A Novel Risk-Based Multi-Factor Authentication (MFA) Approach for Card-Not-Present (CNP) Transactions

Prakash Chandra Mondal[1], Pritu Parna Sarkar[2]

[1]Independent Researcher, Joint Director (ICT), Information and Communication Technology Department, The Central Bank of Bangladesh (Bangladesh Bank), Bangladesh

[2]Graduate Research Assistant, Dept. of Mechanical Engineering, The University of Texas Rio Grande Valley, Edinburg, Texas 78539, United States

DOI: https://dx.doi.org/10.47772/IJRISS.2025.90300240

Received: 15 March 2025; Accepted: 22 March 2025; Published: 10 April 2025

ABSTRACT

Using biometric information and a Personal Identification Number (PIN) is not recommended for Card-Not-Present (CNP) online payments because merchants' portals and payment processors are not standardized to accept or verify biometric data and PINs. Additionally, it increases the risk of critical information interception through keyloggers, malware, or phishing attacks. Similarly, using OTP poses several risks and limitations, including SIM swapping, delayed or failed OTP delivery, and vulnerabilities in the SS7 protocol. In this model, we utilized an innovative, configurable Multi-Factor Authentication (MFA) for user authentication and transaction authorization in CNP online payments, based on the theme "what we want." The proposed additional factor for MFA consists of users' expected transaction amount and time slot. MFA configuration is available via a bank's or financial institution's web portal or mobile app following a successful login and risk-based assessment. The risk-based assessment employs a weighted analysis of users' historical activities to calculate the associative risk score (R). Dynamic Challenge Questions (CQs) are used to verify risky users with high-risk scores (R). The CQ(s) are enabled on a need basis, based on the value of the R for the user who is willing to configure MFA for transaction purposes. Implementing this risk-based MFA approach can significantly reduce financial losses from fraudulent actions in CNP online transactions, as transactions remain within users' consent, predefined limits, and risk acceptance levels, whereas existing MFA solutions often require the use of registered mobile phones, tokens, or biometric information.

Keywords: MFA, Credit Card, Debit Card, E-Commerce Payment, Online Transactions, E-Payment, Authentication, Authorization

INTRODUCTION

Financial Technology (FinTech) enables banks and Financial Institutions (FIs) to provide financial services in an improved way (Schueffel, 2016). FinTech encompasses mobile financial services (MFS), online banking, and payment gateways that provide quick and easy services to users (Ul et al., 2017). The increasing number of FinTech solutions leads to a rise in fraudulent transactions, and preventing such activities remains challenging (Cherif et al., 2023). Fraudulent activities in online card transactions have resulted in substantial financial losses worldwide. 2023 global payment card fraud losses reached approximately $33.83 billion, which increased from $33.45 billion in 2022 (Report, 2025). Merchant losses from online payment fraud are projected to exceed $362 billion globally between 2023 and 2028, with an estimated $91 billion in losses anticipated in 2028 alone (Global Online Payment Fraud Market Report *2023*, 2023). These figures underscore the escalating threat of online payment fraud, highlighting the need for robust security measures and ongoing vigilance to mitigate potential losses for both users and businesses. The researcher aims to identify illegitimate users in order to restrict access and ensure that legitimate users receive quick and smooth services. Users'

behavioral biometrics and interactions with financial systems help assess their quality and generate a risk score, which is used to identify and authenticate legitimate users. (Mondal et al., 2016a, Mondal et al., 2016b)

Authentication is a procedure to verify a user's credentials to prove identity (Meneses et al., 2022). Many recent studies have used machine learning (ML) methods to solve real-world challenges (Lomba et al., 2022, Díaz Redondo et al., 2023, González-Soto et al., 2024, Malta et al., 2023, Paladino et al., 2023, Abumohsen et al., 2023, Owess et al., 2023, Kulatilleke, 2022), such as financial fraud detection. Financial fraud is described as unlawful deception that is done to make money (Gaikwad et al., 2014). NIST publications (Ometov et al., 2018) show a relation between the number of authentication elements and the degree of safety. The European Union (EU) regulation (Burr et al., 2011) suggested a powerful authentication mechanism using two or more factors from separate groups to verify users. Since then, a greater degree of security has been represented by MFA (Kennedy & Millard, 2016), while users are forced to provide multiple authentication credentials (more than two) to access an online system (Dasgupta et al., 2017, Bell, 2022). Some studies incorporate two layers of security, utilizing authenticated users and a machine learning component. Machine learning is triggered when the system detects potential fraud. This machine learning layer employs facial recognition as a decisive authentication factor for further protection of two-factor authentication to verify users (Aburbeian & Fernández-Veiga, 2024).

On the other hand, layered security or Defense in Depth (DiD) is a proven concept used in information security that enables multiple layers of security controls throughout an information technology system (Alsaqour et al., 2021). Like the concept of layered security, MFA for authentication and transaction authorization creates multilayer security controls in the application security layer for user authentication when accessing information assets, as shown in ***Figure 1***.

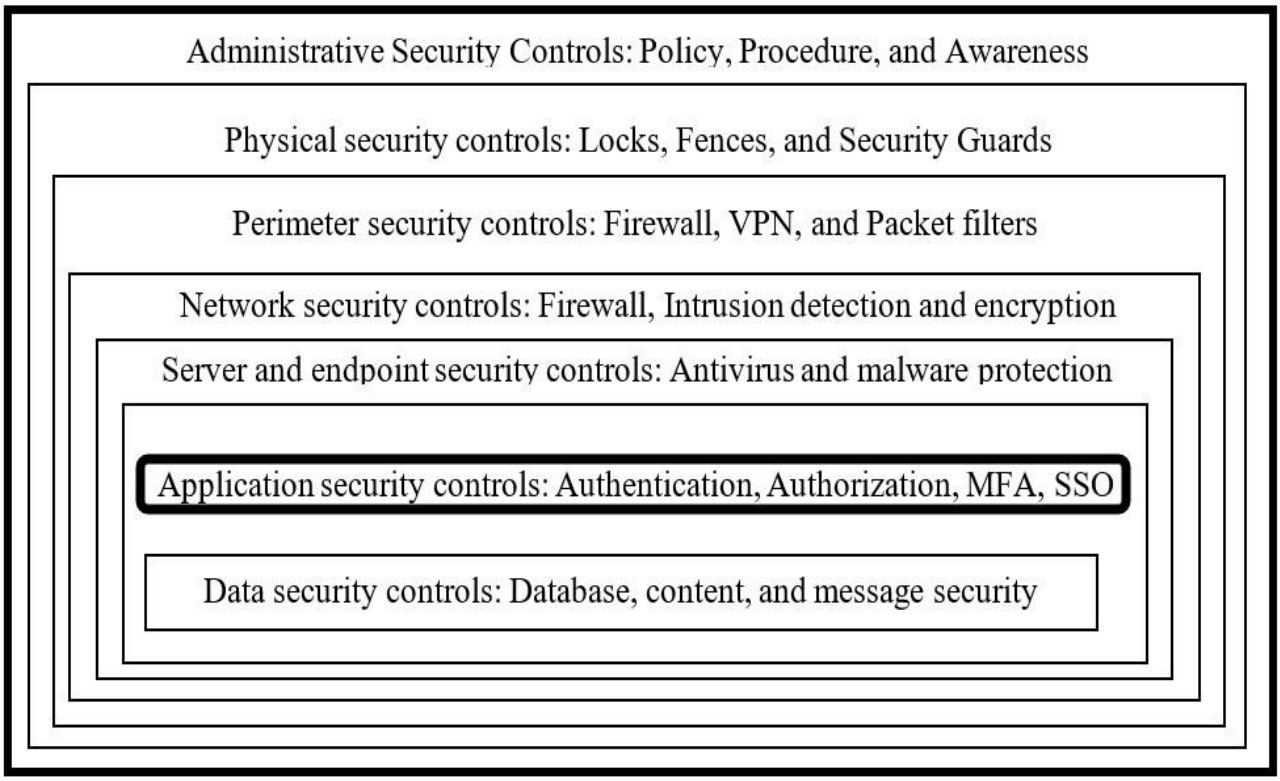

Figure 1 MFA introduces additional layered security within the application for authentication purposes

MFA is a form of layered security using multiple independent authentication factors to verify a user's identity. These factors create layers of security, making it harder for attackers to gain unauthorized access. Commonly used factors are something we know (Card Number, Expire Date, CVV, login, password, PIN, etc.), something we have (OTP, security token, smart card, App, payment card, etc.), and something we are (Face, Fingerprint, IRIS, Retina, Voice, etc.)(A SURVEY AND COMPARISON ON USER AUTHENTICATION METHODS | International Journal of Innovations in Engineering Research and Technology, n.d.) shown in **Figure 2**.

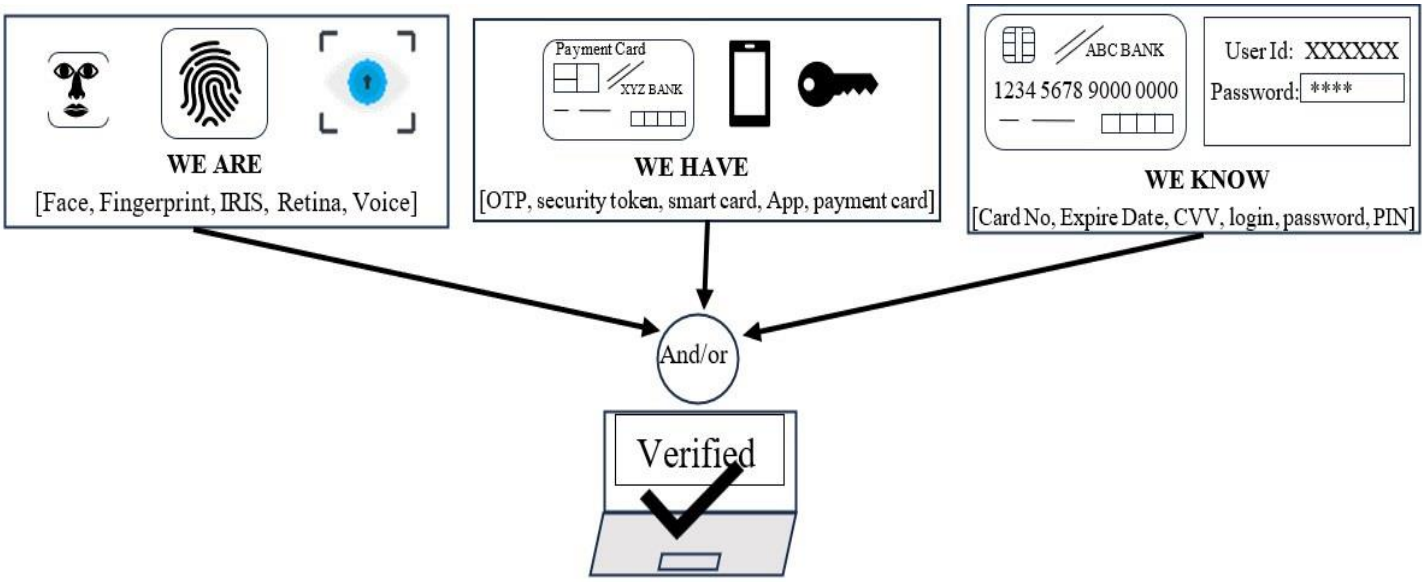

Figure 3 Traditional Multi-factor Authentication (MFA)

MFA enables a multi-layered approach to verify a user before delivering a financial service. An attacker cannot compromise MFA to access financial systems. The financial service provider has a prime obligation to ensure that users receive financial services securely, promptly, and efficiently whenever and wherever they want them. While MFA enhances security, it can also cause inconvenience to legitimate users. Considering user comfort, we have introduced user behavioral activities to assess whether a user is acting with legitimate or fraudulent intent, thereby offering a quicker service to legitimate users. If the user's activities present an unnatural or higher risk score (R), then CQ(s) will be assigned to request further verification from the user before allowing the configuration and preparation of a predefined MFA. Hence, CQ(s) are prepared from users' known information, including Know Your Customer (KYC) information, activity information, and inputted information, with a system- or user-defined weight assigned to each. The number of CQs and the selection of CQs are dependent on the user's risk score (R).

This research employed a novel MFA to authenticate users and authorize transactions, utilizing a term referred to as "what we want." When we make a CNP online transaction, we want a specific amount of money transferred to other accounts within a specified time frame. This requirement is used as a factor in MFA in this model.

Section 3 elaborates on and explores existing works on MFA and risk assessment for online users, with a focus on user authentication and transaction authorization. In Section 4, we classify and analyze the application methods and objects of the model according to technical categories, including process flow, data analysis, and outcome. Section 5 summarizes the test and outcome from the simulation of the process. In section 6, we discussed the result of the process. In Section 7, we addressed the limitations of current research and proposed future research topics to explore the broader applications of MFA. Finally, Section 8 presents the conclusions of this research work.

LITERATURE REVIEW

Assessing risk from the user's approach in the online environment and taking measures to restrict high-risk users is a popular method of promptly allowing financial services only to legitimate users (Cai & Zhu, 2016). MFA is a layered verification method that filters actual users for financial service delivery (Ometov et al., 2018). MFA is highly used in transaction authorization for CNP online payment where payment card number and card registration address are verified with the delivery address for proceeding transaction, which is known as address verification service (AVS) (U.S. Patent Application for Computer Systems and Computer-Implemented Methods for Card-Not-Present Transactions Patent Application (Application #20190026735 Issued January 24, 2019) - Justia Patents Search, n.d.). A research trend focuses on the formal verification of

cashless payment protocols, identifying security vulnerabilities and potential challenges in online card payments, where formal verification is a method to analyze and verify such protocols' security and detect flaws before they are widely deployed (Sakurada & Sakurai, 2024). To achieve the security objectives in CNP online transactions, a paper focused on fraudulent activity, where fraud involves illegal acquisition and unauthorized use of another individual's payment details to engage in online transactions. A crime script approach has been offered in a paper to analyze the steps involved in the commission of crimes, and it also identifies potential areas of disruption through specific crime prevention strategies (Bodker et al., 2023). Some research work rated the integration of keystroke dynamics with OTP rather than using only OTP for MFA purposes(A User Study of Keystroke Dynamics as Second Factor in Web MFA | Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy, n.d.). While security in online payment is a great concern, some combine with a bank-registered device via IP address, cookies, or a digital certificate as an extra layer of security, as MFA for online user authentication(Multi-Factor Authentication Method for Online Banking Services in South Africa, n.d.). To prevent online transaction fraud, the stakeholders of financial transaction-related companies have implemented various secure authentication and authorization practices at all levels. A paper offered an additional factor for secure authentication for online transactions with PIN and OTP, considering transaction initiators' global positioning system (GPS) location to serve the purpose of MFA (Full Article: Implementation of an Additional Factor for Secure Authentication in Online Transactions, n.d.). A framework to secure wireless payment systems was proposed for transaction identification codes and SMS to enforce additional security levels like MFA with existing login/password systems(A Multifactor Secure Authentication System for Wireless Payment, n.d.). Mohammed et al. suggested an innovative authentication model that consists of 5 levels that contain one or a combination of authentication factors, such as knowledge-based, possession-based, or biometric-based factors. The model is then enhanced by adding control information factors, specifically for levels 4 and 5, to support layering needs like MFA(Mohammed & Elsadig, 2013). Chetalam et al. described the authentication process through the incorporation of a voice biometric for the payment platform named MPESA to use as MFA(Chetalam, 2018). Bartłomiejczyk et al. discussed using smartphones for authentication, which enables user authentication using three authentication factors: possession, knowledge, and inherence as MFA (Bartłomiejczyk et al., 2019). A PhD thesis research implemented secure mobile money authentication and authorization by combining multiple securely stored factors, such as MFA, to help mobile money subscribers and stakeholders trust the developed native genuine mobile money (G-MoMo) applications (Guma, 2022). Many researchers have used biometric-based authentication as MFA to prevent fraud in financial transactions, using behavioral biometrics called signatures, fingerprint or palm vein scans, facial recognition, etc., to work as MFA (Scaria & Karman Megalingam, 2018; Hassan & Shukur, 2021, Zadeh & Barati, 2020, Jaspher Willsie Kathrine & Kirubakaran, 2011, Cai & Zhu, 2016, Mondal et al., 2017). The study by Krol et al. on UK-based online banking users suggested that hardware tokens added to the user's mental and physical workload reduced the number of authentication steps and removed features that did not enhance security but negatively impacted the user experience (Krol et al., 2015). A significant amount of research has been conducted on MFA solutions, and some solutions are also being practiced to solve real-world problems remain practiced in the real world. The use of biometric information and PIN as MFA in non-standard e-commerce web portals for online transactions increases the risk of critical data breaches; therefore, a new approach to MFA is required to filter legitimate users in online transactions.

METHODOLOGY

Providing service promptly to the legitimate user and restricting fraudsters in CNP online transactions, we used preconfigured MFA to solve challenges regarding card data breaches, stolen cards, and identity theft-related issues. In this process, we have utilized a newly proposed configurable MFA to apply during transactions. An important part of this study is to identify a legitimate user to allow MFA configuration. Before allowing a user to configure MFA, we classify the user by analyzing their interaction history in the bank database and current behavioral patterns. It is known that legitimate users and fraudsters differ based on their activity patterns, such as changing the IP address, device MAC address, access timing, nature of the interaction (content requests), the time gap between geolocation changes, and frequent failed login attempts in the online portal. Before a user configures MFA, the process redirects them to the risk assessment and verification process.

The detailed data flow of the MFA configuration is depicted in ***Figure 4***. Once users successfully log in to the portal or app to configure MFA, they undergo a risk assessment to evaluate their activities and calculate a risk score, considering various potential factors based on their behavioral patterns. If a user is deemed risky and achieves a higher risk score, they receive CQ(s) for further verification by the bank portal or app. Based on the user's answer to the CQ(s), they allow or deny MFA configuration. If the risk score is nominal and the user is assessed as a trusted user, the MFA configuration is allowed. Hence, only trusted and verified users received the opportunity to configure MFA. The MFA configured for use in this model is based on the concept named "what we want," which means “what the user wants”. According to the concept, an online transaction amount and time slot are used to authenticate a user and authorize a transaction as an additional factor in MFA.

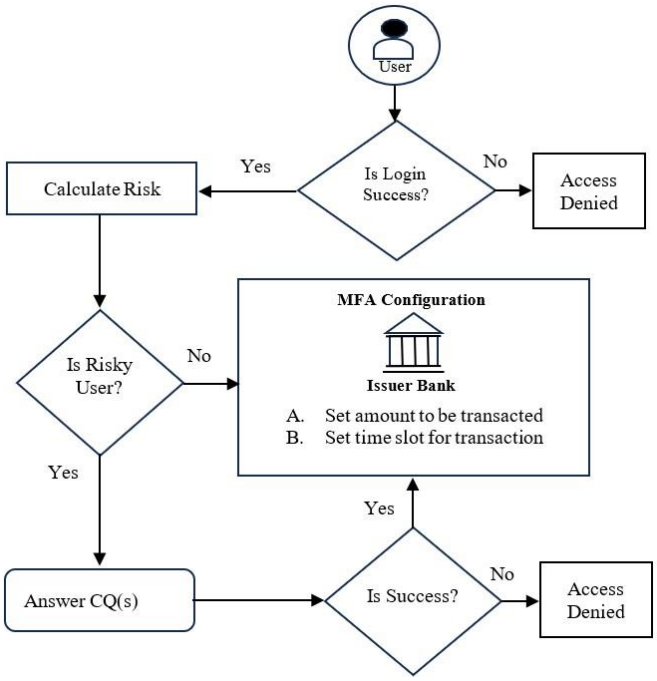

Figure 5 Setting MFA to authenticate users and authorize CNP transactions

In the case of a traditional process, all CNP online transactions and e-commerce transactions are forwarded to the payment processor for verification and a payment request. The payment request is sent to the issuer bank for authorization as a request for authorization. Our MFA effectively works in the issuer bank end to verify and authorize the transaction after matching with the preconfigured MFA (amount and time slot). If the verification is successful with MFA, the system responds to complete the transaction with the acquirer bank through the card network. The complete flow of a transaction is shown in ***Figure 6***. Hence, the MFA plays a crucial role in authenticating users, authorizing transactions from the issuer bank, and executing transactions as the user intends. Since the amount and time slot will be assigned based on the user's desires, the risk in this process remains within the user’s acceptable risk level.

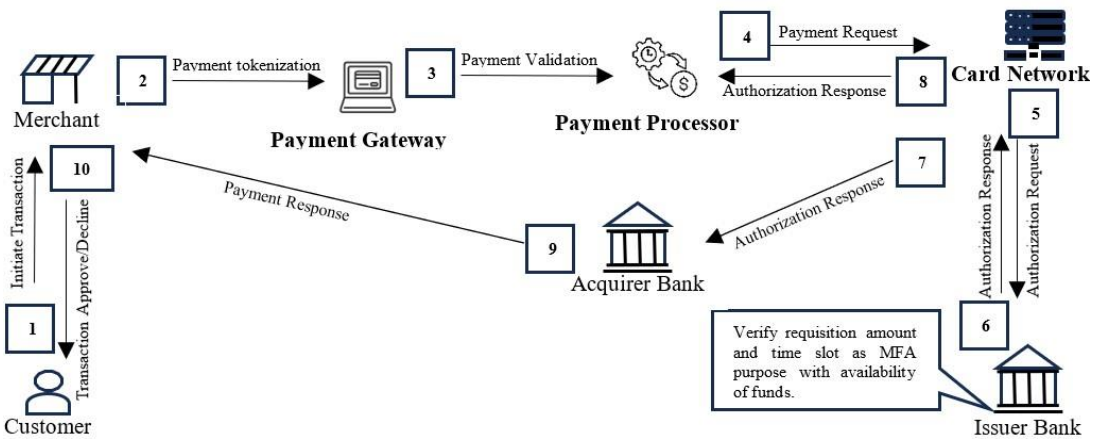

Figure 7 The lifecycle of an online CNP payment with MFA

Within the scope of this work, we employ a novel MFA approach that leverages users' configuration of transaction profiles tailored to their specific requirements. This approach utilizes multiple channels to complete the authentication process in accordance with MFA standards. Since PINs and OTPs may not be feasible for MFA in non-standard payment portals due to risks such as inaccessibility, SIM swapping, or vishing, the use of this preconfigured MFA is considered the most reliable authentication method. The method uses card information and banking portal login information from something we know. During the authentication process, the method verifies the preconfigured MFA (amount and time slot) as something we want, as shown in ***Figure 8***. As the authentication process verifies preconfigured MFA individually, a fraudster cannot initiate a transaction using a stolen identity, compromised card data, or stolen cards. Moreover, a risk assessment-based CQ(s) verification has been used to prevent a fraudster from configuring MFA through a bank portal or app.

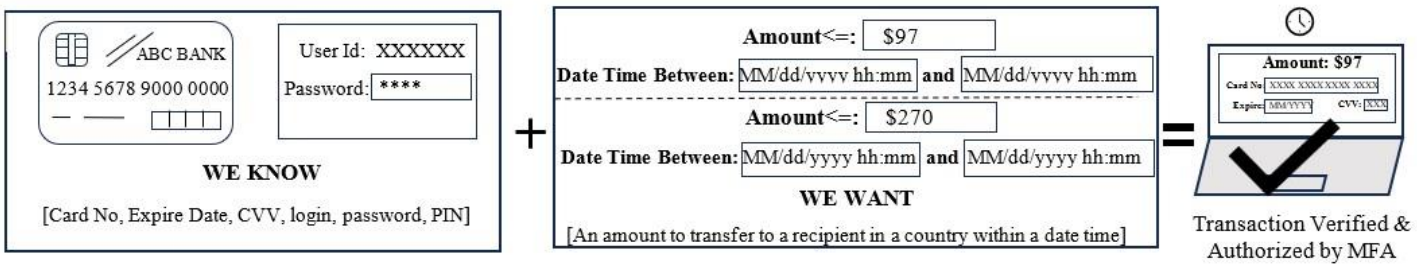

Figure 9 An innovative MFA in CNP online transaction based on something we want

To prevent illegitimate users from configuring MFA, a risk assessment was conducted, and further verification was based on the risk score (R). The activity pattern of the user can be used to assess the risk score (R) of an online user during interaction with the banking app or web portal. Typically, threat actors or hackers modify access IP addresses and geolocations, accessing devices continuously, quickly, and in an unnatural manner to gain access to the portal or app. In most cases, illegal login approaches are initiated using a VPN, ToR, proxy, or a bad-quality IP address. For this reason, the risk score of a user is assessed based on the interaction or behavioral pattern introduced by the user on an app or web portal. The history of the change of geolocations, frequent failed login attempts, requests from suspicious IP addresses, change of Operating Systems (OS), device MAC addresses, change of browsers, changes of access time, the unusual time gap in geolocation change, unusual access time, etc. are considered to carry out risk associate the user. The rules for the risk scoring of a user have been explained in Table 1 Risk scoring on behavioral patterns.

Table 2 Risk scoring on behavioral patterns

Sl.	Risk Factor	Weight (0–10)	Rules/ Algorithm for the Risk Scoring
1	Regular app or portal user login	10/X	0-Legitimate user X-Access Denied
2	Change of Geolocation (R_g)	0-10	Calculated on the previous history of geolocation change. **Risk score**(R_g)= 5× (0/1-geolocation change)+5×(1-P_g) Probability of geolocation change by the user (P_g) = number of accesses from the current geolocation/Total number of accesses in the history.
3	Frequent failed login attempts and requests from suspicious IP addresses (IP quality check)(R_i)	0-10	Calculated the previous history of failed login attempts. **Risk score**(R_i)= 5×(0/1-IP Quality)+5×P_i Probability of login failure by the user (P_i) = Maximum number of failed login attempts /Total number of access history

4	Change of Operating Systems or version/ change of Device/type (mobile, desktop)/MAC address/change of web browser/first-time transaction (R_o)	0-10	Calculated based on the previous history of the device change. **Risk score**(R_o)= 5× (0/1-Device change)+5×(1-P_o) Probability of device change by the user (P_o) = number of accesses from the current device/Total number of accesses in the history.
5	Changing banking portal accessing time(R_t)	0-10	Calculated according to the portal access timing history. **Risk score**(R_t)= 10×(1-P_t) Probability of appearance of the user in current access time (P_t) = Number of accesses in the current hour/Maximum number of accesses per hour
6	Unusual time gap between geolocation change Unusual login locations or times compared to previous logins	10/X(Access Denied)	If geolocation changing time<30 minutes, then it is treated as high-risk and/or lateral movement and directly denied to configure MFA
Total Calculated Risk (R)=MAX(R_g, R_l, R_i, R_o, R_t)			

As shown in *Table 3 Risk scoring on behavioral patterns*, we calculate a user's risk score to select applicable verification measures using CQ. Fraudsters are identifiable from unusual interactions with the banking web portal or app. When using the banking portal and app, a deceptive user usually appears with different patterns.

The risk score from a user's geolocation change (R_g) is crucial, as a malicious user may try to access the bank web portal or app by changing several geolocations, or a geolocation change may be a natural user pattern. Thus, to assess a user's credibility, we evaluate the probability of the user's geolocation change from their historical records of accessing geolocation. The mathematical formula for determining the risk score from geolocation change (R_g) is presented in Equations 1 and 2.

$$\text{Probability of geolocation change by the user } (P_g) = \frac{\text{number of accesses from current geolocation}}{\text{Total number of accesses history}} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

$$\text{Risk score associated with the geolocation change } (R_g) = 5 \times (0 \text{ or } 1) + 5 \times (1 - P_g) \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (2)$$

In Equation 2, we consider 1 for a change in geolocation and 0 for the same geolocation as the last access.

Similarly, the risk score from failed login attempts and bad-quality IP addresses (R_i) is also important, as a fraudulent user may attempt multiple failed attempts, use brute-force attacks, or employ credential stuffing from bad-quality IPs using VPNs or TOR. Thus, to assess the quality of a user, we evaluate the probability of the failed login behavioral pattern against a historical pattern, because in some cases, a failed login may be a natural characteristic of a user. Risk score from the accessing IP address and failed login attempt (R_i) has been calculated using equations 3 and 4

$$\text{Probability login failure by the user } (P_i) = \frac{\text{Maximum number of failed login attempts}}{\text{Total number of access history}} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (3)$$

$$\text{Risk score}(R_i) = 5 \times (1 \text{ or}, 0.5 \text{ or}, 0) + 5 \times P_i \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (4)$$

In Equation 4, we consider 1 for accessing from a bad-quality IP, 0.5 for a suspicious IP, and 0 for a good IP.

Moreover, the risk score from the change in device MAC address (Ro) is significant, as a deceptive user may

attempt to access the bank's web portal or app by using multiple new or spoofed devices, or a legitimate user may have numerous devices naturally. Thus, to assess a user's quality, we evaluate the probability of the user's device change from its historical records of accessing device(s). The risk score for the unusual nature of device change (Ro) is calculated using Equations 5 and 6.

$$\text{Probability of device change } (P_o) = \frac{\text{Number of access from current device}}{\text{Total number of access history}} \ldots\ldots\ldots\ldots\ldots \quad (5)$$

$$\text{Risk score}(R_o) = 5 \times (0 \text{ or}, 1) + 5 \times (1 - \text{Po}) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (6)$$

In Equation 6, we consider 1 for a change of device and 0 for the same device as the last access.

Furthermore, the risk score from changing banking portal accessing time (R_t) is also noteworthy, as a malicious user may try to access the bank web portal or app at an unusual time compared to the legitimate user's natural login time, or a user may be logged in at different times in a day naturally. Thus, to assess a user's quality, we evaluate the probability of the user's appearance at the current time from their historical records of accessing the portal or app.

$$\text{Probability of appearance of the user in current access time}(P_t) = \frac{\text{Number of accesses in the current hour}}{\text{Maximum number of accesses per hour}} \ldots\ldots \quad (7)$$

$$\text{Risk score } (R_t) = 10 \times (1 - P_t) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (8)$$

The effective and final risk score of a user will be computed from the largest risk score across various significant criteria, including geolocation changes, device changes, IP quality, failed login attempts, and changes in access time, as shown in Equation 9.

$$\text{Effective final risk score of a user (R)} = \text{MAX } [\text{R}_\text{g}, R_i, R_o, R_t] \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (9)$$

The highest value from the list of risk criteria is considered a user's risk score(R). The assessed risk score is converted to a CQ weight and used in CQ selection by Equation 10.

$$CQ\ weight = Round\ (2 \times Risk\ Score(R), 5) - 5 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (10)$$

The CQs are prepared from user profile information, KYC information, activity information, and user input, with different weights assigned based on the level of secrecy associated with each type of information regarding the user. For example, the user's name is easy to explore, but the user's national ID card number is not as easy. Table 4 Sample CQs with weight Shows some sample CQs with the type and weight of each question.

Table 5 Sample CQs with weight

Sample Challenge Question (CQ)	**Type of KYC-related data**	**Weight**
Card Number	Profile information	0
Expire Date	Profile information	0
CVV Number	Profile information	0
Name of the country where you used Point of Sale (POS) last time	Activity information	10
Last transaction amount	Activity information	10
Last payment recipient	Activity information	10
Last bill payment/deposit mode (cash/bank transfer/online banking/other)	Activity information	10
Your last transaction time (morning/day/evening/night)	Activity information	10

Which is your most used transaction medium (cash/bank transfer/online banking/or other)	Activity information	10
How many devices do you use for online transactions?	Activity information	10
The largest transaction amount in the last month	Activity information	10
The lowest transaction amount in the last month	Activity information	10
In which country did you use POS the most POS	Activity information	10
In which country did you use an ATM the most ATM	Activity information	10
Own-created questions and answers	Inputted KYC information	10
What is your family name?	Inputted KYC information	5
Your employer's name	Inputted KYC information	5
Your profession	Inputted KYC information	5
What is your family name?	Inputted KYC information	5
Your credit limit or balance (tentative)	Inputted KYC information	5
Do you have a few photos of your childhood friends with their names?	Inputted KYC information	5
Your favorite color	Inputted KYC information	5
What is your highest educational qualification?	Inputted KYC information	5
What is your favourite fruit	Inputted KYC information	5
Your favorite meal	Inputted KYC information	5
Your Passport Number	Inputted KYC information	5
Your Ration Card Number	Inputted KYC information	5
Your Aadhar Card Number	Inputted KYC information	5
Your Driving License Number	Inputted KYC information	5
Your Permanent Account Number (PAN) Card	Inputted KYC information	5
Your NID Number	Inputted KYC information	5
Your TIN Number	Inputted KYC information	5
Your VAT ID Number	Inputted KYC information	5
What is your Marriage anniversary date?	Inputted KYC information	5
Your spouse was born on a date?	Inputted KYC information	5
What was the name of your first employer?	Inputted KYC information	5
Your Favorite drinks?	Inputted KYC information	5
Your most visited country	Inputted KYC information	5
What is your first school name?	Inputted KYC information	5
What is the name of your highest educational institute?	Inputted KYC information	5
What is your first name in your native language?	Inputted KYC information	5

CQ(s) are selected based on a user's risk score. For low-risk or legitimate users, a successful login to the banking portal will be sufficient for configuring MFA. In contrast, for high-risk users or those with a higher risk score, one or two CQs will be required for further verification. Once the verification offered by CQ is

INTERNATIONAL JOURNAL OF RESEARCH AND INNOVATION IN SOCIAL SCIENCE (IJRISS)
ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume IX Issue III March 2025

passed, the user can configure MFA. Failure to log in to the online portal or app automatically denies the user the ability to set up MFA, including the transaction amount and time slot. Similarly, a user who changes geolocation quickly and unnaturally is denied the ability to set an MFA.

Test and Outcomes

In this research, we simulated 1,000 records of user activity logs to observe the risk score (R) of various activities and found that legitimate users are granted smooth access to systems for configuring MFA. On the other hand, suspicious users are requesting additional verification using CQ based on their risk score (R). *Table 6* shows a sample calculation of the risk score (R) for randomly selected two users from a historical activity pattern.

Table 7 Sample risk score calculation for two users

User ID	*Device MAC*	*IP Address*	*IP Quality*	*geolocation*	*Date Time*	*Hourly Count*	*Time Gap (Minutes)*	*Failed Attempt*	*Pg*	*Rg*	*Pt*	*Rt*	*Pi*	*Ri*	*Po*	*Ro*	*R*	*geoloc Change*
U67	6c:e4:c2:83:d5:30	80.239.7.76	0	Germany	2025-02-01 19:43:00	1	105	4	0.9	5.5	0	0	0.5	2.5	0.9	5.5	5.5	
U67	6c:e4:c2:83:d5:30	220.18.126.167	0	Germany	2025-02-01 23:00:00	1	197	0	0.9	0.5	0	0	0.5	2.5	0.9	0.5	2.5	
U67	6c:e4:c2:83:d5:30	30.17.29.252	0	Germany	2025-02-02 01:05:00	1	125	5	0.9	0.5	0	0	0.5	2.5	0.9	0.5	2.5	
U67	6c:e4:c2:83:d5:30	12.57.91.134	1	Germany	2025-02-02 02:55:00	1	110	3	0.9	0.5	0	0	0.5	7.5	0.9	0.5	7.5	
U67	6c:e4:c2:83:d5:30	117.43.167.241	0	UAE	2025-02-02 07:38:00	1	283	2	0.1	9.5	0	0	0.5	2.5	0.9	0.5	9.5	
U67	6c:e4:c2:83:d5:30	65.194.52.34	0.5	Germany	2025-02-02 08:10:00	1	32	4	0.9	5.5	0	0	0.5	5	0.9	0.5	5.5	X
U67	6c:e4:c2:83:d5:30	171.146.13.59	0	Germany	2025-02-02 09:22:00	1	72	0	0.9	0.5	0	0	0.5	2.5	0.9	0.5	2.5	
U67	6c:e4:c2:83:d5:30	25.42.194.14	0	Germany	2025-02-02 11:08:00	1	106	0	0.9	0.5	0	0	0.5	2.5	0.9	0.5	2.5	
U67	6c:e4:c2:83:bf:30	130.244.111.51	0	Germany	2025-02-02 15:27:00	1	259	2	0.9	0.5	0	0	0.5	2.5	0.1	9.5	9.5	
U67	6c:e4:c2:83:d5:30	69.189.96.50	0	Germany	2025-02-02 20:12:00	1	285	5	0.9	0.5	0	0	0.5	2.5	0.9	0.5	2.5	
U165	6a:55:71:c7:e3:dd	192.168.64.125	0	USA	2025-02-01 19:57:00	1	80	1	0.5	5	0.5	5	0.5	2.5	0.8	6	6	
U165	6a:55:71:c7:e3:dd	192.168.242.21	0	USA	2025-02-01 21:26:00	2	89	2	1	0	0	0	0.5	2.5	0.8	1	2.5	
U165	6a:55:71:c7:e3:dd	192.168.141.29	0	USA	2025-02-02 01:07:00	2	221	4	1	0	0	0	0.5	2.5	0.8	1	2.5	
U165	6a:55:71:c7:e3:dd	192.168.64.125	0	USA	2025-02-02 02:41:00	1	94	5	0.5	0	0.5	5	0.5	2.5	0.8	1	5	
U165	6a:55:71:c7:e3:dd	192.168.242.21	0	USA	2025-02-02 08:12:00	1	331	0	0.5	0	0.5	5	0.5	2.5	0.8	1	5	
U165	6a:55:71:c7:e3:dd	192.168.64.125	0	USA	2025-02-02 13:37:00	1	325	3	0.5	0	0.5	5	0.5	2.5	0.8	1	5	
U165	6a:55:71:c7:e3:8e	192.168.242.21	0	USA	2025-02-02 15:01:00	2	84	2	1	0	1	0	0.5	2.5	0.2	9	9	
U165	6a:55:71:c7:e3:dd	192.168.64.125	0	USA	2025-02-02 15:35:00	2	34	1	1	0	1	0	0.5	2.5	0.8	1	2.5	
U165	6a:55:71:c7:e3:8e	192.168.232.239	0.5	USA	2025-02-02 21:01:00	2	326	5	1	0	1	0	0.5	5	0.2	4	5	
U165	6a:55:71:c7:e3:dd	192.168.162.250	0	USA	2025-02-03 01:50:00	2	289	0	1	0	1	0	0.5	2.5	0.8	1	2.5	

Note: The risk score (R) determines CQ weight, while the unusual nature of the geolocation change marked as X, will result in denied access

The assessed risk score (R) was converted to CQ weight for selecting the appropriate CQ from the predefined list.

$$\text{CQ weight} = \text{Round}\,(2 \times \text{Risk Score}(\text{R}), 5) - 5 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (11)$$

CQ(s) is selected based on a user's CQ weight calculated by Equation 11. A legitimate user can easily and quickly access the portal to configure MFA. ***Figure 10*** shows the relation between risk score (R) and CQ weight for CQ selection.

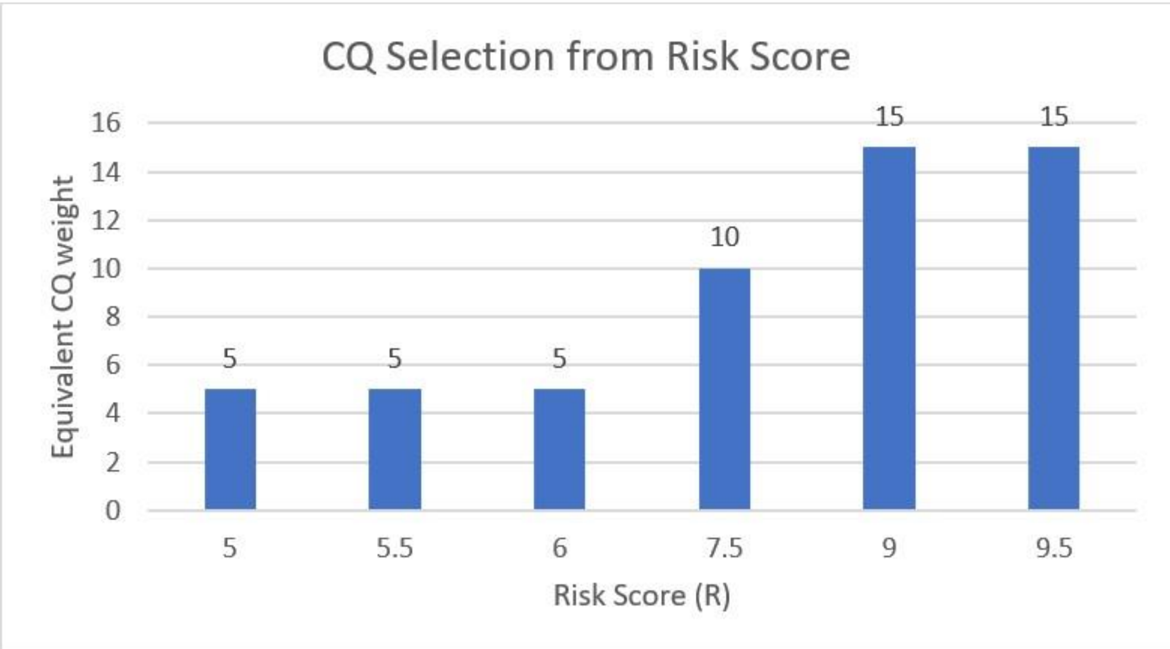

Figure 11 Calculation of CQ weight for selection of CQ from Risk Score (R)

Once the model completes CQ selection, the CQ(s) is/are offered to the logged-in user for verification purposes, allowing those who want to set MFA to select the desired transaction amount and time slot for the CNP transaction. It is also worth mentioning that the model does not suggest asking for CQ who have been assessed as legitimate users with a risk score below the administrator-defined threshold risk score level. In this test and simulation process, we have considered a risk score of 5 as the threshold value to offer CQ to user verification.

The MFA will be used to authenticate the user and authorize transactions by the user from the card issuer bank. In this way, the transaction will be performed as the user wants in the "what we want" based MFA model. The model utilizes pre-authentication configuration to approve a CNP transaction without requiring any authentication-related keys during the transaction, thereby relieving the user from the hassle of entering additional keys.

RESULTS AND DISCUSSION

The user defines MFA after using the banking portal or app before making a transaction. The model assesses the risk associated with the user's activity for restricting illegitimate users from MFA configuration. Legitimate or lower-risk users will gain direct access without requiring CQ to configure MFA. In contrast, higher-risk users will be asked to provide one or two CQs based on the CQ weight derived from their risk score, for further verification. As shown in Table 8 Selection of CQ from the CQ weight, once the risky user can answer the CQs offered, they will gain access to configure MFA; otherwise, they will be denied access.

Table 9 Selection of CQ from the CQ weight

Risk Score(R)	**CQ weight**	**CQ(s)**
<5	0	No CQ, direct access to MFA configuration
5	5	One CQ with a weight of 5
5.5		
6		
7.5	10	One CQ with a weight of 10
9	15	One CQ with a weight of 5 and one CQ with a weight of 10
9.5	15	

MFA is defined by the user based on additional risk assessment and verification through the necessary CQ(s). As a result, the MFA setting is highly secure from threat actors, hackers, or fraudsters. While 100% of the transaction depends on the MFA, as the user defines or as the user wants, it has been proven that the system is foolproof and protected from malicious use. The proposed "what we want" based MFA is powerful and equal to or more effective than PIN, OTP, and/or biometric-based MFA, as discussed in *Table 10 Justification regarding the elimination of risk by using an innovative MFA*. What we want, based MFA is to protect financial services from various potential risks by utilizing its pre-authentication mechanism. Although the method does not require any visible user input, it still prevents bypassing the authentication mechanism through identity theft or stolen MFA keys.

Table 11 Justification regarding the elimination of risk by using an innovative MFA

MFA Type	**The associated risk of compromise**	**Eliminated by "What we want" MFA**
PIN	Database Breaches	A database compromise may result in significant financial loss due to fraudulent activity. "What we want" based on MFA is not always active without the user's requirement, so it is safe from database compromise.

	Shoulder surfing & screen recording	Since there is no visible user input, there is no risk associated with key reception and entry during the transaction. That means "What we want" MFA eliminates all the risks associated with data in rest, process, and transit.
	Reusing the same PIN	
	Weak PIN Choices	
PIN/OTP	Phishing & Social Engineering	
	Malware & Keyloggers	
	Credential Stuffing & Brute Force Attacks	
OTP	SIM Swapping	
	MITM Attacks	
	Delayed or Failed OTP Delivery	
	Signaling System No. 7 (SS7) protocol vulnerability	
Biometric-based	Irreversible Data Exposure	
	Spoofing & Presentation Attacks	
	Data Breaches & Storage Risks	
	Privacy Concerns & Legal Issues	
	False Positives & False Negatives	
	Dependence on Hardware & Environment	

Challenges and Limitations

This research project is an independent initiative based on professional experience, but it lacks sufficient funding. Since user activity data from a financial network is critical, it was impossible to access real data for research purposes; therefore, this work utilized a synthetic dataset for simulation and achieved the expected outcomes. The synthetic data was produced by following necessary natural tendencies with the help of the Python Faker library. The conceptual support and mathematical basis are the basis of this model. There is a significant scope of work for this model, considering real-time data and piloting in a bank or financial institution. As the financial sector is the custodian of public funds and sensitive user data, a rigorous lab test and piloting are indeed necessary for the real-world application of this novel MFA. This research is conducted within limited lab tests, budgets, and time constraints, subject to necessary approval limitations. This research used a weight-based risk assessment where weights are not fixed for every case and may differ based on an organization's threat profile; therefore, during the application of user risk assessment in the real-world scenario, some of the weight regarding IP change, IP type, field attempt, geo-loc change, device change, and timing change may be fixed based on the situation for getting appropriate output and removing false positive. Threat actors continually adapt their strategies, and vulnerability exposure is dynamic; therefore, the risk assessment component of this research is a progressive field that requires ongoing refinement. While the model aims to assess known risks, it is also important to recognize and continue studying emerging challenges to identify potential risks. All the presented limitations are tolerable, considering risk can never be eliminated, and some residual risks may always be present.

CONCLUSION

In this study, we introduce an innovative MFA model, based on the theme "What We Want," to enhance CNP transaction security. This creative "What We Want" based MFA is user-defined and independent of carrying additional devices (registered mobile or hardware/software token) for OTP; additionally, it is free from the use of sensitive biometric information and the risk of identity theft and critical data breaches. While the MFA only exists on a need basis and is configured by the user before making transactions over separate channels, this MFA eliminates all the risks associated with critical authentication data in rest, process, and transit. A

risky/suspicious user is prevented from configuring MFA by using CQ-based verification. Only the legitimate user can configure MFA and transact the defined amount within the configured time window. As a result, the risk of making a fraudulent transaction using identity theft, stolen phones, and user data breaches is eliminated. The complete process runs with the user's consent and under the user's risk acceptance; thus, banks and FIs remain exempt from blame and can preserve customer trust. This MFA is not something carried by the user under what they know, what they have, and what they are; it remains invisible and becomes usable on demand based on what they want so it is out of danger of compromise, theft, loss, and protected from all the contemporary risks introduced by the traditional MFAs. The simulation results suggest that the model provides a flexible facility for MFA configuration by legitimate users, while the assessed risk score indicates one or two strong CQs for restricting illegitimate users. Although the model ensures maximum protection for CNP transactions using pre-authentication-based "what we want" type MFA, fraudsters may still devise new avenues for attack strategies with dynamic motives; therefore, we remain vigilant for further improvements to the model by analyzing the nature of the fraudulent efforts.

REFERENCES

1. A Multifactor Secure Authentication System for Wireless Payment. (n.d.). ResearchGate. Retrieved March 13, 2025, from https://www.researchgate.net/publication/227166369_A_Multifactor_Secure_Authentication_System_for_Wireless_Payment
2. A SURVEY AND COMPARISON ON USER AUTHENTICATION METHODS | International Journal of Innovations in Engineering Research and Technology. (n.d.). Retrieved March 13, 2025, from https://repo.ijiert.org/index.php/ijiert/article/view/1162
3. A User Study of Keystroke Dynamics as Second Factor in Web MFA | Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy. (n.d.). Retrieved March 13, 2025, from https://dl.acm.org/doi/10.1145/3577923.3583642
4. Abumohsen, M., Owda, A. Y., & Owda, M. (2023). Electrical Load Forecasting Based on Random Forest, XGBoost, and Linear Regression Algorithms. 2023 International Conference on Information Technology (ICIT), 25–31. https://doi.org/10.1109/ICIT58056.2023.10225968
5. Aburbeian, A. M., & Fernández-Veiga, M. (2024). Secure Internet Financial Transactions: A Framework Integrating Multi-Factor Authentication and Machine Learning. AI, 5(1), Article 1. https://doi.org/10.3390/ai5010010
6. Alsaqour, R., Majrashi, A., Alreedi, M., Alomar, K., & Abdelhaq, M. (2021). Defense in Depth: A multilayered security. International Journal of Communication Networks and Information Security (IJCNIS), 13(2). https://doi.org/10.17762/ijcnis.v13i2.4951
7. Bartłomiejczyk, M., Imed, E. F., & Kurkowski, M. (2019). Multifactor Authentication Protocol in a Mobile Environment. IEEE Access, 7, 157185–157199. IEEE Access. https://doi.org/10.1109/ACCESS.2019.2948922
8. Bell, J. (2022). What Is Machine Learning? In Machine Learning and the City (pp. 207–216). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781119815075.ch18
9. Bodker, A., Connolly, P., Sing, O., Hutchins, B., Townsley, M., & Drew, J. (2023). Card-not-present fraud: Using crime scripts to inform crime prevention initiatives. Security Journal, 36(4), 693–711. https://doi.org/10.1057/s41284-022-00359-w
10. Burr, W. E., Dodson, D. F., Newton, E. M., Perlner, R. A., Polk, W. T., Gupta, S., & Nabbus, E. A. (2011). Electronic authentication guideline (NIST SP 800-63-1; 0 ed., p. NIST SP 800-63-1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63-1
11. Cai, Y., & Zhu, D. (2016). Fraud detections for online businesses: A perspective from blockchain technology. Financial Innovation, 2(1), 20. https://doi.org/10.1186/s40854-016-0039-4
12. Cherif, A., Badhib, A., Ammar, H., Alshehri, S., Kalkatawi, M., & Imine, A. (2023). Credit card fraud detection in the era of disruptive technologies: A systematic review. Journal of King Saud University - Computer and Information Sciences, 35(1), 145–174. https://doi.org/10.1016/j.jksuci.2022.11.008
13. Chetalam, L. J. (2018). Enhancing Security of Mpesa Transactions by Use of Voice Biometrics. https://www.semanticscholar.org/paper/Enhancing-Security-of-Mpesa-Transactions-by-Use-of-Chetalam/d24be4cad73f3f28386e8cd289b3dc5c3fc67006

14. Dasgupta, D., Roy, A., & Nag, A. (2017). Multi-Factor Authentication. In D. Dasgupta, A. Roy, & A. Nag (Eds.), Advances in User Authentication (pp. 185–233). Springer International Publishing. https://doi.org/10.1007/978-3-319-58808-7_5
15. Díaz Redondo, R. P., Fernández Vilas, A., Ramos Merino, M., Valladares Rodríguez, S. M., Torres Guijarro, S., & Hafez, M. M. (2023). Anti-Sexism Alert System: Identification of Sexist Comments on Social Media Using AI Techniques. Applied Sciences, 13(7), Article 7. https://doi.org/10.3390/app13074341
16. Full article: Implementation of an Additional Factor for Secure Authentication in Online Transactions. (n.d.). Retrieved March 13, 2025, from https://www.tandfonline.com/doi/full/10.1080/10919392.2019.1633123
17. Gaikwad, J. R., Deshmane, A. B., Somavanshi, H. V., Patil, S. V., & Badgujar, R. A. (2014). Credit Card Fraud Detection using Decision Tree Induction Algorithm. 4(6).
18. Global Online Payment Fraud Market Report 2023: Merchant Losses will Exceed $362 Billion to 2028 - Forecasts, Emerging Threats & Segment Analysis - ResearchAndMarkets.com. (2023, October 26). https://www.businesswire.com/news/home/20231026285145/en/Global-Online-Payment-Fraud-Market-Report-2023-Merchant-Losses-will-Exceed-362-Billion-to-2028---Forecasts-Emerging-Threats-Segment-Analysis---ResearchAndMarkets.com
19. González-Soto, M., Díaz-Redondo, R. P., Fernández-Veiga, M., Fernández-Castro, B., & Fernández-Vilas, A. (2024). Decentralized and collaborative machine learning framework for IoT. Computer Networks, 239, 110137. https://doi.org/10.1016/j.comnet.2023.110137
20. Guma, A. (2022). Development of a secure multi-factor authentication algorithm for mobile money applications [Thesis, NM-AIST]. https://doi.org/10.58694/1782
21. Hassan, M. A., & Shukur, Z. (2021). A Secure Multi Factor User Authentication Framework for Electronic Payment System. 2021 3rd International Cyber Resilience Conference (CRC), 1–6. https://doi.org/10.1109/CRC50527.2021.9392564
22. Jaspher Willsie Kathrine, G., & Kirubakaran, E. (2011). FourFactor based Privacy Preserving Biometric Authentication and Authorization Scheme for Enhancing Grid Security. International Journal of Computer Applications, 30(5), 13–20. https://doi.org/10.5120/3639-5083
23. Kennedy, E., & Millard, C. (2016). Data security and multi-factor authentication: Analysis of requirements under EU law and in selected EU Member States. Computer Law & Security Review, 32(1), 91–110. https://doi.org/10.1016/j.clsr.2015.12.004
24. Krol, K., Philippou, E., Cristofaro, E. D., & Sasse, M. A. (2015). "`They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking (arXiv:1501.04434). arXiv. https://doi.org/10.48550/arXiv.1501.04434
25. Kulatilleke, G. K. (2022). Challenges and Complexities in Machine Learning based Credit Card Fraud Detection (arXiv:2208.10943). arXiv. https://doi.org/10.48550/arXiv.2208.10943
26. Lomba, E., Severino, R., & Vilas, A. F. (2022). Work In Progress: Towards Adaptive RF Fingerprint-based Authentication of IIoT devices. 2022 IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA), 1–4. https://doi.org/10.1109/ETFA52439.2022.9921575
27. Malta, S., Pinto, P., & Fernández-Veiga, M. (2023). Using Reinforcement Learning to Reduce Energy Consumption of Ultra-Dense Networks With 5G Use Cases Requirements. IEEE Access, 11, 5417–5428. IEEE Access. https://doi.org/10.1109/ACCESS.2023.3236980
28. Meneses, B., Huamani, E. L., Yauri-Machaca, M., Meneses-Claudio, J., & Perez-Siguas, R. (2022). Authentication and Anti-Duplication Security System for Visa and MasterCard Cards. International Journal on Recent and Innovation Trends in Computing and Communication, 10(7), Article 7. https://doi.org/10.17762/ijritcc.v10i7.5558
29. Mohammed, M. M., & Elsadig, M. (2013). A multi-layer of multi factors authentication model for online banking services. 2013 INTERNATIONAL CONFERENCE ON COMPUTING, ELECTRICAL AND ELECTRONIC ENGINEERING (ICCEEE), 220–224. https://doi.org/10.1109/ICCEEE.2013.6633936
30. Mondal, P. C., Deb, R., & Adnan, Md. N. (2017). On reinforcing automatic teller machine (ATM) transaction authentication security process by imposing behavioral biometrics. 2017 4th International

Conference on Advances in Electrical Engineering (ICAEE), 369–372. https://doi.org/10.1109/ICAEE.2017.8255383

31. Mondal, P. C., Deb, R., & Huda, M. N. (2016a). Know your customer (KYC) based authentication method for financial services through the internet. 2016 19th International Conference on Computer and Information Technology (ICCIT), 535–540. https://doi.org/10.1109/ICCITECHN.2016.7860255
32. Mondal, P. C., Deb, R., & Huda, M. N. (2016b). Transaction authorization from Know Your Customer (KYC) information in online banking. 2016 9th International Conference on Electrical and Computer Engineering (ICECE), 523–526. https://doi.org/10.1109/ICECE.2016.7853972
33. Multi-Factor Authentication Method for Online Banking Services in South Africa. (n.d.). ResearchGate. Retrieved March 13, 2025, from https://www.researchgate.net/publication/358558477_Multi-Factor_Authentication_Method_for_Online_Banking_Services_in_South_Africa
34. Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. Cryptography, 2(1), Article 1. https://doi.org/10.3390/cryptography2010001
35. Owess, M. M., Owda, A. Y., & Owda, M. (2023). Decision Support System in Healthcare for Predicting Blood Pressure Disorders. 2023 International Conference on Information Technology (ICIT), 62–67. https://doi.org/10.1109/ICIT58056.2023.10226098
36. Paladino, L. M., Hughes, A., Perera, A., Topsakal, O., & Akinci, T. C. (2023). Evaluating the Performance of Automated Machine Learning (AutoML) Tools for Heart Disease Diagnosis and Prediction. AI, 4(4), Article 4. https://doi.org/10.3390/ai4040053
37. Report, T. N. (2025, January 6). Payment Card Fraud Losses Approach $34 Billion. GlobeNewswire News Room. https://www.globenewswire.com/news-release/2025/01/06/3004931/0/en/Payment-Card-Fraud-Losses-Approach-34-Billion.html
38. Sakurada, H., & Sakurai, K. (2024). SoK: Directions and Issues in Formal Verification of Payment Protocols. In L. Barolli (Ed.), Advanced Information Networking and Applications (pp. 111–119). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-57916-5_10
39. Scaria, B. A., & Karman Megalingam, R. (2018). Enhanced E-Commerce Application Security Using Three-Factor Authentication. 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS), 1588–1591. https://doi.org/10.1109/ICCONS.2018.8662831
40. Schueffel, P. (2016). Taming the Beast: A Scientific Definition of Fintech. Journal of Innovation Management, 4(4), Article 4. https://doi.org/10.24840/2183-0606_004.004_0004
41. Ul, B., F., R., Mehraj, A., Ahmad, A., & Assad, S. (2017). A Compendious Study of Online Payment Systems: Past Developments, Present Impact, and Future Considerations. International Journal of Advanced Computer Science and Applications, 8(5). https://doi.org/10.14569/IJACSA.2017.080532
42. U.S. Patent Application for Computer Systems and Computer-Implemented Methods for Card-Not-Present Transactions Patent Application (Application #20190026735 issued January 24, 2019)—Justia Patents Search. (n.d.). Retrieved March 13, 2025, from https://patents.justia.com/patent/20190026735
43. Zadeh, M. J., & Barati, H. (2020). Security Improvement in Mobile Banking Using Hybrid Authentication. Proceedings of the 3rd International Conference on Advances in Artificial Intelligence, 198–201. https://doi.org/10.1145/3369114.3369151