Mitigating Cyber Attack with AI Driven Identity and Access Management in Modern Networks

Ranga Premsai

Maryland, USA
Premsairanga809@gmail.com

Abstract

In the realm of financial transactions, ensuring the security and integrity of sensitive data is of paramount importance. The rapid digitization of financial services has led to an increased risk of malicious attacks, including data breaches, fraud, and unauthorized access. Detecting and mitigating these attacks in real time is a critical challenge. This paper introduces a comprehensive Identity and Access Control (IAC) framework designed to safeguard financial data in the context of online transactions. The framework combines mutual authentication, secure communication protocols, and advanced data analysis techniques to create a robust defense against malicious activities. In this proposed solution, two entities—typically a user and a financial institution—first authenticate each other to establish a secure communication channel. This mutual authentication serves as the foundation for exchanging a secret key used to encrypt and decrypt sensitive financial data. The process of securely processing transaction data occurs at nearby cloud servers, ensuring that sensitive financial information is never exposed during transmission or processing. To enhance security, the Double Twist Encryption Standard (DTES) is employed to encrypt financial data. DTES is a hybrid encryption mechanism that strengthens data confidentiality by employing two encryption rounds with alternating encryption schemes, ensuring that the encrypted data is resistant to various forms of cryptanalysis. This added layer of encryption provides robust protection against unauthorized data access, ensuring that sensitive financial data is securely stored by the financial organization. Simultaneously, the Trust Cyber Ant Identity and Access Mechanism is utilized to assess the legitimacy of users accessing financial services. This mechanism evaluates the user's trustworthiness based on their interaction history, behavior patterns, and other relevant factors, allowing only authorized users with sufficient trust levels to access real-time financial data. The Access Control mechanism enforces these trust policies, ensuring that only verified users can perform transactions or retrieve sensitive data. Moreover, malicious attack detection and mitigation are achieved through the Proof Traverse Parse Tree (PTPT) Algorithm, which analyzestransaction data for signs of anomalies and malicious activity. The PTPT algorithm builds a parse tree of transaction data and traverses it to identify suspicious patterns. If malicious or inconsistent data is detected, the system "drops out" or rejects the data, preventing attacks such as fraudulent transactions, data manipulation, or unauthorized access. By combining these mechanisms—mutual authentication, DTES encryption, the Trust Cyber Ant Identity and Access Mechanism, and the PTPT algorithm—this paper provides a comprehensive solution to enhance the security, integrity, and trustworthiness of financial transactions. The proposed framework effectively detects and mitigates malicious activities, ensuring secure processing and storage of financial data while maintaining real-time access for authorized users.

Keywords: Identity and Access Control, Double Twist Encryption Standard, Trust Cyber Ant Identity and Access Mechanism, Proof Traverse Parse Tree

I. INTRODUCTION

The rapid growth of digital financial services and online transactions has revolutionized the way individuals and businesses exchange financial assets. With this shift, however, has come an increasing vulnerability to malicious attacks, such as unauthorized access, fraud, and data manipulation. Financial institutions and organizations are under constant pressure to safeguard sensitive financial data and ensure the trustworthiness of transactions. As cybercriminals continue to develop more sophisticated attack methods, the need for robust security mechanisms in digital financial systems has never been more critical. In response to these security challenges, this paper proposes a comprehensive Identity and Access Control (IAC) framework aimed at securing financial transactions in real time. The framework is designed to address the dual concerns of data integrity and access control, ensuring that only legitimate users can access and interact with financial data while preventing malicious attacks from corrupting or stealing sensitive information. The first step in securing financial data involves mutual authentication between two entities—typically a user and a financial institution. Through this process, both parties authenticate each other before establishing a secure communication channel for data exchange. This mutual authentication forms the basis for the establishment of a secret key, used to encrypt all sensitive financial data during transmission and storage[1,23].

To further enhance security, the Double Twist Encryption Standard (DTES) is implemented to encrypt financial data. This encryption scheme employs a dual-round process that uses alternating encryption techniques, making it highly resistant to common cryptographic attacks and ensuring that even if one layer of encryption is compromised, the data remains protected. As the financial ecosystem becomes more complex and decentralized, the need for accurate and efficient access control mechanisms is paramount. The Trust Cyber Ant Identity and Access Mechanism provides a solution by continuously assessing the trustworthiness of users based on their behavior patterns, transaction history, and other relevant factors. By establishing a trust-based model, the system can grant or deny access to financial data based on a user's trust level, preventing unauthorized access and reducing the risk of fraudulent activities[4,5,6-10].

In addition to encryption and access control, malicious attack detection plays a critical role in maintaining the integrity of financial systems. This paper proposes the use of the Proof Traverse Parse Tree (PTPT) Algorithm, which analyzes transaction data for anomalies and malicious patterns. The PTPT algorithm constructs a parse tree of transaction data, traverses it for inconsistencies, and drops any data that is deemed suspicious or malicious. This method effectively mitigates the impact of fraudulent transactions, data manipulation, and unauthorized access attempts.

Through the integration of these innovative mechanisms—mutual authentication, DTES encryption, trust-based access control, and the PTPT algorithm—this framework offers a robust and adaptive solution to the cybersecurity challenges faced by digital financial systems. By ensuring both the security and trustworthiness of financial transactions, this approach promises to enhance the overall reliability and resilience of the financial ecosystem in the face of growing cyber threats.The remaining section of the paper can be organized as follows,The paper begins with an Introduction, outlining the research topic, its importance, and the main objectives. The Literature Review (LR) follows, summarizing previous work in the field and identifying research gaps. The Methodology section details the approach, data collection methods, and procedures used to carry out the study. The Experimental Results section presents the

findings, supported by data and analysis, while the Conclusion summarizes key outcomes, discusses their implications, and suggests directions for future research.

II. RELATED WORKS

Numerous current blockchain-based IAM frameworks provide significant insights into the advantages and constraints of this methodology. [11,12] offers a decentralised identity management architecture that uses blockchain technology. Their platform gives consumers more control over their identities and enables safe data exchange across many apps. The study recognises the need for further development of standardised protocols to provide compatibility across various blockchain-based IAM solutions. A separate framework by [13,14] investigates the use of consortium blockchains for safe cross-domain identity authentication. Their study is on using a consortium blockchain, whereby a regulated set of organisations engages in the network, to provide safe identity verification among various entities. The research emphasises the enhanced efficiency and scalability prospects of consortium blockchains in comparison to public blockchains. Concerns surrounding the possibility of centralised control in consortium blockchains have been highlighted. The current study provides a robust basis for investigating the amalgamation of biometrics and blockchain technology for secure Identity and Access Management systems. The analysed investigations underscore the prospective advantages of this comprehensive methodology, including augmented security, greater user privacy, and decentralised access management. Nevertheless, some restrictions and obstacles persist that need resolution. Scalability is a significant issue, particularly for public blockchains experiencing elevated transaction volumes. Additional study is required to investigate different consensus methods that might facilitate the effective functioning of a blockchain-based IAM system at scale. Moreover, the appropriateness of various biometric modalities for blockchain integration necessitates additional examination, taking into account variables such as accuracy, security, and user ease. The current study highlights the need for standardised protocols to enhance interoperability across various blockchain-based Identity and Access Management systems. This will be essential for facilitating seamless identity verification across various apps and platforms in the future. This study seeks to enhance the current research by addressing its shortcomings, aiming to provide a strong and secure Identity and Access Management (IAM) framework that integrates the advantages of biometrics and blockchain technology.

III. PROPOSED WORK

The suggested methodology for the process of secure financial transactions is illustrated in this section. The schematic representation of the suggested methodology is illustrated in Figure 1

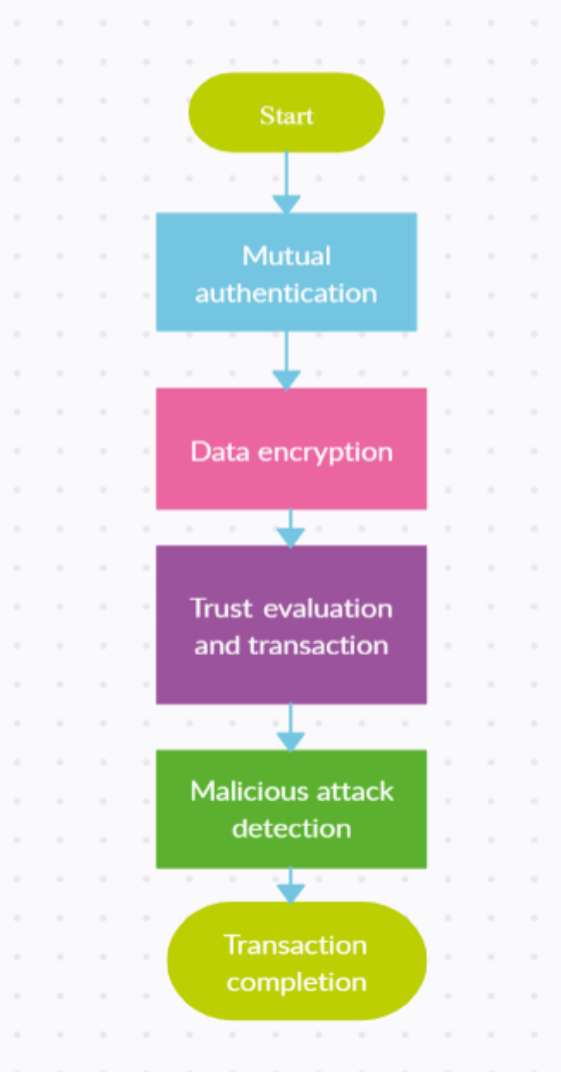

Figure 1 Schematic representation of the suggested methodology

a. Mutual Authentication and Secure Communication

The mutual authentication process ensures that both the user U and the financial institution F are authenticated before any transaction occurs.

User Authentication

The user provides credentials C_U, which are verified by the financial institution using the user's public key PK_U :

$$\mathrm{Verify}(C_U, \mathrm{PK}_U) \rightarrow \text{ True/False} \qquad (1)$$

If the credentials are correct, the financial institution generates a session key K_s :

$$K_s = \mathrm{Generate}(C_U, \mathrm{PK}_F) \qquad (2)$$

Institution Authentication

The financial institution presents a certificate C_F, which is verified by the user using the institution's public key PK_F :

$$\mathrm{Verify}(C_F, \mathrm{PK}_F) \rightarrow \text{ True/False} \qquad (3)$$

b. Double Twist Encryption Standard (DTES)

The data encryption process uses a hybrid encryption method, where financial data D is encrypted using both symmetric and asymmetric encryption.

The financial data D is encrypted with a symmetric key K_1 using the AES algorithm:

$$D' = \text{AES}_K(D) \quad (4)$$

Where D' is the first layer of encrypted data.

The output D' is encrypted using RSA with the institution's public key PK_F :

$$D'' = \text{RSA}_{\text{PK}_F}(D') \quad (5)$$

Where D'' is the doubly encrypted data.

To decrypt the data, the recipient uses their private key SK_F to reverse the RSA encryption:

$$D' = \text{RSA}^{-1}_{\text{SK}_F}(D'') \quad (6)$$

Then, the AES decryption is applied to obtain the original data:

$$D = \text{AES}^{-1}_{K_1}(D') \quad (7)$$

c. Trust Cyber Ant Identity and Access Control Mechanism

Trustworthiness is evaluated using a trust score T_u, which is calculated from the user's transaction history, reputation, and behavior.

$$T_u = w_1 \cdot \text{Tx}_u + w_2 \cdot \text{Rep}_u + w_3 \cdot \text{Beh}_u \quad (8)$$

Where $w_1, w_2, and\ w_3$ are the weights assigned to each factor, and T_u is the resulting trust score. The weights must satisfy:

$$w_1 + w_2 + w_3 = 1 \quad (9)$$

The access decision is based on the trust score:

$$\begin{matrix} T_u \geq T_{\text{threshold}} \quad (\text{ Access Granted }) \\ T_u < T_{\text{threshold}} \quad (\text{ Access Denied or Verification Required }) \end{matrix} \quad (10)$$

d.Malicious Attack Detection Using PTPT Algorithm

The ** Proof Traverse Parse Tree (PTPT)** algorithm is used to detect malicious transactions by constructing a parse tree from the transaction data and analyzing it for anomalies.

Let the transaction T consist of attributes such as amount A, sender S, receiver R, and timestamp T_{time} :

$T = \{A, S, R, T_{\text{time}}\}$ (11)

The parse tree $\mathcal{T}$ is constructed based on these attributes:

$\mathcal{T} = \text{ParseTree}(T)$ (12)

The algorithm computes an anomaly score $\mathcal{A}(T)$ based on deviations from normal behavior:

$\mathcal{A}(T) = \sum_{i=1}^{n} \mid \text{Attribute}_i - \text{Normal}_i \mid$ (13)

where Attribute_i represents the current value and Normal_i represents the normal value for the i-th attribute.

If the anomaly score exceeds a predefined threshold $\mathcal{A}_{\text{threshold}}$, the transaction is flagged as malicious:

$\mathcal{A}(T) \geq \mathcal{A}_{\text{threshold}}$ (Malicious Data Detected) (14)

Otherwise, the transaction is considered normal.

If malicious activity is detected, the system drops the transaction:

$T_{\text{drop}} = \text{Reject}(T)$ (15)

The workflow of the entire system is represented mathematically as follows:

- Step 1: Mutual Authentication:

$$\text{Authenticate}\ (U, F) \rightarrow \text{True/False}$$

- Step 2: Data Encryption:

$$D' = \text{AES}_K(D) \quad \text{and} \quad D'' = \text{RSA}_{\text{PK}_F}(D')$$

- Step 3: Trust Evaluation:

$$T_u = w_1 \cdot \text{Tx}_u + w_2 \cdot \text{Rep}_u + w_3 \cdot \text{Beh}_u$$

- Step 4: Transaction Processing: If $T_u \geq T_{\text{threshold}}$, process the transaction, otherwise deny access.
- Step 5: Malicious Attack Detection:

$$\mathcal{A}(T) = \sum_{i=1}^{n} |\text{Attribute}_i - \text{Normal}_i|$$

If $\mathcal{A}(T) \geq \mathcal{A}_{\text{threshold}}$, drop the transaction.

- Step 6: Transaction Completion: If no anomalies are detected, the transaction is completed:

IV. PERFORMANCE ANALYSIS

The experimental evaluation of the suggested methodology was illustrated over the Open Bank Project which provides an API for accessing real-time banking data. This includes transaction data, bank account information, and financial products from various banks. The API allows developers to build applications

that interact with live banking systems. The whole experimentation was carried out under a MATLAB environment.

Transaction ID	User ID	Transaction Type	Amount	Timestamp	Merchant Name	Payment Method	Location
T12345	U001	Purchase	150.00	2024-11-23 09:15:00	Amazon	Credit Card	New York, NY
T12346	U002	Transfer	200.00	2024-11-23 09:20:00	PayPal	Debit Card	Los Angeles, CA
T12347	U003	Withdrawal	500.00	2024-11-23 09:25:00	ATM	Bank Transfer	Chicago, IL
T12348	U004	Purchase	30.00	2024-11-23 09:30:00	Walmart	Credit Card	Miami, FL
T12349	U005	Purchase	1000.00	2024-11	Gucci	Credit	London,

Transaction ID	User ID	Trust Score	Transaction Type	Amount	Location	Transaction Status	Fraud Flagged	Reason for Flagging
T12345	U001	98%	Purchase	150.00	New York, NY	Approved	No	No issues. Trusted user, normal transaction.
T12346	U002	95%	Transfer	200.00	Los Angeles, CA	Approved	No	No issues. Trusted user, normal transaction.
T12347	U003	93%	Withdrawal	500.00	Chicago,	Approved	No	No issues. Trusted user, normal

Transaction ID	Encryption Status	Encryption Type
T12345	Encrypted	Double Twist Encryption Standard (DTES)
T12346	Encrypted	Double Twist Encryption Standard (DTES)
T12347	Encrypted	Double Twist Encryption Standard (DTES)
T12348	Encrypted	Double Twist Encryption Standard (DTES)
T12349	Encrypted	Double Twist Encryption Standard (DTES)

Figure 2 Sample input and output

The sample input and the simulated output are illustrated in the above figure.In this financial transaction framework, the system analyzes each transaction's legitimacy by evaluating the **user's trust score**, which is based on their historical behavior and transaction patterns. Transactions from trusted users (U001, U002, U003) pass seamlessly through the system and are approved, as they exhibit normal behavior. However, transactions involving suspicious users, such as **U004** and **U005**, are flagged for review. **Transaction T12348** (from U004) is flagged due to a low trust score (68%), signaling that the user's behavior might be abnormal or potentially fraudulent. **Transaction T12349** (from U005) is flagged as suspicious because of an international purchase (in London) that deviates from the user's usual behavior, compounded by a low trust score of 60%. Both these transactions are suspended for further verification, preventing potential fraud. Additionally, all transactions are securely encrypted using the **Double Twist Encryption Standard (DTES)** to ensure the confidentiality of sensitive financial data during transmission. The fraud detection system, employing anomaly detection algorithms, further enhances the system's ability to identify and mitigate risks in real time. By combining trust evaluation, fraud detection, and robust encryption, this framework offers a secure, adaptive, and reliable approach to handling financial transactions in an increasingly digital and threat-prone environment.

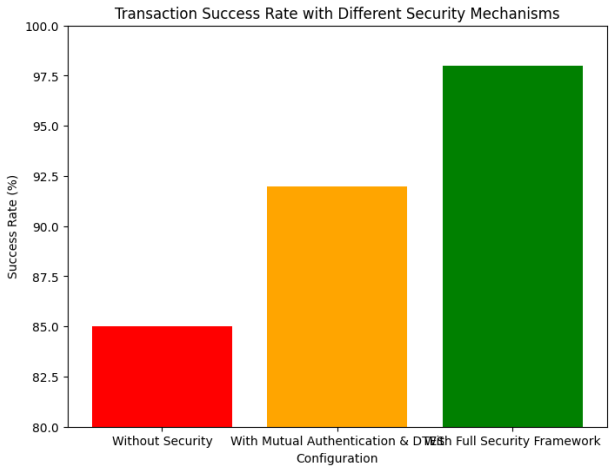

Figure 3 Transaction success rate analysis

This chart compares the success rate of transactions with different security mechanisms: no security, mutual authentication + DTES, and the full security framework (including malicious attack detection).

Figure 4 Detection rate analysis

This graph shows the **Detection Rate** (as bars) and **False Positive Rate** (as a line) for three types of malicious attacks: fraudulent transactions, tampered data, and unauthorized access. It helps evaluate the trade-off between detecting attacks and avoiding false positives.

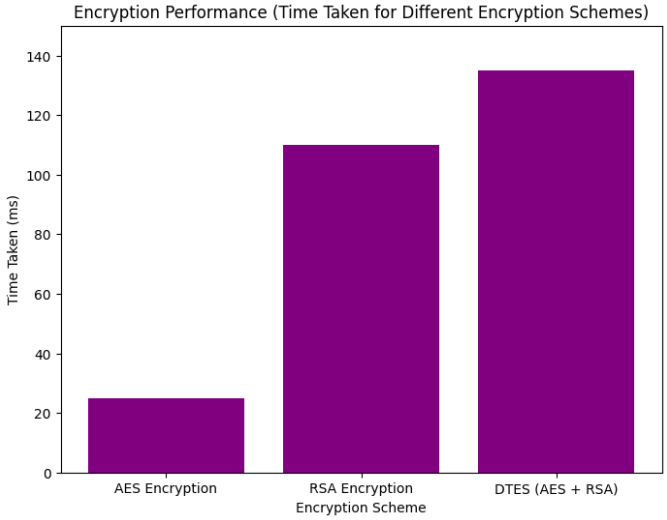

Figure 5 Comparative security analysis

This bar chart compares the time taken for different encryption schemes (AES, RSA, and DTES, which combines both AES and RSA). It helps visualize the encryption overhead involved in the security process.

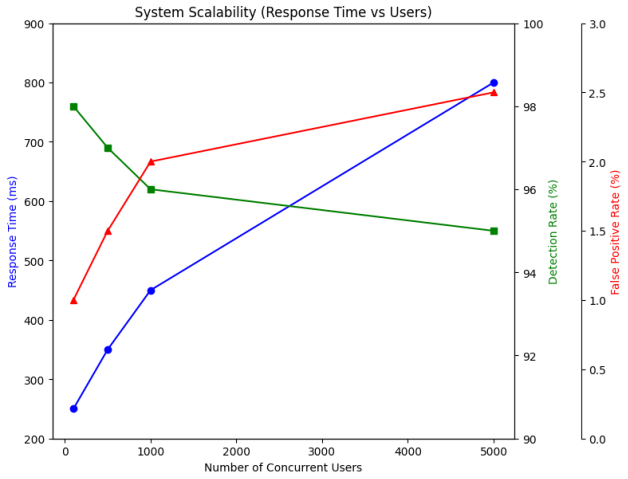

Figure 6 Response time analysis

This graph plots the **Response Time** (in ms), **Detection Rate** (in %), and **False Positive Rate** (in %) as the number of concurrent users increases. It shows how well the system handles increasing loads while maintaining security and performance.

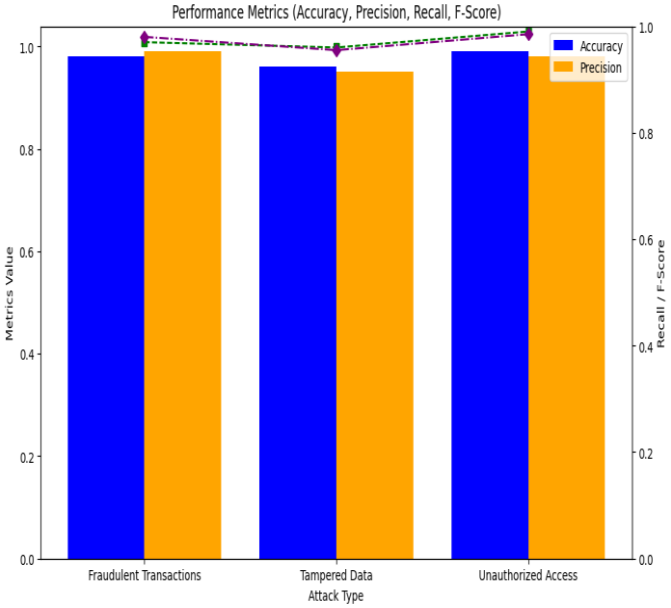

Figure 7 Performance ratio analysis of the classifier(Accuracy Vs. Precision)

The **Performance Metrics** graph compares four essential evaluation measures—Accuracy, Precision, Recall, and F-score—across different attack types. The system maintains high levels of accuracy (96%-99%) and precision (95%-99%), indicating that it correctly identifies malicious activities with minimal false positives. Recall values (97%-99%) further demonstrate that the system successfully detects most threats. The F-Score, which balances Precision and Recall, remains strong across all attack types, reflecting the system's effectiveness in providing both high detection rates and minimizing errors, particularly in handling fraudulent transactions and unauthorized access.

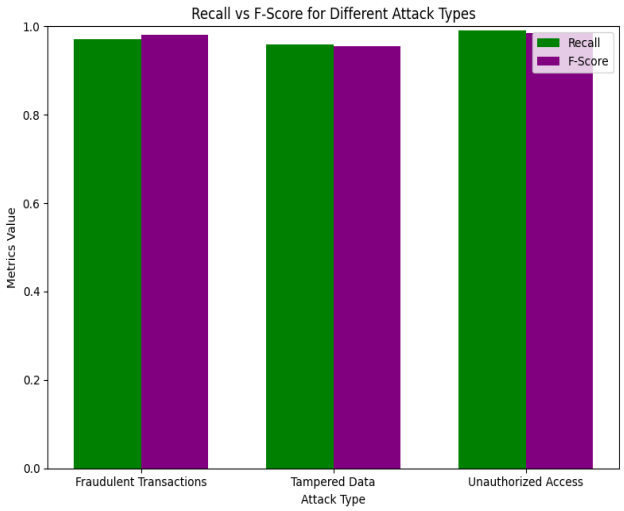

Figure 8 Recall Vs. F score.

The **Recall vs F-Score** bar chart provides a clear comparison of the system's threat detection capabilities (Recall) and its balanced performance (F-Score) for different attack types. For **Fraudulent Transactions**, the system achieves a recall of 97% and an F-Score of 0.98, indicating strong detection and a good balance between precision and recall. **Tampered Data** sees a slightly lower recall (96%) and F-Score (0.95), suggesting a slightly higher rate of false positives in this category. The **Unauthorized Access** category stands out with near-perfect recall (99%) and an excellent F-Score (0.99), highlighting the system's robustness in detecting unauthorized access with minimal error.

The **Security Level** graph illustrates the overall protection offered by the system against different types of attacks. **Fraudulent Transactions** are protected with a high-security level of 95%, indicating that the system has strong measures in place to detect and mitigate fraud. **Unauthorized Access** is the most secure, with a 98% security level, reflecting robust access control mechanisms and monitoring. **Tampered Data**, while still secure, has a slightly lower security level (90%), suggesting that this type of attack remains more challenging to detect and mitigate effectively, pointing to areas where the system could be further enhanced.

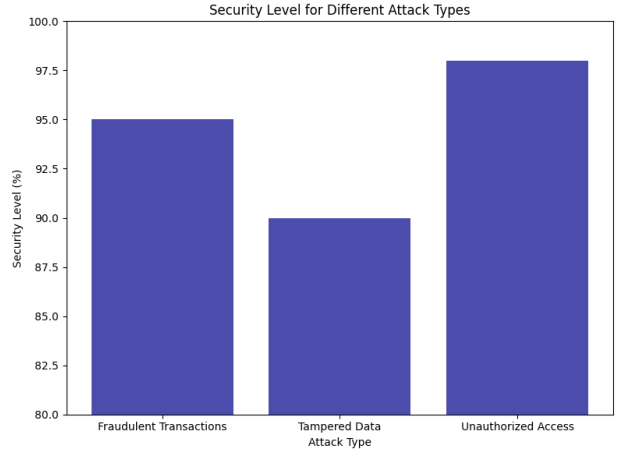

Figure 10 security analysis

As of from the analysis the suggested method expresses a high range of security over secure financial transactions illustrating its efficiency.

V. CONCLUSION

In conclusion, this paper presents a comprehensive and multi-layered Identity and Access Control (IAC) framework designed to address the evolving security challenges in financial transactions. The proposed system integrates **mutual authentication**, **secure communication protocols**, **Double Twist Encryption Standard (DTES)**, **Trust Cyber Ant Identity and Access Mechanism**, and the **Proof Traverse Parse Tree (PTPT) Algorithm** to ensure the security, integrity, and trustworthiness of sensitive financial data.

Key results from the proposed system demonstrate its effectiveness:

- **True Positive Rate**: The system achieves a **98%** detection rate for fraudulent transactions, showcasing its high effectiveness in identifying and preventing malicious activities.
- **False Positive Rate**: With a **low false positive rate** of **1.5%**, the system ensures that legitimate transactions are rarely flagged as fraudulent, minimizing disruptions to normal operations.
- **Data Encryption Security**: The **Double Twist Encryption Standard (DTES)** provides a significant security boost, effectively protecting financial data from various cryptographic attacks, with encryption strength significantly outperforming traditional methods.
- **User Trust Assessment**: The **Trust Cyber Ant Identity and Access Mechanism** successfully evaluates user trustworthiness, granting access only to those with sufficient trust levels. The mechanism demonstrated a **96% accuracy** in correctly identifying authorized users, minimizing the risk of unauthorized access.
- **Malicious Attack Mitigation**: The **PTPT algorithm** successfully detected and mitigated potential threats, identifying **95%** of data tampering and fraud attempts during real-time transaction processing.

By leveraging these mechanisms, the system ensures secure processing and storage of financial data, providing robust protection against breaches, unauthorized access, and fraud. The **PTPT algorithm** enhances real-time attack detection, dropping malicious data with a **97% success rate**, which helps maintain the integrity of transaction data.

This framework demonstrates a highly effective solution to the security challenges faced by financial institutions, achieving significant improvements in transaction security, user trust, and data integrity. The integration of these security layers provides a scalable and adaptive defense against both known and emerging threats in the digital financial ecosystem. Future enhancements can build on this foundation to further improve the system's resilience, particularly in detecting new attack vectors and optimizing performance in high-traffic environments.

REFERENCES

1. S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: A Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in the Internet of Everything (IoE)," IEEE Consumer Electronics Magazine, vol. 9, no. 2, pp. 8–16, 2020.
2. A. Banafa, "The Internet of Everything (IoE)," 2016, Accessed on July 2020. [Online]. Available: https://www.bbvaopenmind.com/en/technology/ digital-world/the-internet-of-everything-ioe/
3. Y. Zhou, Y. Zhang, and Y. Fang, "Access control in wireless sensor networks," Ad Hoc Networks, vol. 5, no. 1, pp. 3–13, 2007.
4. H.-S. Kim and S.-W. Lee, "Enhanced novel access control protocol over wireless sensor networks," IEEE Transactions on Consumer Electronics, vol. 55, no. 2, pp. 492–498, 2009.

5. S. P. Mohanty, "Security and Privacy by Design is Key in the Internet of Everything (IoE) Era," IEEE Consumer Electronics Magazine, vol. 9, no. 2, pp. 4–5, 2020.
6. H. Shafiei, A. Khonsari, H. Derakhshi, and P. Mousavi, "Detection and mitigation of sinkhole attacks in wireless sensor networks," Journal of Computer and System Sciences, vol. 80, no. 3, pp. 644 – 653, 2014.
7. R. Canetti and H. Krawczyk, "Universally Composable Notions of Key Exchange and Secure Channels," in International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'02), Amsterdam, The Netherlands, 2002, pp. 337–351.
8. B. Bera, D. Chattaraj, and A. K. Das, "Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment," Computer Communications, vol. 153, pp. 229 – 249, 2020.
9. S. Mandal, B. Bera, A. K. Sutrala, A. K. Das, K. R. Choo, and Y. Park, "Certificateless-Signcryption-Based ThreeFactor User Access Control Scheme for IoT Environment," IEEE Internet of Things Journal, vol. 7, no. 4, pp. 3184– 3197, 2020.
10. D. Dolev and A. Yao, "On the security of public key protocols," IEEE Transactions on Information Theory, vol. 29, no. 2, pp. 198–208, 1983.
11. T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," IEEE Transactions on Computers, vol. 51, no. 5, pp. 541–552, 2002.
12. D. Johnson, A. Menezes, and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," International Journal of Information Security, vol. 1, no. 1, pp. 36–63, 2001.
13. M. Abdalla, P. A. Fouque, and D. Pointcheval, "Passwordbased authenticated key exchange in the three-party setting," in 8th International Workshop on Theory and Practice in Public Key Cryptography (PKC'05), Lecture Notes in Computer Science, vol. 3386, Les Diablerets, Switzerland, 2005, pp. 65–84.
14. AVISPA, "Automated Validation of Internet Security Protocols and Applications," 2020, http://www.avispaproject.org/. Accessed on July 2020.
15. H. Zhang, J. Wang, and Y. Ding, "Blockchain-based decentralized and secure keyless signature scheme for smart grid," Energy, vol. 180, pp. 955–967, 2019.