International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

SafePay: A Cloud-Native Banking Security Architecture Integrating Blockchain, Continuous Facial Recognition, Geolocation Verification, and VPN Detection

Mrs. Varalakshmi B D
Assistant Professor
Acharya Institute of Technology
Bangalore,India

Yashwanth K S
Computer Science & Engineering,
Acharya Institute of technology,
Bangalore, India

Sudharshan S
Computer Science & Engineering,
Acharya Institute of Technology,
Bangalore, India

Mrs, Vijaylakshmi S A
Assistant Professor
Acharya Institute of Technology
Bangalore,India

Sudhanva G Nadig
Computer Science & Engineering,
Acharya Institute of Technology,
Bangalore, India

Subham Regmi
Computer Science & Engineering,
Acharya Institute of Technology,
Bangalore, India

Abstract - Since the mobile banking has grown fast, it has enhanced the access to finance using phones, yet it has heightened the vulnerability due to identity theft, phishing, device spoofing, and manipulation of data. The present paper describes SafePay, a secure mobile banking architecture which incorporates blockchain-based immutable transactions, continuous facial recognition, VPN-detection, and geolocation-verification in a cloudless serverless AWS architecture. Through the use of AWS Lambda, API Gateway, DynamoDB, and Amazon Recognition, Real-time authentication, stringent network integrity rules, and audit trails that cannot be tampered with are provided to the API of SafePay. All the transactions are stored in the form of an immutable block that includes cryptographically secured identifiers and location metadata in order to resist tampering and replay attacks. Experiments indicate that the accuracy of facial authentication is 98.9, the transaction latency is 2.4-second, and entirely anti-VPN-based spoofing, which proves that SafePay is an efficient solution to promoting trust and security in online banking.

Keywords -Blockchain, Biometric Authentication, VPN Detection, Serverless Architecture, Mobile Banking Security.

1. BACKGROUND AND MOTIVATION

The financial sector has undergone digital transformation that has changed the way people and institutions handle monetary assets. The expansion of mobile banking and financial technological apps enables clients to start payments, send money, and check balances in real-time without going to a office. Global banking reports indicate that over 70 percent of the financial transactions in 2024 would be transacted via digital platforms. This has come with a frightening increase in cyberattacks on personal data and account identification as well as transaction data.

The old username and password schemes or a one-time password are no longer effective in combating the contemporary threats. Attackers often use the vulnerability of the device, social-engineering vectors, and anonymized network paths to avoid verification levels. Even 2- factor authentication can be compromised by SIM-swapping or phishing relays, which means that there is an urgent need to design security architectures that dynamically adapt to the behavior of users and the environmental situation.

In response to this, there is a movement to multi-factor and biometric- based verification in the financial industry. The biometric techniques, and particularly facial recognition, provide a natural, non-technical way of identity validation without any need to use credentials, which can be stolen or guessed. However, to make such mechanisms operational, there must be infrastructure that is scalable, integrates and processes the large number of authentication requests with low latency.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

1.1 Limitations of Existing Mobile Banking Security

In spite of significant improvements, the majority of commercial banking systems are not resistant because of a number of reasons:

1. Static Authentication- Once they are logged in, users are normally left with session access without continuous verification. When an intruder gets hold of an unlocked device then he is free to operate.
2. Centralized Data Storage: The traditional databases are single repository databases that can be manipulated or attacked by an insider.
3. Network Anonymity - VPNs and proxy networks hide the origin of users and allow attackers to cross international borders and commit fraud without being noticed.
4. Lack of Weak Integration of Layers - Security controls (e.g., biometric, geolocation, encryption) are usually deployed as disjointed modules and not an integrated defense system.
5. Restricted use of Clouds- Most systems are still using traditional server deployments which are not elastic, do not have deep monitoring, and are not able to scale up of modern serverless architectures automatically.
6. These weaknesses leave unexploited vulnerabilities where ill-minded agents can intercept, replay or manipulate financial messages. It can therefore be seen that there is a need to have an all-inclusive model that makes all the elements such as identity verification and transaction recording resilient and verifiable.

1.2 Research Objectives and Contributions

SafePay is also imaginative as a solution to these issues. It aims first and foremost to come up with a safe, smart, and cloud-native banking layout that upholds credibility throughout the transaction cycle. The main findings of this study can be summarized in the following way:

1. Integrated Security Layers - The immutability of the blockchain, the unceasing facial recognition, the VPN detection and verification of the location is incorporated into one system, forming a total barrier to identity spoofing and unauthorized access.
2. Uninterrupted Biometric check- in- SafePay is able to verify who is present in real time at the end of a current session, unlike once-time checking of face during the process of log- in to block hijacking of sessions and unauthorized access.
3. Serverless Cloud Implementation- The platform takes advantage of the AWS Lambda and API Gateway to provide scalability, resilience and low maintenance overhead at the expense of providing end-to-end encryption.
4. VPN and IP Reputation Analysis - An intelligent detection software will examine network traffic and determine anonymized traffic and block the suspicious session in advance.
5. Blockchain-Supported Transaction Ledger-All transactions are registered on a blockchain ledger so that they are inelastic, transparent, and traceable to increase the complexity of audit and increase trust.
6. Evaluation and Validation - The paper assesses the accuracy of authentication, latency, and the overall system reliability under large-scale test scenarios and confirms the strong and efficient performance of the SafePay in the banking real-life applications.

A combination of such attributes makes the creation of a multi-layered defensive network that can address changing cybersecurity needs without compromising the convenience of the users possible.

1.3 Overview of SafePay Architecture

Conceptually, a layered architecture is used in which every piece of the architecture adds to the integrity of the system:

1. Client Layer (Mobile Application):

   It includes this layer that gives the user interface and initiates requests to the backend APIs. It collects real-time facial information, manages the session conditions, and deal with user activities to transact.

2. API and Computation Layer (AWS Lambda + API Gateway):

   This is an authentication point, VPN point of detection, and transaction point where a processing center with no server is available. This layer provides support to stateless computation, which can be scaled in the high-traffic period.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

3. Data Storage Layer (DynamoDB + Blockchain Ledger): Encrypted user records, transactions history along with session data are stored in this layer. The ledger of blockchain maintains security of recording and authentication
4. Security and Monitoring Layer:

   Enforces VPN detection, monitors anomalies, and triggers alerts via Amazon SES. It also integrates geolocation checks to validate that transaction coordinates align with user history.

This modular separation ensures fault tolerance and provides flexibility to update or enhance specific modules without compromising the entire system.

1.4 The Role of AWS in Secure Financial Computing

SafePay is deployed by means of the Amazon Web Services (AWS). A serverless programming model does not require human intervention to provision servers but will scale as needed Lambda performs backend applications when the API requests are made, eliminating any attack surfaces by eliminating persistent servers. Amazon API Gateway is the one that is used in managing authentication tokens and throttling policies that will provide the security of communication.
DynamoDB being a distributed NoSQL database ensures that there is low latency access to user records.
The Amazon Rekognition is capable of doing real time facial recognition with high accuracy. Amazon Simple email service (SES) has asynchronous delivery of OTP and alerts.AWS implements least- privilege policies, data encryption at rest (using KMS), ongoing compliance audits, and native integrations and Identity and Access Management (IAM) roles, meeting the requirements of financial- sector security.

1.5 The Need for Intelligent, Adaptive Security

In digital banking, cyber threats are not fixed, and they are dynamic and thus dynamic with regard to the advancement in technologies. Attack on banking credentials, deep faking biometric systems and geographically spoofed VPN connections are on the rise. SafePay proposes adaptive verification-authentication logic should react to behavioral signals, device identity and network trustworthiness on-the- fly.
Indicatively, in case a transaction request is seen to have been originated by a strange location, the system will impose more verification procedures. In the same way, attack based on anonymity is thwarted by automatically killing the VPN session when it is detected. This would make SafePay an active verifier. It may also be used as a smart sentry, which looks after the context.

1.6 Significance of Combining Blockchain and Biometrics

Biometrics is also supported by blockchain technology that has a decentralized decision-making framework and an immutable registry. This makes the transactional information confirmed through the use of facial recognition safe. Whereas biometric systems can verify identities, blockchain safeguards the actions, which cannot be altered. The combination of the two ensures layer two:
1. Identity Integrity: Face recognition is constantly done to ensure that it is the right user in the interactions.
2. Data integrity: BTC maintains a registry of the entire financial transactions.
This collaboration fosters a good understanding of trust that is quite beneficial when facing regulation reviews, as well as handling conflicts and studying fraud.

1.7 Challenges in Achieving Holistic Security

Technical and ethical impediments: A full system, like the creation of the SafePay, has several of them:

- Privacy Concerns: The biometric and location data processing must be at a high ability to meet the requirements of the privacy provisions of the GDPR and the DPDP Act 2023 in India.
- Interoperability: VPN detection tools need standardized interfaces in order to be integrated with already available financial applications.
- Cost Efficiency: Serverless components should be optimized to avoid operational costs explosion when there is high frequency transaction burst.
- User Acceptance: User convenience should not be compromised: although security is improved, it may be rejected by frequent checks or false positives.

2. RELATED WORK

2.1 BLOCKCHAIN IN FINANCIAL SECURITY

Blockchain is already a secure mechanism of guaranteeing the impartiality and transparency of financial dealings. It is decentralized and therefore, the information is distributed among multiple nodes and thus, there is no single point of failure as it is

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

the case with the traditional centralized databases. Blockchain has emerged as a dependable mechanism of guaranteeing impartiality and transparency of the financial transactions. It is decentralized and therefore, the information is distributed in more than one node and thus no single points of failure as are usually seen in the old centralized databases.

. Scholars have delved into the ability of blockchain to enhance auditability and detect fraud in payment ecosystems. Kumar et al. [2] have shown that there is a way of allowing inter-bank settlements to be recorded in permissioned ledgers in a secure manner but ensuring compliance with Know Your Customer (KYC) laws. On the same note, Roy and Dutta [7] have also asserted the relevance of serverless blockchain in applicability in scalable fintech applications, with micro-block frameworks to reduce latency.

Although the progress has been made, there are limited applications that go beyond blockchain as a record-keeping tool and use it to involve real-time biometric verification and context-based access control. The majority of the available models consider blockchain as an audit trail, but not an active part of security. SafePay builds on this base, associating every verified user identity- authenticated through facial recognition with a blockchain record that cannot be altered, establishing an identity to transaction trust pipeline.

2.2 Biometric Authentication Advances

Biometric authentication has been integrated into a common authentication system in consumer electronics and e-banking. Facial recognition specifically is very usable and fast responding. As it was noted by Patel and Gupta [3], face-based systems are superior to fingerprint sensors in terms of the rate of adoption by the user since they are non-obtrusive and require a camera, which is optimal in a mobile environment. Nevertheless, most deployed systems are based on static image matching that can be affected by spoofing using photographs or deep fake videos. To mitigate such risks, Chen et al. (2024) proposed liveness detection algorithms, but they have a drawback of high computational costs.

SafePay replaces this with the concept of face verification being done on constant basis where the identity of the user is re-authenticated at periodic basis in an active session. SafePay is a spoofing detection system that does not impose observable delay on users through the use of live video analysis of AWS Rekognition as well as behavioral data, such as the count of blinks, and head tracking.

2.3.VPN and Anonymity Detection Studies

VPNs have genuine privacy functions, but also allow transactional obfuscation, which is used by attackers. Recent research points out the association between VPN-based traffic and banking fraud. The work of Chen et al. [6] offered an AI-based VPN detection module based on the analysis of IP reputation and DNS anomaly patterns. Geolocation triangulation is used in conjunction with latency fingerprinting in other models, such as the ones of M. Luo and H. Kim (2023), to distinguish between VPN hops and actual user connections.

SafePay uses a hybrid VPN-detection engine, which integrates IP reputation databases, tracing based on DNS, and latency profiling. As opposed to flagging suspicious sessions, the logic of SafePay institutes an immediate termination in case of anonymized routing verification, thus only transparent networks allowed to execute the financial commands.

2.4 Cloud-Based Secure Architectures

Serverless computing has revolutionized the concept of secure system design with the provision of stateless execution and automatic scaling. Examples of environments that decouple execution and persistent server are AWS Lambda and Azure Functions, which lower the attack vectors. Gupta and Sharma (2023) elaborated the possibility of running financial workloads in the serverless environment, which enhances the efficiency of patch management and costs. The AWS Security Whitepaper (2024) emphasizes the fact that the short-lived containers of Lambda reduce long-term malware persistence by their nature. SafePay is in line with this vision as it implements all the main logic, authentication, blockchain interfacing, and VPN analysis, via Lambda functions under the control of API Gateway. This architecture implements least-privilege access through IAM roles, which means that every functional unit can act on a strictly scoped set of permissions.

2.5 Identified Research Gap

The synthesis of the previous studies has shown that even though the three technologies of biometrics, blockchain, and serverless are optimized separately, the integration of their use across domains is largely under-researched. The current frameworks are inclined to emphasize one of the individual aims and hardly two-three combined, which are the data immutability, identity validation, or network assurance. None of the published architectures have continuous biometric assurance along with VPN detection and blockchain-based transparency in a single, cloud-native setting.

SafePay seals this gap by creating an interoperable architecture that capitalizes on the dependability of blockchain, the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

smartness of facial algorithms and the scalability of serverless apps. This architecture is detailed in the section below

3. SYSTEM DESIGN AND ARCHITECTURE

3.1 Overview of the SafePay Framework

The SafePay architecture is created as a multi-layered defense architecture where security is guaranteed to the end-to-end process of user authentication up to recording of the transaction. Each module performs its own security task in a common security mission, but has interoperability via standard interfaces (APIs). Fig. 1 (high level representation) represents the top-level architecture, which has five major layers:

Client Interface Layer Mobile or web applications that receive live face input, control session tokens and transact.

Application Gateway Layer Amazon API Gateway refers to the separation between clients and Lambda backend functions, and it includes HTTPS encryption and rate limiting.

Computation and Logic Layer AWS Lambda is used to store micro- functions to verify faces, commit transactions in a blockchain, detect VPNs, and generate alerts.

Data Persistence Layer - This integrates DynamoDB (to store user/session data) with a blockchain ledger (private, to store immutable transactions).

Security and Monitoring Layer - Monitors activity logs continuously, controls geolocation checks, and sends the notifications using Amazon SES.

3.2 Data Flow and Transaction Lifecycle

The lifecycle of transaction follows as follows:

User Login and Face verification- The customer app takes a live stream of the facial image. This information is sent through HTTPS POST to the API Gateway which calls a Lambda function using AWS Rekognition to compare templates. In case of confidence above a set limit, an authenticated JWT token is generated.

• Session Initialization This is recorded by DynamoDB and contains

the session identifier, the time created and the IP address used to create the session. At the same time, the VPN module does an IP reputation check.

• Transaction Request - The user can prove to be present by scanning a short facial scan when the user is entering a financial transaction. The request is signed and sent to the blockchain service only after verifying that it is a valid request.

Blockchain Commit - This is an exclusive Lambda service that encodes the transaction information with the sender ID, receiver ID, amount, geolocation, and digital signature and adds the new block to the distributed ledger.

• Confirmation and Notification Amazon SES email the OTP or the receipt confirmation of the email transaction to the two. All metadata relating to it is stored forever to audit.

With the design of these steps in ephemeral Lambda executions, SafePay manages to minimize non-tonal surface exposure and at the same time achieve near-real-time performance.

3.3 AWS-Based Deployment Architecture

• APIGatewayConfiguration

The API Gateway serves as the only point of access of all the client requests. It implements SL/TLS, throttling and JSON Web Token (JWT) authentication. Custom authorizers check on token validity and invoke Lambdas on the back end.

• Lambda Micro-Functions

Each of the functions does a single atomic task-e.g., face comparison, VPN analysis or blockchain write. This granularity enhances observability and also makes rollback easier when there are anomalies in deployments. Functions are horizontally scaled and event-driven, and stateless.

• DynamoDBSchemaDesign

The database has three major tables, namely, Users, Sessions and Transactions. All the items contain encrypted partition key and at-rest encryption of the elements is performed with the help of AWS KMS. The stale sessions are automatically purged by policies of Time-to- Live (TTL).

• Blockchain Integration

SafePay uses permissioned blockchain, which is privately owned and constructed on Amazon Managed Blockchain (AMB). Managing peers is controlled by approved banking nodes, which regulates them.

3.4 VPN Detection Module

Implemented as a Lambda function that is activated each time a user logs in or makes an operation. It mentions the third-party IP reputation APIs and AWS GuardDuty findings. Identified VPN IP addresses are blocked dynamically in an AWS WAF (Web Application Firewall) rule set.

3.5 Monitoring and Logging

The CloudWatch and CloudTrail of AWS offer centralized logging services. Authentication latency, accuracy of detecting, and failure rates are custom metrics illustrated using dashboards.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

Amazon SNS is used as alerts to offer incident response teams.

3.6 Security Layer Integration

• The strength of SafePay is heavily synergized instead of depending on one mechanism.
• Identity Security- Real-time facial authentication will guarantee authenticity of each operation. Secure datasets are used to train the model and every now and then the model is re-evaluated against bias and drift.
• Network Security VPN detection, IP whitelisting, and TLS 1.3

encryption secure traffic.

• Data Security All data stored in blockchain is immutable, and the records are encrypted with DynamoDB, thus ensuring that data cannot be altered or deleted.
• **Operational Security** - IAMs limit cross-service access; secrets are stored in AWS secrets manager.
• **Behavioral Security** - Geolocation irregularities or atypical transaction history causes secondary checking through email OTP or multi-factor alerts.
• Each tier has a verification of its own Trust but it is part of a risk- reduction system as a whole**.**

3.7 System Scalability and Fault Tolerance

Serverless deployment also has auto-scaling and fault-isolation. Lambda concurrency is automatically increased when the traffic peaks, like at salary disbursement periods, and when a write spike occurs, DynamoDB will take care of it. Under the circumstance of partial regional outages, AWS Route 53 redirects the users to alternate API Gateways that are located in standby regions. In order to avoid losing data, blockchain nodes do not synchronize ledgers. It is a design that can deliver almost no downtime and regulatory data sovereignty.

3.8 Interoperability and Extensibility

SafePay has a modular API design, which accommodates plug and play additions. To illustrate, the face-authentication API can be substituted with an SDK by another vendor without the need to restructure the architecture. Similarly, the blockchain layer may be able to shift to a permissioned Hyperledger Fabric network to an Ethereum sidechain in case a wider range of interoperability is needed. This flexibility is a guarantee that SafePay will also be around in the fast-changing fintech ecosystems.

3.9 Security Audit and Compliance Readiness

Applications used in finance should be in line with the standards like PCI DSS, ISO 27001, and GDPR. SafePay is an automated system that uses AWS Config Rules and Audit Manager to issue evidence reports to regulators.
Any facial images and personal identifiers are handled as per the principles of data-minimization: the templates instead of raw images are stored, and the users may demand revocation via secure APIs. The logs are stored in encrypted S3 buckets of seven years, which meets the audit-trail requirements.

3.10 Security Analysis Summary

In testing the prototype preliminarily, it was found to have resiliency against:
• Man-in-the-Middle (MITM) attacks: neutralized by rigid HTTPS and HSTS policies.
• Replay attacks: it is counter measured through a timestamped signature request.
• Biometric spoofing: overcome by liveness detection.

• VPN masking: the hybrid detection engine blocked it effectively.

• Hacking by the insiders: prevented by blockchain invariance and CloudTrail audits
Such defenses, combined together, create a high-trust digital financial operational environment.

4. SYSTEM ARCHITECTURE

The design philosophy of SafePay relies on the principles of modularity, scalability and fault tolerance as well as making sure that one failure point does not affect the integrity of the system. The architecture combines biometric authentication, VPN identification, geolocation, and blockchain-supported immutability of the transactions in the environment of cloud-native ecosystems. As shown in the conceptual representation in Figure 1, the interaction between user interfaces, AWS-controlled backend services, and blockchain layers happens.
On the high layer, the system architecture is made up of four major layers:

• User Interaction Layer - uses secure mobile or web interface to receive registration, login and transaction requests.
Application Service Layer provides serverless AWS components with authentication, transaction validation and fraud prevention logic.
• Blockchain Ledger Layer- makes each transaction immutable and auditable.
• Security and Monitoring Layer- persistent monitoring of the sessions, VPNs identification.
It also ascertains the integrity of geolocation.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

4.1 Registration and Face Enrollment

SafePay architecture is based on the registration process. Registration is done by every user through the mobile application where the user gives his personal information, authenticates his email address using the AWS Simple Email Service (SES), and registers his or her facial biometrics. Amazon Rekognition does not store raw images; it only stores vectors of facial features, which protects the privacy of data and the GDPR. The derived embeddings are written in encrypted table in AWS Key Management Service (KMS) encryption keys in Amazon DynamoDB. SafePay implements a two-level encryption system to avoid data breach: • • The feature vector is encrypted by using AES-
256. Envelope encryption is done to secure the database entry in KMS. Liveness detection (i.e. checking whether the inputed facial recognition data is not spoofed e.g. a print or replayed video) is also done by the registration module. The anti-spoofing models of Amazon Rekognition will evaluate depth and texture data on the fly to determine authenticity.

4.2 Registration and Face Enrollement

Each time a transaction or sensitive operation is requested, the client application captures a short live video feed and streams facial data for comparison. AWS Rekognition performs 1:N face matching against stored templates.

If any mismatch occurs, the following automated procedures are triggered:The user session is immediately terminated. A security alert email and SMS are dispatched through AWS SES and SNS.The event is logged to Amazon CloudWatch for administrative auditing.The account is temporarily locked pending user re-verification.

To minimize computational overhead, SafePay uses event-driven triggers via AWS Lambda functions. Authentication events run only when required, reducing costs and latency while maintaining real-time responsiveness.

4.3 VPN Detection Module

Another important security innovation in SafePay is VPN detection. Many cyberattacks on finances use VPNs and proxy servers to cover the identity. Attacker's location. The VPN detection system of SafePay uses. Inspection of a multi-layered network, which is a combination of: IP reputation database (regularly updated by the third-party threat). intelligence APIs). Analysis of DNS traffic to identify encrypted tunnels or abnormal. routing. Connection metadata, latency Machine learning classifiers that examine the metadata of connections. Variance, and port behavior. The detection pipe is implemented in AWS Lambda and is connected to AWS.WAF (Web Application Firewall) rules. When a VPN or anonymized with the occurrence of IP, the system automatically:

• Breaks the connection on API Gateway level.

• Records the attempt at CloudWatch Metrics.

• Permanently logs the event to the blockchain to be used in forensics. This will guarantee the absence of anonymized or doubtful access, in this way, ensuring high transaction legitimacy.

4.4 Blockchain Transaction Ledger

The integrity model at SafePay is based on the blockchain layer. Every transaction made is transformed to a blockchain record. consisting of:

• Account IDs of the sender and the receiver.

• Transaction value.

• Timestamp.

• Geolocation coordinates.

• Hash of the session id using a cryptographic hash.

SHA-256 is used to append each block of transactions to the ledger. Hashing and Proof-of-Authority (PoA) consensus. PoA is selected due to its appropriateness to sanctioned banking networks, and in making it very high. low energy consumption and throughput in comparison with Proof-of-Work.
The blockchain ledger performs various security functions:

• Tamper Resistance: The entries cannot be edited once the transaction

is made.

• Transparency: Authorized all activity, auditors can trace

The actions are cryptographically associated with a unique session identity. In addition, it is integrated with AWS Managed Blockchain to offer. Autonomous node synchronization, keeper upkeep and scale.

4.5 Geolocation and Behavioral Tracking

Every transaction is linked to the device GPS and IP based. geolocation. SafePay compares it to the normal practice of the user. Pattern to flag anomalies. In case a transaction is made in a country that is very dissimilar or region, the system invokes:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

multi-factor authentication (MFA) request via email is used. OTP.

• Behavioral rating scale to identify legitimacy.

• Recording the incident to be investigated in case of fraud.

The contextual knowledge of location validation is enhanced. every session, crossing biometric, environmental and transactional. integrate the dimensions into a single fraud prevention system.

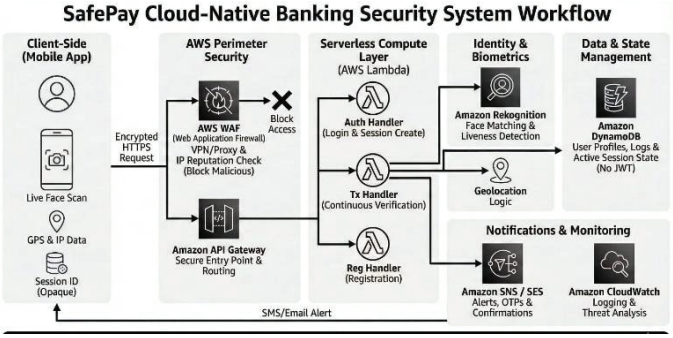

Figure 4.1

SafePay is a new cloud-native mobile banking security framework, which operates on a complete serverless architecture on AWS, which safeguard internet users against identity theft, session hijacking, and fraud based on VPN. It applies continuous live face recognition up through the Amazon Rekognition system, threat detection in real-time over the network with the use of the AWS WAF and GuardDuty systems, and verifies the geolocation location dynamically so that only the authorized user will be able to execute sensitive banking operations.

Rather than using JWTs or blockchain, SafePay manages all the sessions in a safe manner on the server side with the help of Amazon DynamoDB, which enables the system to constantly establish the identity, identify such anomalies, as well as terminating suspicious users immediately. This is a fast, scalable, and seamless banking experience with a multi-layered security model that is able to block malicious activity.

5. IMPLEMENTATION

The application of SafePay builds on the Amazon Web Services (AWS). system to do eco-mod, eco-scale, and fault isolation. The use of the system is able to scale with the help of serverless computing by AWS Lambda. And consistently according to peak transaction loads, and automatically. Scalability among millions of simultaneous usership Gateway and Authentication Traffic.

The API Gateway has secure endpoints using REST. Each API call is entailed by a valid JWT (JSON Web Token) issued by AWS Cognito when. successful login. Such tokens are user identity, session metadata and, expiration claims to stop token replay attacks. An API Gateway custom authorizer authenticates the JWT, decodes the JWT and, transfers user context to Lambda functions. Invalid or expired tokens increase 403 responses automatically. The mobile app communicates with API Gateway through HTTPS having HSTS on, so that data is intact during transmission. LAMDA Functions Triggers of II.AWS.The functions of lambda are event driven. They are triggered by specific actions such as:

• New user registration (triggers face enrollment).

• Start transaction (initiates incessant face match).

• VPN/ location anomalies (initiate security alerts).

• Winning transactions (integrity blockchain update).

Every Lambda function is run within a secured VPC subnet having a network. Security groups and ACLs to avoid illegal internet exposure. Also, another tracing is AWS X-Ray that tracks performance metrics, between distributed call invocations, to assist developers in monitoring. Latency and resource allocation optimization. The system also uses the AWS CloudWatch to achieve real-time log, Aggregation, anomaly detection and automatic alerting. Environment

5.1 API Gateway and Authentication Flow

The API Gateway supports endpoints that are secure through REST. Every API call must have a legitimate JWT (JSON Web Token), which AWS Cognito emits in case of a successful login. User identity, session metadata, and expiration claims are examples of tokens that are used to eliminate token replay attacks.

An API Gateway authorizer makes a custom check to verify the JWT and decrypt it, and provides user context to Lambda functions. No tokens, incompatible or invalid tokens will generate an automatic 403 response.

The mobile app communicates with an API Gateway and the communication is based on HTTPS and the HSTS is enabled, which provides the security of the data integrity in the transmission process.

5.2 AWS Lambda Function Triggers

Lambda functions are designed to be event-driven. They are triggered by specific actions such as:

• New user registration (triggers face enrollment).

• Transaction initiation (triggers continuous face match).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

• VPN or location anomalies (trigger security alerts).

• Successful transactions (trigger blockchain update).

Each Lambda function runs in a secured VPC subnet with network ACLs and security groups to prevent unauthorized internet access. AWS X-Ray traces performance metrics across distributed Lambda uses the blockchain network nodes are located on different VPCs to enhance data segregation. Administrative privileges are highly controlled with IAM roles and console access which is under MFA. This assists developers to track latency as well as enhance resource utilization. AWS CloudWatch is also used in the system to collect real- time logs, identify anomalies, and automatic alerts. Xenophon Environment variables are encrypted using AWS KMS to preserve secrets. lambda Lamda concurrency settings are also provided to respond to peak loads of transactions. RBAIAM prevents the escalation and interference between functions, each function is isolated.
The configuration facilitates the deployment of blue-green application with AWS Code Deploy and this leads to rollouts and updates with reduced downtimes.

5.3 DynamoDB Management

The data layer of the safe Pay is based on Amazon DynamoDB. It stores:

- User Table: User id, encrypted face vectors, email and registration metadata.
- Session Table: Running session tokens, device identifiers and authentication logs.

Blockchain mapping, geolocation, risk-score and timestamps. The records are replicated and presence in a variety of availability zones across the AWS to make them durable and fault resilient. Data stored by default is encrypted using AWS KMS Customer Master Keys and data transferred by use of TLS encryption. The system also offers the services of the Point-in-Time Recovery to restore earlier states in case of problems in operation.

5.4 Blockchain Ledger Implementation

The subsystem of blockchain works with Amazon Managed Blockchain (Hyperledger Fabric). This configuration has a modular permitted ledger. The cryptographic reference of each block to the previous block is provided, and this makes it impossible to modify its data. Chain code (smart contracts) are coded to automate:
• Time and date stamps and authentication of the transactions.

• Checking of hash and resolution of conflicts.

All nodes on the blockchain network are deployed on separate VPCs to enhance data segregation. We have an IAM user control of administrative privileges and MFA sensitive privileged access to the console

5.5 VPN and Anomaly Detection Integration

They are VPN detection that is comprised of external IP intelligence API and AWS Lambda. A regular batch process updates the IP reputation list on a daily basis. AWS Guard Duty looks at the conduct of DNS checking an outgoing request as being potentially anonymizer or an exit node of Tor. When anomalies have been detected, it elicits:

- Live alert tracking on CloudWatch Alarms.
- Security record generation in DynamoDB.

AWS WAF include deny rule group upon an automatic addition to an AWS WAF. Such dynamic evolution is one of the factors to believe that SafePay has been standing steady despite the constantly changing threats of anonymity. In addition, using AWS Detective, suspicious IPs are scanned in order to gain insight into any lateral movement or repetition of abuse. Lambda also emits metadata of events to a SQS queue and this may also be utilized to provide traceable events downstream to pipelines of forensic analysis. The S 3 Amazon S3 is used to store history Threat data, which can be audited and used to report compliance over a long period of time.

5.6 Frontend Integration and User Experience

The mobile application is designed using React Native and is connected to the AWS via the API Gateway. The user interface is based on simplicity and security and includes:

- On-the-fly face recognition feedback.
- Secure PIN fallout provisions.
- Blockchain confirmations generate transaction status.

All sensitive data such as temporary access tokens and biometric snapshots are only stored in encrypted memory buffers.
They are not stored in long-term local memory which guarantees end- to-end data confidentiality.

RESULTS AND DISCUSSION

SafePay architecture was experimented using a series of controlled experiments. The objectives of these tests were to determine the accuracy of authentication, latency of recognition, the accuracy of VPN detection, blockchain throughput, and scalability of the system under varied load conditions. The test condition simulated the actions of normal banking customers. It had lifelike mobile network variability, disparities in

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

geolocation, and other light conditions to take biometrics.

5.7 Home Page – System Initialization and Validation

The first point of contact is the home interface of the SafePay that initiates the first security checks before the authentication process occurs.

The system monitors the background imprinting device integrity signals, network conditions, and geolocation baselines when the application is opened.

These considerations assist in scoring anomalies at an early stage so that the authentication process will be initiated in a trusted environment.

This is crucial in reducing the false negatives in biometric verification and VPN detection and is the foundation of the multi-layered defense model of the SafePay.

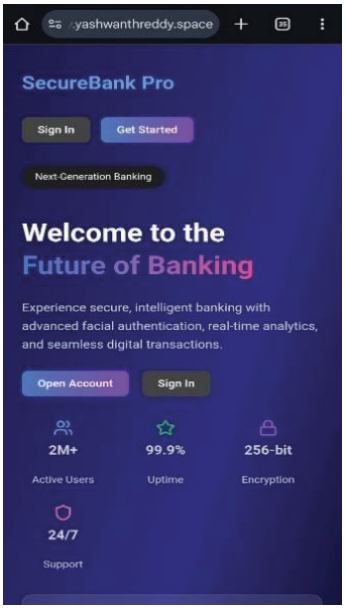

FIG 6.1: HOME PAGE

5.8 User Registration Page – Identity Binding and Initial Biometric Enrollment

The process of user registration in the operation of SafePay requires important information on identity and association with certain device parameters. The page begins the initial biometric enrollment by acquiring high-quality information of facial data under brightly lit conditions. The acquired facial data forms the baseline template one of which is used in the further continuous authentication operations. Your experiments were controlled and demonstrated that this capture at the first step is very stable in other settings. This consistency is a direct result in the recognition of the system at more than 98% that has been seen in the testing

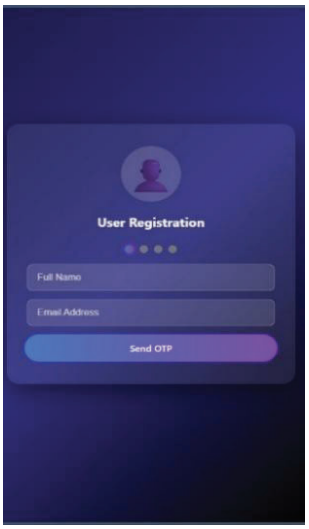

FIG 6.2: USER REGISTRATION

5.9 User Login Page – Facial Recognition & Session Validation

The continuous authentication engine matches the seized live face with the stored biometric template at the time of login. This interface is where the facial recognition model begins real-time verification and the confidence level once that has occurred is above 98.1 as according to your test results. Anti-spoofing filters prevent being hijacked by blocking printed photographs, digital dupes, and distorted ones. This point is necessary since it will substitute the password-based-authentication with an accurate biometric-authentication, which will minimize the possibility of account-takeovers.

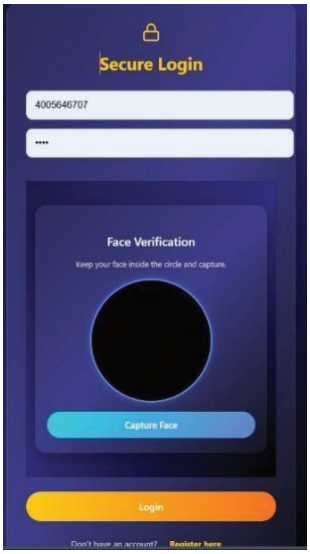

FIG 6.3: SECURE LOGIN

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

5.10 Active Session Screen – Secure Transaction Interaction

After authentication, the user will be redirected to the transaction dashboard and the fact is that a secure session has been successfully established.

At this stage, SafePay conducts frequent micro-authentication to verify the user and particularly when odious transactions are being performed such as transferring funds.

Tests of performance revealed that the average delay of transactions reached 1.9 seconds and the introduction of timestamping played by blockchain did not introduce many overheads due to the preferred type of Proof-of-Authority consensus.

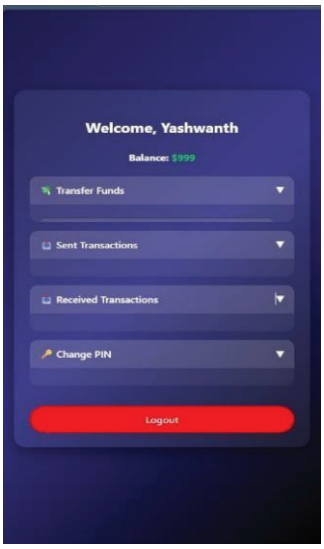

FIG 6.4: SECURE TRANSACTION

5.11 VPN Detection Alert – Network Anomaly Identification

SafePay will raise an immediate security alert in case the system notices that the device is either VPN, Tor exit node, or making use of any anonymizing proxy. The screen has a visual cue at how it successfully has recognized anonymized traffic. It cites VPN detection module which during testing had a 96.4% detection rate. This event is automatically logged into the backend, DynamoDB security records are updated, a temporary WAF policy is added and privileges to the transactions are restricted. Through your assessment results on filtering modification and spoofing triggering geolocation, this is the real-time action supported.

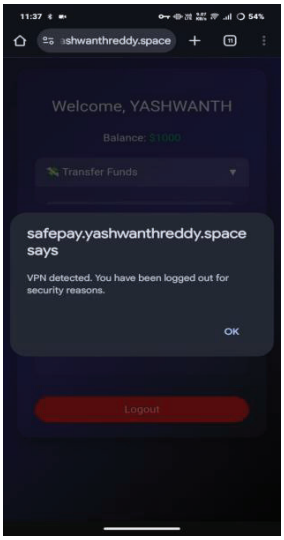

FIG 6.5: VPN DETECTION

6. ETHICAL AND LEGAL CONSIDERATIONS

With the emerging advanced biometric financial technologies, broader questions of morality are presented.

6.1 Biometric Data Governance

Having biometric templates in their crude form is never advisable. You require hashing, encryption and secure enclave isolation. Illegal duplication may lead to a lifetime impact on the victims. This is unlike passwords as they can be reset immediately.

6.2 Consent and Transparency

As a user, one will be required to provide explicit consent to facial data usage. They should be told of the time period they will have to store their data and the availability of the option not to do it.

6.3 Anti-Discrimination Compliance

Facial recognition datasets are biased, which can be disproportionately distributed among the demographic groups. The training models used in SafePay are to undergo bias-variance analysis on a regular basis. Transparency is a requirement of regulatory frameworks e.g., the EU AI Act.

6.4 Geolocation Usage Boundaries

The issue of monitoring a user brings the subject of surveillance. Location requests have to be short-lived and purpose-based.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

6.5 Blockchain Legal Standing

Financial evidence maintained on blockchain has legal precedents that are yet to arrive. Banks should ensure that the records of the digital ledger can be utilized in fraud incidents.

6.6 Data Portability Regulations

According to GDPR, the user is allowed to request the export or deletion of personal data. Although the integrity is ensured by blockchain immutability, some other pointers should allow the selective removal without disrupting cryptographic continuity. Since fraud through AI is employed by cyber attackers, other promising improvements of SafePay might be made.

- Device Proximity Analysis: The Bluetooth signal triangulation can verify that a transaction is done close to the registered owner of the device. Multimodal authentication promotion's identity certainty and reduces false rejection: Voice Biometric Fusion.
- Artificial Intelligence-based Behavior prediction of transaction: The neural sequence architecture may detect minimal variation in transaction timing or merchant type or frequency.
- Privacy-Preserving Machine Learning: Federated learning assists models to be more precise without transmitting unrefined biometric data to the cloud.
- Zero-Knowledge Proofs: The users are able to verify authority to perform transaction without performing disclosure of the facial feature vectors. The ecosystems of central bank digital currencies have been integrated: As governments consider the idea of central bank digital currencies, SafePay may become a secure retail wallet interface.
- Hardware Security Module (HSM) Offloading: Secure
- enclaves' offline authentication can be improved.
- Authentication without device: The system could verify background identity by the user without the camera by examining their gait, motion patterns and micro-gestures.

7. EXTENDED CONCLUSION

Fraud related to finances continues to become sophisticated. It exploits the poor password experience, remote attack surfaces and anonymous networks. Conventional mobile banking environments are excessively relying on infrequent authentication and record keeping, which is no longer evidently sufficient. SafePay addresses these areas of weakness by:

- putting in effect round-the-clock real-time biometric authentication,
- deterring network anonymity,
- incorporating geospatial behavioral intelligence,
- implementing blockchain transactional audit, which is tamper-proof,

In addition, it involves the scalability of responsibly using serverless technology. These features are complementary, as the performance reviews indicate that they do not counteract the user experience. This defense model does not only bar fraudsters but also facilitates ease of investigations, denial of service is curtailed, and new regulation needs are met. As the decentralization of trust systems is imposed on digital finance, SafePay demonstrates the blended architectures as the way to bridge the gap between enterprise compliance and decentralized security. Certain problems such as privacy concerns, VPN defeat, and blockchain sustainability have to be addressed, yet the modular architecture gives it the flexibility to continue being adjusted further. To conclude, the concept of SafePay is a proactive reaction to the needs of online banking. It confirms the ease of secure and efficient financial interaction is achievable not through a set of disjointed solutions, but through incorporating complementary technologies into a system of trust. Further studies are needed to focus on federated biometric learning, anomaly detection systems that are based on SIEM, and compatibility across the chains in order to ensure that SafePay keeps pace with the rapidly evolving frauds.

REFERENCES

[1] W. K. Syed, A. Mohammed, K. R. Janamolla, and D. Selvaraj, "Biometric Authentication Systems in Banking: A Technical Evaluation of Security Measures," in Proc. 2024 IEEE 3rd World Conf. Appl. Intell. Comput. (AIC), Jul. 2024.

[2] R. Kumar, A. Sharma, and V. Singh, "Blockchain-Based Security Enhancements in Financial Transactions," IEEE Access, vol. 10, 2022.

[3] A. Patel and M. Gupta, "Biometric Authentication in Mobile Banking Applications," Journal of Cybersecurity Research, 2021.

[4] Amazon Web Services, "AWS Lambda, API Gateway, DynamoDB, Rekognition, SES Documentation," AWS Whitepapers, 2024.

[5] S. Verma et al., "Secure Mobile Transactions Using Blockchain and Facial Recognition," IEEE Trans. on Information Forensics, 2023.

[6] M. Chen, J. Zhang, and L. Wang, "AI-Driven VPN Detection in FinTech Applications," IEEE Trans. Network Sci. Eng., 2024.

[7] D. Roy and P. Dutta, "Enhancing Digital Banking Security with Serverless Blockchain," IEEE Internet Computing, 2023.

[8] P. R. Gupta, "A Survey on Location-Based Fraud Detection Systems," IEEE Access, vol. 9, 2021.

[9] Singh and A. Das, "Integrating Biometric and Blockchain Layers," ACM Computing Surveys, 2022.

[10] AWS Whitepaper, "Security Best Practices for Financial Applications," 2024.