





IMT Atlantique
Département Pays de la Loire
Ecole Mines Télécom

Hardware Trojan ML Based Security Model for DNN Accelerators (FALCON)

Security for AI Hardware - ULFG - 2025-11-

PhD Student: Abdel Salam BALTAGI

Supervisors: Yehya NASSER, Associate professor, Principle Investigator (PI)

Amer BAGHDADI, Professor, Co-PI, Thesis Director



IEEE

Advancing Technology
for Humanity

ULFG1
Student branch



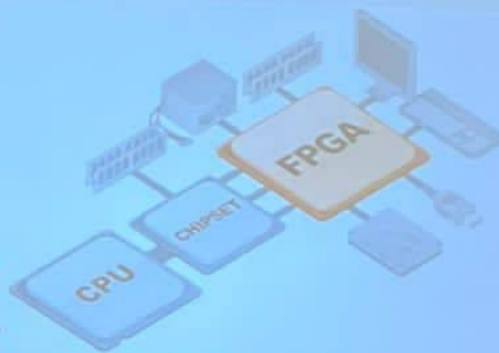
IEEE

Advancing Technology
for Humanity

CLUB
G 1

Model Specific AI Accelerators

Real systems combine different hardware IPs



Advancing Technology
for Humanity

ULFG1
Student branch



AI CLUB
ULFG1



IEEE

Advancing Technology
for Humanity



47:34

Chat People Raise React View More Camera Mic Share Leave

 Maria Wakim	 Chalak Chalak	 Hiba DIAB (Unverified)	 omar khaled (Unverified)
 Amani RAAD (Unverified)	 Abdel-rahman Makkawi	 Georgios Semaan	 Ahmad ali (Unverified)
 Makhlouta NAIM (Unverified)	 Larissa Elia	 salimf765kr	 Habib Nooman (Unverified)
 Majd Almasri	 Tarek (Unverified)	 Rihab Omar	 jihadkassar96

< 1/3 >



Search



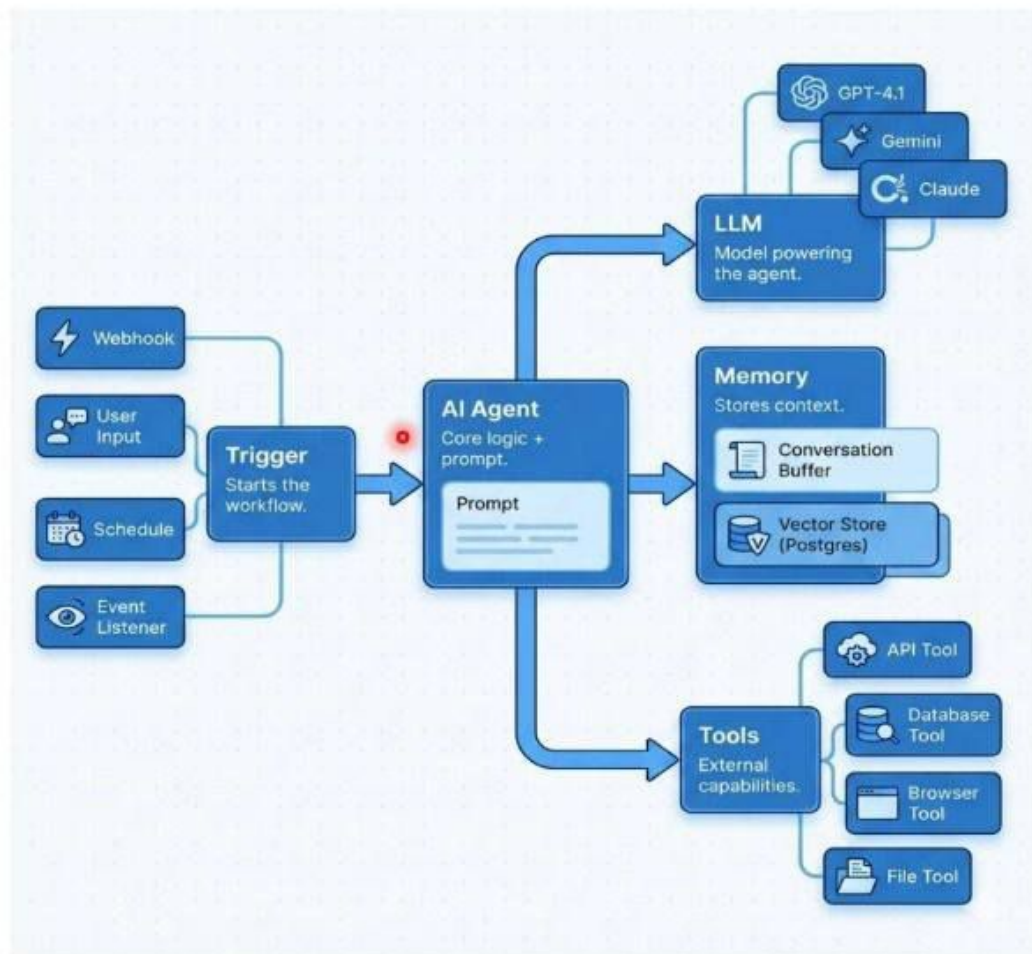
ENG



4:11 PM

11/21/2025

Simple Base Template



HD

Hiba DIAB

CC

Chalak Chalak

Makhlouta NAIM

AR

Amani RAAD (Guest)

1/10

OK

Live quiz(3/5)

13 / 18



How do we connect an AI agent to external tools?

By installing tools inside the LLM itself

0%

By exporting the LLM as a file to the tool

8%

By sending API requests to tool integrations

92%

Reveal answer



Next

AI agents

Show Q&A



teams.microsoft.com is sharing your screen.

Stop sharing

Hide

Amani RAAD (Unverified)



Search



Search



< 1/4 >

LLM VS AI Agents

Large Language Model (LLM) Explained

What is an LLM?

A model designed to understand and generate text.

Can it act independently?

No, it responds to prompts but does not act independently.

What actions can it perform?

It is limited to performing only the actions it is explicitly instructed to do.



3

HD

Hiba DIAB

CC

Chalak Chalak

Makhlouta NAIM

AR

Amani RAAD (Guest)

< 1/10 >

OK

Agentic AI in Action:

From n8n Workflows to a Full RAG Agent

In Collaboration with : AI Club ULFG1

Presented by : Naim Makhlouta



HD

Hiba DIAB

CC

Chalak Chalak

Makhlouta NAJM

Amari RAAD (Guest)

< 1/10 >

OK



wall.sli.do/event/31U2gJnHqCt6d64L773M6R?section=2af10b0f-3f16-4337-9636-28d6cfd83858

Active poll

8



What comes to your mind when we say Artificial Intelligence or AI agents?

Control systems that use ai to take action automatically improve perform

ChatGpt Reasoning entities achieve decisions make

goal—almost systems

assistant digital process Gemini software smart

agents input autonomous simulation of human intelligence processes by machines

Hene intelligent virtual assistant actions AI

Deepseek environment

teams.microsoft.com is sharing your screen. Stop sharing Hide

Join at
slido.com
#3580 377

HD

Hiba DIAB

CC

Chalak Chalak

Makhlouta NAIM

Amani RAAD (Guest)

1/10

OK

01:31:06



Elapsed time 01:31:06

wall.sli.do/event/31U2gJnHqC16d64L773M6R?section=2af10b0f-3f16-4337-9636-28d6cfd83858

Leaderboard



Join at
slido.com
#3580 377



Congratulations, lyne chaar!

#1	lyne chaar	5/5	0:36
#2	Omar khaled	5/5	0:51
#3	Habib Nooman	5/5	0:52
#4	Chalak	5/5	0:54
#5	Judy Ankoud	5/5	1:04

69%

in automation?

teams.microsoft.com is sharing your screen.

Stop sharing

Hide

Amani RAAD (Unverified)



Search



Search



ENG

4:55 PM
11/21/2025

10:24

Take control | Stop all | Chat | People | Raise | React | View | More | Camera | Mic | Share | Leave

← Edit ↻ 🗑️ 📄 🖼️ 🎥 ... WhatsApp Image 2025-11-21 at 3.20.41 PM.jpeg

🌈 📱 🎨 🖌️ 🗑️

— ✎ ✕



CC
Chalak Chalak ...

HD
Hiba DIAB ...

AR
Amani RAAD (Guest) ...

MW
Maria Wakim (Guest) ...

< 1/2 >

OK

AI Study Assistant (RAG Chat)

Purpose: Conversational AI that helps you study by answering questions from your uploaded documents.

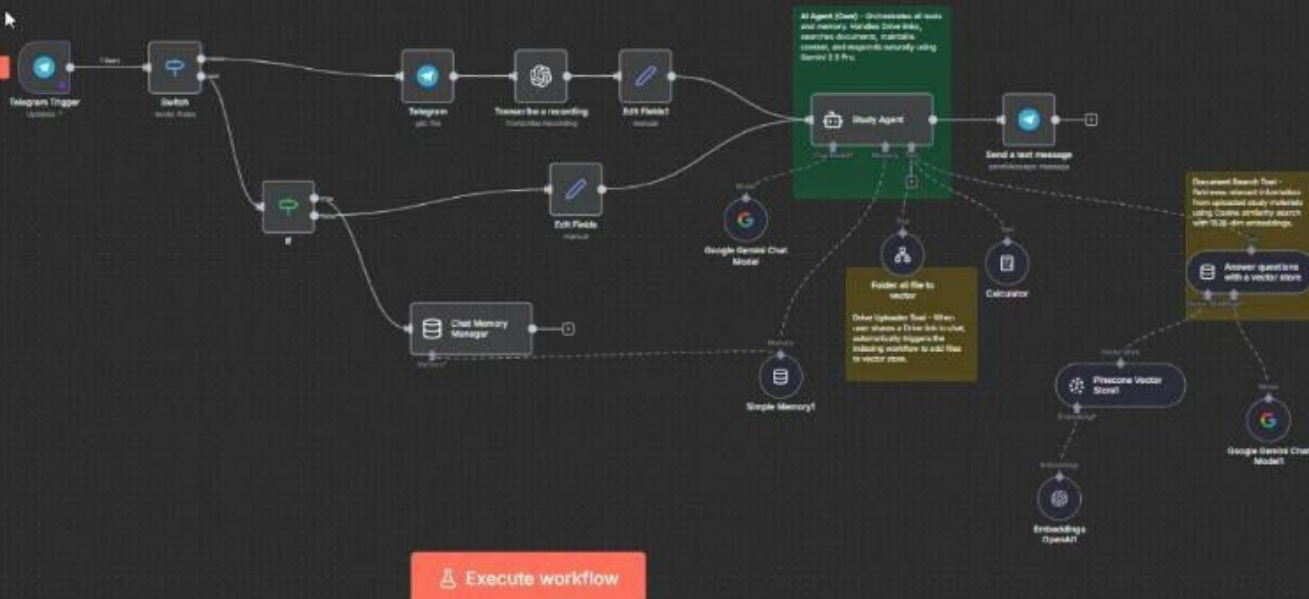
Flow: Chat Input → AI Agent → Vector Search → Memory → Tools → Response

Key Features:

- Natural conversation with you or study materials
- Auto-processes Drive files uploaded to chat
- Custom similarity search across documents
- Persistent chat memory
- Calculator for math problems

Tools Connected:

- Proccess Vector Store (document upload)
- Drive Folder Uploader (auto index new files)
- Calculator (math operations)



Execute workflow

HD

Hiba DIAB

CC

Chalak Chalak

MN

Makhlaouta NAIM

AR

Amani RAAD (Guest)

1/8

OK

Automations & Workflows (Graphs)

- Automations use software or AI to perform tasks automatically without human intervention.
- They rely on workflows—visual graphs showing how a process moves step by step.
- Each node represents an action (fetching data, transforming it, deciding, sending messages...).
- Connections show how information flows through the process.



Live quiz(5/5)

15 / 18



What solution does RAG provide?

It improves GPU speed for LLM training

0%

It gives the AI access to external unseen data without retraining

100%

It replaces the LLM with a search engine

0%

Reveal leaderboard



AI study Assistant - n8n test data - Google Drive

naim1000.app.n8n.cloud/workflow/PHjqhXixzLTACsn/executions/86

Back to canvas

INPUT Schema Table JSON

Edit Fields

Execute previous nodes to view input data

Edit Fields1 1 item

Switch 1 item

Transcribe a recording 1 item

Telegram Trigger 1 item

Telegram 1 item

Variables and context

Study Agent Parameters Settings Docs

Tip: Get a feel for agents with our quick tutorial or see an example of how this node works

Source for Prompt (User Message)

Define below

Prompt (User Message)

```
[[{"text": "input"}]]
```

Yeah, so can you tell me how does what are the best practices while

Require Specific Output Format

Enable Fallback Model

Options

System Message

```
# Role & Scope
You are a Study AI Assistant that helps users explore only the engineering-related study materials stored in the vector database (Pinecone). Do not use outside knowledge or discuss non-engineering topics.
```

Chat Model* Memory Tool

Output Logs Schema Table JSON

1 item

```
"output": "Best Practices for Crafting a System Prompt\n\nCrafting an effective system prompt is crucial for designing robust AI agents. Here are key best practices:\n\n1. Define the Global Role of the Agent: Clearly state the agent's overarching purpose, domain expertise, and limitations.\n\n2. Example: \"You are a professional AI assistant specialized in [domain]. Your role is to handle multi-step workflows, make decisions autonomously, and use available tools effectively while adhering to brand tone and guidelines.\"\n\n3. Establish Goals & Context: Provide clear business objectives. Define primary audiences and their details. Include service or product scope. State tone and personality guidelines. Outline tool usage criteria (when and how to use each tool).\n\n4. Detail Workflow & Process: Include steps like: 1. Understand request. 2. Determine required tools. 3. Plan response. 4. Execute tool calls. 5. Reflect and validate.\n\n5. Integrate Chain of Thought Prompts to encourage step-by-step reasoning. Add Persistence Reminders to ensure task completion. Outline Error Handling for missing information, tool errors, or
```

I wish this node would...

Logs

Makhlouta NAIM (Unverified)

Search

1/3



Security for AI Hardware

DISCOVER THE FUNDAMENTALS OF HARDWARE SECURITY AND LEARN HOW AI-DRIVEN APPROACHES ARE SHAPING THE FUTURE OF SECURE SYSTEMS.

20 THURSDAY
NOVEMBER

AT 12:00 PM

FLOOR -2

KEY TOPICS

- ✓ **Cybersecurity: More Than Just Networks**
- ✓ **AI accelerators**
- ✓ **Hardware attacks and hardware Trojan**
- ✓ **Securing HW using power consumption**

Abdelsalam Baltagi
Engineer and PhD student



@abed.baltaji



Abdelsalam Baltagi





AGENTIC AI IN ACTION



With:

Naim Makhoulta



Friday November 21st



4:00 pm till 5:30 pm



online session!

Don't miss this deep dive from n8n workflows to a full RAG agent!