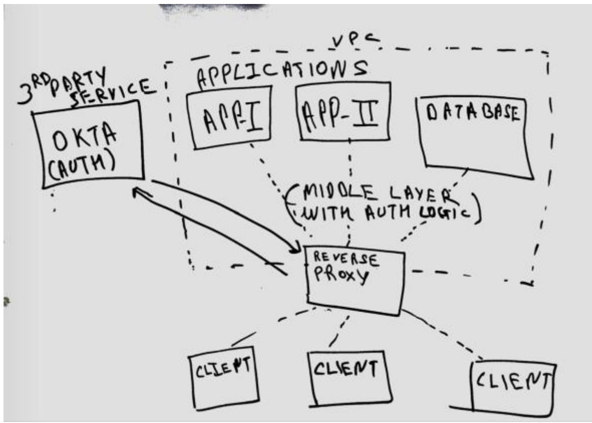
ABSTRACT-MULTI FACTOR AUTHENTICATION

- **Statement of Problem**-
  - The problem addressed in the problem statement is the requirement to create an authentication mechanism by developing a microservice which would successfully authenticate the applications deployed in different geographies built using different technologies(multiple web portals of the Techier organization) with the Authentication Service(OKTA).

- **Objectives**-
  - Our micro service will act as an intermediate layer between OKTA & other websites of Techier, This will surely increase scalability & efficiency of rolling out updates & changes to the Authentication system.
  - So Creating a Microservice that increases usability of existing services like OKTA motivates us working towards this problem.

- **Introduction to Proposed Solution**-



  - The Above Daigram illustrates Our Basic Flow
  - proxy, auto-scaling, upgrading downgrading.
  - Implementing a central authorization layer for applications accessed by HTTPS, so you can use an application-level access control model instead of relying on network-level firewalls.
  - Our Reverse proxy service acts as an middleware between the organisation's applications and client, the proxy server checks the authentication (with the desired logic) with each request from client side. If the client is authenticated it will take the client to the authentication page then to the application, and in case of authenticated client it will serve the application directly.
  - This reverse proxy server will pass the auth info (like Auth token, user information, Unique User identification etc) to the Application services in headers, that can be used by the application for the desired operations.
  - This can serve a common authentication across multiple services/Applications too.

- Reverse proxy Works in layer 7 of OSI networking model, which gives a-lot of flexibility and features which can be implemented which can further enhance security also and prevent common attacks like DDOS.
