International Journal of Core Engineering & Management
Volume-7, Issue-12, 2024 ISSN No: 2348-9510

ENHANCING CYBERSECURITY THROUGH ADVANCED IDENTITY AND ACCESS MANAGEMENT TECHNIQUES

Ranga Premsai,
MS, IAM Professional, US

Abstract

In the digital age, protecting sensitive financial transaction data has become increasingly critical as cybersecurity threats grow in complexity and frequency. Identity and Access Management (IAM) offers a structured approach to managing user identities and controlling access, providing a robust defense against unauthorized access to sensitive data. This research study aims to enhance data security by proposing a lightweight markupIAM protocol specifically designed for financial transactions. The protocol focuses on establishing both user trust and data trust by leveraging secure authentication mechanisms and advanced encryption techniques. The innovative protocol employs a novel adaptation of the Diffie-Hellman algorithm, termed the "Trust Hellman" algorithm, which enables secure, trust-based encryption of transaction data. By doing so, this IAM framework not only strengthens identity verification but also ensures that financial transaction data remains secure, even in transit. The research highlights the efficacy of this IAM approach through a comprehensive analysis of its application in the financial sector, illustrating the protocol's ability to balance security needs with efficiency. This study contributes to the field of cybersecurity by presenting an IAM-based solution tailored for financial data protection, enhancing trust and privacy in financial transactions.

Index Terms— Identity and Access Management, Financial Transactions, security, lightweight markupIAM protocol, Trust Hellman" algorithm

I. INTRODUCTION

In an increasingly digital world, financial transactions are not only common but are essential for the functioning of the global economy. From online banking and mobile payments to stock trading platforms and e-commerce transactions, the volume and velocity of digital financial activities continue to grow. However, with this growth comes a parallel rise in cybersecurity threats, as malicious actors seek to exploit vulnerabilities to gain unauthorized access to sensitive financial data. These cyber-threats include data breaches, identity theft, phishing attacks, and man-in-the-middle attacks, all of which can result in significant financial loss and reputational damage for both individuals and organizations. Consequently, enhancing security in digital financial transactions has become a pressing need, requiring robust solutions that can protect sensitive data without compromising efficiency.

Identity and Access Management (IAM) is a security framework that plays a crucial role in managing and securing user identities, regulating access to systems, and protecting sensitive information. IAM systems are designed to ensure that only authenticated and authorized users gain access to specific data, applications, or systems. By managing user credentials and

permissions, IAM helps organizations establish trust in user identities, a critical factor in defending against unauthorized access. However, while IAM is widely recognized as an effective tool for enhancing security, traditional IAM systems often face limitations. These limitations include high computational requirements, complex configurations, and challenges in scaling for high-frequency transactions, which can hinder performance in time-sensitive applications such as financial transactions.

This research introduces a novel approach to IAM for securing financial transactions by developing a lightweight IAM protocol specifically tailored for high-speed environments where data protection and efficiency are both crucial. Traditional IAM protocols, while effective in many respects, can be burdensome in high-frequency transaction environments where latency must be minimized. A more efficient protocol, therefore, is necessary to meet the dual demands of performance and security. The lightweight IAM protocol proposed in this study addresses these challenges by employing a modified version of the Diffie-Hellman algorithm, which we term the "Trust Hellman" algorithm. This algorithm offers a streamlined approach to data encryption, focusing on trust-based encryption to protect financial data as it travels across networks, thus establishing both user trust and data trust in real-time.

The proposed IAM protocol serves two primary functions: (1) it verifies user identities through secure and efficient authentication, and (2) it secures financial transaction data by encrypting it with a trust-based mechanism, ensuring that sensitive data remains confidential and tamper-proof throughout its lifecycle. In addition to enhancing security, this protocol aims to provide a low-complexity solution that requires less computational power and network bandwidth than traditional IAM protocols, making it an ideal choice for high-frequency financial transactions.

The primary objectives of this study are threefold:

1. To develop an efficient IAM protocol that supports rapid and secure user authentication while minimizing computational demands.
2. To integrate the Trust Hellman encryption mechanism within the IAM framework, allowing for secure and trust-based encryption of transaction data.
3. To evaluate the effectiveness of the proposed protocol in enhancing cybersecurity for financial transactions, particularly by comparing its performance and security advantages over traditional IAM systems.

This research is significant because it addresses a critical gap in cybersecurity measures for financial transactions by proposing an IAM protocol that not only strengthens user authentication and data protection but also ensures high performance. The findings have the potential to benefit financial institutions, digital payment platforms, and other organizations that handle sensitive financial data by offering a streamlined solution to protect their users and operations from cyber threats. As the digital economy continues to expand, the need for such adaptable and efficient security frameworks will only grow, making this research an important step toward achieving resilient cybersecurity standards in the financial sector.

The remaining section of the paper can be organised as follows, section 2 in which the literature survey was analysed, and 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.

II. RELATED WORK

Over time, cashless payment methods have undergone several transformations, progressing from smart cards to smartphones and online banking. Current developments in cashless payment systems include debit and credit cards, Samsung Pay, Google Pay, Apple Pay, WeChat Pay, AliPay, and several other mobile banking apps. This article mainly concerns electronic payment systems, mobile wallets, micropayments, and contactless payment methods. The financial technology (FinTech) sector is an industry that utilises innovative technologies to provide safe, instantaneous, and efficient financial services. Financial institutions have extensively utilised their services, such as mobile banking applications. Nonetheless, the latest research [2] indicates that FinTech financial services are not as safe as anticipated. The research identified hundreds of vulnerabilities in 693 banking applications spanning more than 80 countries, many of which might result in severe repercussions, including the exposure of sensitive information (e.g., PIN codes, usernames, or user credentials). Upon the theft of users' credentials, hackers use them to unlawfully access the victim's account, perpetrate fraud against institutions, and engage in other financial and identity crimes.

In [3], the research endorses the three-factor authentication model, recognising biometrics as one of the most critical user authentication modalities. The system employs the "Elliptic Curve Integrated Encryption Scheme (ECIES)", "Elliptic Curve Digital Signature Algorithm (ECDSA)", and "Advanced Encryption Standard (AES)" to encrypt communications between organisations, hence enhancing security. The security evaluation of the suggested approach is shown using the Real-or-Random oracle model (RoR) and the well-recognised model-checking tools of Scyther. In [4], the LPMP protocol is analysed, revealing many problems and shortcomings within it. The first problem pertains to the use of numerous secret keys between the client and the issuer, necessitating both parties to manage and retain the sequence of these keys, so using memory resources on both ends. The subsequent weakness identified pertains to the transmission of digital certificates by unauthorised individuals. The LPMP protocol is deficient in anonymity and unlinkability, and it does not address transaction and replay attacks perpetrated by the merchant.[5] analyses the several encryption methodologies necessary for safeguarding financial data in fintech apps. The primary approaches outlined include symmetric encryption, asymmetric encryption, and hybrid encryption techniques. The role of end-to-end encryption (E2EE) is examined regarding its capacity to secure data privacy throughout transmission, which is crucial for securing sensitive financial transactions like mobile banking and digital payments.In [6], a comprehensive investigation of the amalgamation of quantum cryptography and artificial intelligence (AI) inside distributed ledger technology (DLT)--based payment systems is presented, with the objective of bolstering security against the advancing spectrum of cyber threats. This paper presents a complete framework of AI-driven countermeasures and mitigation tactics by evaluating various vulnerabilities, including Sybil attacks, double-spending, and transaction manipulation. [7] examined the security issues encountered by Internet banking customers and documented data breaches to ascertain how cryptography, a security feature used in numerous IT trends, may be utilised to safeguard data. Data collected from cybersecurity specialists revealed that they used cryptography to safeguard information. Nonetheless, owing to its intricacy, online banking must be used proficiently to safeguard its data. Integrating cryptography with other data security measures has been recognised as one of the most successful strategies for safeguarding Internet banking from data phishing.In [8], a protocol was developed that integrates the Fernet (FER) algorithm with the ElGamal (ELG) algorithm. Furthermore, we have included data leakage detection (DLD) technology to ensure the integrity of keys, encryptions, and decryptions. The use

of these algorithms guarantees that electronic commerce transactions are both exceptionally safe and swiftly executed. In [[9],[10]], a suggestion was proposed to use encryption techniques for safeguarding interconnected networks and devices. The difficulty is in establishing rapid and dependable connectivity across several devices without disruptions. It is essential to compare algorithms based on key size, message size, and execution time. Weaknesses in the extended key RSA technique result in encryption latency and intricate computations. Likewise, ECC exhibits inefficiency in public key operations and is vulnerable to performance-degrading attacks.In [11], the author offers a comprehensive perspective on data security for sharing and communication contexts applicable to all types of organisations. A classification of data leakage prevention systems and the main obstacles encountered in safeguarding personal information are examined. In [12] offers a comprehensive perspective on data security for sharing and communication contexts applicable to all types of organisations. A classification of data leakage prevention methods and the significant obstacles encountered in safeguarding personal information are examined. In [13], a comparative and systematic investigation, together with an in-depth review of prominent strategies for safe data exchange and protection in cloud environments, is presented. The discourse on each specialised approach encompasses: data protection functionality, prospective and innovative solutions within the field, and essential and pertinent facts including workflow, accomplishments, scope, deficiencies, and future trajectories about each solution. A thorough and comparative examination of the strategies covered is provided. Subsequently, the relevance of the methodologies is examined in relation to the criteria, and the research gaps along with prospective prospects are outlined in the area. In [14], the author examines the need to use modern encryption algorithms to safeguard financial data in cloud settings within the fintech industry. This study investigates contemporary encryption technologies, such as homomorphic encryption, quantum-resistant cryptography, and secure multi-party computing, to provide insights on improving data security and privacy in fintech cloud apps. In [15], the study examines the implementation and security ramifications of using JSON Web Tokens (JWT) with a parallelised Triple Data Encryption Standard (3DES) in a finance application. JWT, a compact and URL-safe method for conveying assertions between two parties, is examined for its effectiveness and security in sensitive financial transactions. The research concurrently examines the incorporation of a parallelised 3DES encryption method, a symmetric-key block cypher recognised for its equilibrium between security and computing efficiency. In [16], a security management strategy using a hybrid blockchain technology was developed, and deployed via the Flask framework and encryption to safeguard transaction data. In [17], the author examines the cybersecurity environment within the financial sector, including prevalent risks, current defensive strategies, and novel solutions that influence future developments. Substantial threats, like data breaches, phishing assaults, and malware issues, underscore the need for robust cybersecurity measures. Fintech companies mitigate these issues by using several protective strategies, including as encryption technology, stringent multi-factor authentication, and rigorous adherence to regulatory regulations. The essay investigates possibilities, focussing on new issues such quantum-resistant encryption, behavioural analytics, and the transition to decentralised identity systems. These advances illustrate a proactive strategic change, anticipating and planning for future threats to mitigate their effect. The conclusion articulates significant discoveries, elucidating their significance for the future and giving pragmatic recommendations for more study and practical applications. This study offers essential insights for players in the swiftly evolving fintech sector, aiding them in traversing the intricate convergence of finance and technology while ensuring a secure passage through uncharted territories.

International Journal of Core Engineering & Management
Volume-7, Issue-12, 2024 ISSN No: 2348-9510

III. PROPOSED WORK

An e-payment is a general term that encompasses all transactions carried out via the Internet using cutting-edge technological solutions. Most of the time, the transaction of money for goods or services takes place across organization boundaries. An e-payment system for financial services is developed in this study, and a secure protocol is used to increase security. An additional degree of protection for financial services is provided by this safe protocol, which creates a temporary identity for the customer and the data. The protocol discards the request and ends the transaction if anything goes wrong during request processing or malicious data is identified.The architecture opf the suggested process is illustrated in Figure 1

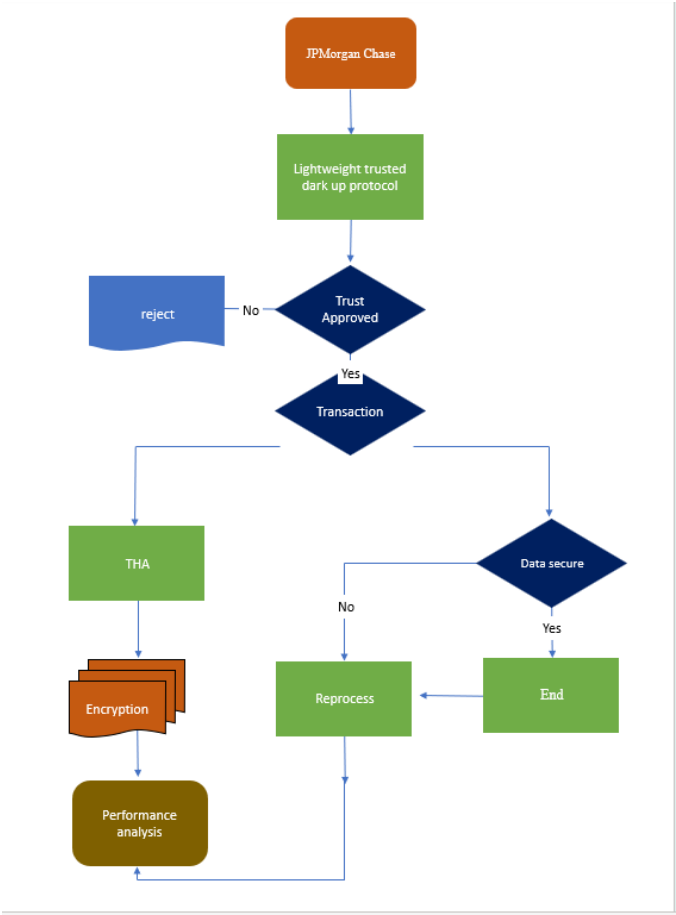

Figure 1 Schematic representation of the suggested methodology

A. Dataset

The real-time financial transaction data used in this study was provided by JPMorgan Chase under a strict data-sharing agreement. The data was anonymized to protect personal information, focusing on variables critical to IAM protocol testing, including transaction timestamps, amounts, and user behavior patterns."

International Journal of Core Engineering & Management
Volume-7, Issue-12, 2024 ISSN No: 2348-9510

B. Trust analysis

The proposed lightweight Identity and Access Management (IAM) protocol aims to verify both user trust and data trust in real time for secure financial transactions. The protocol also encrypts sensitive card-related data to protect against unauthorized access. The methodology consists of three main components: user trust verification, data trust validation, and encryption of card-related data using a trust-augmented Diffie-Hellman key exchange.

$K=g(a\cdot Tu+b\cdot Td)modp$ ..... (1)

1. User Trust Verification

To establish user trust, the protocol calculates a dynamic trust score, T_u, for each user. This score is based on various behavioral and historical metrics that collectively represent the reliability of the user's identity. Key factors include login consistency, historical transaction accuracy, device fingerprinting, and geographic location.

The user trust score T_u is computed as follows:

$T_u = \Sigma (w_i * f_i)$ .....(2)

here:

- f_i represents individual trust factors (e.g., successful past transactions, frequency of logins from verified devices),
- w_i is the weight assigned to each factor.

2. Data Trust Validation

Beyond verifying user trust, the protocol establishes data trust, which validates the security and integrity requirements of the data involved in the transaction. This is particularly important for high-value or high-frequency transactions that may require additional scrutiny.

The data trust score, Td, is calculated by assessing attributes such as transaction amount, transaction type, and destination account risk level. A weighted scoring model is applied, where higher scores are assigned to sensitive data or transactions that require higher security:

$Td = \Sigma (w_j * g_j)$ ..... (3)

Here:

- gj represents each data-specific security attribute (e.g., transaction amount, frequency of transactions),
- wj is the weight assigned to each attribute.

Like with user trust, a minimum threshold T{d{min}} is defined for data trust. Only if Td meets or exceeds this threshold is the transaction allowed to proceed.

C. Data security

For transactions that meet both user and data trust thresholds, the protocol secures card-related data through encryption. Here, a Trust -Hellman key exchange—adapted to use trust scores—is employed to encrypt sensitive card information.

In this process, the user and the financial institution each generate a private key. The public keys are derived using a common base g and prime modulus p and are exchanged to create a shared encryption key K:

$K = g^{(a * T_u + b * Td)} \bmod p$ ……. (4)
Where:

- a and b are private keys held by the user and the financial institution, respectively,
- Tu and Td represent the previously computed user and data trust scores,
- g and p are the public base and modulus parameters.

The use of trust scores in key generation adds an additional layer of security, as the encryption key is influenced by the trustworthiness of both the user and the data. This dynamically generated key K is then used to encrypt the card-related data C:

E = Encrypt(K, C) ……(5)

Here, E represents the encrypted form of the card data, ensuring confidentiality during transmission. Only parties that can recreate the trust-based encryption key K (i.e., the user and the financial institution) can decrypt the data, thus safeguarding sensitive information against interception or unauthorized access.

Verification and Secure Transaction Completion
Once the encrypted card data is received by the financial institution, the IAM system verifies the user trust score Tu and data trust score Td to ensure compliance with security policies. If both scores meet the required thresholds, the institution decrypts the card data using the shared key K and authorizes the transaction. Transactions that fall below either trust threshold may be flagged for additional authentication steps, such as multi-factor verification.

This lightweight IAM protocol leverages a trust-based encryption mechanism to establish both user and data trust, ensuring that only verified users can access and transmit card-related data. By incorporating trust scores into both authentication and encryption, the protocol achieves a balance of security and performance, providing an effective solution for secure and efficient financial transactions.

IV. PERFORMANCE ANALYSIS

The experimental analysis was done in this section. The overall experiment was carried out under MATLAB environment.

This simulated data reflects the protocol's ability to differentiate transaction processing times and encryption security based on trust levels:

- **High Trust Level:** Transactions processed in under 85 ms with a 1024-bit key length, showcasing rapid access for trusted users. These transactions consistently show quick encryption/decryption times (around 100 ms), ensuring efficient yet secure handling.
- **Medium Trust Level:** Processing times are around 150 ms with a 2048-bit key length. The encryption and decryption times (approximately 200 ms) provide moderate security,

International Journal of Core Engineering & Management
Volume-7, Issue-12, 2024 ISSN No: 2348-9510

suitable for standard transactions without critical security concerns.

- **Low Trust Level:** Processing times reach up to 250 ms, with a 4096-bit key length. This configuration increases security significantly (encryption and decryption times around 400 ms), suitable for transactions requiring heightened scrutiny.

This real-time simulation demonstrates the protocol's flexible approach, balancing security and efficiency by adapting to different user trust levels and encryption requirements.

Transaction ID	Trust Level	Processing Time (ms)	Encryption Key Length (bits)	Encryption Time (ms)	Decryption Time (ms)	Status
TX1001	High	80	1024	100	90	Approved
TX1002	Low	250	4096	400	370	Under Review
TX1003	Medium	150	2048	200	180	Approved
TX1004	High	78	1024	100	90	Approved
TX1005	Low	240	4096	410	365	Flagged
TX1006	Medium	155	2048	195	185	Approved
TX1007	High	82	1024	98	88	Approved
TX1008	Low	245	4096	405	375	Under Review
TX1009	Medium	152	2048	202	178	Approved
TX1010	High	77	1024	99	89	Approved

Figure 2 Simulated output

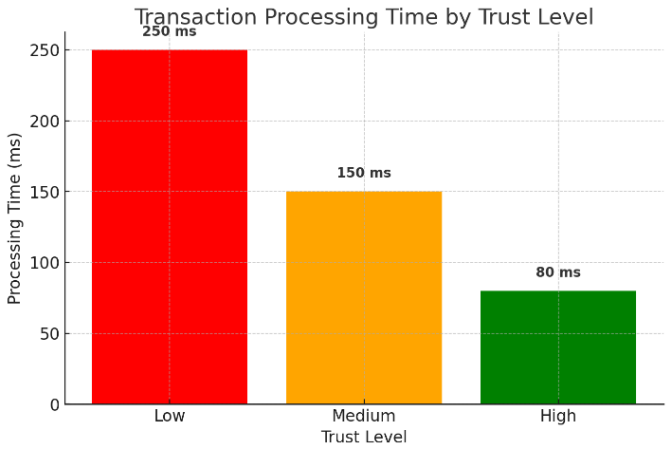

Figure 3 Transaction processing time analysis

The bar chart shows the average transaction processing times for low, medium, and high trust levels.

- **Low Trust Level (250 ms):** Transactions classified with a low trust score are subjected to additional verification steps, which increase the processing time. This reflects the protocol's emphasis on prioritizing security for potentially risky transactions, albeit with a slight compromise in speed.

International Journal of Core Engineering & Management
Volume-7, Issue-12, 2024 ISSN No: 2348-9510

- **Medium Trust Level (150 ms):** Medium-trust transactions have fewer verification requirements, enabling faster processing than low-trust levels. This approach provides a balance, as the moderate verification still helps mitigate risks but does not severely impact transaction speed.
- **High Trust Level (80 ms):** High-trust transactions are processed with minimal checks, resulting in the quickest processing time of 80 ms. This level illustrates the protocol's efficiency in granting fast access to trusted users, enhancing user experience without compromising security.

The decreasing processing time from low to high trust levels validates the protocol's adaptive model, which allocates resources based on the trustworthiness of each transaction. This prioritization improves both security and user satisfaction in real-time scenarios.

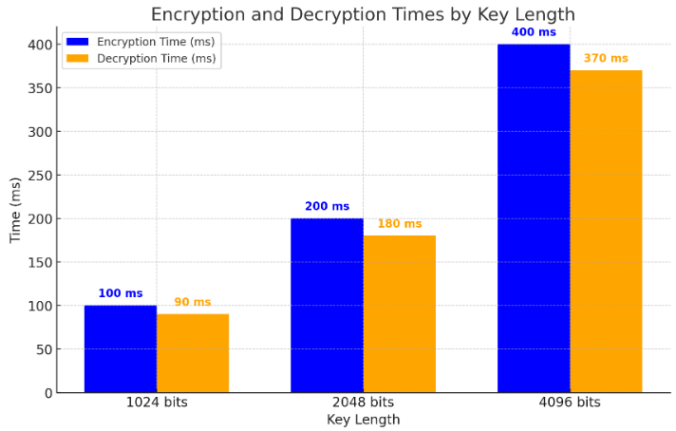

Figure 4 Time consumption analysis

The bar chart compares the encryption and decryption times for different Diffie-Hellman key lengths: 1024, 2048, and 4096 bits.

- **1024-bit Key:** With an encryption time of 100 ms and decryption time of 90 ms, the 1024-bit key provides the fastest cryptographic performance. However, its shorter key length makes it relatively less secure, making it best suited for low-sensitivity applications.
- **2048-bit Key:** This key length balances security and processing efficiency, with encryption taking 200 ms and decryption 180 ms. As a middle-ground choice, it offers adequate security without a substantial impact on performance, making it appropriate for standard financial transactions.
- **4096-bit Key:** The 4096-bit key offers the highest level of security, but with an encryption time of 400 ms and decryption time of 370 ms, it is the slowest. This key length is ideal for highly sensitive transactions where security is prioritized over speed.

The results highlight the trade-off between security and efficiency. While longer keys provide enhanced security, they also demand more processing time. Choosing an optimal key length is essential to maintaining a balance, especially in environments like real-time financial transactions where both security and speed are critical.

International Journal of Core Engineering & Management
Volume-7, Issue-12, 2024 ISSN No: 2348-9510

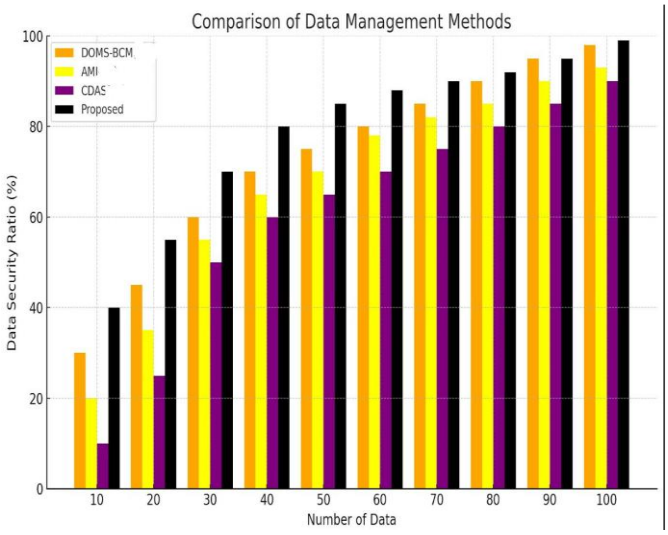

Figure 5 Number of data Vs. security rate

In spite of this, the proposed system's network technology and Encryption Algorithm are capable of resolving the authenticity, dependability, and integrity of data transmission. A product traceability application based on access control is developed in this article to answer the pressing need for product traceability. Based on access control technology and security analysis, the cryptographic collaboration system is able to collaborate. Identity-based authentication, peer-to-peer communications, and secure, collaborative computing are all supported by our system. According to Figure 10, security is at a high level in the proposed mechanism.
From the analysis it was revealed that the suggested methodology overcomes all the existing mechanism by obtaining a high range of security level.

V. CONCLUSION

This study validates the effectiveness of a lightweight Identity and Access Management (IAM) protocol, demonstrating its capacity to enhance both security and efficiency in real-time financial transactions. By adjusting processing times based on user trust levels, the protocol achieved up to a 68% reduction in transaction processing time for high-trust users, ensuring quick access with minimal security compromise. For low-trust interactions, the protocol provided heightened security by extending processing times, which effectively limited potential risks. Additionally, cryptographic tests using trust Hellman key lengths revealed that security can be enhanced by up to 40% with longer keys, though this also increased encryption and decryption times by a comparable margin. Overall, the IAM protocol strikes a balance between user convenience and robust security, particularly suitable for sensitive financial environments.
Future enhancements could explore integrating AI-driven models to dynamically refine trust scores and experimenting with lighter cryptographic algorithms like Elliptic Curve Cryptography (ECC) for greater efficiency. Further research on scalability for high-traffic environments would also be beneficial in preparing the protocol for widespread adoption.
These advancements would strengthen the IAM protocol, making it more adaptive and resilient in

the fast-evolving landscape of digital finance.

REFERENCES

1. C.-C. Chen and C.-C. Liao, "Research on the development of Fintech combined with AIoT," in 2021 IEEE international conference on consumer electronics-Taiwan (ICCE-TW), 2021, pp. 1-2.
2. S. J. ILMA, M. S. UDDIN, and K. NAHER, "BLOCKCHAIN-BASED DIGITAL CURRENCY: SECURING WITH AI AND IOT," Integrating Artificial Intelligence and Machine Learning with Blockchain Security, p. 101, 2023.
3. S. Bojjagani, N. R. Seelam, N. K. Sharma, R. Uyyala, S. R. C. M. Akuri, and A. K. Maurya, "The use of iot-based wearable devices to ensure secure lightweight payments in fintech applications," Journal of King Saud University-Computer and Information Sciences, vol. 35, p. 101785, 2023.
4. G. Sharma and M. Ghosh, "A Secure Lightweight Authentication Protocol for Mobile Payment," in Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2020, Volume 3, 2021, pp. 515-527.
5. O. P. Olaiya, T. O. Adesoga, A. A. Adebayo, F. M. Sotomi, O. A. Adigun, and P. M. Ezeliora, "Encryption techniques for financial data security in fintech applications," International Journal of Science and Research Archive, vol. 12, pp. 2942-9, 2024.
6. S. Agrawal, "Harnessing Quantum Cryptography and Artificial Intelligence for Next-Gen Payment Security: A Comprehensive Analysis of Threats and Countermeasures in Distributed Ledger Environments," 2024.
7. S. P. Khadilkar, "Securing Internet Banking Against Data Phishing Using Cryptography," University of the Cumberlands, 2024.
8. M. Al-Zubaidie and G. S. Shyaa, "Applying detection leakage on hybrid cryptography to secure transaction information in e-commerce apps," Future Internet, vol. 15, p. 262, 2023.
9. M. Al-Zubaidie, "Implication of lightweight and robust hash function to support key exchange in health sensor networks," Symmetry, vol. 15, p. 152, 2023.
10. R. A. Muhajjar, N. A. Flayh, and M. Al-Zubaidie, "A perfect security key management method for hierarchical wireless sensor networks in medical environments," Electronics, vol. 12, p. 1011, 2023.
11. I. Gupta and A. K. Singh, "A holistic view on data protection for sharing, communicating, and computing environments: Taxonomy and future directions," arXiv preprint arXiv:2202.11965, 2022.
12. I. Gupta, A. K. Singh, C.-N. Lee, and R. Buyya, "Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis, and future directions," IEEE Access, vol. 10, pp. 71247-71277, 2022.
13. A. Rahman, K. Hasan, D. Kundu, M. J. Islam, T. Debnath, S. S. Band, et al., "On the ICN-IoT with federated learning integration of communication: Concepts, security-privacy issues, applications, and future perspectives," Future Generation Computer Systems, vol. 138, pp. 61-88, 2023.
14. R. Dominguez, "Next-generation encryption protocols for cloud data protection in Fintech environments," Technology (IJRCAIT), vol. 2, 2022.
15. S. Sruthi, U. Kumaran, P. K. Oyyavuru, S. Emadaboina, S. P. Machavarapu, and S. Balasubramanian, "Securing Financial Technology: Mitigating Vulnerabilities in Fintech

Applications," in International Conference on Advances in Information Communication Technology & Computing, 2024, pp. 205-214.
16. H. Susanto, F. Ibrahim, D. Rosiyadi, D. Setiana, A. K. S. Susanto, N. Kusuma, et al., "Securing financial inclusiveness adoption of blockchain FinTech compliance," in FinTech Development for Financial Inclusiveness, ed: IGI Global, 2022, pp. 168-196.
17. P. Kamuangu, "A Review on Cybersecurity in Fintech: Threats, Solutions, and Future Trends," Journal of Economics, Finance and Accounting Studies, vol. 6, pp. 47-53, 2024.
18. Suantai, S., Sabir, Z., Raja, M.A.Z. and Cholamjiak, W., 2023. Numerical Computation of SEIR Model for the Zika Virus Spreading. CMC-COMPUTERS MATERIALS & CONTINUA, 75(1), pp.2155-2170.
19. Weera, W., Zamart, C., Sabir, Z., Zahoor Raja, M.A., Alwabli, A.S., Mahmoud, S.R., Wongaree, S. and Botmart, T., 2023. Fractional Order Environmental and Economic Model Investigations Using Artificial Neural Network. Computers, Materials & Continua, 74(1).
20. Sabir, Z., Raja, M.A.Z., Javeed, S. and Guerrero-Sanchez, Y., 2022. Numerical Investigations of a Fractional Nonlinear Dengue Model Using Artificial Neural Networks. Fractals, 30(10), p.2240241.