SIH 2017

Deployment Report

Team Name and Title: DEFENDERS and "Multi-Factor Authentication add-on for OpenVPN"

I4C ID: 7914

College Name: THIAGARAJAR COLLEGE OF ENGINEERING

Address: THIAGARAJAR COLLEGE OF ENGINEERING, Madurai, Tamil Nadu, INDIA – 625015.

Ministry: ISRO

Ministry Mentor's Name and Contact Details: Mr.Jigar Raval, PRL

mail id - jigar@prl.res.in phone:079-26314035.

Team Leader Details

Name	Mobile Number	Email-id
SRIRAM M	9655077056	sriramm1997@gmail.com

Team Members Details

Name	Mobile Number	Email-id
RAGUL R	9629123825	ragulrangarajan@gmail.com
PROMOD S	9710644621	promods96@gmail.com
PREETHAM S	9842940376	preethamsathyamurthy@gmail.com
RESHMA KRIS M	7598272381	reshmakrisrk@gmail.com
JEGAN BABU N T	9944638824	jeganbabu33@gmail.com

Mentors Details (if any):

Name	Mobile Number	Email-id
C.V.Nisha Angeline	9842175694	nishaangeline@gmail.com

Application Type: Web / Mobile / Desktop / Other

Hardware Required: Yes/ No (* Please mark yes if your application has any hardware integrated e.g. Camera, Raspberry Pi or any other controller etc....)

Can the Idea be Patented? Yes/ No

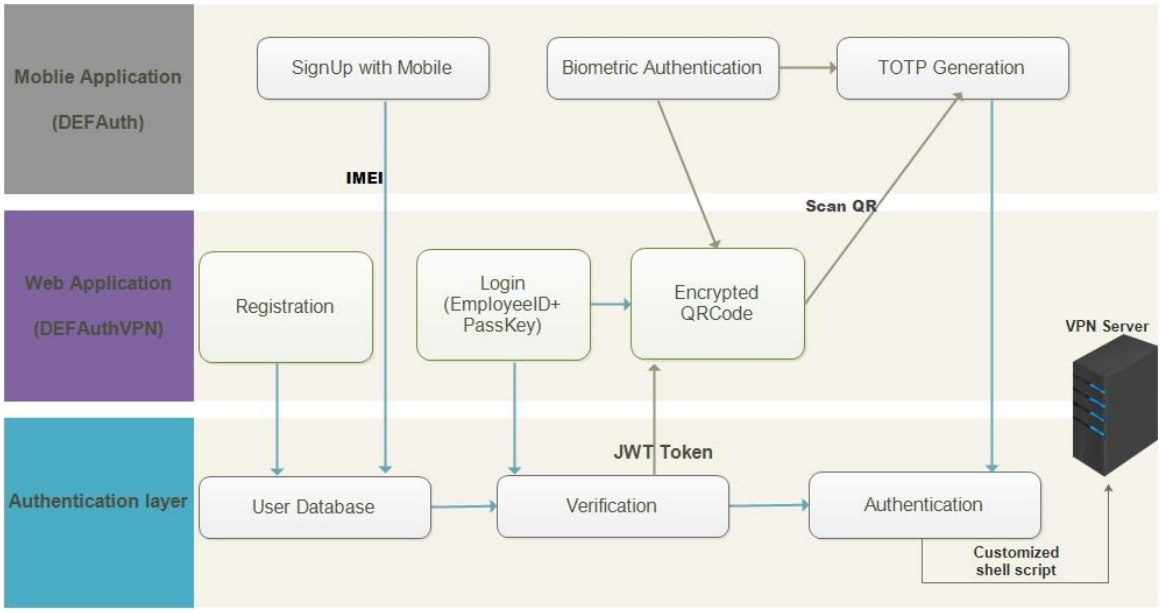
Abstract:

A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. VPN technology was developed as a way to allow remote users and branch offices to securely access corporate applications and other resources. It allows users to establish a virtual private *"tunnel"* to securely enter an internal network, accessing resources, data, and communications. By default, VPN does not provide / enforce strong user authentication. The idea here is to customize popular open-source VPN solution "OpenVPN" to enable secure authentication using Multifactor authentication methods such as Time-Based one-time Password (TOTP), JWT tokens and Mobile based Biometric access integrated. It serves as an add-on for VPN authentication and also a plug and play solution for any user authentication system. The Multi-Factor authentication technologies namely knowledge factor, possession factor and biological trait is integrated with VPN and access to VPN service is provided by verifying the authenticity of the user. This heightens the security of the VPN service and can be easily deployed as an add-on to any authentication server with simple and secure modified shell script code injection. Since it is an API it can be used as a service by any organization / software that require stringent authentication mechanism.

A. Design Process

a. System Architecture

- VPN (Virtual Private Network) technology provides a way of protecting information being transmitted over the Internet, by allowing users to establish a virtual private "tunnel" to securely enter an internal network, accessing resources, data, and communications.
- By default, VPN does not provide / enforce strong user authentication. Most VPN implementations provide limited authentication methods.
- To secure the VPN with MFA a stateless, easy to deploy, cost effective and platform independent solution is required which is JWT (JSON Web Tokens), these are an open, industry standard RFC 7519 method for representing claims securely between two parties.



b. Technologies Used

- LAMP stack
- Android SDK
- OpenVPN server and Client
- Shell Script
- Node.js and JSON Web Tokens
- Web Application

c. Use Cases

- Providing state of art access to VPN services within ISRO and also enhance the authentication mechanism by providing a three-factor integrated safe authentication mechanism for the employees of ISRO. The latest technologies including JWT tokens, AADHAR integration is provided for a state of art experience in authenticating VPN services.

- On successful completion of the project a highly scalable and Multi factor authentication enabled VPN service can be deployed on the ISRO server for VPN access to its employees.

d. Source Code organization details

Web App

- Index _Landing Page of DefAuth server
- Registration page
  - Mobile verification
  - Registration Complete
  - Logout
- Login Page
  - Login credential
  - Login DB.php(passkey verify)
  - TOTP_verify – google lib
  - QR_code generation gangsta file (google authenticator.php)

- Approve_Connect vpn page
- Decline_Connect vpn page

Mobile App

- Admin Rights Accept/Decline
- Setup Backup PIN/passkey
- Device registration
- QR scanner

B. Features Implemented

- Simple, Secure and Scalable solution.
- Stateless Plug and play solution which is platform independent.
- Adhering to industry standards like IETF RFC.
- Affordability for widespread organization like ISRO.
- Simple Web UI and user-friendly Android app for hassle free user experience.
- Integrating Mobile based biometric API for secure user authentication system based on biological trait.
- Outcome of this will be secure user authentication for any management needs in an organization which covers a broader scope with easy profile management and administrator control.

  Easy self-enrollment, complete sync or link your old management system.

C. Deployment Process

- **New User Registration procedure**
  - Employee ID
  - Password (only numeric)
  - IMEI – Fetched secretly from the mobile device for possession factor (Restricted to one mobile device only, else raise ticket to admin to release lock)
  - Now open “DEFAuth” mobile application and select “New User” and enter Employee ID to initiate session in mobile for first time registration
  - The IMEI + User ID is fetched and updated in Database
  - After successful registration of mobile device the user is automatically logged out.

- **Existing User Login Procedure**

  - The existing user shall open the web application and enter Employee id and password
  - Now a QR code is displayed on the web screen
  - Open the “DEFAuth” app - This app is inbuilt with app lock
    - Finger Print verification for Bio metric enabled device
    - PIN lock for other devices
  - The QR code can be scanned only using the previously registered and verified mobile device.
  - Once the IMEI of the mobile device is verified with the database TOTP auto verification from server side takes place in the backend.
  - The TOTP and IMEI is verified using the JWT token against the userID.
  - The JWT token once generated can only be used for 10 minutes and the validity expires thereafter.

Finally, the JWT validity is verified and VPN access is provided using a customized shell script containing the OVPN file credentials to the client.

- **Dynamic User Status details in DB**

(Format: status number -> current status)

  - 0 -> user has registered in website page
  - 1 -> user updated his/her IMEI
  - 2 -> user is logged in
  - 3 -> user is logged out
  - 4 -> TOTP is verified for user

D. Future Scope:

We would like to integrate our Indian Government AADHAAR based biometric verification for authenticating user's biological factor which is more secure and authentic and also it is easier to identify and track the individual user from any organization. This AADHAAR based API for biometric authentication of user provides an added advantage of using our own Indian Government's secure service which is highly scalable across various service offering and multilevel authentication system which is little hard to implement but the results are palpable.

E. Miscellaneous:

The Linux cloud server is used to inject the modified shell script to the authentication VPN server from the user's OpenVPN client. We have developed a customized Android Application named "DefAuth" which includes QRcode scanning library and TOTP (IETF RFC 6238) generation and auto verification algorithm along IMEI verification integrated.