

**Basic Information**

Name	: TEJAS FULZELE	CCPP ID : PB0109
Course	: PG-DBDA, Aug 25	
Address	: Indira Nagar Ward no 4, At post Gondpipari, Ta. Gondpipari, Chandrapur, MAHARASHTRA	

**PG-DBDA Marks**

S.NO.	Module	Maximum Marks (Theory)	Obtained Marks
1	Data Collection & DBMS	40	29
2	Java Programming	40	29
3	Python & R Programming	40	34
4	Advanced Analytics and Statistics	40	30
5	Data Visualization - Analysis and Reporting	40	37
6	Big Data Technologies	40	38
7	Linux Programming and Cloud Computing	40	32
8	Practical Machine Learning	40	37
<b>Total</b>		<b>320</b>	<b>266</b>

**Academic Details**

Level	Stream	Institute	Board/University	Passing Year	Degree %	Division
BE	Information Technology	SINHGAD COLLEGE OF ENGINEERING PUNE, VADGAON BUDRUK	Savitribai Phule Pune University	2025	71.28 %	I
XII	Science	JAWAHAR NAVODAYA VIDYALAYA CHANDRAPUR	CBSE	2020	77.2 %	I
X	General	JAWAHAR NAVODAYA VIDYALAYA CHANDRAPUR	CBSE	2018	89.33 %	I

**Academic Projects**

Title	: AI MEETING MINUTES GENERATOR	
Platform	: Python	<b>Duration : 1 Month</b>
Description	: AI Meeting Minutes Generator and Action Item Tracker automatically converts meeting audio into structured insights. The system performs speaker diarization to identify who spoke when, followed by speech-to-text transcription for each speaker. The transcribed text is merged, cleaned, and summarized using an abstractive model to capture key discussions and decisions. An agentic AI model then extracts bullet points and action items with relevant details. It reduces effort and improves productivity.	
Project Repository	: <a href="https://github.com/tejasfulzele13/PG-DBDA_ML_Project">https://github.com/tejasfulzele13/PG-DBDA_ML_Project</a>	
 Title	 : Smartshield: Dual Phase ML Defense For IoT Botnet Threats	
Platform	: Python	<b>Duration : 12 Months</b>
Description	: SmartShield is an intelligent, lightweight security system designed to detect and prevent IoT botnet attacks using a two-phase (dual-phase) machine learning defense architecture. The goal of the project is to address the growing vulnerabilities in IoT devices such as smart cameras, smart meters, sensors, routers, and home appliances which are frequently targeted by botnets for DDoS attacks, credential theft, and large-scale network exploitation.	
Project Repository	: <a href="https://github.com/tejasfulzele13/BE_Project">https://github.com/tejasfulzele13/BE_Project</a>	

## **Other Information**

---

<b>LinkedIn</b>	: <a href="https://www.linkedin.com/in/tejas-fulzele-808252246/">https://www.linkedin.com/in/tejas-fulzele-808252246/</a>
<b>Extra Curricular</b>	: Project Topic-IPL Match Analytics Using Apache Spark[" <a href="https://github.com/tejasfulzele13/PG-DBDA_Big_Data_Project">https://github.com/tejasfulzele13/PG-DBDA_Big_Data_Project</a> "], Captained College Cricket Team
<b>Hobbies</b>	: Playing Cricket, Reading books on history and social development, Watching web series during leisure time.

## **Personal Information**

---

<b>Date of Birth</b>	: 13/09/2002	<b>Gender :</b> Male
<b>Nationality</b>	: Indian	<b>Languages Known :</b> English,Hindi,Marathi

I hereby declare that the information given above is true to the best of my Information knowledge belief.

**Date** : **Signature :**

P\_DI\_08