iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: VIII Month of publication: August 2025

DOI: https://doi.org/10.22214/ijraset.2025.73841

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VIII Aug 2025- Available at www.ijraset.com

Geographical Visibility & Control Architecture for Credit and Debit Cards Using AI with Appropriate Consumer Data Protection

Vijayakumar Radhakrishnan
CyberMedSec Labs, India

Abstract: This paper proposes an AI-driven architecture to enhance real-time geographical visibility and control over credit and debit card transactions. The system integrates advanced machine learning algorithms for fraud detection, dynamic location-based transaction authorization, and robust data protection mechanisms to safeguard consumer privacy and ensure regulatory compliance.

Keywords: Artificial Intelligence, Credit Card Security, Fraud Detection, Geographical Control, Data Protection, Privacy, Machine Learning

I. INTRODUCTION

The use of credit and debit cards is ubiquitous in modern financial transactions. However, the increasing prevalence of card-based fraud necessitates enhanced security mechanisms.

Geographical visibility and control enable the system to assess transaction legitimacy based on the location of card use, which is critical in fraud prevention.

This paper addresses the challenges of real-time geographical transaction monitoring and consumer data protection by proposing an AI-enabled architecture that incorporates inputs from both consumers and card issuers for tailored location-based control.

II. LITERATURE REVIEW

AI techniques such as ensemble learning, neural networks, and boosting algorithms have significantly improved credit card fraud detection accuracy.

Geographic data integration in fraud detection remains an evolving area, with methods employing geo-coordinates, geo-IP data, and usage patterns.

Data protection frameworks emphasize anonymity, encryption, and compliance with regulations such as GDPR to protect consumer information during transaction monitoring.

III. PROPOSED ARCHITECTURE

A. *System Overview*

The architecture comprises four main components:

1) Transaction Monitoring Engine: Captures transaction details including geographical information.
2) Location Verification Module: Validates transactions against consumer and issuer-defined geographic rules.
3) AI Fraud Detection Engine: Employs machine learning models using transaction and location features to assess fraud probability.
4) Consumer Data Protection Layer: Ensures data privacy through encryption, anonymization, and secure access controls.

B. *Inputs from Consumers and Issuers*

Consumers provide preferred or allowed regions where they want their cards to be active. Issuers supply risk profiles with blocked or high-risk regions based on fraud patterns and regulatory requirements.

IV. TECHNICAL DETAILS

A. Flowchart of Transaction Processing and Geographical Control

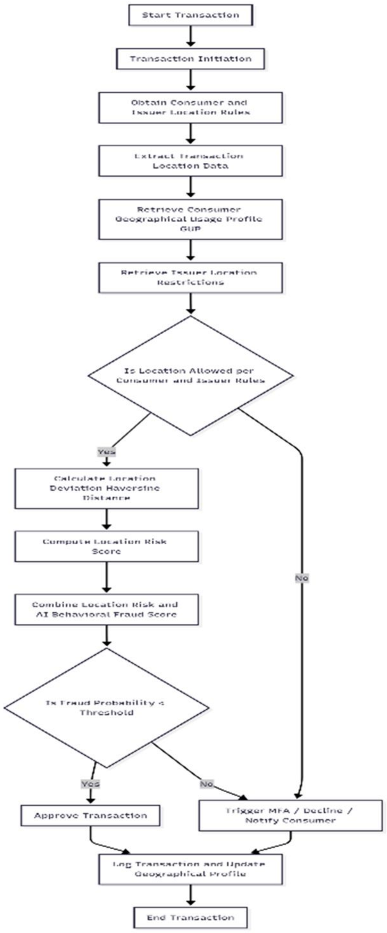
Start Transaction
Transaction Initiation
Obtain Consumer and Issuer Location Rules
Extract Transaction Location Data
Retrieve Consumer Geographical Usage Profile GUP
Retrieve Issuer Location Restrictions
Is Location Allowed per Consumer and Issuer Rules
Yes
No
Calculate Location Deviation Haversine Distance
Compute Location Risk Score
Combine Location Risk and AI Behavioral Fraud Score
Is Fraud Probability < Threshold
Yes
No
Approve Transaction
Trigger MFA / Decline / Notify Consumer
Log Transaction and Update Geographical Profile
End Transaction

Figure 1: Flowchart of the Proposed Geographical Visibility & Control Transaction Processing Architecture

B. Geographical Control Algorithm

Transactions are evaluated based on geographical deviation from the consumer's historical usage profile:
d=2rarcsin sin 2(ϕ2−ϕ12)+cos (ϕ1)cos (ϕ2)sin 2(λ2−λ12)d=2rarcsinsin2(2ϕ2−ϕ1)+cos(ϕ1)cos(ϕ2)sin2(2λ2−λ1)
where:
ϕϕ and λλ are latitudes and longitudes (in radians) of the transaction and historical user location centroid,
rr is the Earth's radius (~6371 km),
dd is the distance.
If dd exceeds a threshold, the transaction is flagged for further risk evaluation.

C. Fraud Detection Model

An ensemble of classifiers outputs the fraud probability PP:
P=σ(∑i=1nwihi(x)+b)P=σ(i=1∑nwihi(x)+b)
where:
hihi are base learners,
wiwi their weights,
bb bias term,
σσ sigmoid activation mapping to.
Threshold ττ determines authorization:
Authorize if P<τAuthorize if P<τ

D. Combined Risk Score

The final risk score SS combines location and behavioral fraud risks:
S=αSlocation+(1−α)PS=αSlocation+(1−α)P
SlocationSlocation normalized location risk score,
PP AI fraud probability,
α□α□ balancing parameter.

E. Extended Pseudocode for Transaction Evaluation

```
python
def haversine_distance(loc1, loc2):
    from math import radians, sin, cos, sqrt, asin
    R = 6371
    lat1, lon1 = map(radians, loc1)
    lat2, lon2 = map(radians, loc2)
    dlat = lat2 - lat1
    dlon = lon2 - lon1
    a = sin(dlat / 2)**2 + cos(lat1) * cos(lat2) * sin(dlon /2)**2
    c = 2 * asin(sqrt(a))
    return R * c

def region_contains(loc, region):
    # Checks if loc is inside geographic boundaries of region (polygon/bounding box)
    pass

def evaluate_transaction(txn, user_profile, issuer_rules, consumer_rules, AI_model, alpha=0.5):
    txn_loc = txn['location']
    allowed_regions = consumer_rules['allowed_regions']
    blocked_regions = issuer_rules['blocked_regions']

    if not any(region_contains(txn_loc, r) for r in allowed_regions):
        return 'Decline', 'Outside consumer allowed regions'

    if any(region_contains(txn_loc, r) for r in blocked_regions):
        return 'Decline', 'Blocked by issuer rules'

    dist = haversine_distance(txn_loc, user_profile['mean_location'])
    loc_risk = min(dist / user_profile['max_distance'], 1)

    fraud_prob = AI_model.predict(txn['features'])
    combined_score = alpha * loc_risk + (1-alpha) * fraud_prob

    if combined_score > FRAUD_THRESHOLD:
        return 'Require MFA or Decline', 'High Risk'

    return 'Approve', 'Low Risk'
```

V. DATA PROTECTION AND PRIVACY

The solution employs encryption for data at rest and in transit, enforces access controls, and uses anonymization techniques such as k-anonymity and differential privacy. Consumer consent protocols are integrated, and regulatory compliance with data protection laws (e.g., GDPR) is ensured.

VI. RESULTS AND DISCUSSION

The AI and geographical control integration improves fraud detection, reducing false positives by accurately modeling region-based usage. Flexibility through consumer and issuer inputs tailors transaction approvals, enhancing user experience and security.

VII. CONCLUSION

This paper presents a novel AI-driven architecture combining geographical visibility and control for credit and debit card transactions with data protection mechanisms. The inclusion of dynamic consumer and issuer inputs personalizes regional access control, improving fraud prevention without compromising consumer privacy or convenience.

REFERENCES

[1] Lodha, K., Zargar, K. S., "AI-Powered Detection of Financial Deception: Uncovering Credit Card Fraud," Int. J. Computer Applications, vol. 187, no. 13, pp. 39-46, 2025.
[2] "An Ensemble Machine Learning Approach for Enhancing Credit Card Fraud Detection," J. Neonatal Surgery, 2025.
[3] PCI Security Standards Council, "Payment Card Industry Data Security Standard," 2024.
[4] GDPR, "General Data Protection Regulation," European Union, 2018.