# OpenClaw / MoltBot Workshop Documentation

## 1. Introduction

OpenClaw (formerly Clawdbot and MoltBot) is an open-source AI agent framework designed to build autonomous agents that can perform real-world tasks such as executing code, calling APIs, and managing workflows. This documentation summarizes the workshop learnings and best practices.

## 2. Tech Stack Overview

• GitHub – Source code management and version control
• OpenRouter – Unified access to multiple LLM providers
• LLM Models – GPT, Gemini, Claude, LLaMA, DeepSeek, Grok
• Docker & Linux VM – Secure deployment environment
• Telegram Bot – User interaction layer

## 3. Chatbot vs AI Agent

Chatbots are limited to generating text, code, images, or video scripts. AI agents like OpenClaw go a step further by executing code, interacting with systems, and creating complete products autonomously.

## 4. OpenClaw Architecture

OpenClaw follows a skills-based architecture. Skills are written in Markdown and may include executable code. Agents use a gateway to invoke these skills, often with system-level access. This allows powerful automation but introduces security risks if not controlled.

## 5. Telegram Bot Integration (POC)

Telegram acts as the front-end interface. User messages are sent via webhooks to the OpenClaw gateway, which processes the request using LLMs and skills, then sends responses back to Telegram.

## 6. Adoption and Community Signals

OpenClaw has gained massive attention with over 138,000 GitHub stars and 20,000+ forks. High fork activity indicates developers actively modifying and securing the codebase for production use.

## 7. Security Considerations

Security researchers reported thousands of exposed OpenClaw instances with authentication bypass issues. Since skills can execute shell commands, improper deployment may lead to credential leaks or system compromise.

## 8. Best Practices for Safe Usage

• Never install OpenClaw on a personal machine
• Use Docker containers or isolated Linux VMs
• Enable authentication and firewall rules
• Avoid executing unverified remote skills
• Regularly update and pin versions

## 9. Recommended Deployment Options

Preferred environments include Docker containers, cloud-based Linux VMs (AWS, GCP, Azure), or VPS providers like Hostinger and GoDaddy with proper isolation.

## 10. Conclusion

OpenClaw is a powerful AI agent framework suitable for advanced users who understand infrastructure and security. When deployed responsibly, it can enable highly autonomous AI-driven products.