Dhruv Dhayal

CyberSecurity:

Threat In Banking System Fraud Prevention Model By Using AI/IOT Enviornments

Presentated by Dhruv Dhayal

dhayaldhruv271@gmail.com

Marketing Strategy

01 **Introduction / Main Aim & Objective**

02 **Purpose and Working Appilications.**

03 **Flow Chart Diagrammes / Prevention Techniques.**

04 **Developing Prevention Strategies ,Train the AI Model, Results, Main Conclusion with Refrences.**


Introduction
&
It’s AIM

Introduction to CyberSecurity

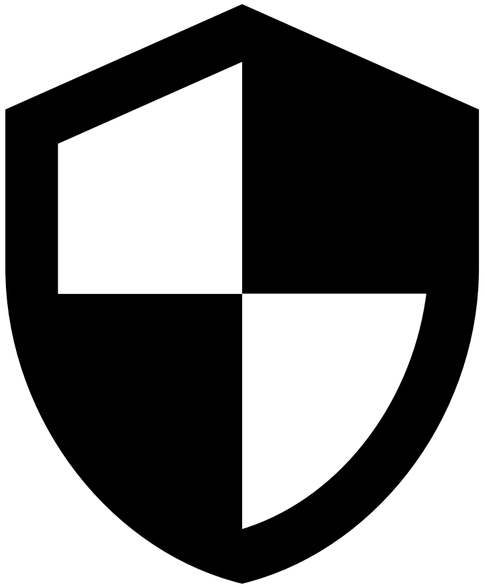
The digital transformation of the banking sector has introduced significant advantages in terms of efficiency and accessibility.

However, it has also exposed banks to a myriad of cybersecurity threats. This paper aims to investigate these threats, their implications, and the advanced technological solutions that are being developed to combat them.

Main AIM / Objective

The primary aim of this research paper is to analyse and understand the various cybersecurity threats facing the banking sector, evaluate the effectiveness of current mitigation strategies, and explore the potential of emerging technologies such as blockchain, artificial intelligence, and machine learning in enhancing cybersecurity.

The paper seeks to provide comprehensive insights into the current cybersecurity landscape in banking and propose future directions for developing robust security frameworks.



Why we need CyberSecurity

This research paper is structured to provide a thorough examination of cybersecurity threats in banking systems. It begins with an introduction that sets the context for the study and outlines its objectives.

The literature review provides a historical overview of cybersecurity in banking, the current threat landscape, and the role of emerging technologies. The core section of the paper delves into the specific types of cybersecurity threats banks face today, supported by real-life case studies that highlight the impact of these threats.

- Protection of Data.
- Prevention from Cyber Attacks.
- Maintain Trust.
- Business Continuity.
- protection of Infrastructure.
- Legal & Regulatory Compliance.

Case Studies

- **JP Morgan Chase Breach (2014)**
  - Hackers gained access to the personal data of 76 million households and 7 million small businesses.
  - Impact: Highlighted the vulnerability of even the largest financial institutions.
- **Bangladesh Bank Heist (2016)**
  - Attackers used the SWIFT network to transfer $81 million fraudulently.
  - Impact: Exposed weaknesses in interbank communication systems.


Mitigation
Strategies

Mitigation Strategies

Technological Solutions.

- Encryption and Data Protections.
- Multi-Factor Authentication (MFA)
- Intrusion Detection Systems

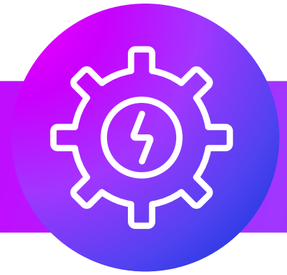
Regulatory Frameworks.

- General Data Protection Regulation (GDPR)
- Payment Card Industry Data Security Standard (PCI DSS)

Best Practices.

- Employee Training and Awareness Programs
- Incident Response Planning
- Continuous Monitoring and Auditing

Types of Banking Frauds



- Phising
- Baiting
- Man-in-the-Middle Attack
- BackDoor Attacks
- Card Not Present(CNP) Fraud

- Account TakeOver.
- Pharming.
- ATM Skimming.
- Malware
- Social Engineering.


How To Prevent
Fraud In Banking
System

Preventive Measures

(i). Implement Strong Encryption and Data Protection

·End-to-End Encryption.

·Data at Rest Encryption.

(ii). Utilize Multi-Factor Authentication (MFA)

·Two Factor Authentication (2FA).

·Biometric Authentication.

(iii). Deploy Intrusion Detection and Prevention Systems (IDS/IPS)

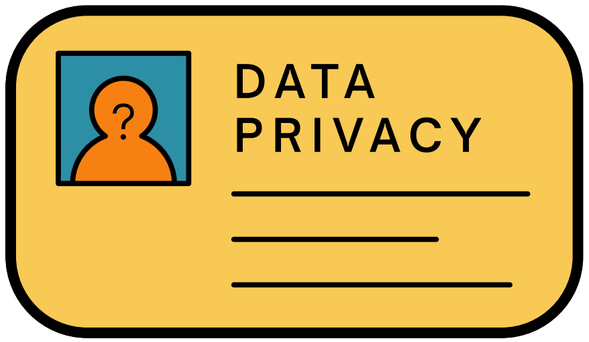
·Real-Time Monitoring.

·Behavioural Analysis.

(iv). Conduct Regular Security Audits and Vulnerability Assessments

·Penetration Testing.

·Vulnerability Scanning.



(v). Develop and Maintain an Incident Response Plan

·Incident Response Team.

·Regular Drills.

Role Of Emerging Technologies

Blockchain Technology

1. **Benefits**

   - Provides decentralized, tamper-proof systems.
   - Example: Implementing blockchain for secure transaction recording.

1. **Case Studies**

   - Santander Bank: Uses blockchain for cross-border payments, enhancing security and reducing fraud.

Artificial Intelligence and Machine Learning

1. **AI-Driven Threat Detection**

   - Analyzes patterns to identify anomalies and potential threats.
   - Example: AI systems that detect unusual login activities.

1. **Predictive Analytics**

   - Uses historical data to predict future threats.
   - Example: Machine learning models that forecast potential cyberattacks.


Challenges
in
FutureDirections

Challenges in Future Directions

Technological Challenges

Challenge-1

1. Scalability and Integration

o Ensuring new technologies integrate seamlessly with existing systems.
o Example: Integrating blockchain with legacy banking systems.

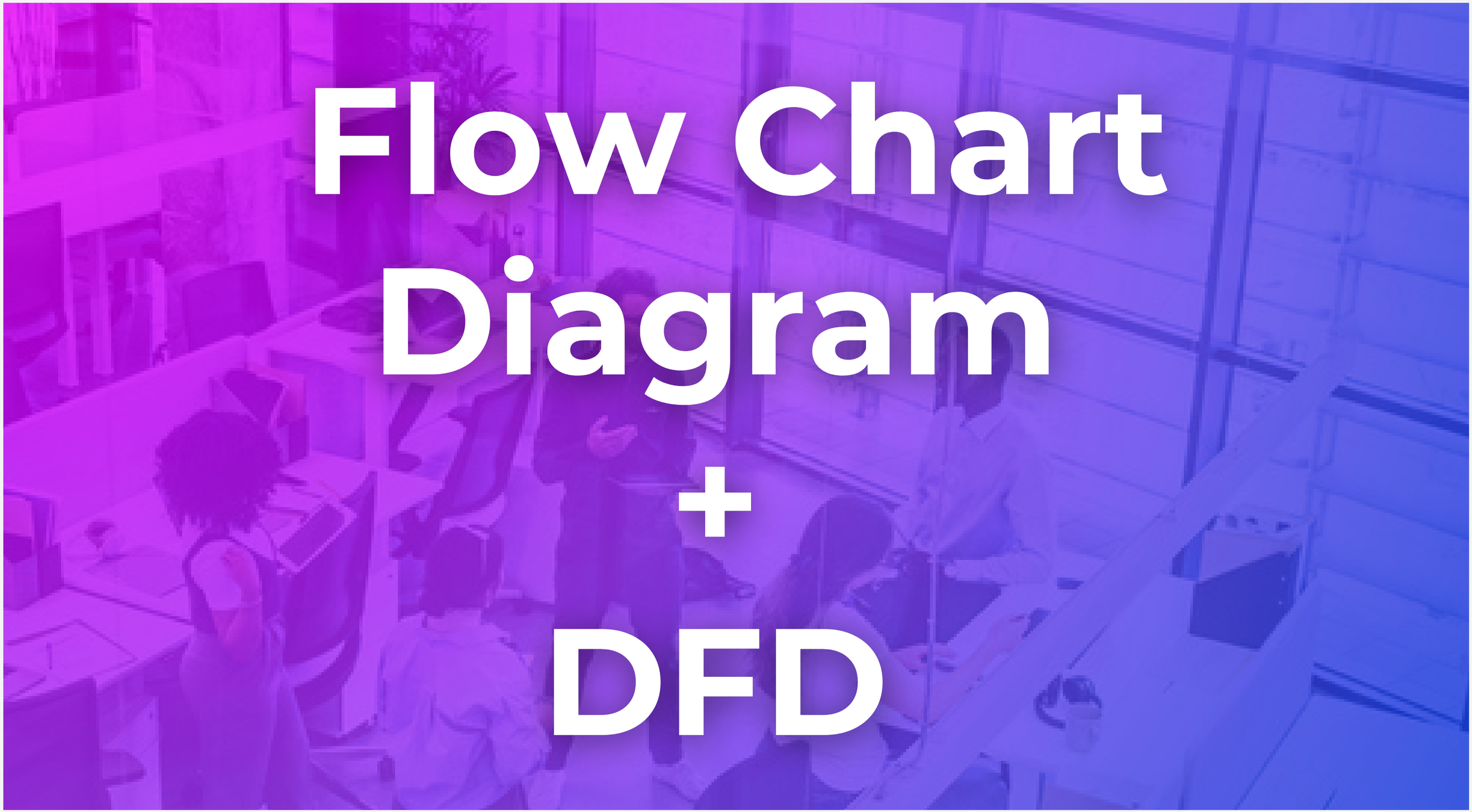
2. Emerging Threats

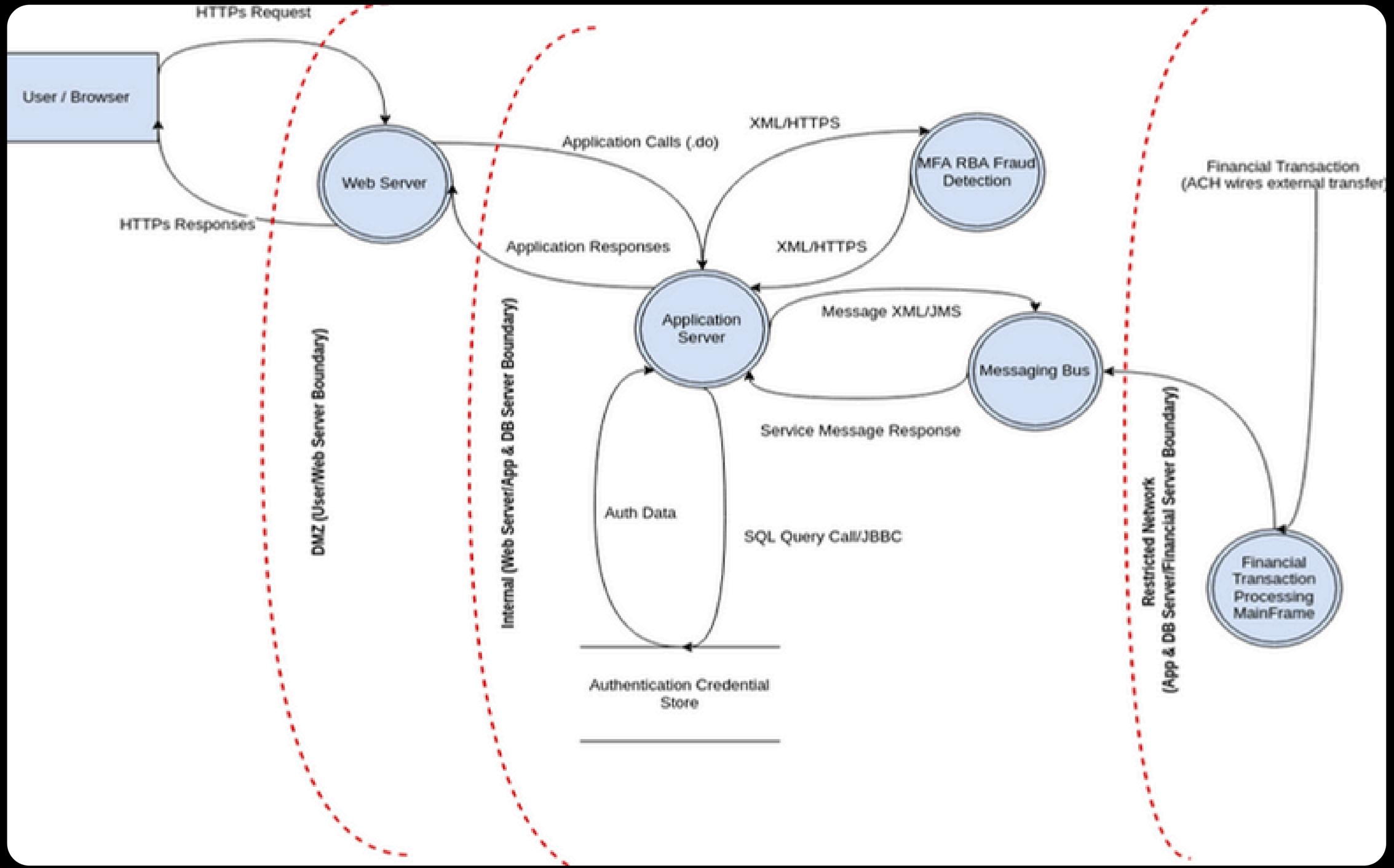
o Adapting to continuously evolving cyber tactics.
o Example: Developing countermeasures for quantum computing threats.

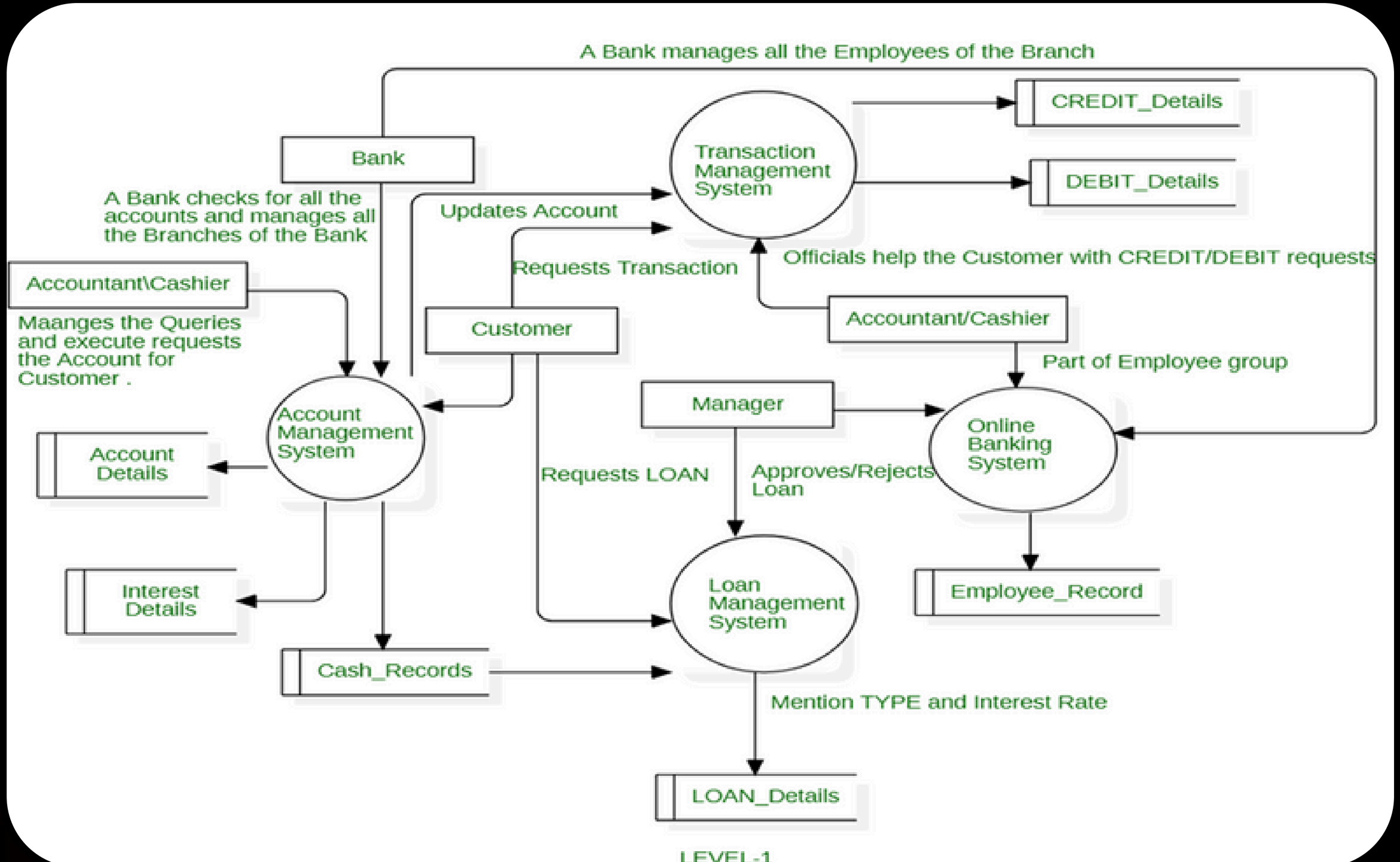
Policy and Regulation

1. Global Standards Harmonization

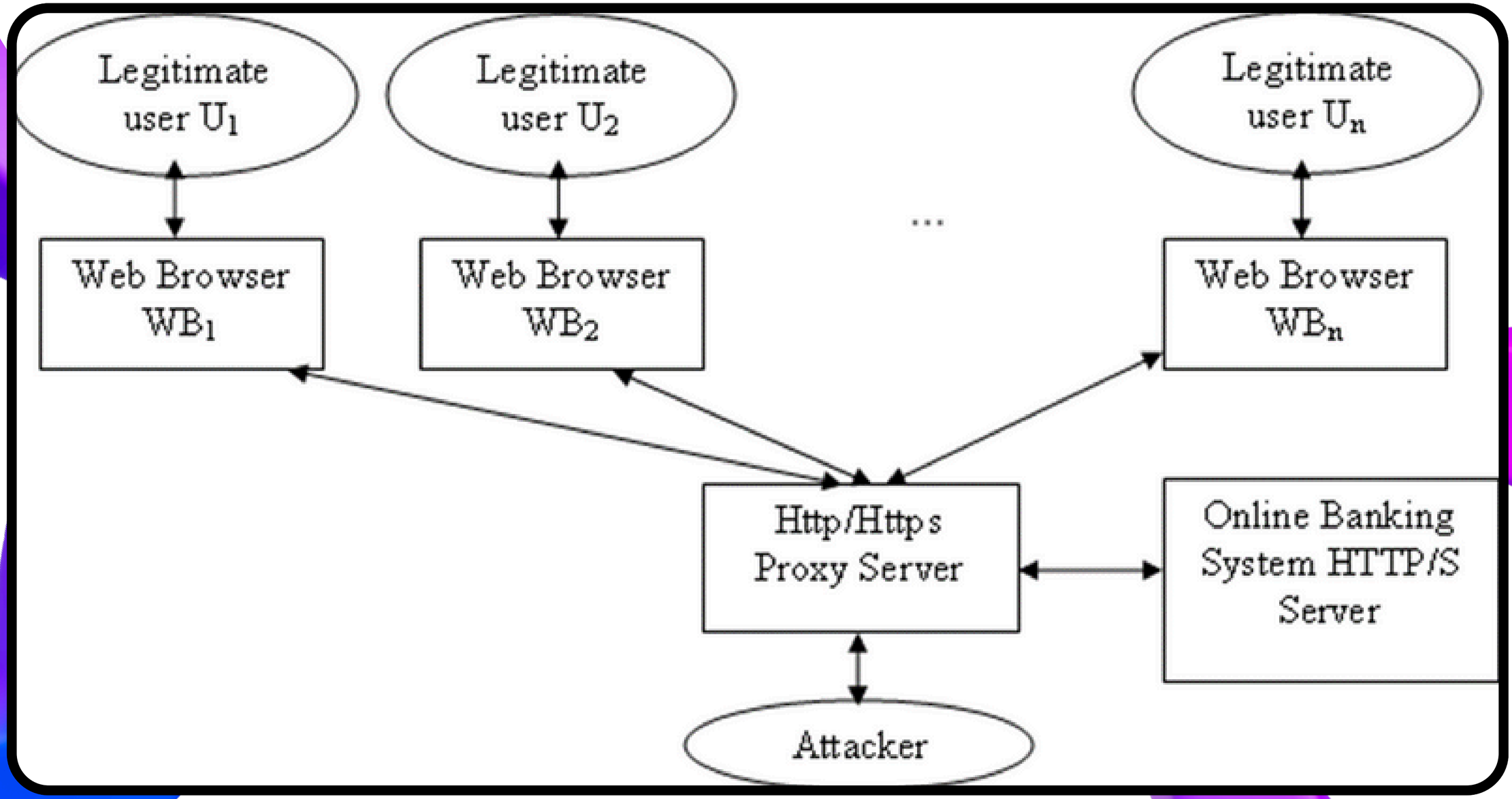
o Aligning cybersecurity regulations across different regions.
o Example: Collaborative efforts between the EU and US on cybersecurity policies.

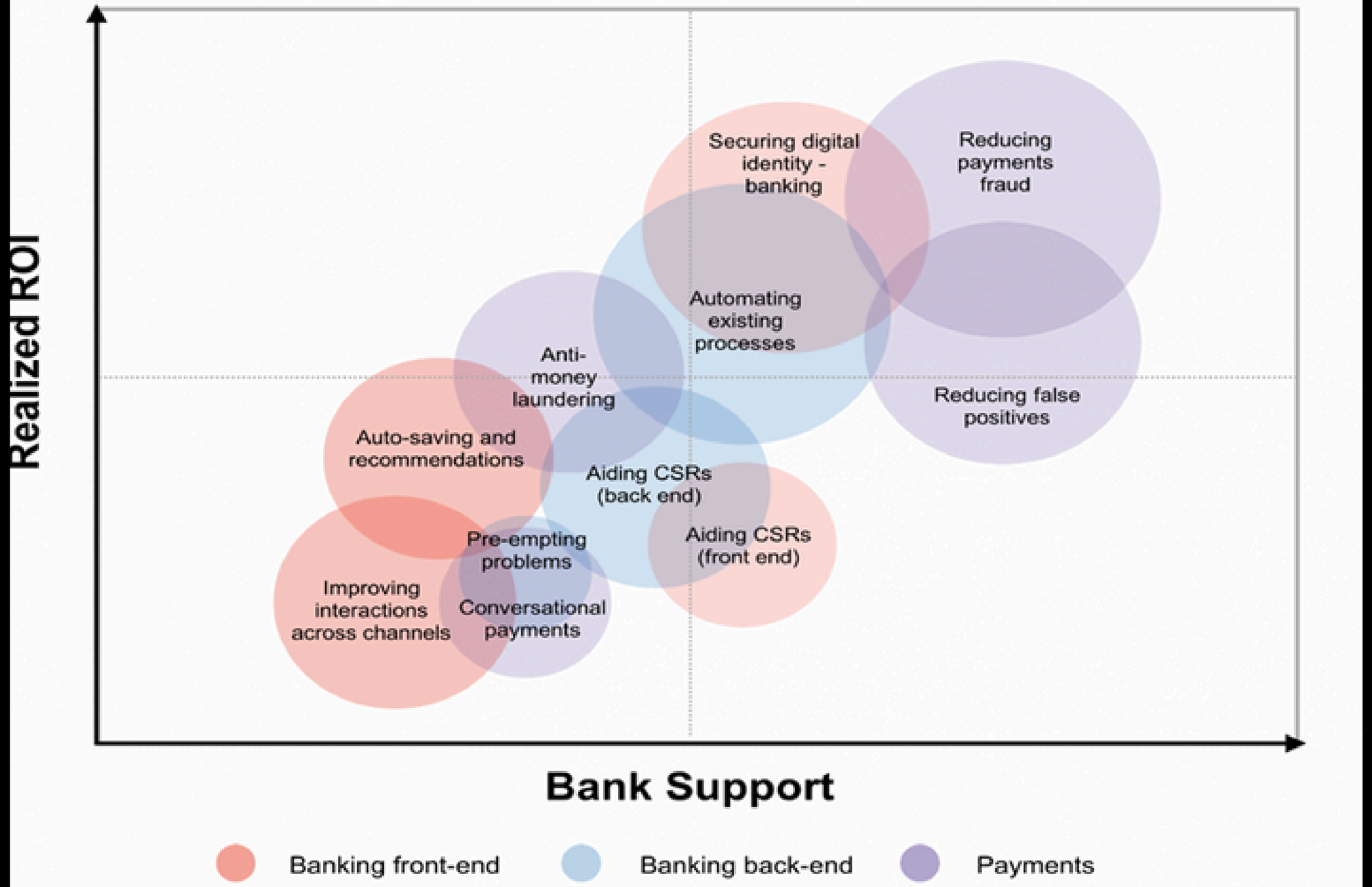

Flow Chart
Diagram
+
DFD


HTTPs Request
User / Browser
Web Server
HTTPs Responses
Application Calls (.do)
Application Responses
XML/HTTPS
MFA RBA Fraud Detection
XML/HTTPS
Application Server
Message XML/JMS
Messaging Bus
Service Message Response
Financial Transaction (ACH wires external transfer)
Auth Data
SQL Query Call/JBBC
Authentication Credential Store
DMZ (User/Web Server Boundary)
Internal (Web Server/App & DB Server Boundary)
Restricted Network (App & DB Server/Financial Server Boundary)
Financial Transaction Processing MainFrame


A Bank manages all the Employees of the Branch
Bank
A Bank checks for all the accounts and manages all the Branches of the Bank
Transaction Management System
CREDIT_Details
DEBIT_Details
Updates Account
Requests Transaction
Officials help the Customer with CREDIT/DEBIT requests
Accountant\Cashier
Maanges the Queries and execute requests the Account for Customer .
Customer
Accountant/Cashier
Part of Employee group
Account Management System
Account Details
Manager
Online Banking System
Requests LOAN
Approves/Rejects Loan
Interest Details
Loan Management System
Employee_Record
Cash_Records
Mention TYPE and Interest Rate
LOAN_Details
LEVEL-1

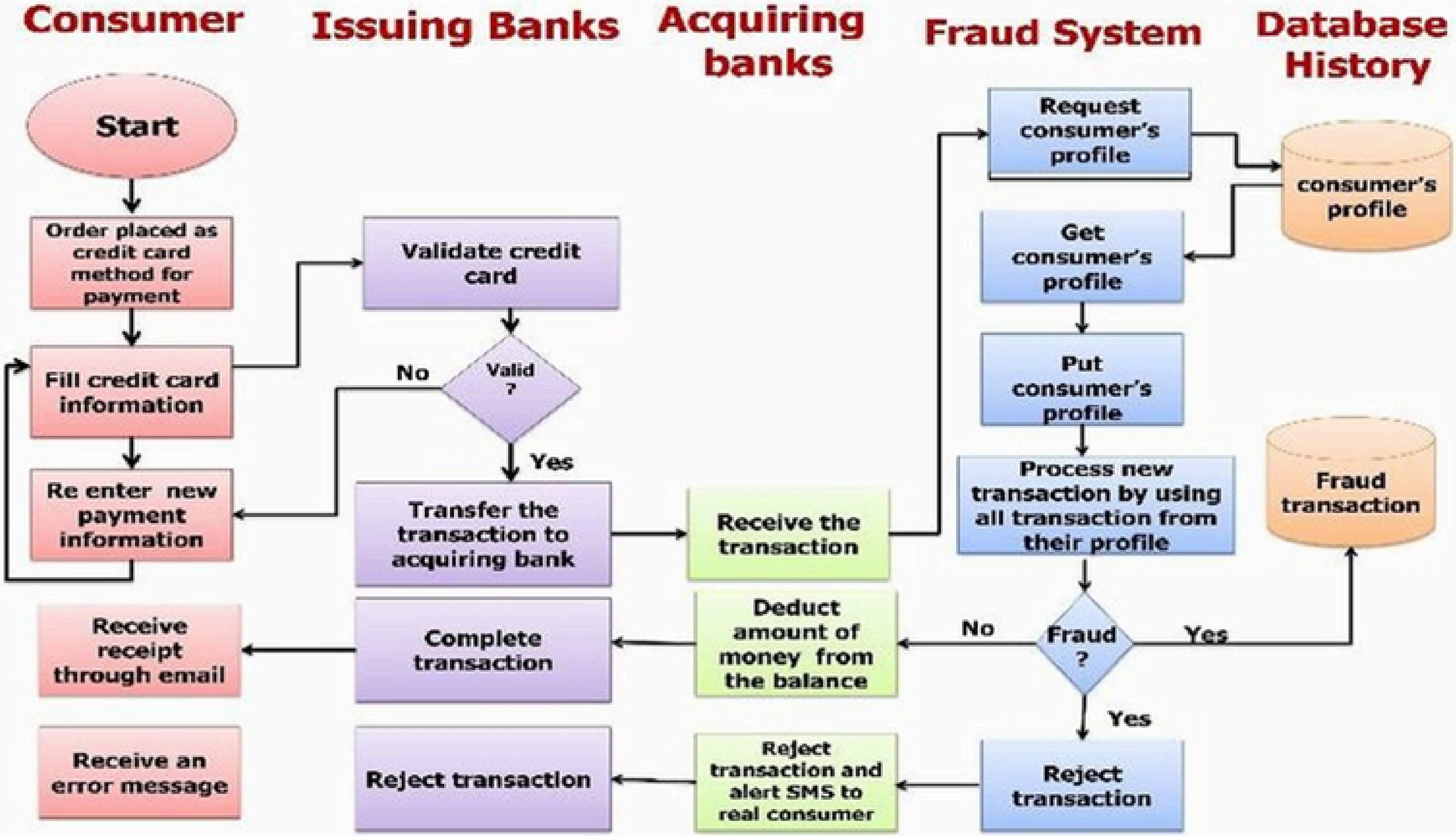
Attacker's Activity in Banking System




Realized ROI
Securing digital identity - banking
Reducing payments fraud
Automating existing processes
Anti-money laundering
Reducing false positives
Auto-saving and recommendations
Aiding CSRs (back end)
Pre-empting problems
Aiding CSRs (front end)
Improving interactions across channels
Conversational payments
Bank Support
Banking front-end
Banking back-end
Payments

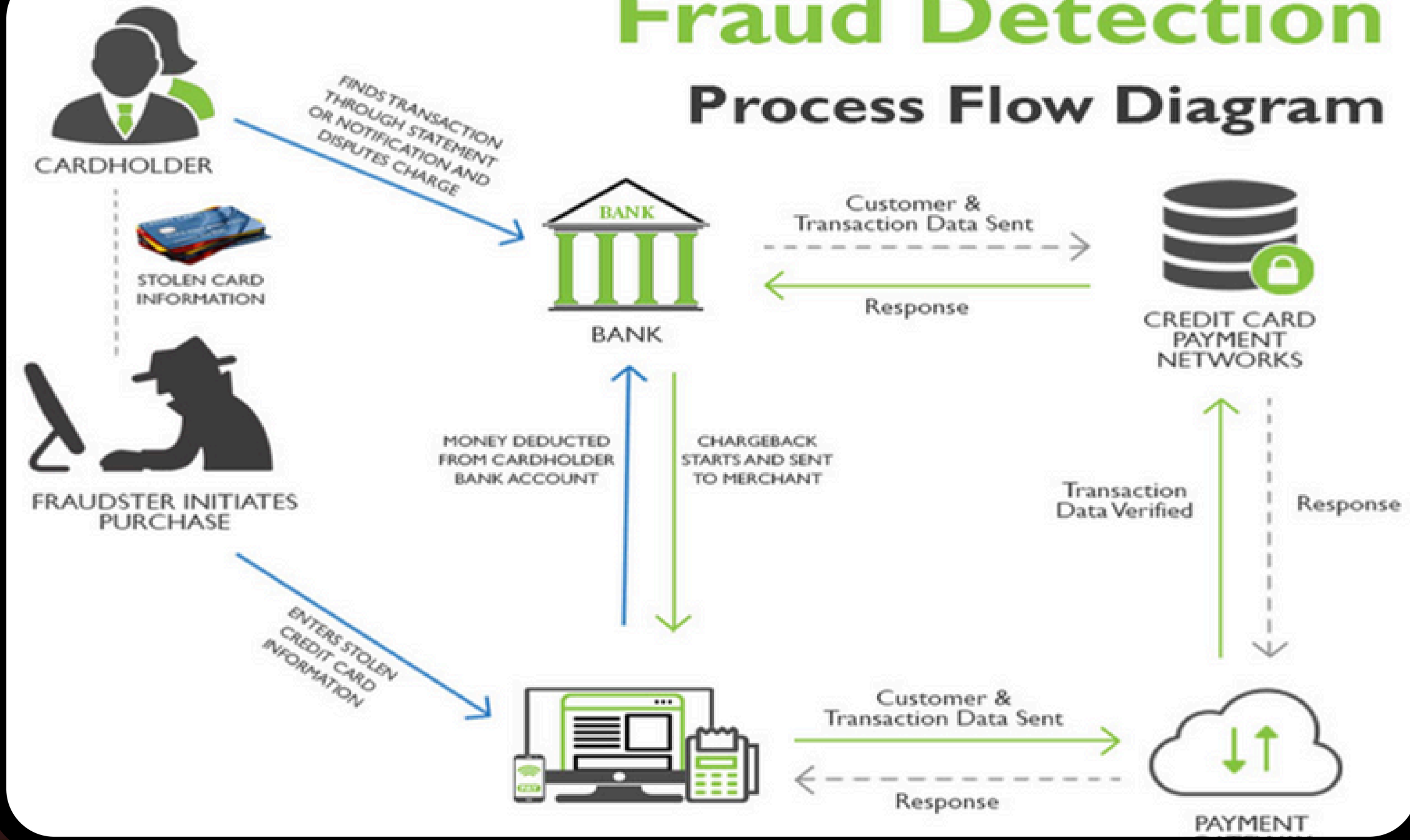

Complete
Process
Of
Fraud
Detection

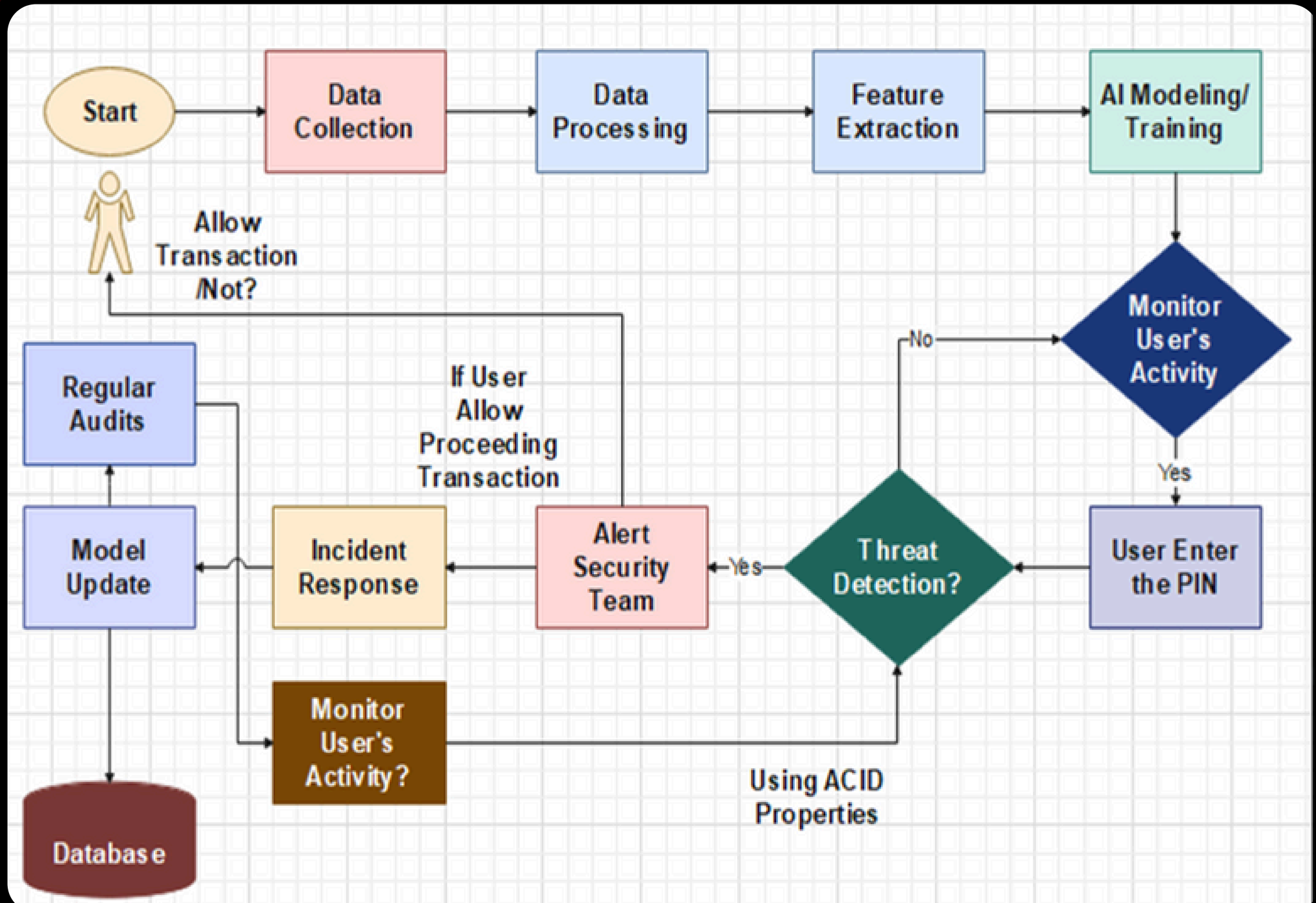
FRAUD DETECTION SYSTEM



Fraud Detection

Process Flow Diagram




Start
Data Collection
Data Processing
Feature Extraction
AI Modeling/ Training
Allow Transaction /Not?
Monitor User's Activity
No
Yes
Regular Audits
If User Allow Proceeding Transaction
Model Update
Incident Response
Alert Security Team
Yes
Threat Detection?
User Enter the PIN
Monitor User's Activity?
Using ACID Properties
Database

Various Application of Threats In Banking System Prevention Model by using AI Enviornment

- Using ACID-Properties.
- Credit – Card Fraud Detection.
- Health Care Fraud Detection.
- Insurance Fraud Detection.
- Blockchain Technology Fraud.
- Gaming & Gambling Fraud Detection.


Algorithm
Used to
Train AI
Model

Algorithm Used In Fraud Detection In Banking System

Input: Transaction details D, Historical data H, Threshold θ

```
1. T ← Initiate transaction by user U
2. D ← Collect transaction details
3. R ← ML_Model(D, H)
4. α ← Anomaly_Detection(D, H)
5. F ← R * α
6. if F ≥ θ then
       Flag transaction for verification
       if Verification(T) then
           Approve transaction
       else
           Reject transaction
   else
       Approve transaction
```

Result

- ·Detailed analysis of the effectiveness of the AI model in detecting and preventing cyber threats.
- ·Case studies or simulations illustrating real-world scenarios and outcomes.
- ·Quantitative metrics (e.g., detection rates, false positives) demonstrating the model's performance compared to traditional methods.

Conclusions

The banking sector is at the forefront of the cybersecurity battle, facing a wide array of threats that require comprehensive and dynamic defence strategies.

Emerging technologies such as blockchain, AI, and ML offer promising solutions to enhance security.

However, continuous innovation, stringent regulatory compliance, and best practices are crucial for safeguarding the financial ecosystem.

Refrences

- ·Iliams, T. (2024). Fortifying Chatbot Technologies. Retrieved from ResearchGate

- ·ThankGod, J. (2024). Cybersecurity in the Age of E-Commerce. Retrieved from SSRN

- ·Paramesha, M., Rane, N., & Rane, J. (2024). Artificial Intelligence, Machine Learning, Deep Learning, and Blockchain in Financial and Banking Services. Retrieved from SSRN,

- · Ali, G., Mijwil, M.M., Buruga, B.A., & Abotaleb, M. (2024). A Comprehensive Review on Cybersecurity Issues and Their Mitigation Measures in FinTech. Retrieved from MUNI

References

1. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and ap-plications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.
2. Martínez-de Dios, J. R., Gámez, J. A. C., & Salido, M. A. M. (2018). A survey of models and algorithms for improving the coordination of rescue units. Journal of Intelligent & Robotic Systems, 91(1-2), 1-22.
3. Ozdemir, S., & Koksal, C. E. (2015). Rapid deployment of a rescue robot in emer-gency situations: A survey. Robotics and Autonomous Systems, 63, 146-157.
4. Cheikhrouhou, O., Hamdi, A., & Ben Hamida, A. (2020). Cloud-based disaster management system utilizing 3D visualization and real-time feedback for en-hanced rescue planning. International Journal of Disaster Risk Reduction, 50, 101756.

References

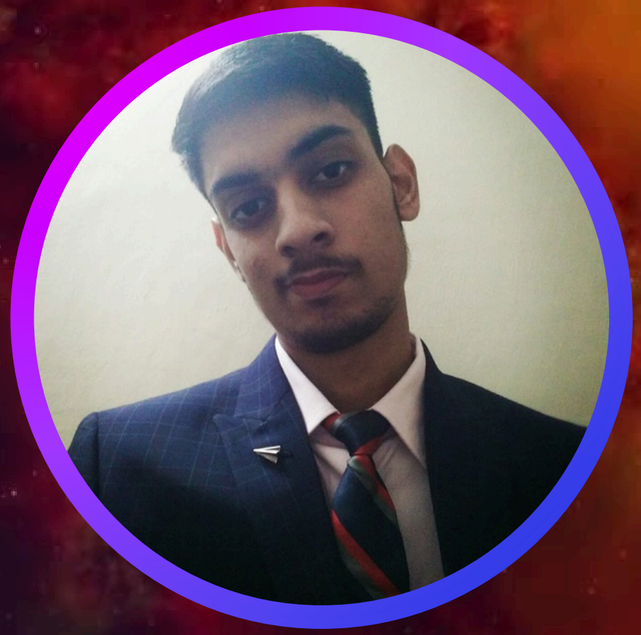
5 Botta, A., De Pellegrini, F., & Pescapé, A. (2021). DewROS: A cloud robotics plat-form for real-time video processing with low network latency. Journal of Cloud Computing, 10(1), 1-16.

6 Liu, Y., Zhang, Q., & Wang, Y. (2022). Cloud-centric IoT-based health manage-ment framework. IEEE Internet of Things Journal, 10(1), 1-10.

7 Botta, A., De Pellegrini, F., & Pescapé, A. (2021). DewROS: A cloud robotics plat-form for real-time video processing with low network latency. Journal of Cloud Computing, 10(1), 1-16.

8 Talavera, R., Rodriguez-Ruiz, J., & Garcia-Cerezo, A. (2023). Autonomous ground robot for indoor emergency interventions. Journal of Intelligent & Robotic Sys-tems, 98(3), 711-726.


ANY
QUESTIONS??



Dhruv Dhayal

CyberSecurity Management

Computer Science & IT, Researcher

+91-8529994515

dhayaldhruv271@gmail.com