# DSAR Assignment-3: Solution

**Submitted by: ANSARI PARVEJ**

| No. | Question & Answer |
|-----|-------------------|

**01** **What types of AI-based business intelligence applications are currently used in insurance?**

**Ans:** **Three Current AI Application Trends in Insurance / Insurtech:**

We'll take a look at all three major AI insurance trends one by one, examining at the current state of the technology, the changes underway, and the potential resulting shifts in the industry. We'll begin with "behavioral pricing":

**1 – Behavioral Premium Pricing: IoT Sensors Move Insurance From Proxy To Source Data**

IoT data is opening a slew of  are three key ways that IoT data will enable personalized insurance pricing:

- **Pay What You Risk:** Telematic and wearable sensor data enables lower premiums for less risky behavior, including driving less and exercising more
- **Bundle Policy and Loss Prevention Hardware:** Smart home companies will offer policy discounts to users of sensorized loss prevention technology, enabling cross-selling of devices and insurance
- **Verify and Settle Claims:** IoT data markets will enable carriers' faster access to verified risk management information, rather than relying on costly assessments and audits
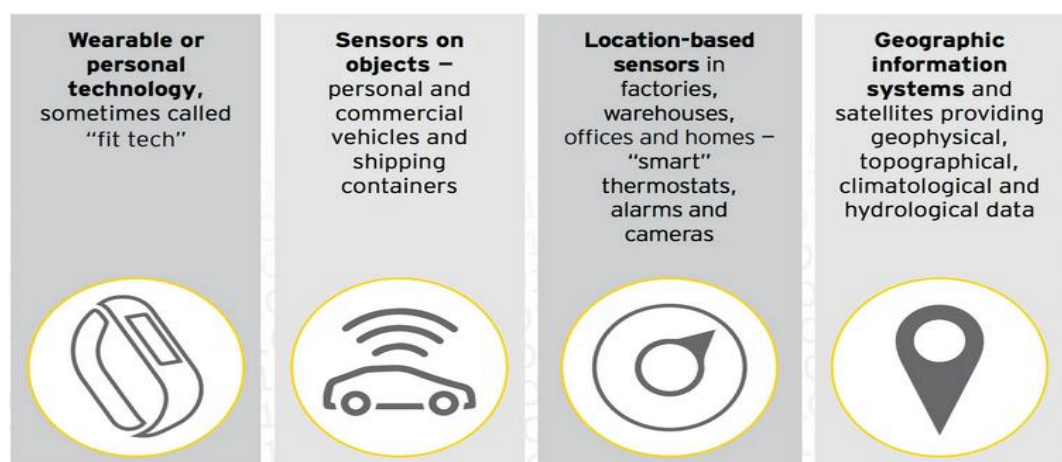


**2 – Customer Experience & Coverage Personalization: AI Interfaces Allow Better Customer Onboarding**

Here are the three key ways that AI will enhance the insurance buying experience:

- **Chatbots Will Recognize You:** Advanced image recognition and social data can be used to personalize sales conversation
- **Platforms Will Verify Your Identity:** Automated personal identity verification can speed authentication necessary for quoting and binding
- **Carriers Can Customize Your Coverage:** Machine learning can allow fully online or app-based shopping experience

**3 – Faster, Customized Claims Settlement: AI Settles Claims Faster While Decreasing Fraud**

Speed and success in settling claims is a critical factor for insurance business efficiencies, as well as for Here are two key ways that AI will improve customer satisfaction after filing a claim:

- **Speed in Settling Claims:** This time-to-settle metric will end up being important for which business lines customers prefer using.
- **Decrease Likelihood of Fraud:** This decreasing-fraud metric will end up being important for which solutions insurance companies prefer using.

**02    What are the applications and techniques of artificial intelligence?**

**Ans:**
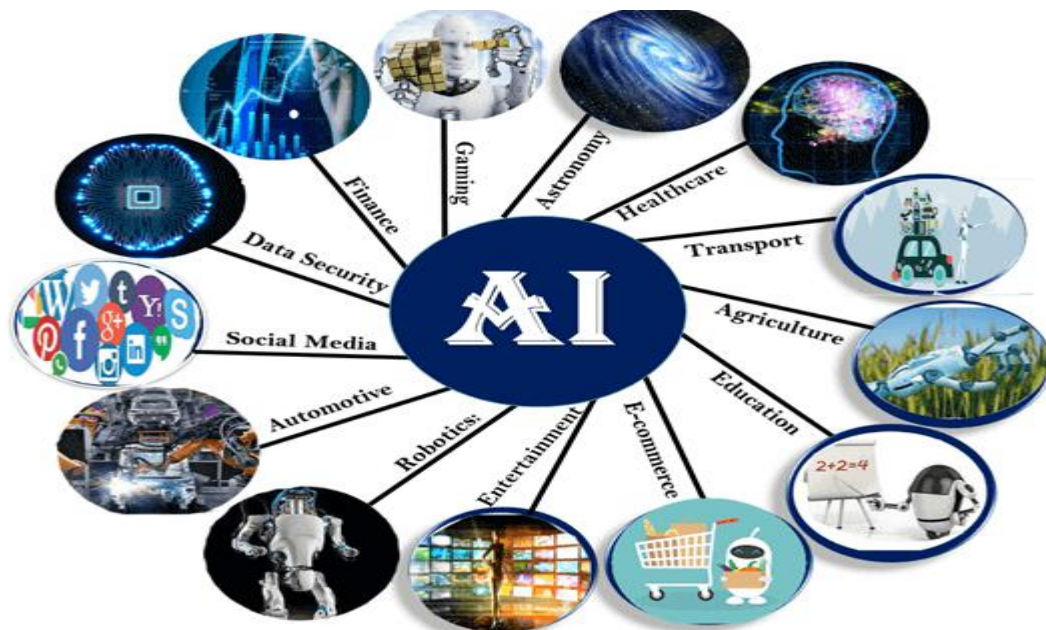


**1. AI in Astronomy**

- Artificial Intelligence can be very useful to solve complex universe problems. AI technology can be helpful for understanding the universe such as how it works, origin, etc.

## 2. AI in Healthcare

- In the last, five to ten years, AI becoming more advantageous for the healthcare industry and going to have a significant impact on this industry.
- Healthcare Industries are applying AI to make a better and faster diagnosis than humans. AI can help doctors with diagnoses and can inform when patients are worsening so that medical help can reach to the patient before hospitalization.

## 3. AI in Gaming

- AI can be used for gaming purpose. The AI machines can play strategic games like chess, where the machine needs to think of a large number of possible places.

## 4. AI in Finance

- AI and finance industries are the best matches for each other. The finance industry is implementing automation, chatbot, adaptive intelligence, algorithm trading, and machine learning into financial processes.

## 5. AI in Data Security

- The security of data is crucial for every company and cyber-attacks are growing very rapidly in the digital world. AI can be used to make your data more safe and secure. Some examples such as AEG bot, AI2 Platform,are used to determine software bug and cyber-attacks in a better way.

## 6. AI in Social Media

- Social Media sites such as Facebook, Twitter, and Snapchat contain billions of user profiles, which need to be stored and managed in a very efficient way. AI can organize and manage massive amounts of data. AI can analyze lots of data to identify the latest trends, hashtag, and requirement of different users.

## 7. AI in Travel & Transport

- AI is becoming highly demanding for travel industries. AI is capable of doing various travel related works such as from making travel arrangement to suggesting the hotels, flights, and best routes to the customers. Travel industries are using AI-powered chatbots which can make human-like interaction with customers for better and fast response.

## 8. AI in Automotive Industry

- Some Automotive industries are using AI to provide virtual assistant to their user for better performance. Such as Tesla has introduced TeslaBot, an intelligent virtual assistant.
- Various Industries are currently working for developing self-driven cars which can

make your journey more safe and secure.

## 9. AI in Robotics:

- Artificial Intelligence has a remarkable role in Robotics. Usually, general robots are programmed such that they can perform some repetitive task, but with the help of AI, we can create intelligent robots which can perform tasks with their own experiences without pre-programmed.
- Humanoid Robots are best examples for AI in robotics, recently the intelligent Humanoid robot named as Erica and Sophia has been developed which can talk and behave like humans.

## 10. AI in Entertainment

- We are currently using some AI based applications in our daily life with some entertainment services such as Netflix or Amazon. With the help of ML/AI algorithms, these services show the recommendations for programs or shows.

## 11. AI in Agriculture

- Agriculture is an area which requires various resources, labor, money, and time for best result. Now a day's agriculture is becoming digital, and AI is emerging in this field. Agriculture is applying AI as agriculture robotics, solid and crop monitoring, predictive analysis. AI in agriculture can be very helpful for farmers.

## 12. AI in E-commerce

- AI is providing a competitive edge to the e-commerce industry, and it is becoming more demanding in the e-commerce business. AI is helping shoppers to discover associated products with recommended size, color, or even brand.

## 13. AI in education:

- AI can automate grading so that the tutor can have more time to teach. AI chatbot can communicate with students as a teaching assistant.
- AI in the future can be work as a personal virtual tutor for students, which will be accessible easily at any time and any place.

# Top 4 Techniques of Artificial Intelligence
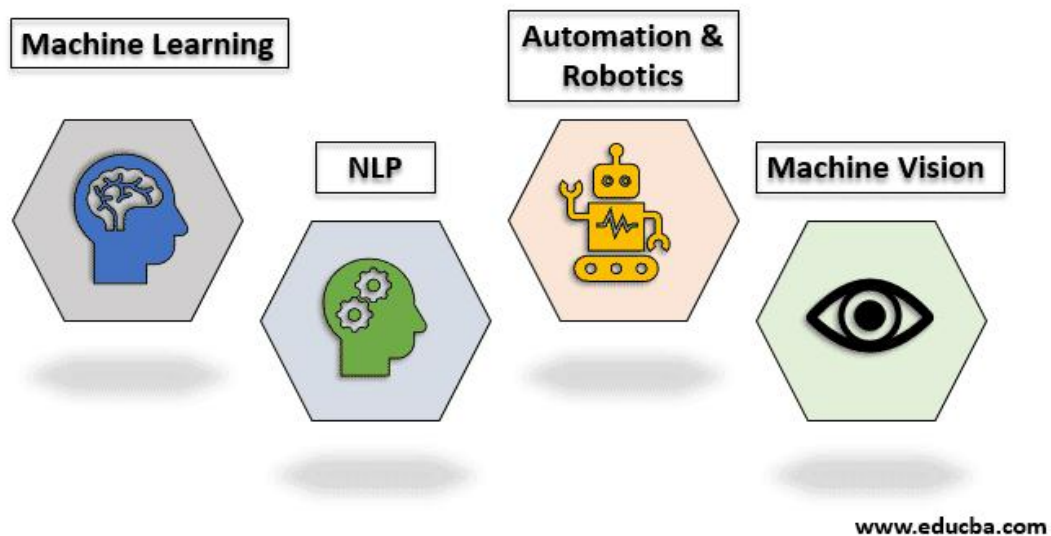
## 1. Machine Learning

It is one of the applications of AI where machines are not explicitly programmed to perform specific tasks; instead, they learn and improve from experience automatically. Deep Learning is a subset of machine learning based on artificial neural networks for predictive analysis. There are various machine learning algorithms, such as Unsupervised, Supervised, and Reinforcement Learning. In Unsupervised Learning, the algorithm does not use classified information to act on it without any guidance. Supervised Learning deduces a function from the training data, consisting of an input object and the desired output. Machines use reinforcement learning to take suitable actions to increase the reward to find the best possible, which should be considered.

## 2. NLP (Natural Language Processing)

Natural Language Processing involves programming computers to process human languages to facilitate interactions between humans and computers. Machine Learning is a reliable technology for Natural Language Processing to obtain meaning from human languages. In NLP, the machine captures the audio of a human talk. After the audio-to-text conversion, the text is processed and converted back into audio data. Then the machine uses the audio to respond to humans. Applications of Natural Language Processing can be found in IVR (Interactive Voice Response) applications used in call centers, language translation applications like Google Translate, and word processors such as Microsoft Word to check the accuracy of grammar in text.

However, the nature of human languages makes Natural Language Processing difficult because of the rules involved in passing information using natural language. They are challenging for computers to understand. NLP leverages algorithms to recognize and abstract the rules of natural languages, converting unstructured human language data into a computer-understandable format. Moreover, NLP can also be found in content optimization, such as paraphrasing applications, which helps to improve the readability of complex text.

### 3. Automation and Robotics

Automation aims to improve productivity and efficiency by having machines perform monotonous and repetitive tasks, resulting in cost-effective outcomes. Many organizations use machine learning, neural networks, and graphs in automation. Using CAPTCHA technology, such automation can prevent fraud issues during online financial transactions. Programmers create robotic process automation to perform high-volume repetitive tasks that can adapt to changes in different circumstances.

### 4. Machine Vision

Machines can capture visual information and then analyze it. This process involves using cameras to capture visual information, converting the analog image to digital data, and processing the data through digital signal processing. Then the resulting data is fed to a computer. In machine vision, two vital aspects are sensitivity, the ability to perceive weak impulses, and resolution, the range to which the machine can distinguish objects. The usage of machine vision can be found in signature identification, pattern recognition, medical image analysis, etc.


**03**    **What is the difference between security and surveillance?**

**Ans:** Surveillance and security cameras are essential pieces of equipment to protect your property. However, while they perform similar functions, there are several differences between the two security solutions.

#### Functionality

The primary distinction between surveillance and security cameras is the function of each device.

Surveillance cameras are intended to monitor a specific public area, usually from a distance, and are typically visible and unmasked. However, security cameras have no control over the environment they're watching, as they simply record what happens in front of them and send the footage to a recorder, either digitally or via cable wiring.

Security cameras, on the other hand, record or capture images and transmit video and audio signals to a Network Video Recorder (NVR), where these signals can be viewed and recorded. Security cameras can detect motion within a specific area and send an alert via email, text message, or mobile app when motion is detected. Some cameras also allow security professionals to remotely monitor and view their cameras in real-time.

#### Technology

Surveillance cameras are used to monitor and control a specific property, typically comprised of an entire network of surveillance cameras. These cameras are frequently connected to IP networks, which can connect remotely to the central location of the cameras.

Security cameras system video feeds from all connected cameras and sends them to

receiving equipment such as a monitor. This connection is typically made using a coaxial cable.

**Features**

Surveillance cameras use digital signals to transmit recorded video to a NVR via a single cable, eliminating the need for multiple power cables.

Security cameras, however, require cabling to transmit video feeds to a limited number of monitors, and the cameras must be strategically placed in a single location.

**Applications**

Surveillance cameras are better suited to simply monitoring a specific area and thus controlling any undesirable situation.

Security cameras are used to manage the security of public and industrial facilities and can be combined with intrusion detection devices to provide enhanced protection.


**04      Can AI be used for security?**

**Ans: 1. Underside vehicle bomb detection**

UVeye, an Israeli startup has developed an artificial intelligence and machine learning product that helps security personnel detect threats by scanning the underside of passing vehicles. The system uses strategically angled high-resolution cameras to create a 3D image of anomalies, such as improvised explosive devices, illegal weapons, drugs, and other suspicious material. UVeye claims that the technology will work even when the vehicle moving up to 28 MPH, meaning that the technology can detect objects that would otherwise escape the human eye.

**2. Infectious disease detection**

From a public-health standpoint, infectious disease can be a huge problem – putting countless lives at risk as medical professionals battle to contain outbreaks. We only have to look towards the Democratic Republic of the Congo and the spread of Ebola to understand the severity of infectious disease outbreak. Ensuring that an outbreak prevention campaign can help the right people and the right time, and preventing the spread of disease is a major challenge for healthcare and humanitarian services.

Fortunately, AI-based technology has been making great strides into the medical sector and companies are developing AI-based tools that can rapidly track, analyze and diagnose infectious diseases before it spreads

In September 2018, scientists from the National Environment Agency in Singapore created an algorithm to forecast dengue outbreaks, a mosquito-borne virus that affects over 400 million individuals.

In addition, Silicon Valley-based medical startup, AIME, has also developed an AI-based

platform that is capable of predicting the exact geolocation data of infectious disease outbreaks like dengue or Zika up to three months in advance.

### 3. Home security

According to new market research, home security is expected to reach $ 74.75 billion by 2023, up from $45.58 billion in 2018. This rise is largely attributed to the introduction of artificial intelligence, deep learning, and the increasing ubiquity of IoT connected devices. Indeed, artificial intelligence is revolutionizing home security as the technology can solve one of the biggest issues faced by traditional home security solutions; human error and false alarms. One solution, Lighthouse AI, uses artificial intelligence to alert you of humans, pets and other things that would be of interest while you're away from home.

### 4. Threat screening for large events

Evolve Technology is an AI-based system that enables threat screening on a huge scale. The technology utilizes artificial intelligence and facial recognition software to analyze live footage of approaching visitors to determine if they are approved persons, such as regular visitors, VIPs, employees and other persons who should be granted entry.

If a visitor is highlighted as a non-permissible person of interest, their profile will be sent to security officers and a human expert can review and verify the data. The technology claims to allow at least one person to be allowed entry per second. This particular technology is not designed to completely eliminate the human element of threat analysis and can be best utilized at locations such as airports, sporting events and schools. If utilized successfully, this would effectively put an end to long lines and bottlenecks.

### 5. Crime prevention cameras

Artificial intelligence and machine learning are adding a layer of proactive trouble detection to CCTV cameras. With the addition of artificial intelligence, CCTV cameras are now able to spot potential shoplifters and alert shopkeepers to suspicious behavior. One solution called "AI Guardman" developed by a Japanese company can scan live video streams to form estimations of "suspicious" behavior. Through artificial intelligence and machine learning, the system tracks the posture and movement of shoppers, and analyses it to match the posture and movement of confirmed shoplifters derived from previous data.

**05    How does AI improve security?**

**Ans:** AI security represents the next evolution in cyber defense, but is it essential? This can be a difficult question to answer definitively. What is apparent is that ongoing advances in malicious programming and other threats are making traditional cybersecurity a much more difficult prospect. In fact, today approximately 60% of organizations believe that they would be unable to identify critical threats without artificial intelligence technologies

**AI helps reinforce gaps in the cybersecurity workforce**

The pace of digital transformation is accelerating world wide. Unfortunately, the availability of trained, experienced cybersecurity professionals is not keeping pace. Artificial intelligence can fill a talent gap that sees millions of unfilled cybersecurity jobs. It is also a scalable solution to use AI for security tools, as they augment the workflows of employees. At the same time, AI frees up valuable resources by reducing time to identify and triage threats. This allows workers to focus on more complex tasks, leaving simpler, more repetitive chores to automation.

**AI promotes faster threat identification**

Hunting down threats takes a great deal of time—single alert investigations can take days to complete. AI powered security tools are capable of triaging events, cutting down on time that is needed for incident response.

**AI allows businesses to counter threat escalation**

While some organizations have been slow to adopt the newest advancements in digital security, it's clear that threat actors are showing no such hesitancy. Microsoft reports that "threat actors have rapidly increased in sophistication over the past year, using techniques that make them harder to spot and that threaten even the savviest targets" (source: [Microsoft](#)). AI for security empowers organizations with the technology they need to outpace this trend.

**Threat exposure**

Threat actors remain viable by constantly improving and refining their tactics, techniques, and procedures. AI provides cybersecurity systems with up-to-date and relevant knowledge of industry-specific and global threats, which help teams make critical decisions about priorities based on what attack strategies may be used against a company.

**Incident response**

AI systems provide context for response and prioritization to security alerts, fast incident responses, and root-cause analysis to mitigate vulnerabilities while analyzing how to prevent a recurrence of such issues.

**Breach risk prediction**

AI systems predict how an organization is likely to be breached. This allows the organization to better plan for resource allocation, mitigating weaknesses in the process. Prescriptive insights taken from AI analysis help improve configuration and enhancement controls to more optimize cyber resilience.