1. What types of AI-based business intelligence applications are currently used in insurance?

AI STREAMLINES INSURANCE PROCESSES AI helps insurers find evidence of potentially fraudulent claims and speeds up the underwriting process, during which insurance companies evaluate potential customers to determine their risk. AI can do these tasks faster — and more cost-effectively — than human employees by training models with historical data and using the models to automatically process new customers and claims.

AI REDUCES BIASES Rates for car insurance are traditionally determined by a buyer's personal factors, such as credit score, income, education level, occupation, and marital and homeowner status. But these factors penalize low-income buyers and aren't directly related to a driver's likelihood of getting into collisions. Companies using AI to build models can reduce these biases by actively excluding these factors during the training process.

AI OFFERS FLEXIBLE INSURANCE OPTIONS Insurers can track the habits of drivers for organizations like Uber and Lyft with wearable technology. If drivers for a service demonstrate safer driving habits, insurers can then offer that service lower premiums. Devices can also be used to activate insurance coverage only when drivers are actually driving, cutting costs while insuring service workers who would otherwise have had to purchase their own policies.

AI PROMOTES SAFER DRIVING HABITS As an example, if a delivery company that insures its drivers is experiencing a spike in accidents or traffic mishaps, AI and machine learning systems can crunch the data collected by connected devices to recognize patterns that would explain the reason for the accidents. Based on that analysis, the insurer can make recommendations to the company that would help reduce the number of accidents and expensive claims.

AI STILL LACKS TRANSPARENCY When AI-based risk models are built, it can be harder to pin down what insurance companies are basing higher premiums on. For instance, if companies use neural nets — an AI technique that's the basis for deep learning — the resulting model is opaque. Insurance companies would know what factors were used to train their AI model, but companies wouldn't know how the model internally related those factors to risk and which inputs are more important.

AI CAN BE INFLUENCED BY PROXY FACTORS Even if companies don't provide data about factors like gender, race and income, AI could still find other factors that stand in for that data and have effectively the same outcome. If something like the time of day when driving is taken into account to build a car insurance model, that could be a proxy for income level.

"If people who drive at a certain time of night are more likely to have claims, an insurer might say we should charge them more," said Daniel Schwarcz, professor of insurance law and regulation at the University of Minnesota. "But it may be that the reason there's a correlation is not because driving at that time is riskier, but because people with lower income drive at the time of night, and people with lower income are more likely to make claims."

2. What are the applications and 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.

3. What is the difference between security and surveillance?

Security camera Security cameras or also known as CCTV cameras are used to transfer signals from a certain area to an exact monitor located at a distance spot. It provides the following advantages:

1. It allows you to observe activities. Security cameras are an effective way to keep track of suspicious visitors in your area. This is helpful in allowing you to observe various activities in your home or business.
2. It deters criminal acts. Whether it is placed tactfully at home or at the office, security cameras discourage any criminal intent. Since the criminals know that they’re being watched, they’ll stop with their plans in fear of getting caught.
3. It provides evidence for a crime. Security cameras are great for obtaining evidence of any unexpected or expected events, especially nowadays where CCTV's have high-quality audio and video. This makes it easier to track culprits of criminal acts.

Consequences of having security cameras

1. Vulnerability to hack Due to the advancement in technology today, criminals have also made themselves tech-savvy. Thus, they have also acquired the knowledge on how to disconnect the cameras from the power source.
2. Your privacy can be compromised Security cameras in the office areas compromise the privacy of the staff. It makes some employees feel that the employer doesn’t trust them. Nevertheless, prevention is still always better than cure. Thus, having a security camera placed in your business to deter any criminal acts.
3. Price Again, due to the advancement in technology, security cameras have a lot of improvements now but the cost of these has also become more expensive.

Surveillance camera Surveillance cameras or known as automatic number plate recognition system works on an IP network that links the camera from a remote area and transfers the video to the security area. This allows for a longer recording time, which is perfect for surveillance activities.

Compared to security cameras who's aim is to deter criminals, surveillance camera aims to catch a targeted individual for certain acts. Thus, this is typically used by police officers to catch a criminal.

What advantages does this deliver? Read on.

1. It reduces the crime rate in public areas. Criminals will less likely to do a crime where they see cameras, even in public places. This reduces the crime rate in areas where there is a high number of criminal acts.
2. It allows for easy monitoring from afar. You can easily monitor areas wherever you are. You can see the feed from the camera through the internet or your mobile device, as long as there’s an internet connection.
3. It helps improve the public’s safety Public safety is improved at public places such as street crossings, malls, and parking areas. With the help of surveillance cameras, criminals are deterred and prevented while safety is increased.

Consequences of surveillance cameras You should know that ordinary citizens are not allowed to easily install surveillance cameras. This requires a certain permit from the government and a justifiable reason why this has to be installed in your private property or business.

Why? This is because it is:

1. Complex People who are not tech-savvy can get lost in using surveillance cameras. You need to learn how it works to use its full potential.
2. Easy to abuse Surveillance cameras placed in public areas are prone to abuse and misuse. Someone can collect the data from it and use it to blackmail another person.
3. Costly installation To use surveillance cameras, you'll need to purchase differently the system accessories. Which is by the way costly. Repairs can be expensive too.

Both cameras are used for protecting certain areas where it is located but they differ in application. Nonetheless, using them both accurately can increase the security level of an area. May it be public safety or home safety. Make sure that you choose a reliable security company to provide you either of the two.

4. Can AI be used for security?

Breach risk prediction Phishing detection Malware detection & prevention User authentication Spam filtering Password protection Bot identification Behavioural analysis Network segmentation & security Fraud detection Thread intelligence Incident response Vulnerability management Identity & access management

5. How does AI improve security?

Faster Threat Detection and Response Leveraging AI helps you better understand your networks and identify potential threats faster. AI-powered solutions can sift through vast amounts of data to identify abnormal behavior and detect malicious activity, such as a new zero-day attack.

AI can also automate many security processes, such as patch management, making staying on top of your cyber security needs easier.

It can help you respond faster to attacks by automating specific tasks, such as rerouting traffic away from a vulnerable server or alerting your IT team to potential issues.

Improved Accuracy and Efficiency AI-based cyber security systems provide improved accuracy and efficiency compared to traditional security solutions. For example, AI can scan scads of devices for potential vulnerabilities in a fraction of the time it would take human operators to do the same task.

Furthermore, AI algorithms can recognize patterns that may be difficult for the human eye to spot, leading to more accurate detection of malicious activity.

Greater Scalability and Cost Savings AI can automate tedious security tasks, freeing valuable resources to focus on other business areas.

It can also process vast amounts of data quickly and accurately to identify threats faster than any human could. This helps reduce response times to security incidents and helps lower the cost of defending against cyber threats.

AI-driven tools can also help identify malicious activity by correlating different data points, allowing you to protect your systems

In [ ]: