Secure IAM Multi-Cloud Federation

Team Name :Code Connectors

MEMBERS:-
Lokesh G
Siddharth B
Sathyanaryanaa T
Manoj k

Theme:

Identity & Privacy Explore decentralized identity for voter ID, health records, education credentials using ENS, ZKPs, SSI.

Problem Statement:

Organizations today operate across multiple cloud platforms like AWS, Azure, GCP, Odoo, and more. But Identity and Access Management (IAM) remains fragmented and unsecure

Solution:

We propose a **Decentralized Multi-Cloud Federation System** that enables a user to authenticate seamlessly across cloud providers using:

Decentralized Identifiers (DIDs)

Verifiable Credentials (VCs)

Zero-Knowledge Proofs (ZKPs)

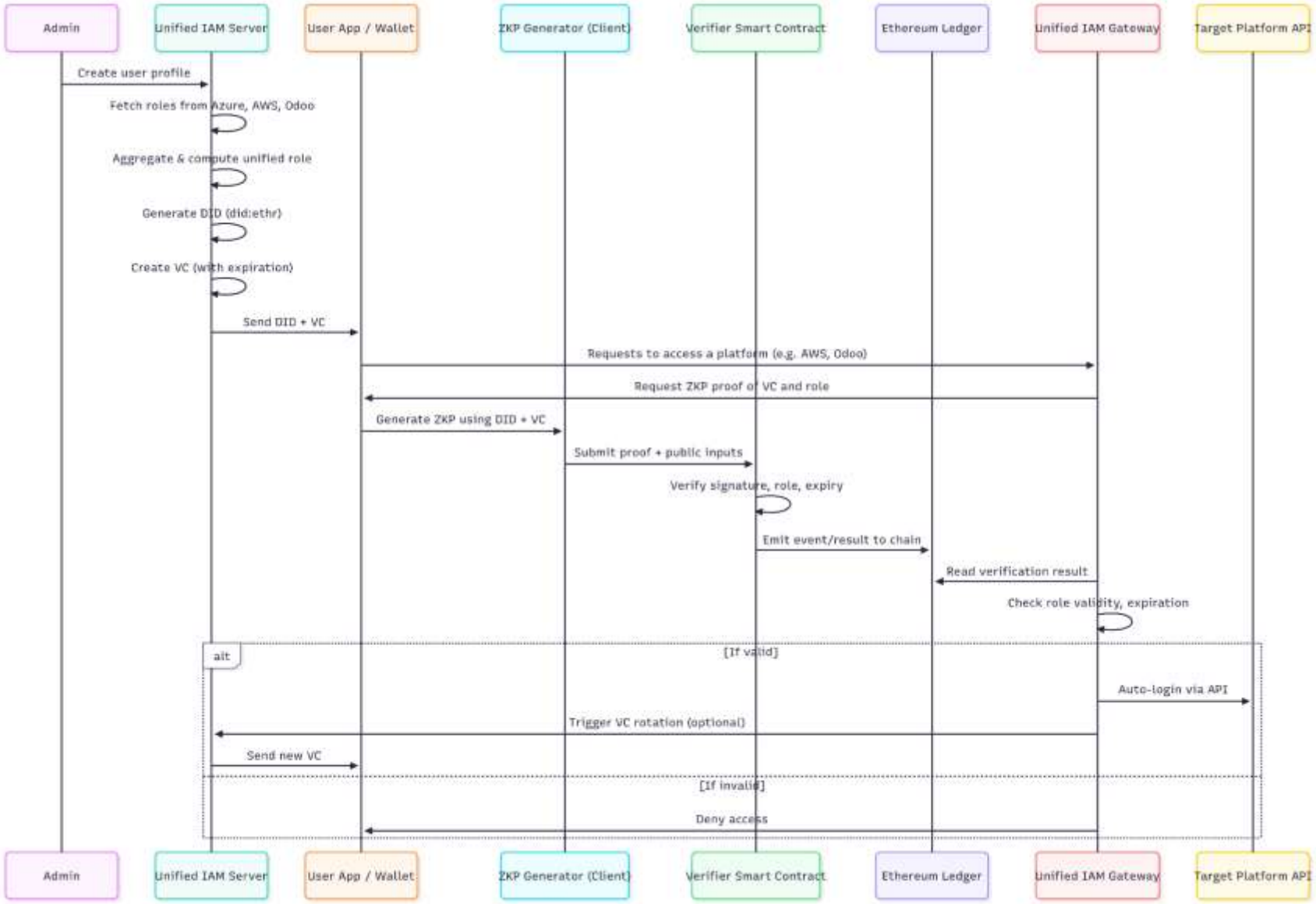
Smart Contracts for on-chain verification

This system allows one-time credential issuance and access to multiple clouds without manual IAM synchronization.

How It Works:

- Fetch roles from AWS, Azure, Odoo, etc.
- Aggregate into a unified VC
- Use ZKP to verify identity, role, and access rights without revealing sensitive data
- Authenticate and auto-login via secure API
- VC expiration and rotation managed seamlessly

WORK FLOW:


Admin
Unified IAM Server
User App / Wallet
ZKP Generator (Client)
Verifier Smart Contract
Ethereum Ledger
Unified IAM Gateway
Target Platform API
Create user profile
Fetch roles from Azure, AWS, Odoo
Aggregate & compute unified role
Generate DID (did:ethr)
Create VC (with expiration)
Send DID + VC
Requests to access a platform (e.g. AWS, Odoo)
Request ZKP proof of VC and role
Generate ZKP using DID + VC
Submit proof + public inputs
Verify signature, role, expiry
Emit event/result to chain
Read verification result
Check role validity, expiration
alt
[If valid]
Auto-login via API
Trigger VC rotation (optional)
Send new VC
[If invalid]
Deny access
Admin
Unified IAM Server
User App / Wallet
ZKP Generator (Client)
Verifier Smart Contract
Ethereum Ledger
Unified IAM Gateway
Target Platform API

Why This Matters:

Cross-Platform Access: One identity across all major clouds

Security & Privacy: Role validation without exposing user data

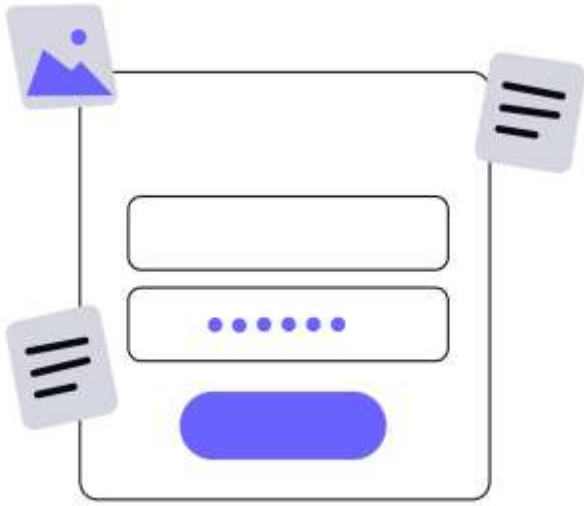
Efficiency: Eliminates IAM sync operations

Vendor Neutrality: Not tied to any specific cloud provider

Blockchain Integrity: Verified access on-chain using smart contracts

Tools Powering Multi-Cloud Federation

- Ethereum (Sepolia) & zkSync: Blockchain + scalability.
- ID: DID/VC management aligned with W3C.
- circom/snarkjs: Zero-Knowledge Proof tooling.
- Flask: Lightweight API backend.
- IPFS: Decentralized VC storage.
- AWS SDK (boto3): Cloud IAM integration.
- Hardhat & ethers.js: Smart contract development.



Future Scope:

Agentic AI Integration: Use AI agents to automate:

Role recommendation and mapping

Real-time anomaly detection in access behavior

Dynamic policy enforcement across platforms

Fine-grained Policy Governance using AI-powered adaptive access control

Decentralized Governance DAO for federated IAM standards

Conclusion

Our **Decentralized Multi-Cloud Federation** system redefines how identity and access are managed across cloud platforms. By leveraging **DID, VC, and ZKP**, we eliminate the need for manual IAM synchronization and enable **seamless, secure, and privacy-preserving access** across AWS, Azure, GCP, and beyond. This not only enhances operational efficiency and security but also opens the door for future innovations like AI-driven identity governance.