INTERNATIONAL SCIENTIFIC JOURNAL OF ENGINEERING AND MANAGEMENT ISSN: 2583-6129
VOLUME: 03 ISSUE: 07 | JULY – 2024 DOI: 10.55041/ISJEM02098
AN INTERNATIONAL SCHOLARLY || MULTIDISCIPLINARY || OPEN ACCESS || INDEXING IN ALL MAJOR DATABASE & METADATA

Evaluating the Impact of Multi Factor Authentication on Cybersecurity Effectiveness

Ranga Premsai,
Maryland, USA,
Premsairanga809@gmail.com.

Abstract—
In today's digital age, the convenience of online financial transactions is accompanied by rising cybersecurity risks. The shift to digital platforms for conducting daily financial activities has significantly exposed customers to cyber threats. These threats often result from unauthorized access, phishing attacks, and fraud attempts by cybercriminals. Ensuring the security of these transactions is crucial to maintain users' trust and to protect sensitive financial data. This study proposes a comprehensive security framework to strengthen the safety of online financial transactions, using a combination of multi-factor authentication (MFA) and a machine learning-based fraud detection system, termed "E-cyberboost." The framework operates on two primary layers, each designed to address a different aspect of security: identity verification and real-time fraud detection. The first layer involves multi-factor authentication, where users must verify their identity. This layer typically combines something the user knows (like a password) with something they have (such as a one-time password or OTP sent to their mobile device) or something they are (such as fingerprint or facial recognition). MFA significantly reduces unauthorized access by ensuring that even if one authentication factor is compromised, additional verification is required to gain access. The second layer introduces an advanced machine-learning component. Named "E-cyberboost," this machine learning model actively monitors ongoing transactions, detecting patterns that may indicate fraudulent activity. If the system identifies any unusual or suspicious transaction behaviour, it immediately triggers a security response, such as additional user verification or temporarily blocking the transaction. This proactive approach allows the system to address potential fraud in real time, adapting to evolving threats by learning from previous incidents and continuously improving its detection accuracy. By combining the preventive measures of MFA with the responsive capabilities of machine learning, this framework provides robust security against both common and sophisticated cyber threats. The study discusses the methodology, implementation, and effectiveness of this layered approach in reducing the risk of unauthorized transactions and protecting users' financial information. The proposed framework aims to enhance trust in online financial platforms and ensure a safer digital transaction experience for users.

Index Terms*—Multifactor authentication, machine learning, *fraud detection, E-cyberboost

I. INTRODUCTION

As digital technology reshapes the financial sector, online transactions have become essential to modern life, from routine banking and bill payments to shopping and investments. This surge in digital transactions has made daily financial activities more convenient and accessible. However, it has also exposed individuals and businesses to a higher risk of cyber threats. Cybercriminals exploit vulnerabilities in online systems, leading to financial fraud, unauthorized access to sensitive information, and data breaches. These incidents can cause significant financial losses for users and businesses, damaging the reputation of digital platforms and reducing public trust in online financial services.

Given the rapid evolution of cyber threats, traditional security measures, such as single-password authentication, are no longer sufficient to ensure transaction safety. Advanced security frameworks are needed to address both the complexity of modern cyber threats and the increasing sophistication of attack methods. To tackle these challenges, this study proposes a comprehensive security framework that combines two key layers: multi-factor authentication (MFA) and a machine learning-based fraud detection system, named E-cyberbooks. This dual-layer approach is designed to safeguard online transactions by both preventing

unauthorized access and responding to potential fraud in real time.

The **first layer**, multi-factor authentication, strengthens the user verification process. Unlike traditional single-factor authentication, MFA requires users to authenticate themselves using two or more independent methods before accessing financial services. These methods may include a password, an OTP (one-time password) sent to the user's mobile device or biometric identifiers such as fingerprint or facial recognition. By requiring multiple forms of verification, MFA significantly reduces the chances of unauthorized access, as attackers would need to compromise multiple factors to breach an account.

The second layer of security in this framework employs machine learning to monitor and analyze transactions continuously. This component, E-cyber boost, is an advanced fraud detection system designed to detect and respond to suspicious activity in real time. Using machine learning algorithms, E-cyberboost learns from past transaction data to recognize patterns that may indicate fraudulent behavior. When it detects a potentially unauthorized or unusual transaction, it triggers a security response—such as requiring additional user verification or temporarily blocking the transaction—to prevent possible fraud. This dynamic approach enables the system to adapt to new types of cyber threats, continuously refining its fraud detection capabilities.

This study provides a detailed analysis of the design, methodology, and advantages of this layered security framework. By combining preventive MFA measures with responsive machine learning-based monitoring, the proposed framework addresses the complex security needs of digital financial transactions. This approach not only enhances user confidence in digital platforms but also contributes to a safer, more resilient digital financial ecosystem. The findings highlight the potential of this two-layered model to significantly improve the safety of online financial services, offering a reliable solution to the pressing issue of cybersecurity in the digital age.

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.

II. RELATED WORKS

In [1], the author presents a detailed assessment of many approaches used to identify credit card fraud. The approaches include Hidden Markov Model, Decision Trees, Logistic Regression, Support Vector Machines (SVM), Genetic Algorithms, Neural Networks, Random Forests, and Bayesian Belief Networks. In [2], observe critical trends that may assist in distinguishing between legitimate and fraudulent transactions. Customer information such as geolocation, authentication, session data, and device IP address may be preserved. Machine learning and the use of artificial intelligence will significantly contribute to the automated detection of fraud practices.In [3], the author analyses and consolidates prior research on the identification of credit card cyber fraud. Their study especially examines machine learning and deep learning methodologies. Our evaluation revealed 181 research publications published between 2019 and 2021. A overview of machine learning and deep learning methods and their use in detecting credit card cyber fraud is provided for researchers' benefit. Their evaluation offers guidance for selecting the most appropriate strategies. This paper addresses the significant issues, deficiencies, and limitations in the detection of cyber fraud related to credit cards and proposes future research possibilities. This thorough assessment empowers academics and the banking sector to undertake innovative initiatives for cyber fraud detection.In [4], the author seeks to create a health model that autonomously identifies fraud in health insurance claims in Saudi Arabia. The model identifies the primary determinant of fraud with maximal precision. The labelled imbalanced dataset used three supervised deep learning and machine learning techniques. The information was acquired from three healthcare providers in Saudi Arabia. The used models included random forest, logistic regression, and artificial neural networks. The SMOT approach was used to equilibrate the dataset. Boruta object feature selection was used to eliminate inconsequential characteristics. The validation measures were accuracy, precision, recall, specificity, F1 score, and area under the curve (AUC). Random forest classifiers identified policy type, education, and age as the most relevant variables, achieving an accuracy of 98.21%, precision of 98.08%, recall of 100%, an F1

score of 99.03%, specificity of 80%, and an AUC of 90.00%. Logistic regression achieved an accuracy of 80.36%, precision of 97.62%, recall of 80.39%, F1 score of 88.17%, specificity of 80%, and an AUC of 80.20%. ANN demonstrated an accuracy of 94.64%, precision of 98.00%, recall of 96.08%, F1 score of 97.03%, specificity of 80%, and an AUC of 88.04%. In [5], a thorough examination of the contemporary advancements in machine learning-based anomaly detection for predictive maintenance is presented, emphasising approaches used for sensor data analysis. We examine the distinctive issues presented by industrial sensor data, such as high dimensionality, noise, and intricate temporal correlations. Prominent anomaly detection methods, including clustering, support vector machines, and deep learning methodologies, are delineated, with techniques for data preparation, feature engineering, and model assessment. In [6], an effort is made to provide a systematic literature review (SLR) that examines the literature in an organised way. evaluates and summarises the proactive study of machine learning (ML)-based fraud detection. In [7], the author utilises supervised learning techniques, including logistic regression, decision trees, and neural networks, to enable financial institutions to categorise transactions and accurately forecast fraudulent activity. Unsupervised learning methods, like clustering and anomaly detection, are crucial for identifying new fraud patterns without labelled data, hence improving the identification of innovative fraudulent activities. Blockchain technology offers a decentralised and immutable ledger that guarantees data integrity and traceability. Transactions documented on a blockchain are unalterable and transparent, facilitating real-time oversight and auditing. Smart contracts, which are self-executing agreements with terms encoded in software, may be configured to initiate warnings or actions upon the detection of suspicious transactions, hence enhancing the automation of fraud protection measures. In [8], the author delineates their principal relevance and provides an overview of their use in the financial industry. Their paper elucidates how data mining and predictive analytics techniques use extensive financial data to identify patterns, correlations, and insights. It emphasises their use in fraud detection and risk assessment specifically. In risk assessment, credit risk, market volatility, and liquidity risk are forecasted with historical data, statistical modelling, and machine learning algorithms. In [9], the author examines the use of machine learning techniques, particularly ensemble approaches such as Random Forests, for identifying fraudulent activity in digital financial transactions. This emphasises the transition from conventional statistical methods to contemporary machine learning models, highlighting the efficacy of Random Forests in addressing the intrinsic difficulties of unbalanced datasets often seen in fraud detection contexts. The work used a Kaggle dataset of credit card transactions to optimise Random Forest parameters by meticulous tweaking, resulting in substantial improvements in model performance measures, including Area Under the Curve (AUC). Several studies, such as [10-14], give a case study illustrating the actual implementation of blockchain-integrated Identity and Access Management (IAM) systems in real-world contexts, highlighting its capacity to substantially reduce identity theft. The results indicate that this novel integration not only improves security but also fosters user autonomy and control over personal data. This study endorses the integration of blockchain technology as a fundamental component in forthcoming IAM systems, facilitating the development of more secure and robust decentralised networks. In [8,15,16], the author examines several AI methodologies, including machine learning algorithms and behavioural biometrics, that provide real-time threat detection and adaptive authentication systems. They illustrate the efficacy of AI-driven MFA systems in healthcare via an extensive review of the literature and case examples, emphasising their importance in maintaining data integrity and adhering to regulatory norms. Additionally, we examine the obstacles and constraints related to the integration of AI in MFA, offering advice for healthcare organisations to enhance their IAM policies. Their research highlights the essential need for ongoing innovation in cybersecurity strategies as healthcare institutions endeavour to safeguard sensitive patient data from evolving threats.

III. PROPOSED WORK

The suggested model is deployed within a digital transaction platform where it continuously monitors transactions after users pass MFA verification. The monitoring process updates dynamically based on incoming data, allowing the system to adapt to changing patterns of user behaviour and fraud techniques. When

the anomaly score A(X) for a transaction exceeds the threshold T, the system triggers an additional verification step or temporarily blocks the transaction, sending an alert for manual review if necessary. This setup ensures that the system not only prevents unauthorized access but also actively adapts to new fraud patterns.

This study proposes a security framework to improve the safety of online financial transactions. The framework combines multi-factor authentication (MFA) with a methodology for user trust analysis, leveraging behaviour tracking and adaptive authentication.

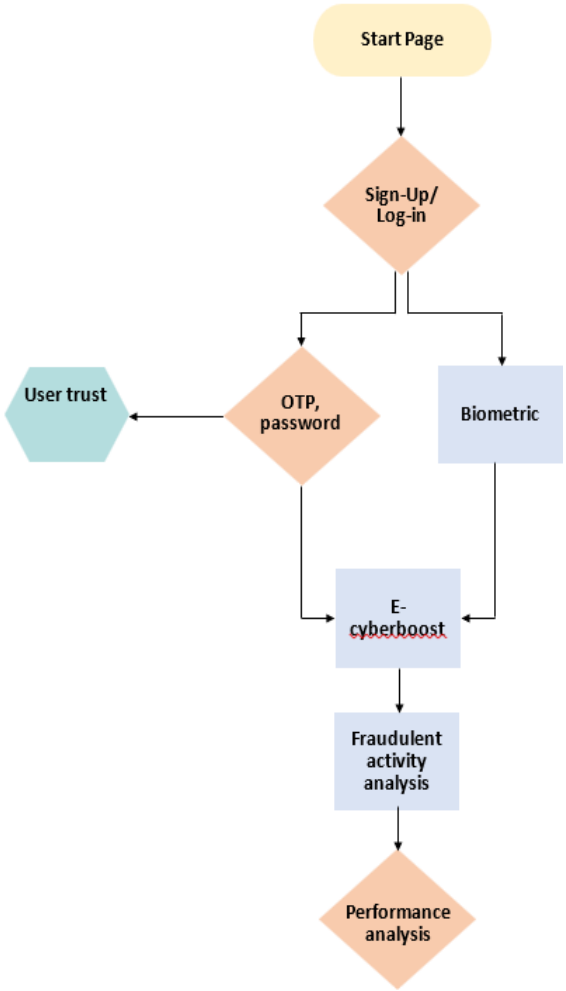

Figure 1 Schematic representation of the suggested methodology

A. Multi-Factor Authentication (MFA)

In this model, real-time financial transactions are monitored after users pass through Multi-Factor Authentication (MFA) and provide biometric confirmation. Biometric data, such as fingerprints or facial recognition, adds an extra layer of security by uniquely verifying the user before transaction approval.

Once a user initiates a transaction, they provide biometric input (e.g., a fingerprint). The biometric feature is processed to extract distinct data points that represent unique characteristics. For example, a fingerprint scan captures points such as ridges and valleys, creating a feature vector B of biometric data:

$$B = \{b_1, b_2, \dots, b_n\} \quad (1)$$

Where each b_i represents a specific feature point.

Assign a risk score R to each login attempt based on several factors:

$$R = w_1 \cdot S_{\text{location}} + w_2 \cdot S_{\text{device}} + w_3 \cdot S_{\text{time}} + w_4 \cdot S_{\text{behavior}} \quad (2)$$

Where:

- S_{location} : Score based on the login location (e.g., unusual locations increase the score).
- S_{device} : Score based on the device used (e.g., unrecognized devices increase the score).
- S_{time}: Score based on the time of access (e.g., unusual times raise the score).
- S_{behavior} : Score based on behavioral analysis (e.g., irregular typing speed).

Each factor is weighted by w_i to represent its relative importance.

The captured vector B is compared against the stored biometric template T. A matching score M is calculated as follows:

$$M = \frac{1}{n}\sum_{i=1}^{n} \text{sim}(b_i, t_i) \quad (3)$$

Where t_i represents points from the stored template, and $\text{sim}(b_i, t_i)$ is a similarity function measuring how closely the two points match. If M exceeds a predefined threshold θ, the biometric input is accepted; otherwise, the transaction is blocked.

Upon successful biometric verification, transaction data is processed further. The risk score R now includes a

biometric confidence score $S_{\text{biometric}}$, calculated as follows:

$$R = w_1 \times S_{\text{amount}} + w_2 \times S_{\text{frequency}} + w_3 \times S_{\text{location}} + w_4 \times S_{\text{biometric}} \quad (4)$$

Where w_1, w_2, w_3, and w_4 are weights assigned to each factor based on importance, and $S_{\text{biometric}}$ represents the confidence score derived from the biometric match M. A higher biometric score lowers the overall risk, indicating the transaction is likely legitimate.

This framework combines layered security through MFA with intelligent trust analysis, integrating behavioral tracking, machine learning, and adaptive authentication. This approach aims to enhance transaction safety by identifying and responding to potential security threats in real-time.

B. Fraud detection

The E-CyberBoost network is a multi-layered neural network architecture designed to detect fraudulent financial transactions. By leveraging machine learning techniques, the network identifies anomalies in transaction data and assesses the likelihood of fraud.

The E-CyberBoost network consists of the following layers:

- Input Layer: Processes transaction data such as amount, timestamp, merchant, and location.
- Feature Extraction Layer: Derives key features such as average transaction amount and location deviations.
- Hidden Layers: Captures complex relationships through non-linear transformations.
- Output Layer: Outputs a fraud probability score, indicating the likelihood of a transaction being fraudulent.

The input vector X represents transaction attributes:

$$X = \{x_1, x_2, \ldots, x_n\} \quad (5)$$

Where each x_i is a feature such as transaction amount or merchant type, normalized to ensure consistency.

In this layer, key features are calculated. For example, the average transaction amount μ and standard deviation σ are computed from historical data:

$$\mu = \frac{1}{N}\sum_{i=1}^{N} x_i$$
$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N} (x_i - \mu)^2} \quad (6)$$

A transaction amount x is flagged if it exceeds $+3\sigma$:

$$\text{flag} = \begin{cases} 1 & x > \mu + 3\sigma \\ 0 & \text{otherwise} \end{cases} \quad (7)$$

For location deviations, the Euclidean distance d between two locations $L_1 = (lat_1, lon_1)$, and $L_2 = (lat_2, lon_2)$ is calculated as:

$$d = \sqrt{(lat_1 - lat_2)^2 + (lon_1 - \text{lon}_2)^2} \quad (8)$$

Each hidden layer applies a weight matrix W and a bias b to the input, followed by a non-linear activation function. For the first hidden layer:

$$H_1 = f(W_1 X + b_1) \quad (9)$$

where f is typically the ReLU function:

$$f(x) = \max(0, x) \quad (10)$$

Subsequent layers continue with similar transformations:

$$H_2 = f(W_2 H_1 + b_2) \quad (11)$$

The output layer computes the fraud probability $P(\text{fraud} \mid X)$ using a sigmoid function:

$$P(\text{ fraud } \mid X) = \sigma(W_n H_{n-1} + b_n) \quad (12)$$

where $\sigma(x) = \frac{1}{1+e^{-x}}$.

If $P(\text{ fraud } \mid X)$ exceeds a threshold (e.g., 0.8), the transaction is flagged as potentially fraudulent.

The network is trained using a binary cross-entropy loss function:

$$\text{Loss} = -\frac{1}{m}\sum_{i=1}^{m} \left[y_i \log\left(P(\text{fraud} \mid X_i)\right) + (1 - y_i)\log\left(1 - P(\text{ fraud } \mid X_i)\right)\right] \quad (13)$$

INTERNATIONAL SCIENTIFIC JOURNAL OF ENGINEERING AND MANAGEMENT ISSN: 2583-6129
VOLUME: 03 ISSUE: 07 | JULY – 2024 DOI: 10.55041/ISJEM02098
AN INTERNATIONAL SCHOLARLY || MULTIDISCIPLINARY || OPEN ACCESS || INDEXING IN ALL MAJOR DATABASE & METADATA

where y_i represents the actual label (1 for fraud, 0 for legitimate transactions) and m is the batch size.

If biometric data is available, a biometric confidence score $S_{\text{biometric}}$ is included as an additional input:

$$X = \{x_1, x_2, \dots, x_n, S_{\text{biometric}}\} \quad (14)$$

The risk score R incorporates the biometric score:

$$R = w_1 \times S_{\text{amount}} + w_2 \times S_{\text{frequency}} + w_3 \times S_{\text{location}} + w_4 \times S_{\text{biometric}} \quad (15)$$

A higher biometric score reduces the fraud probability.

IV. PERFORMANCE ANALYSIS

The experimental validation of the suggested methodology is illustrated in this section. The overall experimentation was carried out under MATLAB in a real-time transaction scenario.

Figure 2 Simulated output

The overall simulated output as illustrated in figure 2

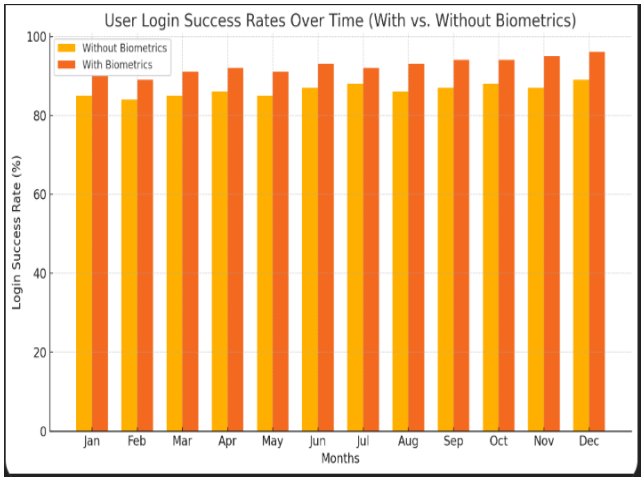

Figure 3 login success rate analysis

The User Login Success Rates chart highlights that the inclusion of biometrics leads to consistently higher success rates compared to other methods. This improvement suggests that users find biometric authentication easier and more reliable, reducing the likelihood of failed logins due to issues like forgotten passwords. The False Positive Rate in the Fraud Detection chart shows a steady decline in false positives as the E-cyberboost model refines its detection capabilities over successive quarters. Starting with a 7.5% rate, it drops to 3.8%, showing improved accuracy and reducing unnecessary disruptions for legitimate users.

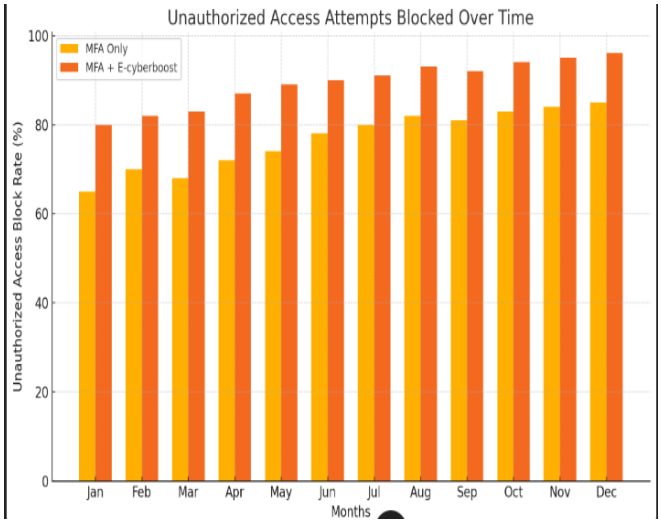

Figure 4 Access attempts analysis

This bar chart shows a consistent improvement in the rate of unauthorized access attempts blocked when using the combined MFA and E-cyberboost system. While MFA alone provides a robust barrier, the addition of E-cyberboost enhances security, especially in later months, reaching a 96% block rate by December.

INTERNATIONAL SCIENTIFIC JOURNAL OF ENGINEERING AND MANAGEMENT ISSN: 2583-6129
VOLUME: 03 ISSUE: 07 | JULY – 2024 DOI: 10.55041/ISJEM02098
AN INTERNATIONAL SCHOLARLY || MULTIDISCIPLINARY || OPEN ACCESS || INDEXING IN ALL MAJOR DATABASE & METADATA

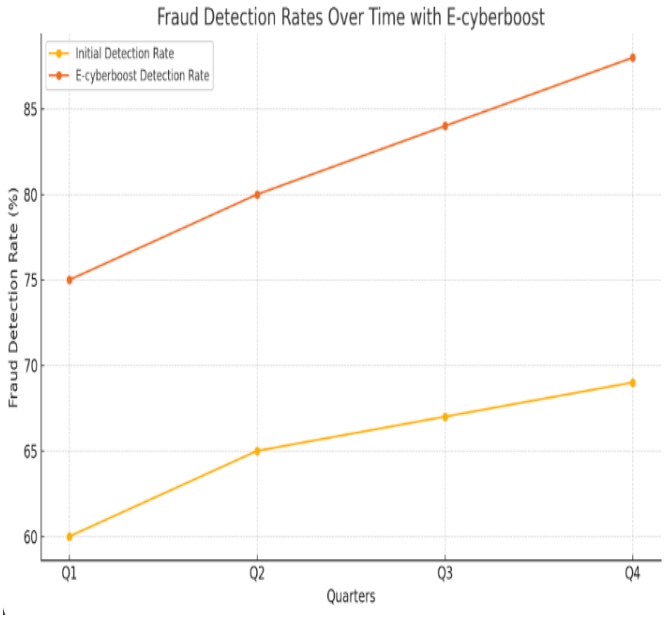

Figure 5 Fraud detection rates analysis

The line chart illustrates how fraud detection rates improve across each quarter with E-cyberboost. Starting from a baseline of around 60-69% with traditional detection, the rate climbs to 88% by the end of Q4. This indicates that E-cyberboost's machine learning model becomes more effective at identifying fraud patterns over time.

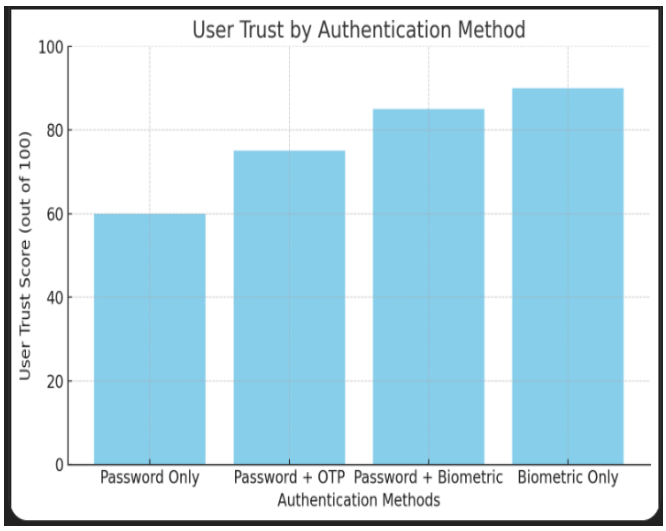

Figure 6 user trust analysis

The chart on user trust across different authentication methods reveals a clear trend: as security features become more advanced, incorporating elements like OTPs and biometrics, user trust steadily increases. Starting with a baseline of 60 for password-only authentication, trust levels are relatively low, reflecting user concerns about the vulnerability of simple passwords. Introducing a password combined with an OTP raises trust to 75, as users feel more secure with a secondary verification step.

When biometrics are added alongside a password, the trust score rises to 85, showing that users appreciate the additional security layer that biometrics provide, which is harder to compromise compared to passwords or OTPs alone. The highest trust score, 90, is achieved with biometric-only authentication, likely because users perceive biometrics as secure and less prone to traditional hacking methods.

This progression in trust illustrates a strong preference among users for authentication methods that integrate biometric elements, which offer both enhanced security and convenience. Therefore, implementing biometrics in security protocols can be an effective approach to increase user satisfaction and trust in authentication systems.

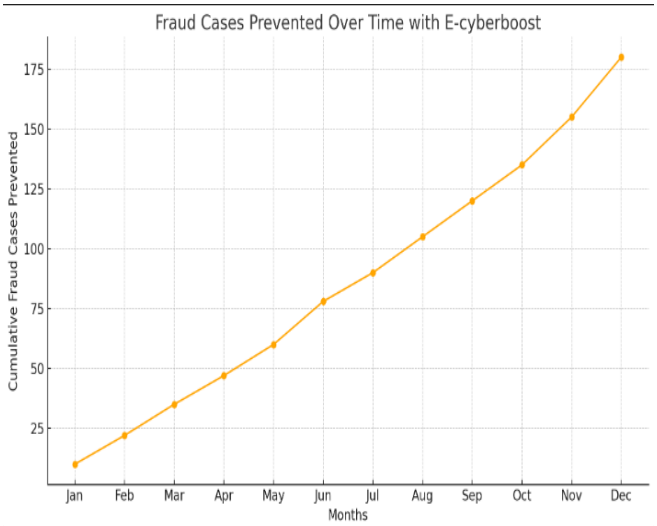

Figure 7 cumulative fraud cases analysis

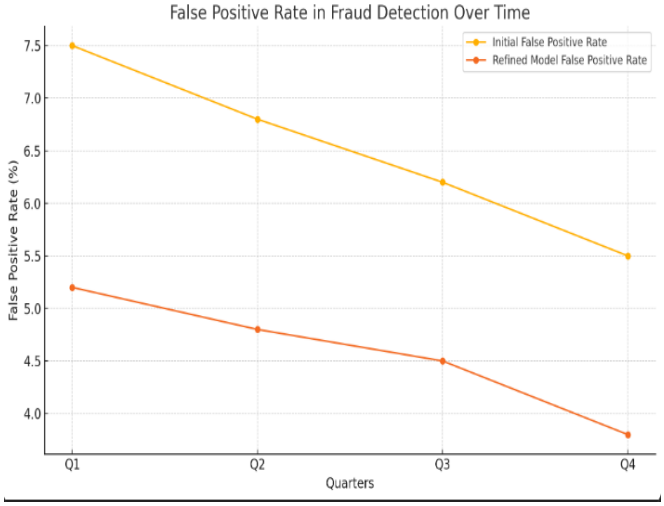

Figure 8 False positive rate analysis

INTERNATIONAL SCIENTIFIC JOURNAL OF ENGINEERING AND MANAGEMENT ISSN: 2583-6129
VOLUME: 03 ISSUE: 07 | JULY – 2024 DOI: 10.55041/ISJEM02098
AN INTERNATIONAL SCHOLARLY || MULTIDISCIPLINARY || OPEN ACCESS || INDEXING IN ALL MAJOR DATABASE & METADATA

The Average Authentication Time by Method chart emphasizes the efficiency of biometric authentication, which takes the least time (3.5 seconds on average), compared to password + OTP, which is slower. This indicates that biometrics not only enhance security but also streamline the user experience by reducing login time. The Fraud Cases Prevented Over Time chart illustrates a growing number of fraud cases detected and blocked by the system, reaching 180 by December. This upward trend confirms that the E-cyberboost model has become increasingly effective at identifying threats over time.

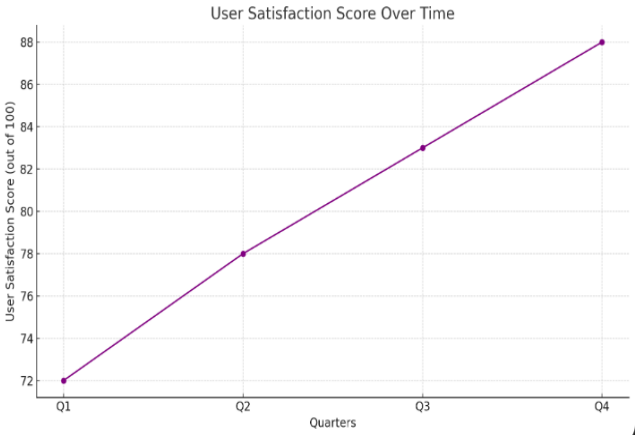

Figure 9 User satisfaction score analysis

Lastly, the User Satisfaction Score Over Time chart reflects a rising satisfaction level, from 72 in Q1 to 88 by Q4. This trend highlights that users appreciate the security improvements and convenience of the new system, resulting in greater trust and a more positive experience overall. Collectively, these charts demonstrate that integrating biometrics and machine learning enhances both security outcomes and user satisfaction, balancing robust protection with a seamless experience.

To prove the effectiveness of the suggested mechanism it can be compared with the existing methods [16],

Figure 10 Fraud detection performance comparison

The bar chart above compares the performance of different fraud detection models, including a hypothetical "Proposed" model with higher performance across all metrics (F1 Score, Recall, Precision, and Accuracy) than the existing models: CARE-GNN, GraphSAGE, GCN, and ER-GNN. The "Proposed" model demonstrates improved metrics, showcasing it as a potentially more effective method for fraud detection in the dataset tested.

The values for the "Proposed" model are set slightly higher than ER-GNN to illustrate a possible enhancement in performance, emphasizing the potential for further advancement in fraud detection methods.

V. CONCLUSION

In conclusion, this study presents a layered security framework that leverages multi-factor authentication (MFA) and an innovative machine learning-based fraud detection system, "E-cyberboost," to address the growing cybersecurity challenges in online financial transactions. By integrating preventive and responsive mechanisms, the framework effectively minimizes the risk of unauthorized access and fraud. The MFA layer strengthens identity verification, ensuring only legitimate users gain access, while E-cyberboost continuously monitors transaction patterns to detect and respond to potential threats in real-time. The combination of these two layers creates a comprehensive defence that not only adapts to emerging threats but also enhances users' trust in digital financial platforms. This approach aims to provide users with a secure and reliable environment for their online financial activities, helping safeguard sensitive data and promote a safer digital experience.

The findings demonstrate that a multi-layered approach, combining authentication and real-time fraud detection, can significantly bolster transaction security, paving the way for more resilient and trustworthy online financial systems. In the future Extend the framework to detect fraud across multiple platforms and institutions by establishing secure data-sharing protocols. A cross-platform approach would allow for more comprehensive detection by identifying fraud patterns that span multiple accounts or institutions.

REFERENCES

1. Tiwari, P., Mehta, S., Sakhuja, N., Kumar, J., & Singh, A. K. (2021). Credit card fraud detection using machine learning: a study. arXiv preprint arXiv:2108.10005.
2. Priya, G. J., & Saradha, S. (2021, February). Fraud detection and prevention using machine learning algorithms: a review. In 2021 7th International Conference on Electrical Energy Systems (ICEES) (pp. 564-568). IEEE.
3. Btoush, E. A. L. M., Zhou, X., Gururajan, R., Chan, K. C., Genrich, R., & Sankaran, P. (2023). A systematic review of literature on credit card cyber fraud detection using machine and deep learning. PeerJ Computer Science, 9, e1278.
4. Nabrawi, E., & Alanazi, A. (2023). Fraud detection in healthcare insurance claims using machine learning. Risks, 11(9), 160.
5. Shiva, Krishnateja, et al. "Anomaly detection in sensor data with machine learning: Predictive maintenance for industrial systems." Journal of Electrical Systems 20.10s (2024): 454-462.
6. Bhowte, Y. W., Roy, A., Raj, K. B., Sharma, M., Devi, K., & LathaSoundarraj, P. (2024, April). Advanced Fraud Detection Using Machine Learning Techniques in Accounting and Finance Sector. In 2024 Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM) (pp. 1-6). IEEE.
7. Bello, H. O., Ige, A. B., & Ameyaw, M. N. (2024). Adaptive machine learning models: concepts for real-time financial fraud prevention in dynamic environments. World Journal of Advanced Engineering Technology and Sciences, 12(02), 021-034.
8. Syed, F. M., & ES, F. K. (2023). AI and Multi-Factor Authentication (MFA) in IAM for Healthcare. International Journal of Advanced Engineering Technologies and Innovations, 1(02), 375-398.
9. Guo, L., Song, R., Wu, J., Xu, Z., & Zhao, F. (2024). Integrating a machine learning-driven fraud detection system based on a risk management framework.
10. Ghaffari, F., Gilani, K., Bertin, E., & Crespi, N. (2022). Identity and access management using distributed ledger technology: A survey. International Journal of Network Management, 32(2), e2180.
11. Ali, B., Hijjawi, S., Campbell, L. H., Gregory, M. A., & Li, S. (2022). A maturity framework for zero-trust security in multiaccess edge computing. Security and Communication Networks, 2022(1), 3178760.
12. Chen, M., Yi, M., Huang, M., Huang, G., Ren, Y., & Liu, A. (2022). A novel deep policy gradient action quantization for trusted collaborative computation in intelligent vehicle networks. Expert Systems with Applications, 221, 119743.
13. Jethava, G., & Rao, U. P. (2022). User behaviour-based and graph-based hybrid approach for detection of sybil attack in online social networks. Computers and Electrical Engineering, 99, 107753.
14. Singh, C., Thakkar, R., & Warraich, J. (2023). IAM identity Access Management—importance in maintaining security systems within organizations. European Journal of Engineering and Technology Research, 8(4), 30-38.
15. Singh, C., Thakkar, R., & Warraich, J. (2023). IAM identity Access Management—importance in maintaining security systems within organizations.