Six Weeks Industrial Training Project Report On

On

“Honeypot”

Submitted in complete fulfillment of the requirement for the award

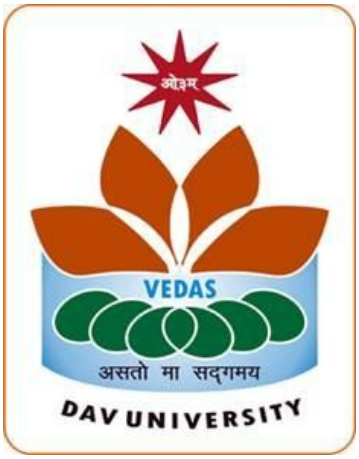
of degree of

Bachelor of Technology

in

Computer Science and Artificial Intelligence

Batch (2022-2026)



Submitted to:

Er. Bindu Goyal

Assistant Professor (CS Department)

Submitted by:

Ujjwal Sharma

12200145

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

DAV UNIVERSITY

JALANDHAR-PATHANKOT NATIONAL HIGHWAY NH 44,

SARMASTPUR PUNJAB

144012

ACKNOWLEDGEMENT

I express my gratitude to all those who helped us in various stages of the development of this project. First, I would like to express my sincere gratitude to Er. Bindu Goyal (Assistant Professor) of DAV University for allowing me to undergo the summer training of 45 days at O7 Services. I am also thankful to all faculty members of the Department of Computer Science and Engineering, for their true help, inspiration and for helping me for the preparation of the final report and presentation.

Last but not least, I pay my sincere thanks and gratitude to all the Staff Members DAV University for their support and for making our training valuable and fruitful.

DECLARATION

I, Ujjwal Sharma, hereby declare that the work which is being presented in this training titled "**Honeypot**" by me, in partial fulfilment of the requirements for the award of Bachelor of Technology (B.Tech) Degree in "Computer Science and Artificial Intelligence" is an authentic record of my own work carried out under the guidance of Mohit Mittal. To the best of my knowledge, the matter embodied in this report has not been submitted to any other University/ Institute for the award of any degree or diploma.

Ujjwal Sharma

(12200145)

ABSTRACT

Cybersecurity threats are increasing rapidly as attackers continuously search for vulnerable systems to exploit. Traditional security mechanisms focus mainly on detection and prevention, offering limited visibility into the behavior, techniques, and motives of malicious actors. To address this gap, honeypots serve as an effective defensive strategy by creating controlled decoy systems that intentionally attract attackers and record their activities for analysis.

This project presents the development of a **Python-based Multi Honeypot System** designed to study unauthorized access attempts, malicious interactions, and suspicious user behavior in a safe and isolated environment. The honeypot simulates a vulnerable web application using **Flask**, offering trap interfaces such as a fake login page, admin probe page, and file upload functionality. All interactions are captured and stored in a **SQLite database**, creating a structured dataset of attack logs for further interpretation. Additional features include a web-based dashboard for viewing logs, a CSV export system for report generation, and a modular architecture enabling easy customization.

The system was entirely executed and tested on my personal machine through the terminal, ensuring complete safety and isolation while replicating realistic attack scenarios. Through this project, I gained hands-on experience in backend development, database management, logging systems, cybersecurity defense strategies, and attacker behavior monitoring.

The honeypot successfully demonstrates how deception techniques can be used to understand cyber threats more deeply. It provides a lightweight, practical, and extendable platform for educational research, threat analysis, and cybersecurity skill development. This project, completed during my six-week industrial training at **TCIL-IT Chandigarh**, reinforces the importance of monitoring, logging, and analyzing malicious activities to strengthen modern cybersecurity defense mechanisms.

CERTIFICATE

Telecommunications Consultants India Ltd. - Information Technology

Ref. No. TCIL-IT/Trng./2024/8709 Date: 28th October, 2025

To Whom It May Concern

This is to certify that **Mr. Ujjwal Sharma S/o Sh. Sanjiv Sharma, University Roll No. 12200145 of D.A.V. University, Jalandhar (Punjab)** has successfully completed his six weeks Industrial training in **Cyber Security** from **5th June, 2025 to 20th July, 2025** During his tenure, he was actively involved with our development team and worked on the project title "**Honeypot (Multiple)**".

It is further certified that the work done during this period is a result of candidate's own effort.

We wish him all the best for upcoming future.

Head – Training & Development

TABLE OF CONTENTS