Smart Hotel: Ethical, Privacy And Security Problems Versus Artificial Intelligence

Ethical Problem 1

Although artificial intelligence has the speed and capacity of processing that's far beyond that of humans, it cannot always be trusted to be fair and neutral. AI can be used to identify people, objects and scenes. However, it still make mistakes, such as when a camera missed the mark on racial sensitivity, or when a software used to predict future criminals showed bias against black people. We shouldn't forget that AI systems are created by humans, who can be biased and judgmental. Now this will cause a major issue. (Dietz, 2019)

Solution For Ethical Solution 1

AI do their work as the way how they were taught and trained. Therefore, people who are researching AI need to be neutral minded to determine what data should be programmed. Before implementing AI in smart hotel, all the robot butlers should be tested thoroughly to avoid bias and racist problem.

Ethical Problem 2

Future job losses are another ethnical issue that concerns people with AI. A new report estimates that robotics could destroy as much as 800 million jobs worldwide by 2030. The report, published by the McKinsey Global Institute, claims advances in AI and robotics will have a drastic impact on day-to-day work. (Vincent, 2017) Just imagine that all the works such as cleaning, reception and other jobs related to hotel industry soon be replaced by robot butlers, hotel management doesn't need to employ human workers to do those jobs. This will eventually cause people to lose jobs and most importantly, their household income, leading to their difficulty in supporting their family expenditure.

Solution For Ethical Solution 2

First and foremost, it is undeniable that AI and robot can do things effectively compare to humans, but the hotel management should determine a balance between using robot butlers and employing human workers. They should be aware of the importance of humanity in hospitality industry as only humans have emotion. Besides that, the younger generations should learn more skill and gain knowledge in certain area that will not be replaced by AI in the near future.

Privacy Problem 1

Privacy of information is related to the protection of the information related to a subject's identity. Thus, privacy is focused on protecting individual's rights when it comes to the personal information.

Recently, newspapers are flooded with hijacking cases. The most recent case was 500 million guest accounts stored in a major hotel information reservation system being hacked. It is undeniable that hotel cybersecurity is once again disappointed every hotel service provider. Hotels receive and store masses of personal data via the smart devices as they are vulnerable to cyber-attacks, they must take action to protect their guests and themselves.

Gartner estimates that in 2020, there will be 20 billion of IoT devices deployed worldwide. This number is doubled compared to 2018 which only has 11 billion. (Hung, 2017) Gartner identified there are 7,000 IoT devices on one 5-star hotel which is 7,000 targets for the cybercrime to breach and obtain the private data.

Every IoT device in hotel can be hacked to access hotel servers and provide access to guests' personal information which disrupts the security. All these convenient IoT devices can also become a backdoor to guests' smartphones and personal computers to reveal their personal data or install viruses and spyware.

Solution For Privacy Problem 1

As the owner of the premise, hotel management can change the default usernames and passwords on all IoT devices. In order to prevent third-party physical access to the data storage, hotel management should send employees to accompany any outside technicians or maintenance teams when they are working on all the IoT devices. These people must obtain permission to access to networked computers. For more advanced protection, hotel management should create discrete, firewalled networks that separate IoT devices from hotel business, guest and visitor Wi-Fi. Finally, IoT devices network in every guest room should be separated from the hotel server. This action can reduce the risk of privacy data leakage.

Visitors should unplug all TVs and VUIs if discussions or other activities in the room are confidential. This is because every smart device can be turned on via network if the devices are plugged. Next, it is recommended not to use the room's USB ports and standard cables to charge phone or tablet. Instead, plug a personnel charger directly into an electrical outlet, or be sure to use accessories such as those available from PortaPow that allow charging and block the transfer of data to and from the personal devices.

Privacy Problem 2

Hotels now have the access to guest location, voice commands, and other relevant data by providing various features to the guests. The hotel now can track every bit details of the guests while they are in the hotel area. If guests order anything inside the hotel, they will be able to know what specific dish they ordered, specific drinks, and all other purchases. Linking the phone to a smart hotel, gives them access to not only phone data, voice commands, GPS tracking, but also your photo stream and other private data.

Besides the management, smart devices in hotel also transmitting the guest's personal information such as name, address, date of birth, health care information, credit card detail and much more to third parties without encryption.

A Study carried between Northeastern University and Imperial College London, found that 72 of

the 81 IoT devices shared data with third-parties completely unrelated to the hotel management. (Lindsey, 2019) The data they shared went far beyond the minimum requirement, which included IP addresses, device specifications and configurations, usage habits, and location data. Some of these third-parties are Google, Amazon and Akamai which provide the Wi-Fi, Internet networking or cloud storage functionality needed to run these IoT products.

Solution For Privacy Problem 2

One of the most popular ways to protect consumer data is by using virtual private network providers for their services. VPNs are extremely practical, useful, and safe because they provide encrypted data besides masking the IP address which prospective attackers see them as streams of incomprehensible characters. By activating a VPN on the Wi-Fi router or smartphone, guest can immediately protect their own devices which are on the network.

Beside setting up private network, there are some practical steps that guest can take to limit day-to-day privacy risks. Guest need to avoid sharing their exact location using the smart devices provided by hotel as this indicates that they are not at home. Plus, this allows the trackers to track the guest offline habits so they can make money targeting them with adverts.

When guests are setting up their smartphone to the smart devices, they are basically handing over their key details that make them an easy target for data mining, censorship, targeted advertisements and other invasive practices. By reading through the fine print, they will find out whether they are comfortable with how the website deal with their information and ultimately protect their privacy rights.

Security Problem 1

The first security issue is the whole system itself. If the system is under attacked by the hacker, the hacker will access the information of the hotel and the information of the guests. Other than that, appliances such as guestroom television apps requires the guests to input usernames and passwords. The issue lies between the apps between wireless internet. In order to give freedom for the guests to enjoy the apps, not much administrative actions are done towards the apps, causing it to be vulnerable to viruses. When the security barrier breaks down, the privacies of the guests are eventually threatened.

Figure 8: Information theft can access to personal data stored in unprotected systems.

Solution For Security Problem 1

Administrative department of the smart hotel can install new defensive software such as antivirus or update the software and servers to decrease the vulnerability of the system to viruses. Besides that, firewalls should be used to prevent the intrusion by indirect or unauthorized users and detect intrusion attempts so the cybersecurity department can block the intrusion in time.

Figure 9: Cybersecurity is essential for the protection of information system

Security Problem 2

Other than that, it is possible that the guests will become a hardware theft out of greed. After enjoying high-technology appliances, some of them might want to take the things as their own. Hardware theft is defined as unauthorized taking and defacing of computer hardware. Due to hardware thefts, smart hotel might suffer great loses when the hardware is taken away frequently as more and more portable items are costly in the future due to nanotechnology. Besides that, smart hotel has no authority to install surveillance cameras inside the rooms since the privacy of guests are protected. This causes the greedy guests to have the chance to take away what they wanted without being noticed.

Figure 10: Hardware can be stolen easily and silently when there are no people around

Solution For Security Problem 2

However, there are solutions that are very effective against the hardware thefts. The appliances in the rooms should be installed with real time tracking device to inform the administrators about the locations of the stolen device. Other than that, every appliance should be installed with mini security systems which contains the information that is linked to the anti-theft gates as stolen items that passes through the gate will trigger the alarm and thus the theft can be caught easily (Damag313, 2014).

Figure 11: Anti-theft gate will be triggered to alarm the security guards about the hardware theft.

Privacy Problem 3

In this video, privacy remains a big question mark when it comes to real life applications. Hotels serves as a home away from home, which should be providing customers with highest level of privacy. However, from the video, we can see that one of the main selling points of the hotels in the future is all about tailor-made experience. This brings up a question, where exactly they can harvest the data? Thru questionnaire? Or use surveillance camera to check out the customers' behavior. Besides that, how will the hotels keep the data and prevent outsiders to gain access to their customers' private personal information.

Solution For Privacy Problem 3

I believe that back to basics will be the best way to prevent further issues, at least before the perfect solution that somehow is acceptable for everyone. Instead of using computers or artificial intelligence to obtain behavioural data. Word of mouth works better as there will not be any information that will be stored in some forms of storage which will eliminate any risk of privacy information being leaked. Additionally, this also gives customers peace of mind knowing they are dealing with human, especially the older spectrum of the consumers.

Security Problem 3

Beside the major security issues stated above, there is another apparent issue that is integral to the hotel intelligent systems. To achieve full personalisation, they will either have to ask their

guests whether how they want their stay to be, or use surveillance cameras to estimate their requirements based on the guests action. The former brings out one security issue - where the data goes or how will the hotel personnel deal with the data they have on hand. The latter raises an even bigger concern as it doesn’t just involve privacy, the disposal of the data will be a tall hurdle and they put themselves on massive risk of the footage being intercepted.

Solution For Security Problem 2

To tackle these issues, the network designers have to ensure that their system is fully equipped against external interceptions. This is a crucial part when setting up the entire network system as quite a lot of information involved are highly sensitive. The recording part, the designers could design a system that does not keep the footages so that they can focus on protecting the camera from external access, if they decided to go with that solution when they wanted to achieve true personalisation.