Job Title: AI Security Engineer
Work Location : Bangalore, Hyderabad or Chennai preferred (Anyone)
Experience (Relevant) : 8+
Shift Timings : IST Business
Remote / Hybrid : Remote
Start date : ASAP
Client Name: Teachers Insurance and Annuity Association of America (Confidential)

Salary: 22 Lakhs CTC

Top 3 skills which is mandatory : Full stack development (java or like) - Primary, AI (Python or like)- Knowledgeable

Job Duties: AI Security Engineer contributes to the development of horizontal enterprise level security solutions built by "Shared Security Services Engineering" Team.
As a member of the team, you will be responsible for development, deployment, and maintenance of software security solutions to protect AI resources in the enterprise.

Key Responsibilities and Duties :-

• Collaborate with AI/ML and Security architecture teams to understand use case requirements, platform security posture and develop software solutions to protect AI applications
• Design and implement robust security measures to protect AI models from adversarial attacks, prompt injection, and jailbreaking attempts
• Develop data protection mechanisms to prevent data exposure in AI systems
• Create and maintain API services for AI security tools using modern frameworks
• Build and enhance monitoring solutions for AI security posture assessment
• Collaborate with cross-functional teams to integrate security controls into ML/AI workflows
• Implement data loss prevention capabilities for sensitive information across various communication channels
• Document security processes, architecture, and implementation details

Minimum Skills Required:
Work Experience : 8+ Years required

Technology :
Full Stack (Java), React/Angular frameworks, Python or similar programming languages, AI/ML training and inference platforms (e.g., AWS Bedrock, AWS SageMaker), open-source and custom AI/ML models, Data Science tools, Terraform, and Helm charts.

Mandatory Skills:

• 8+ years of full stack development using Java, with hands-on experience in building scalable web applications.
• Strong foundation in machine learning, including model development, training, and integration into production systems.
• Capable of delivering end-to-end intelligent solutions by combining robust backend systems with AI-driven features.
• Experienced with modern frontend frameworks such as React or Angular for creating responsive and user-friendly interfaces.
• 3+ years' experience in API development based on REST, gRPC methodologies using FastAPI, Spring REST or similar frameworks
• 3+ years' experience in development and maintenance of cloud native applications using Kubernetes or other container management solutions
• Experience with development, deployment, performance tuning and maintenance of AI models and applications on cloud platform

Preferred Skills :

• Well versed in Python programming language including unit testing frameworks such as Pytest will be an added advantage.
• Good understanding of OWASP top 10 for AI and CISA guidelines for AI development. Preferrable to have a cybersecurity certification such as CISSP or like
• Understanding of security risks in AI & Gen AI applications related to prompt injection attacks, data leakage, adversarial testing etc.
• Experience with observability frameworks (OpenTelemetry)