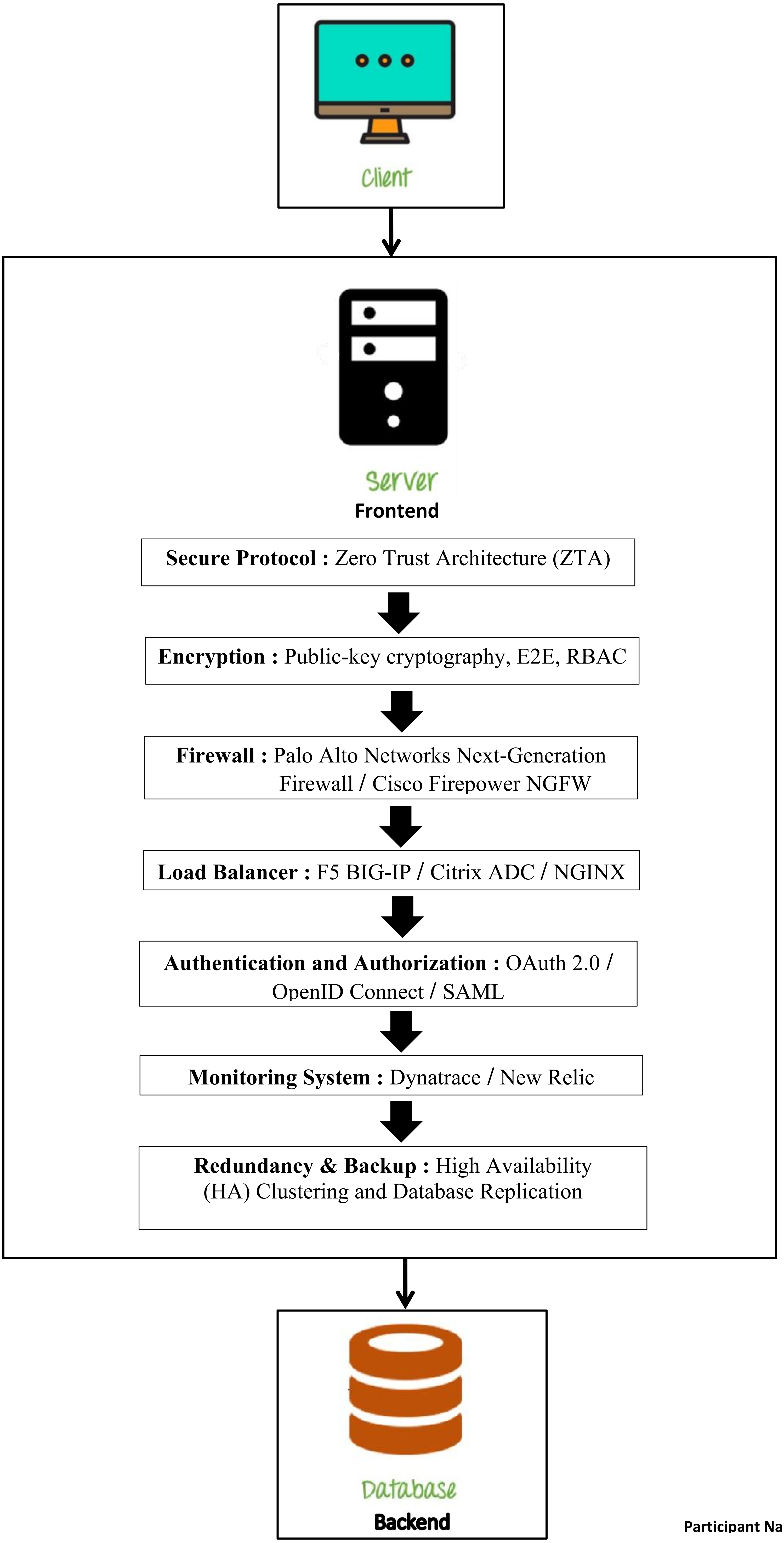
SwiftShield FinTech System - 3-Tier Architecture



Secure Protocol : Zero Trust Architecture (ZTA)

Encryption : Public-key cryptography, E2E, RBAC

Firewall : Palo Alto Networks Next-Generation Firewall / Cisco Firepower NGFW

Load Balancer : F5 BIG-IP / Citrix ADC / NGINX

Authentication and Authorization : OAuth 2.0 / OpenID Connect / SAML

Monitoring System : Dynatrace / New Relic

Redundancy & Backup : High Availability (HA) Clustering and Database Replication

Participant Name: JANVEE SINGH

WHY ZTA AS SECURE PROTOCOL ?

Zero Trust Architecture (ZTA) is an innovative security framework that assumes no trust in any user or system, regardless of its location, and incorporates multiple layers of security controls. It focuses on verifying and validating every user and device attempting to access resources, both within and outside the network perimeter. ZTA employs various technologies and techniques, including:

1. **Identity and Access Management (IAM):** Implementing robust IAM solutions helps ensure that only authorized individuals can access sensitive data during transit.

2. **Multi-factor Authentication (MFA):** By requiring users to provide multiple forms of authentication, such as passwords, biometrics, or smart cards, MFA adds an extra layer of security to prevent unauthorized access.

3. **Microsegmentation:** Microsegmentation divides the network into smaller, isolated segments, allowing for granular control and reducing the impact of potential breaches by limiting lateral movement within the network.

4. **Software-Defined Perimeter (SDP):** SDP creates a secure overlay network that allows access to specific resources based on user and device authentication, effectively hiding them from the broader network.

5. **Advanced Threat Detection:** Employing AI and ML-based techniques for real-time monitoring and detection of anomalous activities can help identify potential threats and respond swiftly.

6. **End-to-End Encryption:** Additional encryption methods like IPsec (Internet Protocol Security) or VPN (Virtual Private Network) can provide stronger protection for data during transit.

The secure protocol, such as ZTA, is established as the first step to ensure identity verification, access control, and secure communication channels between different tiers or components of the architecture.

ENCRYPTION - Post-quantum encryption algorithms, End-to-end encryption (E2E), Public Key Cryptography(FIDO), Role-based access control (RBAC)

To ensure that there is no data in plain text during transit, a combination of encryption algorithms has been used in this architecture that complement each other's strengths and weaknesses. The process of encryption using these techniques and standards can be explained stepwise as follows:

STEP 1: The sender generates a pair of keys: a public key and a private key.

STEP 2: The sender shares the public key with the receiver, and keeps the private key secret.

STEP 3: The sender encrypts the data using a post-quantum encryption algorithm and the private key.

STEP 4: The sender sends the encrypted data to the receiver using E2E encryption.

STEP 5: The receiver receives the encrypted data and decrypts it using the private key and the same post-quantum encryption algorithm.

STEP 6: The receiver verifies the sender's identity using public-key cryptography and FIDO standard.

STEP 7: The receiver accesses the decrypted data based on their role using RBAC.

After the secure protocol is established, encryption is applied to protect data confidentiality and integrity. By combining post-quantum encryption algorithms, E2E encryption, public-key cryptography, FIDO authentication, and RBAC, this 3-tier architecture establishes a robust encryption framework. This ensures data remains encrypted during transit, unauthorized access is prevented, users are authenticated securely, and access to sensitive data is controlled.

FIREWALL - Palo Alto Networks Next-Generation Firewall / Cisco Firepower NGFW

Both Palo Alto Networks Next-Generation Firewall and Cisco Firepower NGFW are reputable and widely used firewall solutions in the industry. Both offer advanced security features and capabilities to protect data and ensure real-time availability. The choice between the two depends on various factors, including specific requirements, budget, and existing infrastructure.

Palo Alto Networks Next-Generation Firewall is known for its:

- Advanced Threat Prevention Capabilities,
- Including Deep Packet Inspection,
- Application-Level Visibility, And
- Integration With Palo Alto Networks' Cloud-Based Security Platform.

It offers granular control and advanced security features suitable for highly regulated industries like fintech.

On the other hand, **Cisco Firepower NGFW** combines traditional firewall functionality with

- Advanced Threat Protection Features
- Provides Comprehensive Security Services
- Including Intrusion Prevention
- Malware Protection, And
- Url Filtering.

Cisco Firepower NGFW is known for its scalability and robustness, making it suitable for organizations with high traffic volumes and complex network environments.

The firewall comes into play after encryption. It filters network traffic, allowing only authorized traffic and blocking unwanted or malicious requests.

LOAD BALANCER - F5 BIG-IP / Citrix ADC / NGINX Plus

F5 BIG-IP: F5 BIG-IP load balancers offer

- ❖ Advanced Traffic Management Capabilities,
- ❖ Including SSL/TLS Termination,
- ❖ Application Acceleration, And
- ❖ Robust Security Features.

They can integrate well with a ZTA approach by incorporating access controls, authentication, and authorization mechanisms. F5 BIG-IP provides flexibility and scalability to handle the demands of a fintech environment while ensuring data security and real-time availability.

Citrix ADC is another load balancer that provides

- ❖ Comprehensive Application Delivery Features,
- ❖ Including SSL Offloading, Caching, And
- ❖ Application Firewall Capabilities.

It offers integration with ZTA principles through advanced access controls and authentication mechanisms. Citrix ADC's scalability and security features make it a suitable choice for fintech companies looking to ensure data security and real-time availability in their 3-tier architecture.

NGINX Plus is a lightweight and high-performance load balancer that can

- ❖ Also Function As a Reverse Proxy And Web Server
- ❖ Offers Load Balancing,
- ❖ SSL/TLS Termination, And
- ❖ Content Caching Capabilities.

NGINX Plus can be integrated with ZTA principles by implementing access controls and authentication mechanisms at the frontend layer. Its high performance and flexibility make it a good choice for fintech applications.

The load balancer is positioned after the firewall. It distributes incoming network traffic across multiple servers to improve performance, scalability, and availability.

AUTHENTICATION AND AUTHORIZATION - OAuth 2.0 / OpenID Connect / SAML

OAuth 2.0 is an industry-standard protocol for authentication and authorization.

- ✓ It allows users to grant limited access to their resources on one site to another site without sharing their credentials.
- ✓ OAuth 2.0 can be used in a 3-tier architecture to authenticate and authorize users accessing the frontend and backend layers.
- ✓ It supports various grant types, such as authorization code, implicit, and client credentials, which can be tailored to the specific needs of a fintech application.

OpenID Connect is a widely adopted authentication protocol built on top of OAuth 2.0.

- ✓ It provides a standardized way to authenticate users and obtain their identity information.
- ✓ OpenID Connect can be used in a 3-tier architecture to authenticate users at the frontend layer and propagate their identity information to the backend layer securely.
- ✓ It works well with ZTA principles by enabling user-centric authentication and federated identity management.

SAML (Security Assertion Markup Language) is an XML-based standard for exchanging authentication and authorization.

- ✓ It enables single sign-on (SSO) capabilities and
- ✓ It can be used to authenticate users across multiple applications and services in a 3-tier architecture.
- ✓ SAML supports ZTA principles by providing secure identity propagation and attribute-based authorization.

Once the network traffic is filtered by the firewall, the authentication and authorization mechanisms come into play. Users and servers are authenticated and authorized using standards like OAuth 2.0, OpenID Connect, or SAML.

MONITORING SYSTEM - Dynatrace / New Relic

Dynatrace:

- Full-stack monitoring platform that offers advanced AIOps capabilities.
- Provides automated monitoring, intelligent observability, AI-driven analytics to detect-resolve performance issues proactively.
- Dynatrace is suitable for organizations looking for an AI-powered monitoring solution with advanced features.

New Relic:

- Cloud-based application performance monitoring platform.
- Offers end-to-end monitoring capabilities, including real-time performance monitoring, error tracking, and distributed tracing.
- Provides deep insights into application performance and user experience.
- Suitable for organizations that prioritize application performance monitoring and observability.

The monitoring system has been set up in this 3-tier architecture to continuously monitor the servers, network traffic, and receive alerts for any security-related events or vulnerabilities. This helps in proactively identifying security risks and taking appropriate actions.

REDUNDANCY & BACKUP - High Availability (HA) Clustering and Database Replication

HA clustering involves:

- Setting up multiple servers in a cluster where they work together to provide high availability and fault tolerance.
- In an active-passive configuration, one server (active) handles the workload while the other server (passive) remains in standby mode, ready to take over if the active server fails.
- In an active-active configuration, both servers share the workload, ensuring load balancing and high availability even if one server fails.
- Clustering ensures seamless failover and minimizes downtime by quickly redirecting traffic to a standby server in case of a failure.

Database Replication involves:

- Creating and maintaining multiple copies of the database in real-time or near real-time.
- In a master-slave replication setup, changes made to the master database are replicated to one or more slave databases.
- The slave databases can serve as backups and also be used for read operations, improving scalability and availability.
- In a multi-master replication setup, multiple databases act as master databases, allowing for read and write operations across multiple nodes. This enhances both availability and scalability.
- Database replication provides data redundancy, disaster recovery capabilities, and improved performance by distributing the workload among replicated databases.

Both HA clustering and database replication work together to ensure high availability and data integrity in SwiftShield FinTech System' 3-tier architecture. By employing these techniques, potential single points of failure are minimized, and the system can handle failures seamlessly while maintaining real-time availability and data security.

Redundancy and backup mechanisms are implemented to ensure high availability and data resilience. This involves setting up high availability clustering and database replication to ensure failover and data backup in case of server failures or maintenance.