**GUNASEKARAN M**
**AI Architect | ML | Gen AI | Responsible AI | Advanced Prompting | RAG | MLOps | Computer Vision | Cybersecurity | Unix | Expert in Building Secure, High-Performance AI Solutions**
**Mobile: +91-9791062871 | Email: gunasekaran81m@gmail.com**
**LinkedIn: linkedin.com/in/gunasekaran-m-38798452**

With 21+ years in IT, I am a seasoned Project Designer and AI Architect specializing in Unix systems, cybersecurity, and artificial intelligence. My expertise spans Machine Learning (ML), deep learning architectures (CNNs), advanced AI techniques, and Responsible AI. I bridge technical precision with strategic insights to design secure, high-performance AI solutions that drive measurable impact.

Armed with a Master's in Software Systems from BITS Pilani, I am committed to future-proofing AI and IT projects, ensuring they remain innovative, scalable, and resilient in the face of evolving industry challenges.

## ***Key Areas of Expertise***

AI & Machine Learning – Deep expertise in TensorFlow, PyTorch, CNNs, NLP, Transformers, Unsloth, Groq, FT LLM, GenAI, Langchain, LlamaIndex, NeoGraph, LangGraph, Agents and Large Language Models (LLMs).
MLOps & AI Deployment – Proficient in MLflow, Kubeflow, Vertex AI, and model fine-tuning, training, and monitoring.
Unix & Cybersecurity – Advanced knowledge of Unix systems, infrastructure security, and high-availability architectures.
Cloud & API Integration – Skilled in Azure, AWS, GCP, OCI, and scalable AI deployments using Gradio, FastAPI, and VectorDB (Pinecone, FAISS, ChromaDB).
Responsible & Ethical AI – Strong focus on bias mitigation, AI fairness, SHAP, LIME, XAI and implementing secure AI governance frameworks.
AI Security & Compliance – Expertise in MLSecOps, ModelScan, LLM Pen Testing, and ensuring adherence to GDPR, HIPAA, and ISO frameworks.
Threat Intelligence & Risk Management – Experience with IOC, Darktrace, SentinelOne, GitHub Security Tools, and penetration testing for AI models.
Benchmarking & Evaluation Tools – MMLU, BLEU, ROUGE, BERTScore, Drop, Winog, Hswag

## ***AI Leadership & Development***

Architected and deployed custom AI solutions that reduced operational costs by 23% and increased prediction accuracy by 17% across key business functions
Spearheaded weekly technical architecture discussions and established AI best practices documentation adopted by 4 departments, resulting in standardized development processes
Partnered with cross-functional teams (Product, Marketing, Operations) to transform complex business requirements into detailed technical specifications, reducing implementation time by 30%
Engineered a suite of scalable NLP and computer vision models processing 500,000+ daily transactions with 99.7% uptime
Implemented quarterly technology reviews to evaluate emerging AI frameworks, resulting in the adoption of 3 cutting-edge technologies that improved model performance by 28%
Established comprehensive AI governance frameworks ensuring ethical implementation and compliance with GDPR and industry-specific regulations
Mentored a team of 5 junior data scientists and AI engineers
Delivered monthly data-driven presentations to C-level executives, translating complex technical
Engineered machine learning solutions on Snowflake cloud data platform, optimizing processing workflows for 1,000TB of enterprise data
Developed complex SQL queries and stored procedures to transform raw data into actionable insights supporting critical business decisions

Created interactive PowerBI and Tableau dashboards that visualized key performance metrics, increasing data accessibility for non-technical stakeholders
Implemented LIME and SHAP frameworks to enhance model interpretability, providing transparent explanations of AI decision-making processes to compliance teams
Established robust MLSecOps practices that reduced security vulnerabilities in production models by implementing automated scanning and continuous monitoring
Utilized ModelScan to identify and remediate potential weaknesses in ML pipelines, ensuring data integrity and model reliability
Led AI systems through successful SOC compliance assessments and ISO audit frameworks, achieving certification with minimal remediation requirements
Implemented comprehensive vulnerability scanning using Nessus and OpenVAS to secure AI infrastructure and ML pipelines
Deployed self-learning AI security solutions (Darktrace, IBM Watson) for proactive threat detection, reducing false positives by 35%
Utilized MISP and YETI platforms for predictive threat intelligence, enabling early detection of potential attacks
Established robust methodologies to identify and mitigate AI model bias in historical training data
Developed AI governance frameworks ensuring ethical implementation and compliance with GDPR, HIPAA, and industry regulations
Led penetration testing initiatives specifically targeting AI systems to identify and remediate security vulnerabilities
Implemented countermeasures against emerging threats including deepfakes, AI-powered malware, and advanced phishing

***Projects Implemented***

**Object Detection in Image & Video**
we are utilizing the surveillance system capability of scanning the workshop floor and identify the potential security incidents using YOLO11n,RoboFlow,OpenCV,Pillow,DarkNet,ServiceNow,EmailIntegration,Gradio.
**MCQ Generation for Assessment**
Developed a system for generating multiple-choice questions for Linux, security, and network assessment using RAG, PYPDF, LAMA2, OpenAPI, JSON, Gemini, vertexAI and Moodle.
**Ticketing Tool Chatbot**
Designed a chatbot for managing knowledge bases and internal processes using OLAMA, FastAPI-Uvicorn.
**Email Spam Filtering**
Built an advanced spam filter utilizing BERT on Dataset collected from sentinel and firewall logs with a deployment on Uvicorn.
**ISO Audit Checker**
Created an ISO audit checker using RAG, VectorDB, PyPDF, LAMA2,VertexAI, Gemini Flask to streamline compliance reviews.
**Machine Learning & Predictive Analytics**
Built ML models on Snowflake (1000TB) using Random Forest, Decision Trees, GridSearchCV for optimization. Applied Confusion Matrix for evaluation and developed AI-driven defect analysis frameworks for anomalydetection.

***Recent Use Case***
**Restaurant Recommendation Engine**
Engineered a recommendation tool with Azure OpenAI, SerpAPI, Gemini, Function Calls, Moderation Check, Flask.

**Travel Advisory Platform**
Developed a travel advisory platform with Azure OpenAI, SerpAPI, Gemini,Function Calls, Streamlit for customized itineraries.

***Experience Summary:***

**Hexaware Technologies Ltd.**
May 2015 – Present
Project Delivery Design - Architect | AI | ML | Gen AI | MLOps | Responsible AI | Unix | Cybersecurity

- Enterprise Architecture & Infrastructure Design
  - Defined technical requirements and led data center management, including server, storage, and infrastructure sizing.
  - Designed and implemented load balancing and clustering solutions aligned with architectural standards.
  - Spearheaded a zero-downtime data center migration project.
  - Reduced operational costs by transitioning proprietary systems to open-source solutions.
  - Developed disaster recovery (DR) solutions and recovery plans for mission-critical systems.
- AI/ML & Emerging Technologies
  - Architected and developed solutions across AI/ML, Computer Vision, NLP, VectorDB, and LLM fine-tuning.
  - Recommended best practices in Responsible AI and MLOps for enterprise clients.
  - Conducted research, evaluation, testing, and implementation of AI-driven solutions.
- Technical Implementations & Migration
  - Migrated Windows file server to an open-source NAS solution (Nas4Free).
  - Transitioned physical OEL servers to RHEL VMs, optimizing performance and scalability.
  - Led the implementation of Nutanix for high-performance virtualized infrastructure.
- Infrastructure & Cybersecurity Expertise
  - Implemented Oracle Secure Backup, Sun Fire x4470M2, ODA 2HA, and Exadata (Half & Quarter Rack).
  - Managed storage solutions including HP 3PAR 7200, Dell EqualLogic PS6110, Storage SL150, and EMC Iomega px12-350r.
  - Coordinated with DB, storage, and networking teams to ensure seamless IT operations.
  - Provided support for internal and external audits, ensuring compliance and security best practices.
- Leadership & Process Optimization
  - Led knowledge transfer & mentoring programs for Unix and cross-functional teams.
  - Handled escalation calls, root cause analysis (RCA), and issue resolution to maintain system stability.
  - Contributed to RFP (Request for Proposal) processes, helping secure strategic business deals.
  - Managed DCC (Data Center Consolidation) migration activities, streamlining infrastructure efficiency.

**Nov 2010 - May2015: Associate Consultant at HCL Technologies Ltd -Chennai**
**Oct 2009 - Nov 2010: Sr. Software Engineer at L&T InfoTech - Bangalore**
**July 2007 - October 2009: Customer Support Engineer at Mukesh Info serve Pvt Ltd,**
**June 2003 - July 2007: System Administrator at Vinodh Computers, Chennai**

***Educational Qualification***

- Master's in software systems at Birla Institute of Technology and Science, Pilani in the year 2012.
- Bachelor of Engineering in Electronics and Communication at Jaya Engineering College, Chennai in the year 2003.

***Professional Certifications & Learnings Completed:***

***AI/ML/DL/CNN/GenAI***

- Sonic-High-Level Abstraction of Technology Nuances on Generative AI
- Sonic- Generative AI for Aspiring Architects
- ISRO - AI/ML for Geodata Analysis
- Upgrad- GEN AI Architects
- Coursera – AI For Everyone
- Microsoft-Azure AI Fundamentals: Generative AI
- Microsoft-Fundamentals of Responsible Generative AI
- Microsoft-Fundamentals of Generative AI
- Microsoft – AI Genius Series on Production-Ready RAG with Azure AI Search
- Udemy-The Complete 'No-Code' ChatGPT & OpenAI API Course
- Udemy-Generative AI ChatGPT | Google Gemini for Software Engineers
- Udemy-PyTorch for Deep Learning and Computer Vision
- Udemy-Complete Machine Learning, NLP Bootcamp MLOPS & Deployment
- Udemy-Generative AI Course with Langchain and Huggingface
- Udemy- Computer Vision Masterclass
- Udemy- Complete MLOps Bootcamp With 10+ End To End ML Projects
- Udemy- Automated Machine Learning with Auto Gluon Library in Python
- DeepLearning.AI-Building Systems with the ChatGPT API
- DeepLearning.AI-LangChain Chat with Your Data
- DeepLearning.AI-Building Generative AI Applications with Gradio
- DeepLearning.AI-Evaluating and Debugging Generative AI
- DeepLearning.AI-AI Agents in LangGraph
- DeepLearning.AI-Pair Programming with a Large Language Model!
- DeepLearning.AI-Red Teaming LLM Applications
- DeepLearning.AI-Serverless LLM Apps Amazon Bedrock!
- DeepLearning.AI-How Business Thinkers Can Start Building AI Plugins With Semantic Kernel!
- DeepLearning.AI-Carbon Aware Computing for GenAI developers!
- DeepLearning.AI- Getting Started with Mistral!
- DeepLearning.AI-ChatGPT Prompt Engineering for Developer
- DeepLearning.AI-LangChain for LLM Application Development
- DeepLearning.AI-How Diffusion Models Work

***Cybersecurity***

- Udemy- AI Security Bootcamp: LLM Hacking Basics
- Udemy- Developing a Security and Compliance Program with GenAI
- Udemy- ChatGPT for SOC Analyst: Master Cyber Security with AI
- Udemy-Advanced Ethical Hacking: Mastery AI & ChatGPT -Volume 2

- Udemy-Artificial Intelligence & ChatGPT for Cyber Security 2024
- Udemy-Malware Forensics v5:AI &ChatGPT Mastery in Malware Analysis
- EC-Council- Building Resilience with AI- and ML-Driven Cybersecurity Strategies
- EC-Council- AI-Powered Ethical Hacking: Revolutionizing Cybersecurity Defense
- EC-Council- AI and ML in Digital Forensics: The Future of Forensic Investigations
- EC-Council- Harnessing AI for Ethical Hacking: Challenges and Opportunities
- Protect AI - MLSecOps Foundations
- Certified Ethical Hacking – CEHv10

***Data Engineering/Data Science/Data Analyst***

- Snowflake- Hands on Essentials Data Warehouse
- Snowflake- Collaboration, Marketplace & Cost Estimation Workshop
- Snowflake- Hands-On Essentials: Data Lake Workshop
- Snowflake- Hands-On Essentials: Data Engineering Workshop
- Snowflake- Snowflake X GenAI: LLM Functions
- Udemy- Data Architecture for Data Scientists
- Udemy- Data Analysis | SQL, Tableau, Power BI & Excel | Real Projects

***Infrastructure***

- Datacenter – CDCP.
- HP-UX - CSE, CSA.
- HP – APC (Integrity Servers), APP (Enterprise Solutions).
- Citrix – Presentation Server 4.5 and Xen App 5.0 for Windows Server 2003: Administration.
- VMware - vSphere: ICM v5.0, Vcloud 5.0
- Symantec - Veritas - VXVM5.0
- ITIL V3 – Foundation

Place: Chennai
Date:

**(GUNASEKARAN.M)**