Secure Video KYC

Aditya Khedekar[1], Saurabh Katkar[2], Darpan Bhorade[3]

[1,2,3] *Student, Degree(Computer Engineering), Atharva College of Engineering, Mumbai*

Abstract - *Official KYC Process requires verification and authentication of a person to be done by a physical presence i.e. for this a person is required to visit and present themselves to verify and authenticate their documents and themselves.*

So, as of now ongoing pandemic of covid-19, these activities could not be fulfilled completely as it's not possible or in some cases not allowed to have human interactions.

Thus various of these verification and authentication activities in the above-mentioned scenarios are not possible.

Therefore there is a need to handle such activities by remote interactions of people.

The challenge is to perform such activities via online interaction is to maintain integrity and authenticity within the system. Various cybersecurity threats and attack vectors can compromise the legitimacy of the process. Thus there is an increasing need for a secure and robust online video-based identification and verification system.

1.INTRODUCTION

Our main motto is to create a secure video-based identification system and to make remote customer acquisition easier. We plan to build an application for both web and mobile platforms to carry out the Video KYC process.

1.1 Need and Motivation

Government Regulation for Video Kyc - Amendment to Master Direction (MD) on KYC Government of India, vide Gazette Notification G.S.R. 582(E) dated August 19, 2019, and Gazette Notification G.S.R. 840(E) dated November 13, 2019, has notified amendment to the Prevention of Money-laundering (Maintenance of Records) Rules, 2005. Further, to leverage the digital channels for Customer Identification Process (CIP) by Regulated Entities (REs), the Reserve Bank has decided to permit Video-based Customer Identification Process (V-CIP) as a consent-based alternate method of establishing the customer's identity, for customer onboarding.

1.2 Basic Concept

Our solution is a mobile application that will mainly focus on performing video KYC processes. Along with this, it will also run different security processes in real-time to maintain the integrity and authenticity of the process. It will detect any fraudulent activities via various algorithms and mechanisms implemented by us. So that to ensure the person is real and the data provided is authentic and verified.

2. REPORT ON PRESENT INVESTIGATION

As this problem is very recent, there is very few application in the market which tries to solve this problem and most of them are not capable of tackling advanced attack vectors or are not specifically developed for carrying out identification and verification processes.

Fintech, wallets, and tech-enabled start-ups had built their business models by considering the usage of Aadhaar enabled e-KYC. Everything went for a toss after the Supreme Court verdict. Many wallets closed their businesses as physical KYC was difficult. Now with Video Kyc identification and verification processes, those processes which require physical interactions can be done remotely via online solutions.

Various attacks which can be faced by video-based identification system are:-

Presentation attack - Biometric data used to attack the system by creating spoofs or fakes. Biometric data can obtain directly from a person having an online identity or by hacking systems. This hacked data can be used to create spoofs and fakes and used on other biometric devices. These attacks can be like using a printed photo, the 3D mask of a person, a photo or video of the person, or a fake fingerprint. The vulnerability of face recognition is increasing day by day.

Overriding Capture device - A malware or script can be injected into computer devices to gain access to peripheral devices. These scripts interact with the available API provided by OS and gain access to devices. Techniques can be screen capture, accessing camera devices, etc. By using these techniques, attackers can gain victim's data and use it for malicious purposes.

Override Feature Extraction - This attack interferes with the feature extraction routines to manipulate or provide false data for further processing. Alternatively, this attack can be used to disable a system and create a DoS attack.

Deepfake Attacks for False Impersonation - Today, there are most damaging and successful cyberattacks and it affects security systems. Deepfakes are realistic, hard to detect, and easy-to-create of real people. Deepfakes can be used to spread fake news, hoaxes, or conspiracy. Evolving cybersecurity attacks make rethink decision on security approach of the app. The possibility of deep fakes is endless and the threat is real.

3.AIM AND OBJECTIVES

3.1 Aim

We aim to create a seamless video-based customer identification process and defending against various advanced attack vectors.

3.2 Objectives

- Video KYC can make various identification and verification processes more convenient for users.
- Multiple products such as remote onboarding of savings account customers and acquiring a credit card can be done through the video KYC process.
- A large number of financial services can be carried out through Video KYC.
- Video KYC costs become much less as compared to IPVs (in-person visits) for both users and organizations in long run.
- Efficiency increases as more Video KYC processes can be carried out at a given time as compared to that normal physical processes.

4.PROPOSED SYSTEM

4.1 Explanation

Process Flow is as follows :
Step 1: Register on the platform

Step 2: Fill the form:
- Enter Aadhar Number
- Upload Pan-card photo
- Upload your latest photo
- Ask the user to select the preferred language for the interview from the list of languages available

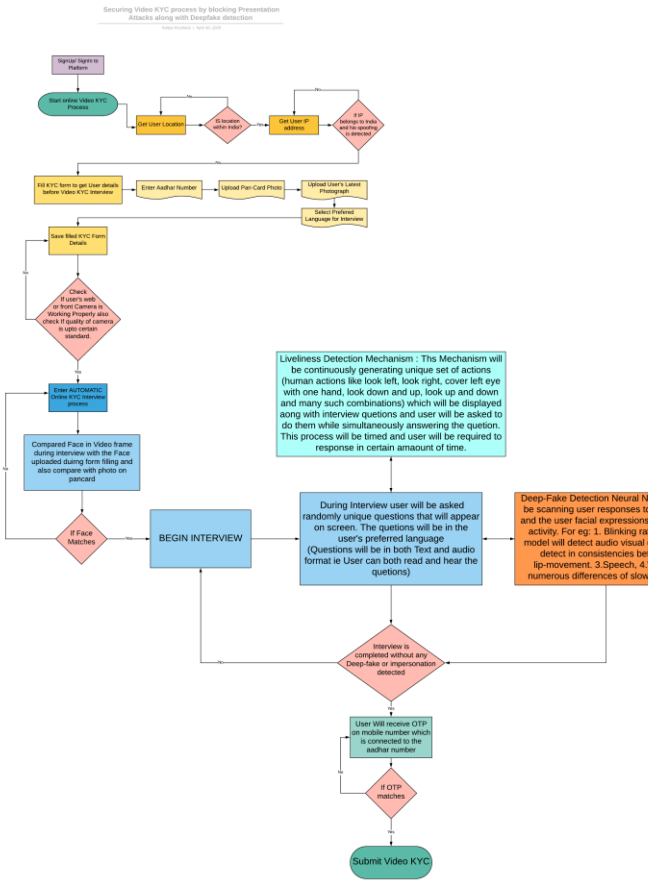
Step 3: Before the Interview Processes:
3.1 If the user's camera is not up to certain megapixels with bad video quality or can't detect a person in the video frame then the user will be alerted accordingly.
3.2 User will be requested to access location and to check if the user is in India or not (If not alert accordingly and the process is closed)
3.3 Along with user location also check user IP address and check if the user is not using VPN or any other spoofing techniques (if any spoofing recognized alert accordingly)
3.4 Before the interview begins to check if the person in the video matches the face in both the Latest photo uploaded and photo on Pan-card (Using face detection models with neural networks that also, recognize age-separated faces) uploaded while registering.
3.5 Identification details in Aadhaar/PAN shall match with the details provided by the customer.

Step 4: During Interview
4.1 During the Interview users will be asked randomly unique questions that will appear on the screen. (Questions will be in both Text and audio format)
4.2 Liveness Detection of the user to block Presentation Attacks on the process:
● Along with questions users would also be asked to perform random actions during answering the questions. (Set of actions to be performed will be displayed along with questions in the form of descriptive animation or pictures of the action to be done) for example: Look left and right two times, cover your left eye, etc…
● Each set of questions and activities will be completely random and unique to every user. The questions and actions asked to do so will be completely randomized by various combinations of both questions and actions to each user.
● In most cases, the eye blinking rate in fake videos is slower or extremely faster than the normal person blinking rate. This enables the detection of fake videos from real videos by using an eye blinking rate.

4.3 Deep Face Detection:
● While the user is giving the interview and liveness detection is running during the whole process, the Deep Fake detection model will be continuously checking for any signs or patterns of deep fakes. If the detected KYC process will be terminated. And bank authorities will be warned accordingly.
● The deepfake detection technique uses the audio-visual dataset to detect inconsistencies between lip movements, speech, and numerous differences of slow images. Recurrent Neural Network(RNN) to discover temporal discrepancies across frames and Long Short Term Memory (LSTM) for temporal sequence analysis.

Step 5: After Interview
Once the interview is over. Then the user will receive OTP on the phone number connected to the Aadhar number they entered in the form. Users will need to enter the correct OTP to successfully submit the KYC interview.

4.2 System Design


Securing Video KYC process by blocking Presentation Attacks along with Deepfake detection
Aditya Khedekar | April 30, 2020
SignUp/ SignIn to Platform
Start online Video KYC Process
Get User Location
IS location within India?
No
Yes
Get User IP address
If IP belongs to India and No spoofing is detected
No
No
Fill KYC form to get User details before Video KYC Interview
Enter Aadhar Number
Upload Pan-Card Photo
Upload User's Latest Photograph
Select Prefered Language for Interview
Save filled KYC Form Details
No
Check If user's web or front Camera is Working Properly also check If quality of camera is upto certain standard.
Yes
Enter AUTOMATIC Online KYC Interview process
Compared Face in Video frame during interview with the Face uploaded duirng form filling and also compare with photo on pancard
No
If Face Matches
Yes
BEGIN INTERVIEW
Interview is completed without any Deep-fake or impersonation detected
No
Yes
User Will receive OTP on mobile number which is connected to the aadhar number
No
If OTP matches
Yes
Submit Video KYC

Liveliness Detection Mechanism : Ths Mechanism will be continuously generating unique set of actions (human actions like look left, look right, cover left eye with one hand, look down and up, look up and down and many such combinations) which will be displayed aong with interview quetions and user will be asked to do them while simultaneously answering the quetion. This process will be timed and user will be required to response in certain amaount of time.

During Interview user will be asked randomly unique questions that will appear on screen. The quetions will be in the user's preferred language (Questions will be in both Text and audio format ie User can both read and hear the quetions)

Deep-Fake Detection Neural N
be scanning user responses to
and the user facial expressions
activity. For eg: 1. Blinking ra
model will detect audio visual
detect in consistencies be
lip-movement. 3.Speech, 4.
numerous differences of slow

5. SCOPE AND FEASIBILITY

5.1 Scope

Video KYC can make various identification and verification processes more convenient for users. A various scenario such as in remote onboarding of customers for various banking processes as well as authenticating in the various government process. Example: Acquiring a credit card can be done through the video KYC process. Video KYC costs become much less as compared to IPVs (in-person visits) for both users and organizations.

5.2 Feasibility

5.2.1 Operational Feasibility

This Solution can be deployed to both on-premise servers or on the cloud. But Ideally, it would be easy and comfortable to deploy it on Cloud Server because of features provided by the cloud provider and by seeing the scope of the solution. The solution requires Machine Learning algorithms and it would be extremely efficient to use Cloud.

5.2.2 Technical Feasibility

Technical Feasibility, includes the development of a working prototype of the final product. Flutter is the most trending and used framework for cross-platform applications. With the availability of good modules plus the strong customization options, dynamic features, good connectivity offered by flutter language and Firebase, implementation of the current product is very much possible.

5.2.3 Economic Feasibility

Economic feasibility is the cost and logistical outlook for a business project. The cost incurred will be at the time of product development and deployment i.e. Database, API's, Server Deployment and hosting, Play Store, Maintenance, and Upgrades for Firebase, which will be required if the user pool is higher than expected. Also, we provide local deployment of the Video KYC process so the private data remains protected.

6. Design Details

6.1 Face Matching Flow Chart

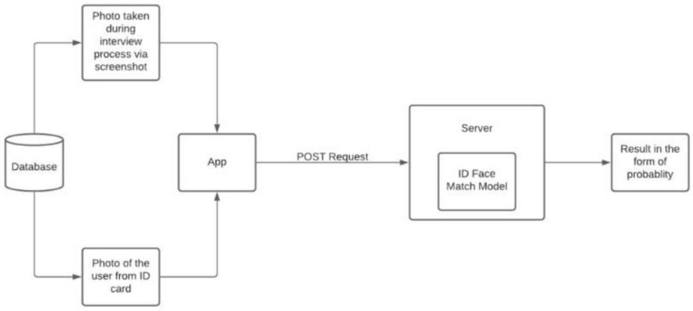
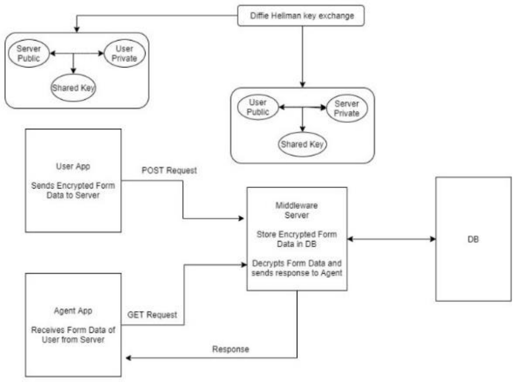
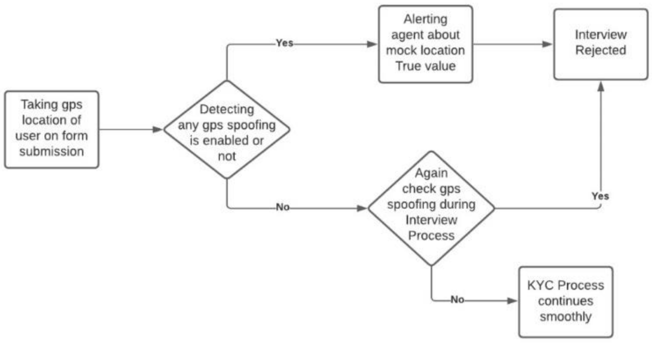


Photo taken during interview process via screenshot
Database
App
POST Request
Server
ID Face Match Model
Result in the form of probablity
Photo of the user from ID card

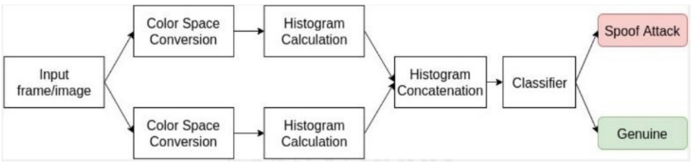
6.2 Encryption Flowchart


Diffie Hellman key exchange
Server Public
User Private
Shared Key
User Public
Server Private
Shared Key
User App
Sends Encrypted Form Data to Server
POST Request
Middleware Server
Store Encrypted Form Data in DB
Decrypts Form Data and sends response to Agent
DB
Agent App
Receives Form Data of User from Server
GET Request
Response

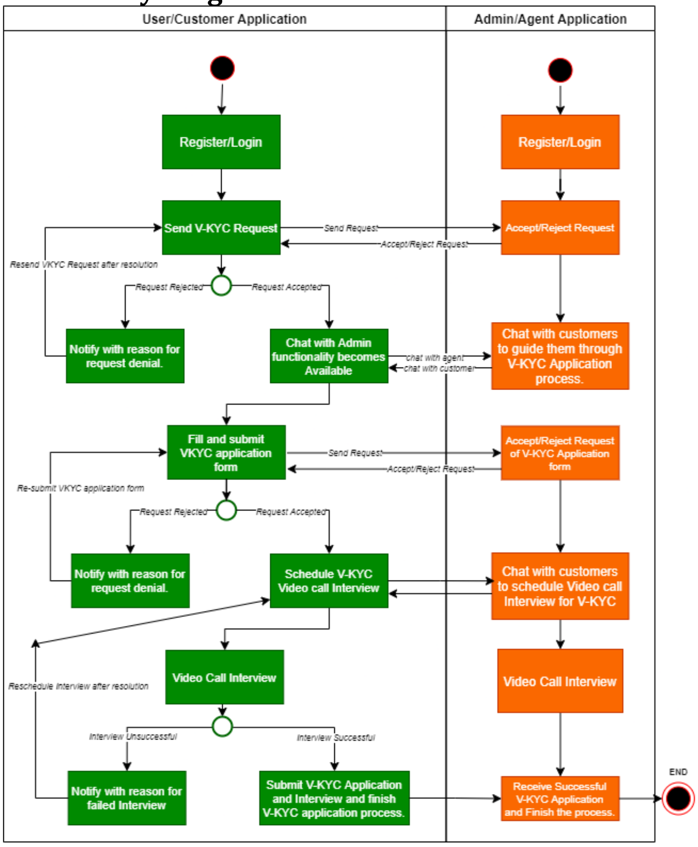
6.3 Geo-Coding Flowchart


Taking gps location of user on form submission
Detecting any gps spoofing is enabled or not
Yes
Alerting agent about mock location True value
Interview Rejected
No
Again check gps spoofing during Interview Process
Yes
No
KYC Process continues smoothly

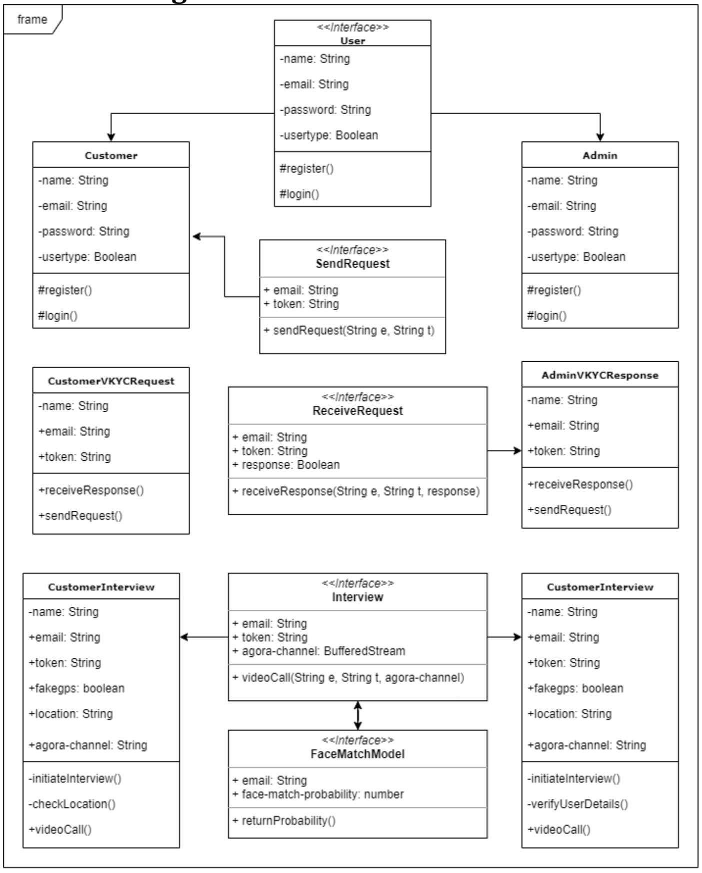
6.4 Spoofing Flowchart



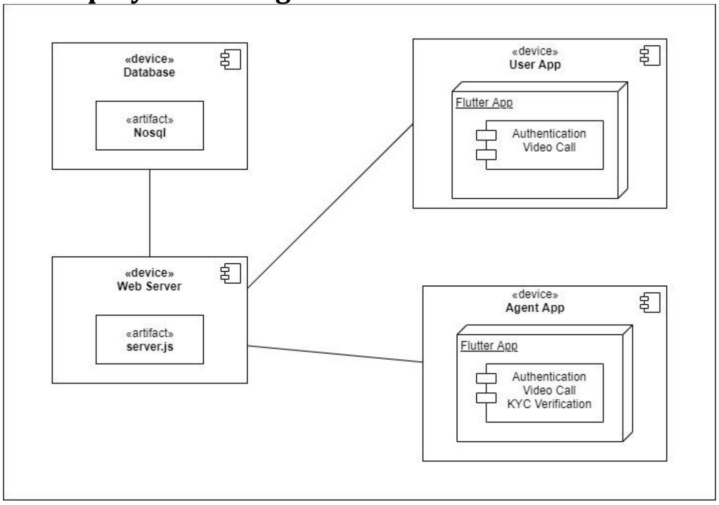
6.5 Activity Diagram


User/Customer Application
Admin/Agent Application
Register/Login
Send V-KYC Request
Send Request
Accept/Reject Request
Resend VKYC Request after resolution
Request Rejected
Request Accepted
Notify with reason for request denial.
Chat with Admin functionality becomes Available
chat with agent
chat with customer
Fill and submit VKYC application form
Send Request
Accept/Reject Request
Re-submit VKYC application form
Request Rejected
Request Accepted
Notify with reason for request denial.
Schedule V-KYC Video call Interview
Video Call Interview
Reschedule Interview after resolution
Interview Unsuccessful
Interview Successful
Notify with reason for failed Interview
Submit V-KYC Application and Interview and finish V-KYC application process.
Register/Login
Accept/Reject Request
Chat with customers to guide them through V-KYC Application process.
Accept/Reject Request of V-KYC Application form
Chat with customers to schedule Video call Interview for V-KYC
Video Call Interview
Receive Successful V-KYC Application and Finish the process.
END

6.6 Class Diagram



6.7 Deployment Diagram



7. MODULES

The application comprises the following major modules:

1. **Register Module:** Register Module contains the registration of users and agents. In this module, we have two separate sections for agent and user.

a. **Agent section:** Agent has to fill in necessary details about their organization eg: bank, to get registered on the platform. These details are then verified by the admin. After verification, the agent can start the video KYC process.

b. **User Section:** The user has to fill in personal details about him/her like Pan card, Aadhar card, to get registered on the platform. After user details verification, the user can request the video KYC process.

2. **Form Module:** Before filling the form, the following steps are performed:-

a. If the user's camera is not up to certain megapixels with bad video quality or can't detect a person in the video frame then the user will be alerted accordingly.

b. User will be requested to access the location and to check if the user is in India or not (If not alert accordingly and the process is closed)

c. Along with user location also check user IP address and check if the user is not using VPN or any other spoofing techniques (if any spoofing recognized alert accordingly)

d. Before the interview begins to check if the person in the video matches the face in both the Latest photo uploaded and photo on Pan-card (Using face detection models with neural networks that also, recognize age-separated faces) uploaded while registering.

e. Identification details in Aadhaar/PAN shall match with the details provided by the customer.

3. **Liveness Detection Module:** Liveness Detection of the user to block Presentation Attacks on the process: In most cases, the eye blinking rate in fake videos is slower or extremely faster than the normal person blinking rate. This enables the detection of fake videos from real videos by using an eye blinking rate.

4. **Deep Face Detection Module:** While the user is giving the interview and liveness detection is running during the whole process, the Deep Fake detection model will be continuously checking for any signs or patterns of deep fakes. If the detected KYC process will be terminated. And bank authorities will be warned accordingly. The deep fake detection technique uses the audio-visual dataset to detect inconsistencies between lip movements, speech, and numerous differences of slow images. Recurrent Neural Network(RNN) to discover temporal discrepancies across frames and Long Short-Term Memory (LSTM) for temporal sequence analysis

8. CONCLUSIONS

Our project Secure video KYC is an outcome of current emerging need. We believe various banks and regulated entities can greatly benefit from our application in the current scenario as well as in long run in secure onboarding their customers while also maintaining integrity and authenticity of the entire process.

9. ACKNOWLEDGEMENT

We owe sincere thanks to our college Atharva College of Engineering for giving us a platform to prepare a project on the topic "**Secure Video KYC**" and would like to thank our Principal **Dr. Shrikant Kallurkar** for instigating within us the need for this research and giving us the opportunities and time to conduct and present research on the topic. We are sincerely grateful for having **Prof. Shweta Sharma** as our guide and **Prof. Suvarna Pansambal**, Head of Computer Engineering Department, and our project co-ordinators **Prof. Samidha Kurle** during our research to help specially-abled children and contribute towards, which would have seemed difficult without their motivation, constant support and valuable suggestions. Moreover, the completion of this research would have been impossible without the cooperation, suggestions, and help of our friends and family.

REFERENCES

1. Face Spoofing Video Detection Using Spatio-Temporal Statistical Binary Pattern
2. An Anomaly Detection Approach to Face Spoofing Detection: A New Formulation and Evaluation Protocol
3. Multiple Face Detection and Recognition System Design Applying Deep Learning in Web Browsers using JavaScript
4. Face Recognition Based on Euclidean Distance and Texture Features
5. Key Management Using Combination of Diffie–Hellman Key Exchange with AES Encryption
6. https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11783&Mode=0
7. https://pub.dev/packages/agora_rtc_engine
8. https://firebase.google.com/docs/ml-kit/detect-faces
9. https://pub.dev/packages/flutter_face_detection

10. https://www.agora.io/en/blog/add-real-time-video-to-your-flutter-apps-using-the-agora-flutter-sdk/
11. https://medium.com/@mundorap2010/face-detection-with-tflite-model-without-firebase-in-flutter-6eadf888f3b0
12. https://www.sciencedirect.com/science/article/pii/S016740480600215X
13. http://adityakhedekar.me/