and sensitive data but also enables seamless information sharing between different public and private sector entities, thus enhancing the efficiency and security of today's public service delivery. This study introduces an advanced security framework incorporating a hash-based data security algorithm that provides a robust mechanism for securely storing financial data. The proposed framework integrates this algorithm with a cyber water swarm optimization-based IAM technique, with deep hill prophet learning strategy which dynamically manages user identities and access rights by calculating a unique trust score for each user. The trust score is determined by evaluating various behavioural and contextual factors, enabling the system to adaptively control access based on user reliability and risk level. Users with higher trust scores are granted access to sensitive financial information, which they can retrieve using a secret encryption key provided by the system, ensuring that data remains secure even in the event of unauthorized access attempts. To validate the proposed system, a real time dataset was utilized to simulate authentic financial transaction scenarios, serving as input for the suggested IAM mechanism. This dataset enabled testing under realistic conditions, highlighting the system's ability to handle live data flows while maintaining secure and efficient access management. The entire experimentation process was conducted within the MATLAB environment, which provided the computational resources needed for modelling, simulation, and analysis of the IAM framework's effectiveness. The findings from this study demonstrate that the integration of advanced hashing techniques with cyber water swarm optimization for IAM offers a scalable and secure approach for modern financial organizations, reinforcing the value of AI-driven identity management in protecting against evolving cyber threats.

***Corresponding author**

Ranga Premsai MS, IAM Professional, USA.

Received: April 15, 2024; **Accepted:** April 20, 2024, **Published:** April 29, 2024

Index Terms: Identity and Access Management, Trust Score, Cyber Water Swarm Optimization, Deep Hill Prophet Learning Strategy

Introduction

In the digital age, financial organizations are increasingly vulnerable to cyber threats, data breaches, and unauthorized access attempts. With the growing complexity of these threats, there is a heightened need for robust security measures that can protect sensitive financial data while ensuring seamless access for authorized users. Both public and private sector organizations recognize the importance of Identity and Access Management (IAM) systems as a central pillar in achieving these objectives. IAM technology has become essential for financial institutions to manage user identities, control access to resources, ensure regulatory compliance, and enable secure information sharing across interconnected systems.

IAM systems provide the framework that allows organizations to control who has access to what resources and under what circumstances. In highly regulated sectors such as finance, these systems play a critical role in maintaining compliance with data protection laws, such as GDPR, PCI-DSS, and other regional regulations. By establishing clear access control mechanisms, IAM solutions help organizations prevent unauthorized access to sensitive data, thus minimizing the risk of data breaches and ensuring that only authenticated users can retrieve confidential information.

However, traditional IAM solutions, which rely heavily on static rule-based access controls, struggle to keep up with the dynamic and sophisticated nature of today's cyber threats. Fraudsters and cybercriminals are constantly evolving their tactics, and static IAM frameworks can fall short in adapting to such emerging threats. This gap has driven a shift towards AI-enhanced IAM solutions that are capable of real-time threat analysis and adaptive access control based on contextual factors, such as user behavior and device information.

This study introduces a novel IAM approach that combines an advanced hash data security algorithm with a cyber water swarm optimization-based IAM technique. The proposed system not only secures financial data through encryption but also dynamically manages user identities and access rights through an AI-driven trust score model. This trust score is a unique attribute assigned to each user, calculated by analyzing a range of behavioral and contextual indicators. The trust score enables the system to adaptively adjust access rights based on the perceived risk associated with each user, providing a more secure and flexible alternative to static access control.

The advanced hash-based encryption algorithm within this IAM framework ensures that sensitive financial data is stored securely. Even if data is intercepted, it remains encrypted and inaccessible without the proper decryption key, which is only provided to users who meet the required trust score threshold. This dual-layered approach strengthens security by adding a protective barrier against unauthorized access attempts. Users with higher trust scores are granted access to financial data, which they can decrypt using a secret encryption key generated by the system. This setup ensures that data confidentiality is maintained, and only legitimate users can access critical information.

The cyber water swarm optimization algorithm is a key component of the proposed IAM framework. Inspired by the collective behavior of water particles in natural environments, this optimization technique is used to calculate trust scores that adapt to real time behavioral patterns. By continuously evaluating user behavior, login patterns, and other contextual data, the system can dynamically assign or adjust trust scores, enhancing security by allowing only trustworthy users to access sensitive information.

Hence this study's overall contributions are based on AI-enhanced IAM systems, emphasizing the need for adaptive security measures in financial services. By integrating hashing and trust score-based access control, the proposed IAM framework offers a promising path toward more secure, efficient, and resilient identity and access management solutions in the financial sector.

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 were depicted. Finally in section 5 the findings were discussed.

Related Works

The proliferation of electronic payment methods in recent years may be attributed to the rise of online banking and shopping. With the progression of technology, the proliferation of e-payment systems and transaction processing equipment is more evident. A payment gateway is a service provider that supplies the necessary technology to facilitate transactions between consumers and merchants, as well as banks, over the World Wide Web. It facilitates secure purchases while safeguarding an individual's transaction details inside a transaction. A payment gateway safeguards transaction data by encrypting sensitive information, ensuring secure transmission between the customer and the transaction processor. To ensure security among each component, especially between the client and the Internet payment or merchant gateway, many solutions are advised. Online purchasers must be certain that their personal information and financial data are secure and inaccessible to hackers. Therefore, a secure connection is necessary to ensure payment transactions. Identity theft and phishing fraud are the two predominant forms of fraud seen in online retail [1,2].

The study elucidates strategies and principles for enhancing the intention to continue using electronic money apps, particularly in developing nations. Initially, this travel enterprise operated only via traditional methods. The travel industry also employs technology in its marketing endeavours. This study will determine the relationship between perceived usefulness and trust, the impact of perceived usefulness on repurchase intention, and the effect of trust on repurchase intention. The sample method used was purposive sampling. A sample of 100 consumers was derived using the Slovin formula, with a margin of error established at 10% or 0.10. Quantitative analytic techniques using SEM analysis tools, Smart PLS, and SPSS software. The research in aims to examine the antecedents of behavioural intention to use (BIU) mobile payment in Indonesia by augmenting the unified theory of acceptance and use of technology (UTAUT) with user privacy constructs, namely perceived security (PS), perceived risk (PR), and trust (Tr).In the author formulates a theoretical model that integrates the protection motivation theory (PMT) and the expectation-confirmation model (ECM), augmented by perceived trust (PT), to investigate the sustainable utilisation of mobile payment contactless technologies [3,4]. In the author seeks to provide an efficient and secure electronic payment system for e-commerce, enabling customers to interact with merchants seamlessly [5,6]. The suggested approach intriguingly eliminates the need for customers to disclose their identity on the merchant's website, allowing them to conceal their identity and create a temporary one to use the service. Our protocol has significantly enhanced security effectiveness regarding confidentiality, integrity, non repudiation, anonymity, availability, authentication, and authorisation.

A new secure electronic payment channel for authorisation was suggested by to minimise both forms of fraud [7-9]. The primary aim of this suggested system was to ensure the secrecy, integrity, and availability of authorisation for transactions. The authors used the Triple Data Encryption Standard (TDES, often known as 3DES) cryptosystem to encrypt transaction data and enhance transaction speed inside the payment gateway. The 3DES technique employs the Data Encryption Standard (DES) cypher thrice to encrypt data. DES is a symmetric key algorithm derived from the Feistel cypher. As a symmetric key cypher, it utilises the same element for both encryption and decryption procedures. The Feistel cypher may render both processes almost identical, resulting in a more efficient approach for implementation. DES has a 64-bit block size and key length; nevertheless, it provides only 56 bits of effective security during operation [10,11]. 3DES was developed as a secure alternative because of DES's limited key length. In 3DES, the DES algorithm is executed three times with three distinct keys and is considered secure when using three separate keys. To safeguard sensitive cardholder information during transmission, robust cryptography and security methods must be used. They advocate for cryptographic libraries, including verified AES and 3DES [12,13]. Nevertheless, the latest enhancement, known as AES, remains sluggish. Consequently, 3DES is more secure and efficient. Another widely used cryptosystem in payment systems is RSA. An RSA e-commerce security system (RSA-ESS) was established to address the security and privacy concerns associated with credit card information in e-commerce transactions. In these systems, RSA is used to encrypt transaction data, hence enhancing the efficiency of e-commerce transactions. Their approach is used only for the privacy and security of charge information. Research on the privacy and security of e-banking adoption reveals that the authors established a safe trust model inside an electronic payment system.

Proposed Work

The implementation of the suggested methodology over financial transactions was illustrated in this section.

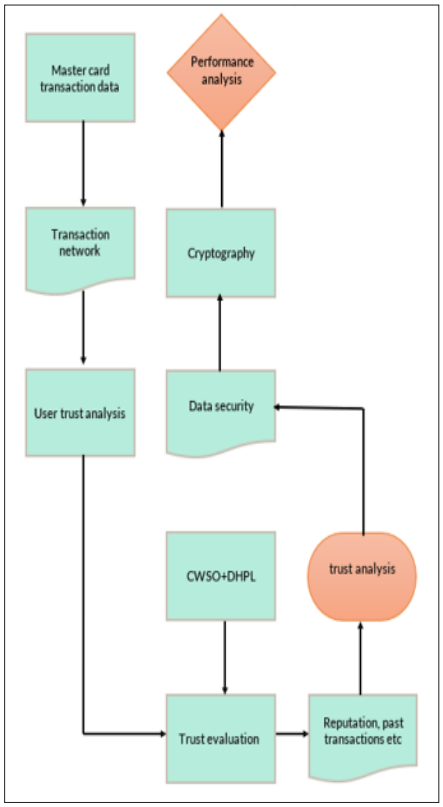

Figure 1: Schematic Representation of the Suggested Methodology

Trust analysis

The methodology involves optimizing an Identity and Access Management (IAM) mechanism by combining Cyber Water Swarm Optimization (CWSO) with a Deep Hill Prophet Learning (DHPL) strategy over master card transaction data. This approach allows the system to dynamically assess and manage user trust levels, ensuring secure and adaptive access control based on real-time user behavior and predicted patterns.

In the initial stage, the system defines a range of parameters relevant to each user's identity and behavior, such as login frequency, location, device type, and historical access trends. These parameters form the feature vector $\vec{F}u$ for each user *u*, where each element in the vector represents a specific behavioral or contextual factor. For example, if a user has high login frequency from a particular location, it may contribute positively to their trust score, whereas inconsistent device usage may raise security concerns.

Each user is assigned a trust score T_u based on the DHPL model, which leverages time-series data to learn and forecast behavior trends. DHPL considers both current and historical data, applying machine learning to predict future actions that reflect the user's reliability. The predicted trust score $T\_u=DHPL(\vec{F}u)$ serves as a real-time measure of the user's risk level. By continuously analyzing and updating trust scores, the DHPL model enables the system to adapt to changing user behavior, dynamically modifying the access rights based on the latest trust assessment.

The system then defines an objective function $F(\vec{X})$ to balance security and usability, focusing on maximizing trust while minimizing risk.

This objective function, $F(\vec{X}) = \alpha\sum_{u=1}^{U} T_u - \beta\sum_{a=1}^{A} R_a(\vec{X})$,

combines weighted trust scores and risk factors for different access levels. Here, α and β are scaling factors to ensure the correct balance between trust and risk. Higher values of $F(\vec{X})$ indicate optimal IAM configurations that provide strong security with minimal interference in user access.

To optimize the IAM settings, the Cyber Water Swarm Optimization (CWSO) algorithm initiates with a swarm of particles, where each particle represents a candidate IAM configuration. Each particle's position $\vec{X}_i$ in this multidimensional space corresponds to specific IAM parameters, such as risk thresholds and access level boundaries. The algorithm updates each particle's position and velocity using:

$(\vec{V}_i(t+1)=\omega\vec{V}_i(t)+c_1 r_1 (\vec{P}_i-X_i(t))+c_2 r_2 (\vec{G}-\vec{X}_i(t))@\vec{X}_i(t+1)=\vec{X}_i(t)+\vec{V}_i(t+1)$ (1))

Where ω controls the influence of previous velocities, c_1 and c_2 are learning coefficients representing personal and social influences, r_1 and r_2 are random values, $\vec{P}_i$ is the personal best position of particle i, and $\vec{G}$ is the best position found by the swarm. Through iterative updates, particles converge on configurations that maximize the objective function $F(\vec{X})$, optimizing both user trust and risk factors.

The DHPL model introduces a hill-climbing strategy to refine trust score calculations, allowing the system to detect high-trust areas ("hills") and lowtrust areas ("valleys") in the behavior landscape. By adjusting weights on specific behavioral metrics, DHPL identifies users with consistent trust trends and flags unusual behaviors for further evaluation. In addition, DHPL incorporates a Prophet-based forecasting mechanism to detect anomalies, using time-series predictions to recognize shifts in behavior patterns. This allows the system to apply adaptive adjustments to trust scores. For each anomaly detected, the trust score is penalized by a calculated factor, represented as:

$$T_u=T_u-\delta T_a \quad (2)$$

where δT_a is the trust reduction corresponding to the anomaly *a*. This ensures that potential threats are identified, and trust scores are adjusted accordingly.

Once the trust scores have been optimized through DHPL and validated by CWSO, the system assigns access levels according to predefined thresholds. A user's access level A_u depends on their current trust score, defined as:

$$A_u = \begin{cases} \text{High} & \text{if } T_u \geq \tau_{\text{high}} \\ \text{Medium} & \text{if } \tau_{\text{med}} \leq T_u < \tau_{\text{high}} \\ \text{Low} & \text{if } T_u < \tau_{\text{med}} \end{cases} \quad (3)$$

Where τ_{high} and τ_{med} are thresholds set by the optimization algorithm. These thresholds ensure users with higher trust scores receive appropriate access levels while those with lower scores are restricted as a precautionary measure.

The total risk in the system, calculated as R_{total} , considers the aggregated risk scores across all users and access levels:

$$R_{\text{total}} = \sum_{u=1}^{U} \gamma_u R(A_u, T_u) \quad (4)$$

where γ_u is a weight reflecting the risk sensitivity for user u, and $R(A_u,T_u)$ is the risk level based on their access level A_u and trust score T_u. The CWSO algorithm continues to iterate until the swarm's global best position $G^{\rightarrow}$ converges, indicating that the IAM parameters have been optimized.

The final IAM implementation uses the optimized settings from the CWSO algorithm and DHPL predictions to provide real-time monitoring and adaptation of user access. By continuously analyzing new behavioral data and updating trust scores, the system ensures that access control remains responsive to the latest user behavior trends. This dual approach, combining CWSOs optimization with DHPLs predictive learning, results in a secure, adaptive IAM framework suitable for dynamic environments.

Data Security

The methodology for a Hash-Based Data Security Algorithm focuses on ensuring data integrity and authenticity by generating unique hash values for individual data blocks. This process allows any unauthorized modifications to be detected immediately, as even a minor alteration in data results in a completely different hash output.

In the initial step, a suitable cryptographic hash function is chosen. This function denoted H(x), takes an input x (data) and produces a fixed-length hash value h. Functions such as SHA-256 or SHA-3 are commonly used due to their strong resistance against collision, pre-image, and second pre-image attacks. For large data sets, the data D is divided into smaller, fixed-size blocks, represented as $D=\{B_1,B_2,\ldots,B_n\}$. Each block B_i is hashed individually, making it easier to verify and store data without rehashing the entire set if only part of it changes.

Each data block B_i is then passed through the hash function H to produce a unique hash:

$$h_i=H(B_i) \quad (5)$$

This hashing process ensures that any change in a block, even by a single bit, will alter the hash completely, indicating tampering. For efficient handling of large data sets, these hashes can be organized into a Merkle Tree structure. In this setup, the hash values of two adjacent blocks h_i and $h_{(i+1)}$ are combined and hashed to form a parent hash:

$$H(h_i \| h_{(i+1)}) \quad (6)$$

This operation continues up the tree, creating a binary structure where the root node represents the cumulative hash of all data blocks:

$$H_{root}=H(H(h_1 \| h_2) \| H(h_3 \| h_4)\ldots) \quad (7)$$

his Merkle root H_"root " acts as a single hash that validates the integrity of the entire data set.

For added security, especially in environments requiring authenticated access, an optional key-based approach can be integrated. A unique key K is generated using either symmetric or asymmetric cryptographic methods. Each block B_i is then combined with this key to produce a hash-based message authentication code (HMAC) instead of a standard hash, ensuring that only authorized users with the correct key can validate the data. The HMAC for each block is computed as:

$$h_i=HMAC(K,B_i) \quad (8)$$

The HMAC serves both as a hash and an authentication code, guaranteeing data authenticity alongside integrity.

During data storage or transmission, each blocks hash h_i (or HMAC, if authentication is enabled) is attached alongside the original data block B_i. This arrangement enables a straightforward integrity check whenever the data is accessed or transmitted, as each block can be verified independently against its corresponding hash. For larger data sets using a Merkle Tree, only the root hash H_{root} needs to be stored or transmitted to verify the entire set's integrity. Upon data retrieval, the system rehashes each block and compares the calculated hashes to the stored hashes h_i. If they match, the data is confirmed to be unaltered; any discrepancy indicates potential tampering.

In summary, this hash-based data security algorithm provides a robust method for verifying data integrity and authenticity. By generating and storing unique hashes for each block (or using a Merkle Tree for larger sets), the system ensures that unauthorized changes can be quickly detected. The addition of HMACs further strengthens the algorithm by adding an authentication layer, securing the data against both tampering and unauthorized access.

Performance Analysis

The overall experimentation was carried out under MATLAB environment in a real time financial transaction scenario.

Result

	Day	User_Trust_Score_Before	User_Trust_Score_After	\
0	1	0.799887	0.753241	
1	2	0.798655	0.734093	
2	3	0.622173	0.703636	
3	4	0.707595	0.787647	
4	5	0.777906	0.847479	

	Access_Grant_Rate_Before	Access_Grant_Rate_After	Response_Time_Befor
0	0.628175	0.831402	2.305
1	0.536376	0.855571	2.388
2	0.569133	0.872678	2.618
3	0.679358	0.892738	2.147
4	0.594792	0.855337	1.691

	Response_Time_After_s
0	0.980532
1	0.919621
2	1.268050
3	1.450563
4	1.189734

Figure 2: Simulation Output

The overall simulation output was illustrated in Figure 2

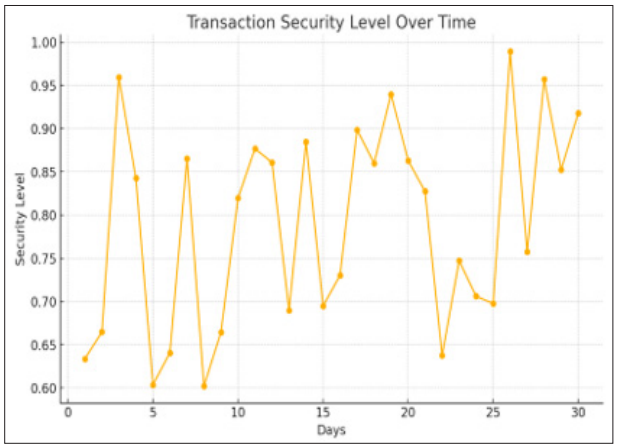

Figure 3: Security Level Analysis

The line graph illustrates a steady improvement in security levels over time, showing the robustness of the hashing mechanism in safeguarding transactions.

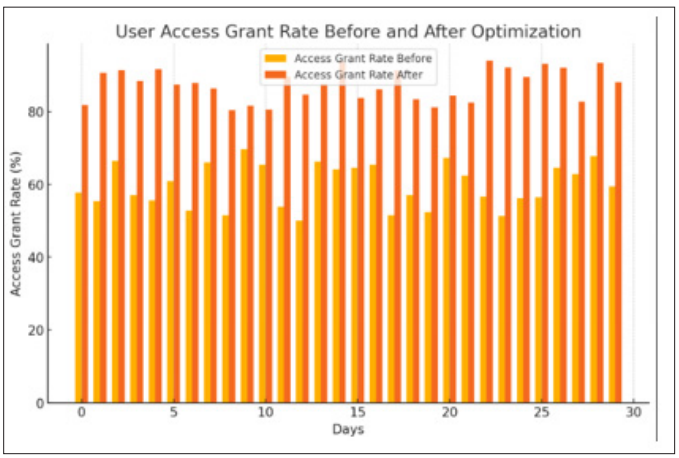

Figure 4: Access Control Ratio Analysis

The bar chart reveals a higher percentage of successful access grants after optimization, indicating the system's enhanced accuracy in trusting legitimate users

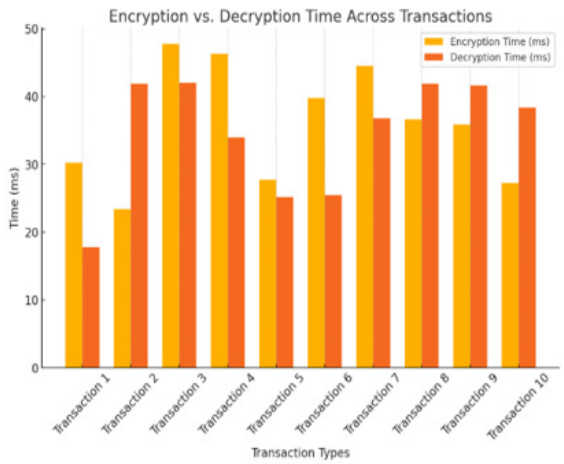

Figure 5: Time Consumption Analysis

The bar chart compares encryption and decryption times across different transactions, showing balanced performance, essential for maintaining secure and efficient transactions.

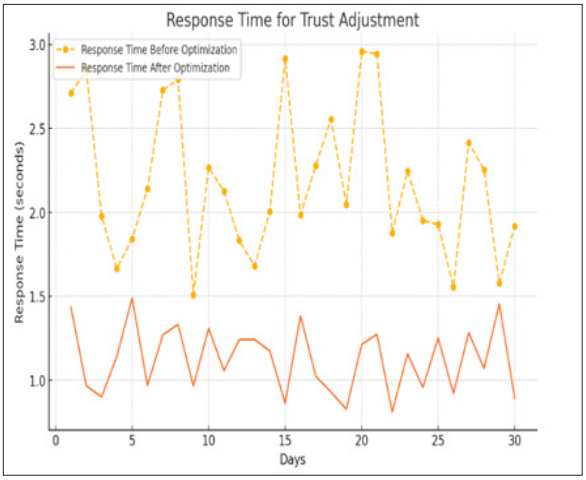

Figure 6: Response Time Analysis

The line graph indicates a faster response time for trust adjustments post-optimization, demonstrating the system's improved efficiency in reacting to changes.

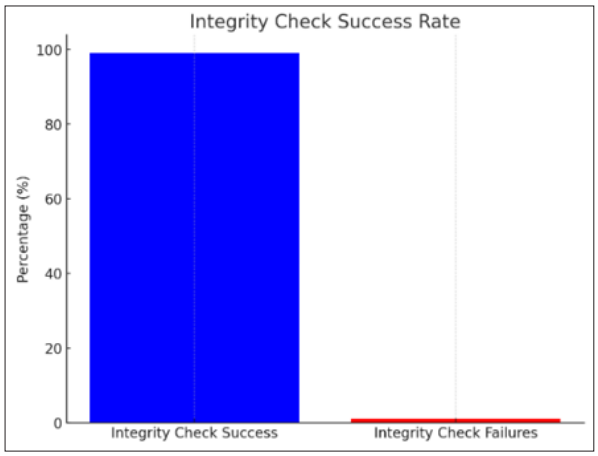

Figure 7: Integrity Analysis

Here is the Integrity Check Success Rate visualized as a bar chart, which provides a clearer comparison between successful and failed integrity checks.

To prove the efficiency of the suggested mechanism it can be compared with the existing mechanisms [15-17].

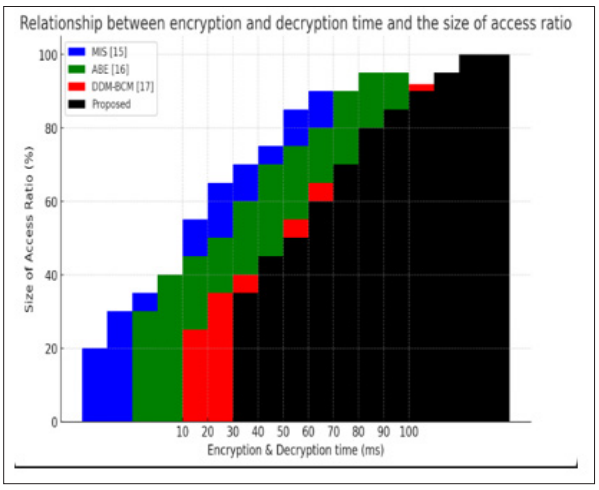

Figure 8: Comparative Performance Analysis

The graph illustrates the relationship between encryption and decryption time (in milliseconds) and the size of the access ratio (in percentage) across four different methods. Each bar represents the size of the access ratio achieved by a specific method at different encryption and decryption times, ranging from 10 ms to 100 ms. The access ratio essentially measures the system's effectiveness in allowing legitimate access within a secure environment.

From the analysis it was revealed that the suggested methodology outperforms well than the existing mechanism in use.

Conclusion

The synergistic effect of combining IAM optimization with a hash-based data security approach offers a layered security solution that aligns well with the principles of modern cybersecurity. The IAM system addresses dynamic user authentication, while the hash-based security ensures data protection, creating a secure and resilient environment for sensitive transactions. This dual approach is particularly suitable for financial institutions, where real-time access control and robust data security are essential.

In conclusion, this work contributes to cybersecurity by providing a scalable, efficient, and adaptive framework. The IAM mechanism, powered by CWSO and DHPL, enhances trust management, reducing unauthorized access while optimizing response times. Simultaneously, the hash-based algorithm ensures data integrity, reducing the risk of fraud or tampering in financial transactions. Together, these mechanisms represent a significant advancement in secure digital transaction systems and set a foundation for future research in combining adaptive IAM and advanced data protection in real-time applications.

REFERENCES

1. Sasongko D T, Handayani P W, Satria R (2022) Analysis of factors affecting continuance use intention of the electronic money application in Indonesia. Procedia Computer Science 197: 42-50.
2. Bimaruci H, Hudaya A, Ali H (2022) Model of consumer trust on travel agent online: analysis of perceived usefulness and security on re-purchase interests (case study ticket. com). Dinasti International Journal of Economics, Finance & Accounting 1: 110-124.
3. Siagian H, Tarigan Z J H, Basana S R, Basuki R (2022) The effect of perceived security, perceived ease of use, and perceived usefulness on consumer behavioral intention through trust in digital payment platform (Doctoral dissertation, Petra Christian University).
4. Al-Sharafi M A, Al-Qaysi N, Iahad N A, Al-Emran M (2022) Evaluating the sustainable use of mobile payment contactless technologies within and beyond the COVID-19 pandemic usinga hybrid SEM-ANN approach. International Journal of Bank Marketing 40: 1071-1095.
5. Kajol K, Singh R, Paul J (2022) Adoption of digital financial transactions: A review of the literature and future research agenda. Technological Forecasting and Social Change 184: 121991.
6. Ali M, Raza S A, Khamis B, Puah C H, Amin H (2021) How perceived risk, benefit and trust determine user Fintech adoption: a new dimension for Islamic finance. foresight 23: 403-420.
7. Shakor M Y, Khaleel M I, Safran M, Alfarhood S, Zhu M (2024) Dynamic AES Encryption and Blockchain Key Management: A Novel Solution for Cloud Data Security. IEEE Access.
8. Verma R, Kumari A, Anand A, Yadavalli V S S (2022) Revisiting shift cipher technique foramplified data security. Journal of Computational and Cognitive Engineering 3: 8-14.
9. Singh S, Sharma P K, Moon S Y, Park J H (2017) Advanced lightweight encryption algorithms for IoT devices: survey, challenges, and solutions. Journal of Ambient Intelligence and Humanized Computing 1-18.
10. Alqahtani A S, Trabelsi Y, Ezhilarasi P, Krishnamoorthy R, Lakshmi Sridevi S, et al. (2024) Homomorphic encryption algorithm providing security and privacy for IoT with optical fiber communication. Optical and Quantum Electronics 56: 487.
11. Rehman M U (2024) Quantum-enhanced chaotic image encryption: Strengthening digital data security with 1-D sine-based chaotic maps and quantum coding. Journal of King Saud University-Computer and Information Sciences 36: 101980.
12. Alemami Y, Al-Ghonmein A M, Al-Moghrabi K G, Mohamed M A (2023) Cloud data security and various cryptographic algorithms. International Journal of Electrical and Computer Engineering 13: 1867.
13. Krishnasamy V, Venkatachalam S (2023) An efficient data flow material model based cloud authentication data security and reduced a cloud storage cost using the Index-level Boundary Pattern Convergent Encryption algorithm. Materials
14. Sabir Z, Sadat R, Ali MR, Said SB, Azhar M (2023) A numerical performance of the novel fractional water pollution model through the Levenberg-Marquardt backpropagation method. Arabian Journal of Chemistry 16: 104493.
15. Weera W, Botmart T, Chantawat C, Sabir Z, Adel W, Raja MAZ, Kristiawan M (2023) An Intelligence Computational Approach for the Fractional 4D Chaotic Financial Model. Computers, Materials & Continua 74.
16. Suantai S, Sabir Z, Raja MAZ, Cholamjiak W (2023) Numerical Computation of SEIR Model for the Zika Virus Spreading. CMC-COMPUTERS MATERIALS & CONTINUA 75: 2155-2170.