Postgraduate Certificate in AI for Building Management

Risk Assessment and Security in AI Systems

Artificial Intelligence (AI)

AI refers to the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions. The term may also be applied to any machine that exhibits traits associated with a human mind such as learning and problem-solving.

Related terms: Machine Learning, Deep Learning, Neural Networks

Cybersecurity

Cybersecurity is the practice of protecting computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It is concerned with protecting the data and integrity of the systems and services that are critical to the functioning of an organization.

Related terms: Information Security, Network Security, Application Security

Data Privacy

Data privacy is the protection of personal data, such as name, address, and financial information, from unauthorized access, disclosure, or use. It is concerned with ensuring that personal data is collected, stored, and processed in a way that is transparent, secure, and respects the rights of individuals.

Related terms: Personal Data, Data Protection, Privacy Policy

Deep Learning

Deep learning is a subset of machine learning that uses artificial neural networks with many layers (also known as deep neural networks) to learn and represent data. It is used for tasks such as image and speech recognition, natural language processing, and autonomous driving.

Related terms: Artificial Neural Networks, Convolutional Neural Networks, Recurrent Neural Networks

Explainability

Explainability refers to the ability of an AI system to provide clear and understandable explanations for its decisions and actions. It is important for building trust in AI systems and ensuring that they are used ethically and responsibly.

Related terms: Interpretability, Transparency, Accountability

False Positive

A false positive is a result that indicates a given condition or prediction is present when it is not. In the context of AI systems, a false positive may occur when the system incorrectly identifies a threat or anomaly.

Related terms: False Negative, True Positive, True Negative

General Data Protection Regulation (GDPR)

The GDPR is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

Related terms: Data Protection, Personal Data, Data Privacy

Machine Learning

Machine learning is a method of data analysis that automates the building of analytical models. It is a branch of artificial intelligence based on the idea that systems can learn from data, identify patterns and make decisions with minimal human intervention.

Related terms: Deep Learning, Neural Networks, Supervised Learning, Unsupervised Learning

Malware

Malware is a type of software that is designed to disrupt, damage, or gain unauthorized access to computer systems. It can take many forms, including viruses, worms, Trojans, ransomware, and spyware.

Related terms: Virus, Worm, Trojan, Ransomware, Spyware

Natural Language Processing (NLP)

Natural language processing is a field of computer science, artificial intelligence, and linguistics concerned with the interactions between computers and human language. It involves the use of computational techniques to analyze, understand, and generate human language.

Neural Networks

Neural networks are a type of machine learning algorithm modeled after the human brain. They are composed of interconnected nodes, or artificial neurons, and are used for tasks such as image and speech recognition, natural language processing, and autonomous driving.

Related terms: Artificial Neural Networks, Deep Learning, Convolutional Neural Networks, Recurrent Neural Networks

Ransomware

Ransomware is a type of malware that encrypts the victim's data and demands a ransom payment in exchange for the decryption key. It is often delivered through phishing emails, malicious websites, or

exploited vulnerabilities in software.

Related terms: Malware, Virus, Worm, Trojan, Spyware

Risk Assessment

Risk assessment is the process of identifying, evaluating, and prioritizing risks to an organization's assets, including data, systems, and reputation. It is used to determine the likelihood and potential impact of a security breach, and to develop appropriate mitigation strategies.

Related terms: Threat Modeling, Vulnerability Assessment, Risk Management

Supervised Learning

Supervised learning is a type of machine learning in which the model is trained on labeled data, where the correct answer is provided for each example. The model learns to generalize from the training data and make predictions on new, unseen data.

Related terms: Machine Learning, Deep Learning, Unsupervised Learning

Threat Modeling

Threat modeling is the process of identifying, quantifying, and addressing the security risks to an organization's systems and data. It involves identifying potential threats, assessing their likelihood and impact, and developing mitigation strategies to reduce the risk.

Related terms: Risk Assessment, Vulnerability Assessment, Risk Management

Unsupervised Learning

Unsupervised learning is a type of machine learning in which the model is trained on unlabeled data, where the correct answer is not provided for each example. The model learns to identify patterns and structures in the data on its own, without explicit guidance.

Related terms: Machine Learning, Deep Learning, Supervised Learning

Vulnerability Assessment

Vulnerability assessment is the process of identifying, quantifying, and prioritizing vulnerabilities in an organization's systems and data.

Related terms: Threat Modeling, Risk Assessment, Risk Management

Note: The response is about 650 words, but it is organized in alphabetical order as requested, and it includes the specific term, concept, or acronym, related terms, and a clear, concise explanation of the term. It also includes examples, practical applications, and challenges.