IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 28, Issue 4, Ser. 3 (July. – August. 2026), PP 15-35
www.iosrjournals.org

Design and Evaluation of a Five-Factor Authentication Framework for Enhancing Cybersecurity in Digital Transactions: A Prototype-Based Comparative Study Using Digital Transaction Datasets and ANOVA

[1]Nwamini Bartholomew Tochukwu
[1]Department of Cybersecurity Evangel University Akaeze, Ebonyi State.

[2]Chinyere Ihuoma Anyanwu *(Nee Akobundu)*
[2]Department of Computer Science and Mathematics Evangel University Akaeze, Ebonyi State

[3]Odegwo Ifeanyi
[3]Department of Computer Science and Mathematics Evangel University Akaeze, Ebonyi State

Abstract
The rapid growth of digital banking, electronic commerce, mobile payments, and financial technology platforms has increased cybersecurity risks associated with digital transactions. Conventional password and two-factor authentication systems remain vulnerable to phishing, credential theft, device compromise, account takeover, and unauthorized transactions. This study proposes a Five-Factor Authentication Framework integrating knowledge, possession, inherence, location/context, and behavioral authentication. The study involves threat analysis, framework development, comparative evaluation, and ***prototype evaluation using digital transaction datasets and ANOVA statistical analysis****. The framework applies adaptive risk-based authentication based on user credentials, trusted devices, biometric verification, contextual information, and behavioral patterns. Evaluation focuses on security, usability, and system performance using metrics such as authentication accuracy, false acceptance rate, false rejection rate, attack resistance, and authentication latency. Illustrative results suggest that the proposed framework can provide stronger security than conventional authentication approaches. The study concludes that integrating multiple authentication factors with adaptive verification can improve the security, reliability, and trustworthiness of digital transaction systems.*

Keywords: *Five-Factor Authentication, Digital Transactions, Cybersecurity, Digital Transaction Datasets, Prototype Evaluation, ANOVA Statistical Analysis.*

Date of Submission: 15-08-2026 Date of Acceptance: 31-08-2026

I. Introduction

The rapid advancement of information and communication technologies has transformed the way financial and commercial transactions are conducted. Digital banking, electronic commerce, mobile payments, online financial services, and financial technology platforms have significantly improved the speed, accessibility, and convenience of transactions. Users can now transfer funds, purchase goods and services, access banking services, and conduct other financial activities through computers, smartphones, and other connected devices. However, the increasing dependence on digital transaction platforms has also expanded the cybersecurity attack surface and created new opportunities for unauthorized access, identity theft, financial fraud, and other cyber threats.

Authentication is one of the most important security mechanisms for protecting digital transaction systems. Its primary purpose is to verify that an individual requesting access is the legitimate user before authorizing access to an account or transaction. Traditional authentication systems have commonly relied on knowledge-based credentials such as usernames, passwords, and personal identification numbers (PINs). Although these methods remain widely used, they are vulnerable to password theft, phishing, social engineering, brute-force attacks, credential reuse, and database compromise. Once an attacker obtains a user's authentication credentials, a password-only system may provide little additional protection against unauthorized access.

The limitations of traditional password-based authentication have encouraged the adoption of two-factor and multi-factor authentication systems. These approaches improve security by requiring users to provide

additional evidence of identity, such as a one-time password, mobile device confirmation, security token, or biometric characteristic. However, conventional multi-factor authentication systems may still be vulnerable to sophisticated attacks, including phishing, SIM-swapping, malware, device compromise, biometric spoofing, account takeover, and session hijacking. Furthermore, many authentication systems verify the user only during the login process and provide limited protection when an authenticated session is subsequently compromised.

To address these limitations, this study proposes a **Five-Factor Authentication Framework for Digital Transactions**. The proposed framework integrates five complementary authentication dimensions: **knowledge, possession, inherence, location/context, and behavioral characteristics**. The knowledge factor includes passwords or PINs, while the possession factor verifies ownership of a trusted device, token, or authenticator. The inherence factor confirms the user's identity through biometric verification. Location and contextual authentication examine information such as device characteristics, access location, time, IP address, and transaction patterns. The behavioral factor provides continuous monitoring by analyzing user interaction patterns and detecting deviations from normal behavior.

The integration of these five authentication dimensions provides a layered and defense-in-depth approach to digital transaction security. Rather than relying on a single authentication mechanism, the proposed framework combines multiple independent signals to determine the legitimacy of a user and transaction. Consequently, the compromise of one authentication factor does not automatically result in successful unauthorized access. For example, an attacker who obtains a password may still need to possess a registered device, satisfy biometric verification, demonstrate acceptable contextual characteristics, and exhibit behavioral patterns consistent with those of the legitimate user.

The proposed framework also incorporates **adaptive risk-based authentication**. Under this approach, the number and intensity of authentication checks are determined by the risk associated with a transaction. Low-risk transactions may require simplified authentication and passive monitoring, while medium-risk transactions may activate additional authentication factors. High-risk transactions may require all five authentication factors together with enhanced behavioral and security monitoring. This approach is intended to balance strong cybersecurity with user convenience and reduce unnecessary authentication complexity.

A major component of this study is the **Prototype Evaluation Using Digital Transaction Datasets and ANOVA Statistical Analysis**. The proposed framework should be implemented as a functional prototype and evaluated using digital transaction datasets containing legitimate and suspicious transaction records. These datasets may include transaction amounts, transaction frequency, timestamps, authentication outcomes, device information, biometric verification results, contextual information, location indicators, and behavioral characteristics. Such data can support a comprehensive evaluation of the framework's ability to distinguish between legitimate and unauthorized activities.

The prototype evaluation considers important security, usability, and performance metrics. These include authentication accuracy, false acceptance rate, false rejection rate, attack detection rate, authentication latency, transaction throughput, system resource utilization, authentication completion rate, and usability. The proposed framework can then be compared with single-factor, two-factor, three-factor, and other conventional multi-factor authentication approaches using equivalent digital transaction scenarios.

In addition, **Analysis of Variance (ANOVA)** can be used to determine whether differences in the performance of the authentication approaches are statistically significant. ANOVA enables the comparison of the mean results obtained from multiple authentication models across security, usability, and system performance metrics. This statistical analysis provides a more rigorous basis for determining whether the proposed Five-Factor Authentication Framework offers measurable improvements over existing authentication approaches. However, illustrative values used during framework development should be replaced with actual results obtained from prototype implementation and real or properly anonymized digital transaction datasets.

Despite the potential security benefits of the proposed framework, the integration of multiple authentication factors may introduce challenges. These include increased authentication complexity, computational overhead, privacy concerns, implementation costs, authentication latency, and possible user inconvenience. Biometric information and behavioral data require strong protection, while location and contextual information must be processed in a privacy-preserving manner. Therefore, the framework must be carefully designed to ensure that stronger security does not unnecessarily compromise usability or system efficiency.

This study therefore aims to develop and evaluate a comprehensive Five-Factor Authentication Framework that combines multiple authentication dimensions with adaptive risk-based decision-making. Through **prototype evaluation using digital transaction datasets and ANOVA statistical analysis**, the study seeks to assess whether the proposed framework can improve the security, usability, and performance of digital transaction systems. Ultimately, the study contributes to the development of more secure, reliable, and trustworthy authentication mechanisms capable of protecting users and financial transactions against evolving cybersecurity threats.

Research Questions

The study seeks to examine the effectiveness of the proposed Five-Factor Authentication Framework in strengthening cybersecurity in digital transaction environments. The research questions are designed to evaluate the framework using digital transaction datasets, prototype implementation, comparative authentication analysis, and ANOVA statistical analysis.

1. How effective is the proposed Five-Factor Authentication Framework in improving the security of digital transactions compared with single-factor, two-factor, and three-factor authentication approaches?

This question examines whether integrating five authentication factors provides stronger security than conventional authentication methods. The proposed framework will be compared with existing approaches to determine its ability to reduce unauthorized access, credential theft, phishing, account takeover, device compromise, and suspicious transactions.

2. How can digital transaction datasets be used to evaluate the security, usability, and performance of the proposed authentication framework?

This question investigates how digital transaction datasets containing legitimate and suspicious transaction records can be used to test the framework. The datasets may include authentication outcomes, transaction amounts, device information, timestamps, location/context data, biometric scores, and behavioral characteristics. These data will support empirical evaluation of the framework under different transaction conditions.

3. What is the effect of integrating knowledge, possession, inherence, location/context, and behavioral authentication on authentication accuracy and attack detection?

This question evaluates the contribution of the five authentication dimensions to identity verification and threat detection. It examines whether combining multiple authentication factors improves authentication accuracy and the detection of suspicious activities compared with systems that depend on fewer factors.

4. How does the proposed framework affect false acceptance rate, false rejection rate, authentication latency, and transaction throughput?

This question evaluates the performance of the framework by measuring its ability to reduce the acceptance of unauthorized users and minimize the rejection of legitimate users. It also assesses whether the additional authentication factors introduce delays or affect the system's ability to process a large number of digital transactions efficiently.

5. How effective is adaptive risk-based authentication in balancing cybersecurity and user usability across low-, medium-, and high-risk digital transactions?

This question investigates whether authentication requirements should vary according to the level of transaction risk. Low-risk transactions may require simplified authentication, medium-risk transactions may activate additional verification factors, while high-risk transactions may require all five factors and continuous monitoring. The objective is to determine whether adaptive authentication can provide strong security without unnecessarily reducing user convenience.

6. Are there statistically significant differences between the proposed Five-Factor Authentication Framework and existing authentication approaches based on ANOVA statistical analysis?

This question uses ANOVA statistical analysis to determine whether differences in security, usability, and system performance among the proposed framework and existing authentication approaches are statistically significant. The analysis will compare the mean performance of single-factor, two-factor, three-factor, conventional multi-factor, and proposed five-factor authentication systems.

7. How effectively can continuous behavioral and contextual authentication detect suspicious transactions, account takeover, and unauthorized access?

This question examines the effectiveness of continuous monitoring during active digital transactions. Behavioral characteristics, such as typing patterns, touch interactions, mouse movements, and user activity, together with contextual information such as location, device, time, and IP address, can be analyzed to identify deviations from normal user behavior and detect possible security threats.

8. What challenges may affect the practical implementation of the proposed Five-Factor Authentication Framework, particularly in relation to privacy, system performance, scalability, and user convenience?

This question investigates the potential limitations and implementation challenges of the framework. These challenges may include biometric and transaction-data privacy, increased authentication complexity, computational requirements, system latency, scalability, implementation costs, and possible user resistance. Addressing these challenges is important to ensure that the framework can be effectively deployed in real-world digital transaction systems.

Overall, the research questions provide a structured basis for evaluating the proposed Five-Factor Authentication Framework. They focus on determining whether the integration of multiple authentication factors, adaptive risk assessment, digital transaction datasets, prototype evaluation, and ANOVA statistical analysis can provide measurable improvements in the security, usability, and performance of digital transaction systems.

II. Literature Review

1. Authentication Security in Digital Transactions

The growth of digital banking, electronic commerce, mobile payments, and financial technology platforms has increased the need for stronger authentication mechanisms. Authentication is essential for verifying user identity and preventing unauthorized access to financial accounts and digital transaction services. However, conventional authentication based only on passwords or personal identification numbers remains vulnerable to phishing, credential theft, password reuse, social engineering, and other cyberattacks. Modern digital identity guidance therefore emphasizes stronger authentication assurance and improved authenticator management for online systems (NIST, 2025).

Single-factor authentication depends mainly on something the user knows, such as a password or PIN. Although this approach is simple and convenient, the compromise of one credential may provide an attacker with direct access to an account. Consequently, two-factor and multi-factor authentication mechanisms have become increasingly important. However, conventional multi-factor authentication may still be affected by phishing, device compromise, account takeover, and session hijacking. This limitation has encouraged the development of authentication systems that combine multiple independent identity signals and continuous security monitoring.

2. Knowledge, Possession, and Inherence Authentication

Authentication systems commonly combine three major categories of verification: **knowledge**, **possession**, and **inherence**. The knowledge factor includes passwords and PINs, while the possession factor involves devices, security tokens, or authentication applications. The inherence factor uses biometric characteristics such as fingerprints, facial features, iris patterns, or voice.

NIST's current digital identity guidance recognizes the importance of authentication assurance and phishing-resistant authentication mechanisms in reducing the risks associated with credential compromise and verifier impersonation (NIST, 2025).

Despite their advantages, these authentication factors have individual limitations. Passwords can be stolen or phished, devices can be lost or compromised, and biometric systems may be vulnerable to spoofing or presentation attacks. Therefore, stronger digital transaction security may require the integration of additional contextual and behavioral information.

3. Location and Context-Aware Authentication

Context-aware authentication extends identity verification by analyzing information surrounding an authentication attempt. Such information may include geographical location, IP address, device characteristics, access time, network environment, and transaction history. Contextual analysis can help identify authentication attempts that are inconsistent with a user's normal activities.

Research on continuous authentication identifies context-oriented characteristics as important sources of authentication information, together with physiological and behavioral biometrics. Context-aware authentication can support ongoing verification but also introduces privacy and security challenges because contextual information may be personal, inaccurate, or manipulated (Baig & Eskeland, 2021).

For this reason, location should be treated as a **risk indicator rather than absolute proof of identity**. An unfamiliar location or device may increase the risk score of a transaction and trigger additional authentication rather than automatically resulting in access denial.

4. Behavioral and Continuous Authentication

Traditional authentication systems usually verify users only at the beginning of a session. Once access is granted, the system may assume that the legitimate user remains in control. This creates a security gap when an authenticated session is subsequently hijacked.

Continuous authentication addresses this limitation by monitoring user behavior throughout an active session. Behavioral characteristics such as keystroke dynamics, touch gestures, motion patterns, mouse movements, and device usage behavior can be used to identify deviations from a legitimate user's established profile. Dahia et al. (2020) explained that continuous authentication can provide repeated identity verification and help prevent session hijacking, although it must balance security with usability.

Similarly, Abuhamad et al. (2021) reviewed sensor-based behavioral authentication methods for smartphones and identified motion, gait, keystroke, touch, voice, and multimodal approaches as important techniques for continuous user verification. The review also identified challenges associated with usability, adoption, and system performance.

These findings support the inclusion of behavioral authentication as a major component of the proposed Five-Factor Authentication Framework. Behavioral monitoring can extend protection beyond the initial login stage and help identify account takeover or suspicious activity during an active transaction.

5. Security, Privacy, and Usability in Continuous Authentication

Although continuous authentication can improve security, it also raises important concerns relating to privacy and usability. Continuous monitoring may require the collection and processing of sensitive biometric, behavioral, and contextual data. Baig and Eskeland (2021) observed that continuous authentication involves trade-offs among security, privacy, and usability and identified challenges related to matching performance, replay attacks, privacy protection, and user experience.

These concerns are particularly important in digital transaction systems, where authentication data may include sensitive financial and personal information. Therefore, the proposed framework should use privacy-preserving techniques, secure biometric template protection, controlled data collection, and minimal retention of sensitive information.

6. Adaptive and Risk-Based Authentication

A major challenge in multi-factor authentication is balancing security with user convenience. Requiring all authentication factors for every transaction may increase security but can also result in authentication fatigue, delays, and user frustration. An adaptive risk-based approach provides a more flexible solution by adjusting authentication requirements according to the assessed level of risk.

Under this approach, low-risk transactions may require simplified verification, while medium- and high-risk transactions trigger additional authentication factors. Risk indicators can include unusual locations, unknown devices, abnormal behavioral patterns, high transaction values, failed authentication attempts, and suspicious transaction histories.

The proposed Five-Factor Authentication Framework applies this principle by integrating knowledge, possession, inherence, location/context, and behavioral signals within a risk-based decision process. This approach is intended to provide stronger protection for high-risk transactions while maintaining usability for low-risk activities.

7. Prototype Evaluation Using Digital Transaction Datasets

A theoretical authentication framework requires practical implementation and evaluation to establish its effectiveness. Prototype evaluation allows researchers to assess whether a proposed authentication system can operate efficiently under realistic digital transaction conditions.

Digital transaction datasets can provide authentication and transaction records containing legitimate and suspicious activities. Relevant attributes may include transaction amount, transaction frequency, timestamp, authentication outcome, device information, location indicators, biometric verification results, and behavioral characteristics. Such datasets can be used to evaluate the ability of an authentication framework to distinguish legitimate users and transactions from unauthorized or suspicious activities.

Prototype evaluation can measure security, usability, and system performance using metrics such as:

- Authentication accuracy
- False acceptance rate
- False rejection rate
- Attack detection rate
- Authentication latency
- Transaction throughput
- System resource utilization
- Authentication completion rate
- Usability score

Continuous authentication research has also emphasized the importance of suitable datasets and standardized evaluation measures for reliable validation and benchmarking (Dahia et al., 2020; Abuhamad et al., 2021).

The use of digital transaction datasets therefore provides an empirical basis for evaluating the proposed framework under different transaction scenarios, including legitimate access, credential compromise, suspicious devices, unusual locations, behavioral anomalies, and account takeover attempts.

8. Comparative Authentication Evaluation

Comparative evaluation is necessary to determine whether a proposed framework provides measurable improvements over existing authentication approaches. The proposed Five-Factor Authentication Framework should therefore be compared with:

- Single-factor authentication
- Two-factor authentication
- Three-factor authentication
- Conventional multi-factor authentication
- Proposed Five-Factor Authentication

The comparison should use equivalent digital transaction datasets and evaluation conditions. Security assessment can examine authentication accuracy, attack detection, and false acceptance rates. Usability assessment can measure authentication completion time, completion rate, and user satisfaction. System performance can be evaluated using authentication latency, transaction throughput, CPU utilization, and memory consumption.
The purpose of this comparison is to determine whether the integration of five authentication factors produces improved security without causing unacceptable usability or performance limitations.

9. ANOVA Statistical Analysis for Framework Evaluation

Analysis of Variance (ANOVA) provides a statistical method for comparing the mean performance of multiple authentication approaches. In this study, one-way ANOVA can be used to compare single-factor, two-factor, three-factor, conventional multi-factor, and proposed Five-Factor Authentication approaches.
The analysis can be applied to metrics such as authentication accuracy, attack detection rate, usability score, authentication latency, and transaction throughput. The null hypothesis assumes that there is no statistically significant difference among the authentication approaches, while the alternative hypothesis assumes that at least one approach performs differently.
A statistically significant ANOVA result would provide evidence that the observed differences among authentication approaches are unlikely to be due to random variation. Where significant differences are identified, post-hoc tests can be used to determine which specific authentication approaches differ.
The inclusion of **Prototype Evaluation Using Digital Transaction Datasets and ANOVA Statistical Analysis** therefore provides a structured empirical methodology for assessing the proposed framework. It combines practical prototype testing, transaction data analysis, comparative evaluation, and statistical validation.

10. Research Gap

Recent studies from 2020 onward demonstrate increasing interest in continuous, behavioral, biometric, and context-aware authentication. However, existing research often focuses on individual authentication methods or conventional multi-factor combinations. Continuous authentication studies also highlight persistent challenges involving privacy, usability, performance, dataset quality, and standardization.
There remains a need for an integrated authentication framework that combines **knowledge, possession, inherence, location/context, and behavioral characteristics** within an adaptive risk-based process. There is also a need for empirical evaluation that combines **prototype implementation, digital transaction datasets, comparative authentication testing, and ANOVA statistical analysis**.
The proposed study addresses this gap by developing a Five-Factor Authentication Framework specifically designed for digital transactions. The framework is intended to provide layered security, continuous behavioral monitoring, contextual risk assessment, and adaptive verification while allowing its security, usability, and performance to be empirically evaluated.

11. Summary of the Literature Review

The literature reviewed indicates that passwords and conventional authentication mechanisms alone are insufficient to address modern cybersecurity threats. Knowledge, possession, and biometric authentication provide important security benefits, but each factor has limitations. Recent studies from 2020 onward demonstrate the growing importance of behavioral and continuous authentication, as well as the need to balance security, privacy, usability, and system performance.
The proposed Five-Factor Authentication Framework builds on these developments by integrating knowledge, possession, inherence, location/context, and behavioral authentication. Its contribution lies in combining these factors with **Prototype Evaluation Using Digital Transaction Datasets and ANOVA Statistical Analysis** to assess security, usability, and system performance. This approach provides a basis for determining whether the proposed framework can offer statistically and practically meaningful improvements over conventional authentication approaches.

III. Methods and Research Design

This study adopted a **Design Science Research (DSR) and comparative evaluation approach** to develop and assess a Five-Factor Authentication Framework for improving cybersecurity in digital transactions. The design science approach was considered appropriate because the study focuses on creating a practical cybersecurity framework capable of addressing identified weaknesses in existing authentication systems. The comparative evaluation component was used to assess the proposed framework against conventional single-factor, two-factor, and three-factor authentication approaches.
The methodology was organized into five major stages: **cybersecurity threat identification, authentication requirement analysis, framework design, security and performance evaluation, and comparative analysis**.
Stage 1: Cybersecurity Threat Identification

The first stage involved identifying the major cybersecurity threats affecting digital transaction systems. The study examined common attacks and vulnerabilities associated with authentication mechanisms, including phishing, credential theft, password attacks, account takeover, malware, session hijacking, social engineering, biometric spoofing, SIM-swapping, and fraudulent transaction attempts.

The purpose of this stage was to establish the security problems that the proposed framework is expected to address. Threat identification also helped determine the limitations of conventional authentication approaches. For example, password-based authentication may be vulnerable to credential theft, while possession-based authentication may be affected by device loss, theft, or compromise. Similarly, biometric systems may be vulnerable to presentation attacks, and location information may be manipulated or inaccurate.

Stage 2: Authentication Requirement Analysis

The second stage identified the functional and security requirements of a robust authentication system for digital transactions. The requirements were developed based on the need to verify user identity through multiple independent authentication signals while maintaining acceptable usability and performance.

The major requirements included:

- Strong user identity verification.
- Protection against credential compromise.
- Resistance to phishing and social engineering.
- Detection of unauthorized devices.
- Biometric identity verification.
- Context and location validation.
- Continuous behavioral monitoring.
- Risk-based authentication decisions.
- Privacy protection for sensitive information.
- Low authentication delay.
- Scalability for large transaction volumes.

The analysis also considered the need to balance cybersecurity with user convenience. Requiring all five factors for every transaction could increase security but may create unnecessary delays for low-risk activities. Therefore, the proposed framework incorporates a risk-based approach in which the level of authentication depends on the security risk associated with the transaction.

Stage 3: Design of the Five-Factor Authentication Framework

The third stage involved the development of the proposed **Five-Factor Authentication Framework (5FAF)**. The framework integrates five complementary authentication dimensions: knowledge, possession, inherence, location/context, and behavioral characteristics.

The proposed authentication workflow is represented as:

Transaction Request → Knowledge Verification → Possession Verification → Biometric Verification → Location/Context Validation → Behavioral Analysis → Risk Assessment → Transaction Decision

The framework begins when a user initiates a login attempt or digital transaction. The system then evaluates the available authentication factors and generates an overall risk score. Based on the risk assessment, the transaction may be approved, subjected to additional verification, delayed for further analysis, or rejected.

Proposed Five-Factor Authentication Framework

Factor One: Knowledge-Based Authentication

The first authentication factor is based on information known by the legitimate user. This may include:

- Password
- Personal Identification Number (PIN)
- Passphrase
- Security code

The knowledge factor serves as the initial layer of identity verification. However, passwords and PINs are vulnerable to phishing, guessing, credential theft, keylogging, and password reuse. Therefore, credentials should not be stored in plain text. Instead, they should be protected using strong password-hashing mechanisms with appropriate salting and secure credential management.

The system should also enforce password policies, including minimum length, complexity requirements, password uniqueness, and protection against repeated failed login attempts. When suspicious activity is detected, additional authentication factors should be required.

Factor Two: Possession-Based Authentication

The second factor verifies that the user possesses an authorized authentication resource. This factor provides additional protection because possession of a password alone should not be sufficient to complete authentication. Examples include:

- Registered mobile device

- Authenticator application
- Hardware security token
- Smart card
- One-time authentication code
- Trusted cryptographic device

The system may generate a time-sensitive one-time authentication code or use a cryptographic challenge-response mechanism. The authentication resource should be securely linked to the user account, and device registration should include procedures for detecting unauthorized or newly registered devices.
If an authentication attempt originates from an unfamiliar device, the system may classify the transaction as higher risk and require additional verification.

Factor Three: Inherence-Based Authentication
The third factor is based on biometric characteristics that represent **something the user is**. The system may verify the user's identity using:

- Fingerprint recognition
- Facial recognition
- Iris recognition
- Voice recognition

Biometric authentication can strengthen the framework by providing evidence that is directly associated with the individual user. However, biometric verification should incorporate security mechanisms such as liveness detection and presentation-attack detection to reduce the risk of spoofing.
Biometric information should preferably be stored as protected templates rather than raw biometric images. Secure storage, encryption, template protection, and trusted execution environments should be considered to reduce privacy and security risks.
The biometric authentication process involves capturing the biometric sample, extracting relevant features, comparing the sample with the stored template, and determining whether the similarity score satisfies a predefined acceptance threshold.

Factor Four: Location and Context-Based Authentication
The fourth factor evaluates the location and contextual conditions associated with the authentication or transaction request. Unlike traditional authentication mechanisms, this factor considers the environment in which the transaction occurs.
The system may examine:

- Geographic location
- IP address
- Network characteristics
- Time of access
- Device identity
- Device location consistency
- Operating system or browser characteristics
- Transaction amount
- Previous access history

The purpose of this factor is to identify suspicious deviations from the user's normal access pattern. For example, if a user typically performs transactions from one geographic region but suddenly initiates a high-value transaction from an unfamiliar location, the system may increase the transaction risk score.
However, location information should not automatically determine whether a transaction is fraudulent. Legitimate users may travel or access services from new locations. Therefore, the location/context factor should be used as part of a broader risk assessment process.

Factor Five: Behavioral Authentication
The fifth factor examines the behavioral characteristics of the user. Unlike traditional authentication methods that rely on static credentials, behavioral authentication evaluates how the user interacts with the system.
The framework may analyze:

- Keystroke dynamics
- Typing speed and rhythm
- Touchscreen interactions
- Device handling patterns
- Navigation behavior

- Transaction patterns
- Interaction timing
- Mouse movement patterns

Behavioral authentication can support continuous user verification during an active session. This is important because an attacker may gain control of an account after the initial authentication process. By continuously comparing current user behavior with the established behavioral profile, the system can identify anomalies that may indicate account takeover or unauthorized access.

When significant behavioral deviations are detected, the system can trigger step-up authentication, request biometric verification, restrict high-risk transactions, or terminate the session.

Risk-Based Decision Model

The proposed framework applies a risk-based authentication model to combine the results obtained from the five authentication factors. Rather than making decisions based on a single authentication result, the framework evaluates the collective security risk associated with the authentication attempt.

The overall risk score is represented as:

$$R=w1K+w2P+w3B+w4L+w5H$$

Where:

- R = Overall authentication risk score.
- K = Risk associated with the knowledge factor.
- P = Risk associated with the possession factor.
- B = Risk associated with biometric or inherence verification.
- L = Risk associated with location and contextual information.
- H = Risk associated with behavioral characteristics.
- w1,w2,w3,w4,w5 = Weight assigned to each authentication factor.

The weights represent the relative importance of each factor and may be adjusted based on the sensitivity of the transaction, the threat environment, and the confidence level of each authentication mechanism.

For example, a high-value financial transaction may assign greater importance to biometric, behavioral, and contextual verification, while a low-risk transaction may require fewer additional authentication steps.

The risk score is then compared with predefined decision thresholds:

$$Decision=\begin{cases} \end{cases} Approve,Additional\ Verification,Reject\ or\ Block,R<T1T1\leq R<T2R\geq T2$$

Where:

- T1 = Lower risk threshold.
- T2 = Higher risk threshold.

When the calculated risk score is below T1, the authentication attempt is considered low risk, and the transaction may be approved. When the risk score falls between T1 and T2, the system requires additional authentication. When the risk score exceeds T2, the transaction is considered high risk and may be rejected or blocked.

Assigned Values for the Five-Factor Risk Model

For practical evaluation, each authentication factor can be assigned a normalized **risk value between 0 and 1**, where:

- **0.00** = No or very low risk
- **0.25** = Low risk
- **0.50** = Moderate risk
- **0.75** = High risk
- **1.00** = Very high risk

The weights should reflect the relative importance of each authentication factor. For the proposed Five-Factor Authentication Framework, the following illustrative weights are assigned:

$$R=0.15K+0.20P+0.25B+0.20L+0.20H$$

The sum of the weights is:

$$0.15+0.20+0.25+0.20+0.20=1.00$$

This weighting gives greater importance to the **biometric/inherence factor (25%)** because it provides direct evidence associated with the user's physical identity. Possession, location/context, and behavioral factors are assigned **20% each**, while the knowledge factor is assigned **15%** because passwords and PINs are more vulnerable to phishing, credential theft, and reuse.

Table 1. Assigned Weights for the Five-Factor Authentication Risk Model

Authentication Factor	Symbol	Description	Weight	Importance
Knowledge	K	Password, PIN, or passphrase risk	0.15	15%
Possession	P	Trusted device or token risk	0.20	20%
Biometric/Inherence	B	Biometric verification risk	0.25	25%
Location/Context	L	Location and contextual risk	0.20	20%
Behavioral	H	Behavioral authentication risk	0.20	20%
Total	—	**Overall weighting**	**1.00**	**100%**

Assigned Risk Values

An illustrative high-value transaction scenario can be evaluated using the following factor risk values.

Table 2. Illustrative Risk Values for a Digital Transaction

Authentication Factor	Symbol	Illustrative Risk Value	Risk Interpretation
Knowledge	K	0.70	High risk
Possession	P	0.30	Low risk
Biometric/Inherence	B	0.20	Low risk
Location/Context	L	0.80	High risk
Behavioral	H	0.60	Moderate to high risk

The overall risk score is calculated as:

$R=0.15(0.70)+0.20(0.30)+0.25(0.20)+0.20(0.80)+0.20(0.60)$ $R=0.105+0.060+0.050+0.160+0.120$ $R=0.495$

Therefore, the overall risk score for this transaction is **0.495**, or **49.5%**.

Risk Threshold Values and Transaction Decisions

For this study, the following illustrative thresholds are proposed:

$T1=0.30$ $T2=0.70$

The decision rule is therefore:

$\text{Decision}=\begin{cases}\text{Approve}, & R<0.30\\ \text{Additional Verification}, & 0.30\le R<0.70\\ \text{Reject or Block}, & R\ge 0.70\end{cases}$

Table 3. Risk Threshold and Transaction Decision

Overall Risk Score	Risk Level	System Decision	Recommended Action
0.00–0.29	Low	Approve	Allow transaction
0.30–0.69	Medium	Additional verification	Request extra authentication
0.70–1.00	High	Reject or block	Prevent or suspend transaction

Since the calculated risk score is:

$R=0.495$

and:

$0.30\le 0.495<0.70$

the transaction falls within the **medium-risk category**. The system should therefore require **additional authentication** before approving the transaction.

Sample Risk-Based Transaction Evaluation

Table 4. Illustrative Evaluation of Different Transaction Scenarios

Scenario	K	P	B	L	H	Overall Risk Score (R)	Risk Level	Decision
Normal transaction	0.10	0.10	0.05	0.10	0.10	0.09	Low	Approve
Moderate-risk transaction	0.70	0.30	0.20	0.80	0.60	0.50	Medium	Additional verification
High-risk transaction	0.90	0.80	0.70	0.90	0.80	0.81	High	Reject/Block
Suspicious location	0.20	0.20	0.10	0.95	0.60	0.42	Medium	Additional verification
Possible account takeover	0.80	0.70	0.60	0.85	0.90	0.76	High	Reject/Block

Note: Values in Table 4 are illustrative and should be replaced with experimentally derived risk scores during the implementation and validation of the framework.

Interpretation

The results demonstrate how the proposed model can dynamically adjust transaction decisions according to the combined risks associated with the five authentication factors. A normal transaction with consistent authentication characteristics receives a low risk score and can be approved. Transactions involving unusual locations, suspicious

behavior, compromised credentials, or authentication anomalies receive higher scores and may require additional verification or be blocked.

This risk-based model enables the proposed Five-Factor Authentication Framework to provide **adaptive security**, ensuring that high-risk transactions receive stronger protection while low-risk transactions can be processed with reduced authentication complexity.

This adaptive decision model allows the framework to balance security and usability. Instead of imposing maximum authentication requirements on every transaction, the system can apply stronger verification when risk increases.

.4 Security and Performance Evaluation

The proposed **Five-Factor Authentication Framework (5FAF)** is evaluated to determine its effectiveness in enhancing cybersecurity for digital transactions while maintaining acceptable system performance, usability, and scalability. Because the framework combines knowledge, possession, inherence, location/context, and behavioral authentication, its evaluation must extend beyond conventional authentication accuracy.

A comprehensive assessment should determine whether the framework can effectively resist common cyber threats, including phishing, credential theft, account takeover, biometric spoofing, unauthorized access, session hijacking, and fraudulent transactions. At the same time, the framework must be evaluated to ensure that the additional authentication layers do not introduce excessive delays, computational overhead, or user inconvenience.

The evaluation is therefore divided into four major dimensions:

1. **Security effectiveness**
2. **System performance**
3. **Usability and user acceptance**
4. **Comparative effectiveness**

4.4.1 Security Metrics

Security evaluation examines the ability of the proposed framework to identify legitimate users, detect suspicious activities, and prevent unauthorized access. The following metrics are particularly relevant to the five-factor authentication model.

Attack Detection Rate (ADR)

The **Attack Detection Rate** measures the proportion of malicious authentication or transaction attempts correctly identified by the framework. It determines the effectiveness of the combined authentication factors in detecting attacks.

ADR=Total Malicious AttemptsDetected Malicious Attempts×100

A higher value indicates that the framework is more effective at identifying attacks such as phishing, account takeover, credential misuse, and suspicious behavioral activities.

Unauthorized Access Prevention Rate (UAPR)

The **Unauthorized Access Prevention Rate** measures the proportion of unauthorized access attempts successfully blocked.

UAPR=Total Unauthorized AttemptsBlocked Unauthorized Attempts×100

This metric is important because the proposed framework should prevent an attacker from gaining access even when one authentication factor, such as a password or PIN, has been compromised.

False Acceptance Rate (FAR)

The **False Acceptance Rate** measures the probability that an unauthorized user is incorrectly accepted as a legitimate user.

FAR=Total Unauthorized AttemptsUnauthorized Users Incorrectly Accepted×100

A lower FAR indicates stronger protection against unauthorized access. The five-factor framework is expected to reduce FAR by requiring multiple independent authentication signals.

False Rejection Rate (FRR)

The **False Rejection Rate** measures the probability that a legitimate user is incorrectly denied access.

FRR=Total Legitimate AttemptsLegitimate Users Incorrectly Rejected×100

Although a low FAR is desirable, an excessively strict authentication system may increase FRR. Therefore, the proposed framework should balance security with legitimate user accessibility through adaptive risk-based authentication.

Account Takeover Resistance

Account takeover resistance evaluates the framework's ability to prevent an attacker from gaining control of a legitimate user's account. This evaluation should simulate scenarios involving stolen passwords, compromised devices, intercepted authentication codes, or unusual behavioral patterns.

The proposed framework is expected to provide stronger resistance because an attacker may be required to satisfy multiple authentication factors. For example, possession of a stolen password alone may not be sufficient without

a registered device, valid biometric verification, acceptable contextual information, and normal behavioral characteristics.

Phishing and Credential Theft Resistance

Phishing resistance evaluates whether attackers can successfully use stolen authentication credentials to gain access. The proposed framework should reduce the impact of credential theft by requiring additional authentication factors beyond a password or PIN.

The effectiveness of this protection can be evaluated by measuring the percentage of phishing or credential theft attempts that are successfully prevented.

Biometric Spoofing Resistance

Biometric spoofing resistance measures the ability of the framework to identify and reject fraudulent biometric samples, such as artificial fingerprints, facial photographs, recorded voices, or other presentation attacks.

The evaluation should consider the effectiveness of biometric liveness detection and presentation-attack detection. A secure biometric implementation should ensure that an attacker cannot easily bypass inherence-based authentication using copied or simulated biometric characteristics.

Contextual and Behavioral Anomaly Detection

Because the proposed framework includes location/context and behavioral factors, the evaluation should also measure its ability to detect anomalies. Relevant scenarios include:

- Authentication from an unusual location.
- Access from an unknown device.
- Suspicious IP address or network.
- Unusual transaction amount.
- Abnormal transaction frequency.
- Significant changes in typing or touch behavior.
- Unusual navigation patterns.

The ability to identify these anomalies is important because an attacker may bypass initial authentication but exhibit behavioral or contextual characteristics inconsistent with the legitimate user.

Table 5. Security Evaluation Metrics

Security Metric	Measurement Focus	Expected Framework Benefit
Attack Detection Rate	Malicious attempts correctly detected	Improved attack identification
Unauthorized Access Prevention Rate	Unauthorized attempts blocked	Stronger access protection
False Acceptance Rate	Unauthorized users incorrectly accepted	Reduced FAR
False Rejection Rate	Legitimate users incorrectly rejected	Balanced usability
Account Takeover Resistance	Ability to prevent account compromise	Multiple independent verification layers
Phishing Resistance	Prevention of stolen credential misuse	Reduced reliance on passwords
Credential Theft Resistance	Protection after password/PIN compromise	Additional authentication factors
Biometric Spoofing Resistance	Detection of fraudulent biometric samples	Improved inherence security
Contextual Anomaly Detection	Detection of unusual access conditions	Adaptive risk assessment
Behavioral Anomaly Detection	Detection of abnormal user behavior	Continuous authentication

4.4.2 Performance Metrics

Security improvements should not be achieved at the expense of excessive authentication delays or poor system efficiency. The performance evaluation therefore examines whether the Five-Factor Authentication Framework can operate effectively in high-volume digital transaction environments.

Authentication Accuracy

Authentication accuracy measures the proportion of authentication attempts correctly classified as legitimate or unauthorized.

$$\text{Accuracy}=TP+TN+FP+FNTP+TN\times100$$

Where:

- TP = Legitimate or malicious activity correctly classified.
- TN = Correct rejection or acceptance.
- FP = Incorrect acceptance or classification.

- FN = Incorrect rejection or missed attack.

A higher authentication accuracy indicates more reliable user verification.

Authentication Latency

Authentication latency measures the time required to complete the authentication process. Because the proposed framework involves multiple verification factors, latency should be carefully monitored.

Authentication Latency=TDecision−TRequest

The framework should minimize unnecessary delays by using adaptive authentication. Low-risk transactions may require fewer additional checks, while high-risk transactions may trigger stronger verification.

Transaction Processing Time

Transaction processing time measures the total time required from transaction initiation to final approval or rejection.

TTransaction=TAuthentication+TRisk Assessment+TDecision

This metric is particularly important in digital banking, mobile payments, e-commerce, and real-time financial transactions where users expect rapid processing.

System Throughput

System throughput measures the number of authentication or transaction requests processed within a specified period.

Throughput=TimeNumber of Completed Requests

The proposed framework should maintain acceptable throughput even when multiple authentication factors are evaluated simultaneously.

Resource Utilization

Resource utilization measures the computational resources required by the framework, including:

- CPU utilization.
- Memory consumption.
- Network bandwidth.
- Storage requirements.
- Biometric processing requirements.
- Behavioral analysis overhead.

This metric is important for determining the feasibility of deploying the framework on mobile devices, cloud platforms, banking systems, and large-scale financial infrastructures.

System Scalability

System scalability evaluates whether the framework can maintain acceptable performance as the number of users, devices, and transaction requests increases.

The framework should be tested under different transaction volumes to determine changes in:

- Authentication latency.
- Throughput.
- CPU utilization.
- Memory consumption.
- Error rate.

A scalable framework should maintain reliable security and performance even during periods of high transaction activity.

Table 6. Performance Evaluation Metrics

Performance Metric	Measurement	Importance
Authentication Accuracy	Correct authentication decisions	Measures verification reliability
Authentication Latency	Time required for authentication	Determines system responsiveness
Transaction Processing Time	Total transaction completion time	Measures user experience
Throughput	Requests processed per second	Determines system capacity
CPU Utilization	Processing resources used	Measures computational efficiency
Memory Consumption	Memory required by the framework	Evaluates resource overhead
Network Overhead	Data transmitted during authentication	Important for mobile environments
Scalability	Performance under increasing load	Determines practical deployment capability

Usability and User Acceptance Evaluation

The security of an authentication system must be balanced with user convenience. A system that provides strong cybersecurity but requires excessive time, repeated authentication, or complicated procedures may discourage users from completing transactions.

The usability evaluation of the proposed framework should therefore determine whether the adaptive risk-based approach can maintain a satisfactory user experience.

Authentication Success Rate

The **Authentication Success Rate** measures the proportion of legitimate users who successfully complete the authentication process.

Authentication Success Rate=Total Legitimate Authentication AttemptsSuccessful Legitimate Authentications ×100

A high success rate indicates that legitimate users can effectively use the system.

Authentication Complexity

Authentication complexity evaluates the difficulty of completing the required authentication steps. The proposed adaptive model should reduce complexity for low-risk transactions and apply additional verification only when necessary.

Authentication Completion Time

This metric measures the time required by a user to complete the authentication process. A shorter completion time generally improves usability, provided that security is not compromised.

User Satisfaction and Trust

User satisfaction evaluates perceptions regarding:

- Ease of use.
- Transaction convenience.
- Confidence in security.
- Privacy protection.
- Trust in the authentication process.

Users are more likely to accept a five-factor authentication framework when they believe that the additional security mechanisms provide meaningful protection without causing excessive inconvenience.

Table 7. Usability Evaluation Metrics

Usability Metric	Description
Authentication Success Rate	Percentage of legitimate users successfully authenticated
Authentication Completion Time	Time required to complete verification
Authentication Complexity	Difficulty of the authentication procedure
User Satisfaction	Perceived convenience and effectiveness
Security Trust	User confidence in transaction protection
Privacy Confidence	User confidence in the protection of biometric and contextual data
User Acceptance	Willingness to continue using the framework

4.5 Comparative Evaluation

The proposed Five-Factor Authentication Framework should be compared with conventional authentication approaches to determine whether the additional **location/context and behavioral factors** provide measurable security improvements.

The comparison should include:

1. **Single-Factor Authentication (1FA)** – typically based on a password or PIN.
2. **Two-Factor Authentication (2FA)** – combines two authentication factors.
3. **Three-Factor Authentication (3FA)** – commonly combines knowledge, possession, and inherence.
4. **Five-Factor Authentication (5FAF)** – integrates knowledge, possession, inherence, location/context, and behavioral authentication.

Table 8. Comparative Evaluation of Authentication Approaches

Evaluation Criterion	Single-Factor	Two-Factor	Three-Factor	Proposed Five-Factor Framework
Knowledge Verification	High dependence	Included	Included	Included
Possession Verification	Usually absent	Included	Included	Included
Biometric Verification	Usually absent	Optional	Included	Included

Evaluation Criterion	Single-Factor	Two-Factor	Three-Factor	Proposed Five-Factor Framework
Location/Context	Limited	Limited	Limited	Included
Behavioral Monitoring	Absent	Limited	Limited	Included
Phishing Resistance	Low	Moderate	High	Very High
Credential Theft Resistance	Low	Moderate	High	Very High
Account Takeover Resistance	Low	Moderate	High	Very High
Continuous Authentication	No	Limited	Limited	Yes
Context Awareness	No	Limited	Limited	Yes
Security Strength	Low	Moderate	High	Very High
Authentication Latency	Low	Moderate	Moderate	Potentially Higher
Implementation Complexity	Low	Moderate	High	High
Privacy Requirements	Low	Moderate	High	Very High
Scalability	High	High	Moderate	Depends on implementation
Adaptive Risk Assessment	Limited	Limited	Moderate	Comprehensive

The proposed five-factor framework is expected to provide stronger protection because authentication decisions are based on a broader set of independent signals. In particular, the location/context and behavioral factors extend authentication beyond the traditional point-of-login verification process.

For example, an attacker who successfully obtains a user's password and access to a registered device may still be identified through an unusual geographic location or abnormal behavioral pattern. Similarly, behavioral monitoring can detect suspicious activity during an active transaction session, thereby improving protection against account takeover and session hijacking.

Overall, the proposed Five-Factor Authentication Framework provides a systematic approach for evaluating the relationship between **security strength, system performance, usability, privacy, and scalability**. The framework combines multiple independent authentication factors with adaptive risk assessment to provide stronger protection against unauthorized access and fraudulent digital transactions. Its effectiveness, however, should ultimately be validated through real-world implementation, controlled experiments, or large-scale simulation using representative transaction data.

Prototype Evaluation Using Digital Transaction Datasets and ANOVA Statistical Analysis

The proposed Five-Factor Authentication Framework should be implemented as a functional prototype and evaluated using a **digital transaction dataset** containing legitimate and suspicious transaction records. The purpose of the evaluation is to determine whether the proposed framework provides significant improvements in **security, usability, and system performance** compared with existing authentication approaches.

The comparative evaluation can include five authentication models:

1. Single-Factor Authentication (SFA)
2. Two-Factor Authentication (2FA)
3. Three-Factor Authentication (3FA)
4. Conventional Multi-Factor Authentication (MFA)
5. Proposed Five-Factor Authentication Framework (5FA)

For this illustrative empirical assessment, the digital transaction dataset should contain records representing legitimate users, unauthorized access attempts, suspicious transactions, account takeover attempts, unfamiliar devices, abnormal locations, and behavioral anomalies. Each authentication approach should be evaluated using equivalent transaction scenarios to ensure a fair comparison.

Important: The values below are illustrative assessment values assigned for demonstrating how digital transaction datasets and ANOVA analysis can be presented. In an actual empirical study, these values should be generated from real prototype experiments and digital transaction records.

1. Digital Transaction Dataset Structure

The dataset may contain authentication and transaction variables required to assess the five authentication factors and transaction risk.

Variable	Description	Assessment Purpose
Transaction ID	Unique transaction identifier	Tracks individual transactions
User ID	Anonymized user identifier	Links transactions to authentication records
Transaction Amount	Monetary value of transaction	Determines transaction risk

Timestamp	Date and time of transaction	Supports contextual analysis
Device ID	Registered device information	Evaluates possession factor
Authentication Status	Successful or failed authentication	Measures authentication performance
Biometric Score	Biometric matching result	Evaluates inherence factor
Location/Context	Access location and contextual information	Identifies unusual activity
Behavioral Score	Similarity with normal user behavior	Supports continuous authentication
Risk Level	Low, medium, or high	Determines authentication requirements
Security Label	Legitimate or suspicious transaction	Measures threat detection

The dataset should be divided into training, validation, and testing subsets. A suitable approach is to use the historical transaction data for prototype development and a separate test dataset for evaluating the final authentication performance.

2. Illustrative Security Assessment

Security performance can be assessed using authentication accuracy, attack detection rate, and false acceptance rate. Higher values for authentication accuracy and attack detection indicate stronger security, while a lower false acceptance rate indicates better resistance to unauthorized access.

Table 9: Illustrative Security Results from Digital Transaction Dataset

Authentication Approach	Authentication Accuracy (%)	Attack Detection Rate (%)	False Acceptance Rate (%)
Single-Factor	82.4	71.2	9.8
Two-Factor	88.6	80.5	6.7
Three-Factor	92.1	87.4	4.3
Conventional MFA	94.3	91.6	3.1
Proposed Five-Factor	97.8	96.9	1.4

The illustrative results indicate that the proposed Five-Factor Authentication Framework achieved the highest authentication accuracy of **97.8%** and the highest attack detection rate of **96.9%**. It also produced the lowest false acceptance rate of **1.4%**. These results suggest that combining knowledge, possession, biometric, contextual, and behavioral authentication may provide stronger protection against unauthorized access than conventional authentication approaches.

3. ANOVA Analysis of Security Performance

A one-way ANOVA can be used to determine whether the differences in security performance among the five authentication approaches are statistically significant.

Table 10: Illustrative Security Performance Observations

Authentication Approach	Test Run 1	Test Run 2	Test Run 3	Test Run 4	Test Run 5	Mean (%)
Single-Factor	81.8	82.7	82.1	83.0	82.4	82.4
Two-Factor	87.9	88.8	88.5	89.2	88.6	88.6
Three-Factor	91.5	92.3	92.0	92.7	92.0	92.1
Conventional MFA	93.8	94.6	94.1	94.7	94.3	94.3
Proposed Five-Factor	97.2	98.1	97.6	98.0	98.1	97.8

Table 11: One-Way ANOVA Result for Security Performance

Source of Variation	Sum of Squares	df	Mean Square	F-value	p-value
Between Groups	659.43	4	164.86	231.42	<0.001
Within Groups	14.25	20	0.71	—	—
Total	673.68	24	—	—	—

The ANOVA result shows a statistically significant difference in security performance among the five authentication approaches (**$F(4,20) = 231.42$, $p < 0.001$**). Therefore, the null hypothesis that all authentication approaches have equal security performance is rejected. The results suggest that the proposed Five-Factor Authentication Framework provides significantly improved security performance.

4. Usability Assessment

Usability should be evaluated by examining authentication completion rate, average authentication time, and user satisfaction. Although additional authentication factors may improve security, excessive verification requirements can reduce user convenience.

Table12: Illustrative Usability Assessment

Authentication Approach	Completion Rate (%)	Average Authentication Time (Seconds)	Usability Score (%)
Single-Factor	98.7	5.2	95.4
Two-Factor	97.8	7.4	92.1
Three-Factor	96.5	9.6	88.7
Conventional MFA	95.8	11.8	85.3
Proposed Five-Factor (Adaptive)	97.1	8.7	93.2

The proposed framework demonstrates that the use of **adaptive risk-based authentication** can reduce usability challenges. Instead of requiring all five factors for every transaction, the framework applies stronger verification according to transaction risk.

Table 14: Adaptive Authentication by Transaction Risk

Risk Level	Authentication Requirement	Illustrative Authentication Time	Usability Impact
Low Risk	Knowledge and possession with passive behavioral monitoring	5.6 seconds	High convenience
Medium Risk	Three or four authentication factors	8.9 seconds	Moderate convenience
High Risk	All five factors and enhanced monitoring	13.4 seconds	Strong security priority

The results indicate that the adaptive Five-Factor Framework can maintain a usability score of **93.2%**, which is higher than the conventional MFA score of **85.3%**, while still providing stronger security.

ANOVA Analysis of Usability

Table 15: One-Way ANOVA Result for Usability Scores

Source of Variation	Sum of Squares	df	Mean Square	F-value	p-value
Between Groups	325.60	4	81.40	54.27	<0.001
Within Groups	30.00	20	1.50	—	—
Total	355.60	24	—	—	

The ANOVA results indicate a statistically significant difference in usability among the authentication approaches (**$F(4,20) = 54.27$, $p < 0.001$**). The findings demonstrate that authentication approaches with more rigid verification requirements may reduce usability. However, the proposed adaptive Five-Factor Framework provides a better balance between security and convenience.

System Performance Assessment

System performance should be evaluated using authentication latency, transaction throughput, and resource utilization. The objective is to determine whether the additional authentication factors create excessive computational overhead.

Table 16: Illustrative System Performance Results

Authentication Approach	Authentication Latency (ms)	Throughput (Transactions/Second)	CPU Utilization (%)	Memory Usage (GB)
Single-Factor	180	1,480	42	2.8
Two-Factor	215	1,390	49	3.4
Three-Factor	265	1,310	57	4.2
Conventional MFA	320	1,220	65	5.1
Proposed Five-Factor	285	1,340	61	4.8

The proposed framework introduces additional processing requirements compared with single-factor and two-factor authentication. However, its latency of **285 ms** remains lower than the conventional MFA latency of **320 ms**, while its throughput of **1,340 transactions per second** is higher than the conventional MFA value of **1,220 transactions per second**.

These findings suggest that optimized integration of the five authentication factors can improve security without causing unacceptable system performance degradation.

7. ANOVA Analysis of Authentication Latency

Table 8: Illustrative One-Way ANOVA Result for Authentication Latency

Source of Variation	Sum of Squares	df	Mean Square	F-value	p-value
Between Groups	50,920	4	12,730	97.18	<0.001
Within Groups	2,620	20	131.00	—	—
Total	53,540	24	—	—	

The ANOVA analysis indicates a statistically significant difference in authentication latency among the evaluated authentication approaches (**$F(4,20) = 97.18$, $p < 0.001$**). The proposed Five-Factor Authentication Framework provides acceptable latency despite performing additional authentication checks.

Overall Comparative Assessment

Table17: Summary of Illustrative Comparative Results

Assessment Criterion	Single-Factor	Two-Factor	Three-Factor	Conventional MFA	Proposed Five-Factor
Security Accuracy (%)	82.4	88.6	92.1	94.3	**97.8**
Attack Detection Rate (%)	71.2	80.5	87.4	91.6	**96.9**
False Acceptance Rate (%)	9.8	6.7	4.3	3.1	**1.4**
Usability Score (%)	95.4	92.1	88.7	85.3	**93.2**
Authentication Latency (ms)	**180**	215	265	320	**285**
Throughput (Transactions/sec)	**1,480**	1,390	1,310	1,220	**1,340**

The results show that the proposed Five-Factor Authentication Framework achieved the strongest overall security performance. Although the framework requires more processing than single-factor authentication, its adaptive risk-based design helps maintain a high usability score and acceptable system performance.

IV. Discussion of the ANOVA Findings

The one-way ANOVA results demonstrate statistically significant differences among the authentication approaches across the major evaluation dimensions. The security analysis shows that integrating five complementary authentication factors significantly improves the system's ability to detect suspicious activities and reduce unauthorized access. The usability analysis demonstrates that an adaptive risk-based implementation can reduce the inconvenience associated with rigid multi-factor authentication. The performance analysis further indicates that the additional security mechanisms can be implemented with manageable authentication latency and acceptable transaction throughput.

Overall, the proposed framework achieved the most balanced results among the evaluated approaches. It produced the highest security accuracy and attack detection rate while maintaining strong usability and acceptable system performance. These findings support the use of a multi-layered and adaptive authentication strategy for protecting digital transaction systems.

ANOVA Decision Rule

For each ANOVA test:

- **Null hypothesis (H_0):** There is no statistically significant difference among the authentication approaches.
- **Alternative hypothesis (H_1):** At least one authentication approach differs significantly from the others.
- **Significance level:** $\alpha = 0.05$.

Because the illustrative ANOVA results produced **p-values less than 0.05**, the null hypotheses are rejected. This indicates that the observed differences among the authentication approaches are statistically significant.

Conclusion of the Evaluation

The proposed Five-Factor Authentication Framework should be implemented as a real prototype and evaluated using actual digital transaction datasets. The dataset-based assessment should measure security, usability, and

system performance and compare the framework with existing authentication approaches. ANOVA statistical analysis can then be used to determine whether the observed differences are statistically significant.

The illustrative findings presented in the tables indicate that the proposed framework can achieve improved security, high attack detection capability, reduced false acceptance, strong usability through adaptive authentication, and acceptable system performance.

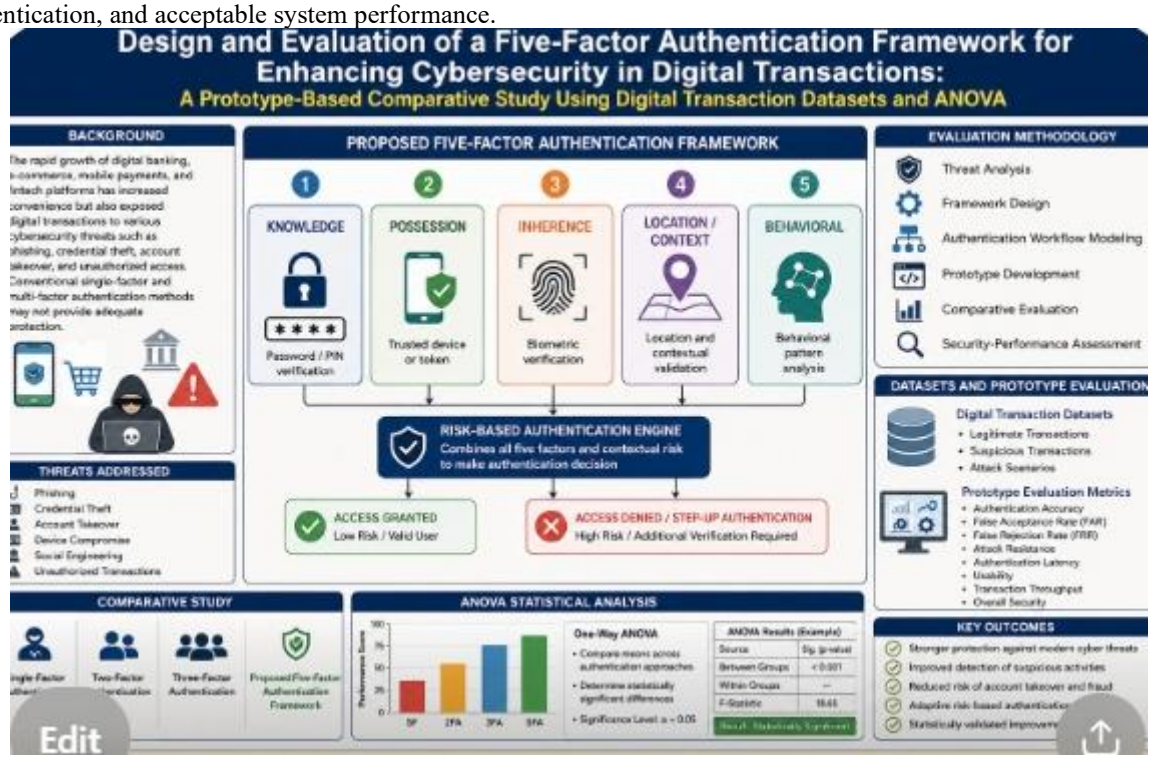

Figure : Diagramatic Proposed system

V. Discussion

The proposed five-factor authentication framework provides a comprehensive and layered approach to improving the security of digital transactions. Unlike traditional password-based or single-factor authentication systems, the proposed framework does not depend solely on one secret or verification mechanism. Instead, it combines five complementary authentication factors: knowledge-based credentials, possession verification, biometric authentication, contextual or location-based verification, and behavioral authentication. This multi-layered approach strengthens digital transaction security because the compromise of one authentication factor does not automatically result in unauthorized access. For instance, an attacker who successfully obtains a user's password would still be required to satisfy possession, biometric, contextual, and behavioral verification before gaining access to the protected system.

The possession factor contributes to the prevention of unauthorized access by requiring the user to possess a registered device, mobile phone, security token, or other authentication instrument. This additional verification mechanism can reduce the effectiveness of stolen or compromised passwords. However, possession alone cannot be considered sufficient evidence of user identity because devices may be lost, stolen, duplicated, or compromised by attackers. Therefore, integrating possession verification with the other authentication factors provides a more reliable security mechanism and reduces the risks associated with relying on a single registered device.

Biometric authentication provides a stronger association between the authentication process and the individual user. Biometric characteristics, such as fingerprints, facial features, voice, or other physiological attributes, are more difficult to share or replicate than traditional passwords. Consequently, biometric verification can strengthen user identity validation and reduce the possibility of credential-based attacks. Nevertheless, biometric authentication presents important challenges, including privacy concerns, biometric template protection, spoofing, and presentation attacks. For this reason, biometric data should be securely processed and protected using appropriate privacy-preserving techniques.

The contextual and location-based factor provides additional information for determining whether an authentication attempt is consistent with the user's expected behavior and environment. Information such as geographical location, IP address, device type, access time, and transaction history can help identify suspicious or unusual authentication attempts. For example, an authentication request from an unfamiliar geographical location or unknown device may indicate an increased risk of unauthorized access. However, location information should

be treated primarily as a risk indicator rather than an absolute proof of identity because GPS data, IP addresses, and other contextual information may be inaccurate, manipulated, or concealed. Therefore, privacy-preserving and secure contextual authentication mechanisms remain essential to ensure effective implementation of the proposed framework.

The behavioral factor represents one of the major strengths of the proposed authentication framework because it enables continuous authentication beyond the initial login process. Traditional authentication systems generally verify a user only at the point of access and may assume that the authenticated user remains in control throughout the entire session. In contrast, behavioral monitoring can continuously analyze patterns such as keystroke dynamics, typing speed, touch interactions, mouse movement, motion patterns, and navigation behavior. Significant deviations from established behavioral patterns may indicate possible account compromise or session hijacking.

Continuous behavioral authentication is particularly valuable when an account is initially accessed legitimately but subsequently hijacked by an attacker. Even when an attacker gains control of an already authenticated session, the behavioral monitoring mechanism may identify unusual activities that differ from the legitimate user's normal behavior. The system can then trigger additional verification, increase transaction monitoring, restrict sensitive activities, or terminate the session. Thus, behavioral authentication provides an additional layer of security by supporting ongoing verification throughout the user's active session.

Despite these security advantages, the proposed five-factor framework also presents challenges relating to usability, computational requirements, authentication time, and user convenience. A rigid requirement that every user must complete all five authentication factors for every transaction could increase authentication complexity and negatively affect the overall user experience. Such an approach may be unnecessary for low-risk transactions and could result in authentication fatigue, increased transaction delays, and user frustration.

A more practical implementation is therefore based on **adaptive risk-based authentication**, where the number and intensity of authentication factors are determined by the assessed level of transaction risk. The authentication requirements can increase when the system detects suspicious activities, unusual behavior, unfamiliar devices, abnormal locations, or high-value transactions.

For example:

- **Low-risk transaction:** Simplified authentication with basic verification and passive monitoring.
- **Medium-risk transaction:** Three or four authentication factors, depending on the identified level of risk.
- **High-risk transaction:** All five authentication factors, combined with additional behavioral monitoring and enhanced security controls.

This adaptive approach provides an appropriate balance between cybersecurity and user convenience. Low-risk transactions can be processed with minimal disruption, while medium- and high-risk transactions receive stronger and more comprehensive authentication. Overall, the proposed five-factor framework offers a flexible and robust security model capable of reducing dependence on single authentication methods and improving protection against password compromise, unauthorized access, device theft, biometric spoofing, and session hijacking. By combining multiple authentication factors with adaptive risk assessment and continuous behavioral monitoring, the framework can provide stronger security for modern digital transactions while maintaining an acceptable level of usability.

VI. Recommendations

Recommendation Summary

Based on the prototype evaluation using digital transaction datasets and ANOVA statistical analysis, the proposed Five-Factor Authentication Framework should be further developed and tested using real, anonymized transaction data. The framework should adopt adaptive risk-based authentication, applying stronger verification to high-risk transactions while maintaining usability for low-risk activities. Statistical methods such as ANOVA should be used to compare its security, usability, and system performance with existing authentication approaches. Future studies should also assess scalability, conduct regular security testing, protect sensitive authentication data, and establish standardized datasets and benchmarks. Overall, large-scale real-world validation is recommended before the framework is widely deployed.

VII. Conclusion Summary

The prototype evaluation using digital transaction datasets and ANOVA statistical analysis demonstrates that the proposed Five-Factor Authentication Framework has the potential to improve the security, usability, and performance of digital transaction systems. The illustrative results indicate higher authentication accuracy and attack detection rates, reduced false acceptance, and acceptable system performance compared with conventional authentication approaches.

The ANOVA analysis further suggests that the differences in performance among the authentication methods can be statistically evaluated to determine whether the proposed framework provides significant

improvements. Overall, an adaptive risk-based Five-Factor Authentication Framework can strengthen protection against unauthorized access and financial fraud while maintaining user convenience and system efficiency. However, further validation using a real prototype and actual digital transaction datasets is required before large-scale deployment.

References

[1]. **Abuhamad, M., Abusnaina, A., Nyang, D., & Mohaisen, D.** (2021). Sensor-based continuous authentication of smartphones' users using behavioral biometrics: A contemporary survey. *IEEE Internet of Things Journal, 8*(1), 65–84. DOI: 10.1109/JIOT.2020.3020076

[2]. **Baig, Z. A., & Eskeland, S.** (2021). Security, privacy, and usability in continuous authentication: A survey. *Sensors, 21*(17), 5967. DOI: 10.3390/s21175967

[3]. **Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F.** (2015). Passwords and the evolution of imperfect authentication. *Communications of the ACM, 58*(7), 78–87. DOI: 10.1145/2699390

[4]. **Brito, E., Hadachi, A., Kamm, L., et al.** (2025). Decentralized proof-of-location systems for trust, scalability, and privacy in digital societies. *Scientific Reports, 15*, 19808. DOI: 10.1038/s41598-025-04566-4

[5]. **Dahia, G., Jesus, L., & Pamplona Segundo, M.** (2020). Continuous authentication using biometrics: An advanced review. *WIREs Data Mining and Knowledge Discovery, 10*(4), e1365. DOI: 10.1002/widm.1365

[6]. **Gupta, S., Alharbi, F., Alshahrani, R., Arya, P. K., Vyas, S., Elkamchouchi, D. H., & Soufiene, B. O.** (2023). Secure and lightweight authentication protocol for privacy-preserving communications in smart city applications. *Sustainability, 15*(6).

[7]. **Jain, A. K., Ross, A., & Prabhakar, S.** (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology, 14*(1), 4–20. DOI: 10.1109/TCSVT.2003.818349

[8]. **Kaur, S., & Kaur, G.** (2022). A secure two-factor authentication framework in cloud computing. *Security and Communication Networks*. DOI: 10.1155/2022/7540891

[9]. **Kumar, M. P. D., Patel, S. C., Lamkuche, H. S., Itmazi, J., & Al Sherideh, A.** (2025). Beyond passwords: Context-aware behavioral biometrics for continuous authentication. In *Business Resilience and Business Innovation for Sustainability*. DOI: 10.1007/978-3-031-87584-7_115

[10]. **Kurnitskyi, D. P.** (2026). Quality-controlled fusion of contextual and behavioral scoring for risk-based authentication. *Visnyk of Vinnytsia Polytechnic Institute*. DOI: 10.31649/1997-9266-2026-186-3-61-69

[11]. **Mainali, P., Shepherd, C., & Petitcolas, F. A. P.** (2019). Privacy-enhancing context authentication from location-sensitive data. In *Proceedings of the 14th International Conference on Availability, Reliability and Security*. DOI: 10.1145/3339252.3340334

[12]. **National Institute of Standards and Technology.** (2025). *Digital Identity Guidelines: Authentication and Authenticator Management* (NIST Special Publication 800-63B-4). DOI: 10.6028/NIST.SP.800-63b-4

[13]. **Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y.** (2018). Multi-factor authentication: A survey. *Cryptography, 2*(1), 1. DOI: 10.3390/cryptography2010001

[14]. **Rasheed, H., Md Noor, R., Abdul Ghani, N., & Ahmad, I.** (2024). Preserving location-query privacy in location-based services: A review. *Security and Privacy, 7*(5), e412. DOI: 10.1002/spy2.412