What are the risks of connected petrol pumps?

There is currently a lot of focus on how businesses are leveraging automation solutions to improve their processes and drive efficiencies. One of the ways this is happening is by utilising internet connected devices, collectively known as the internet of things (IOT).

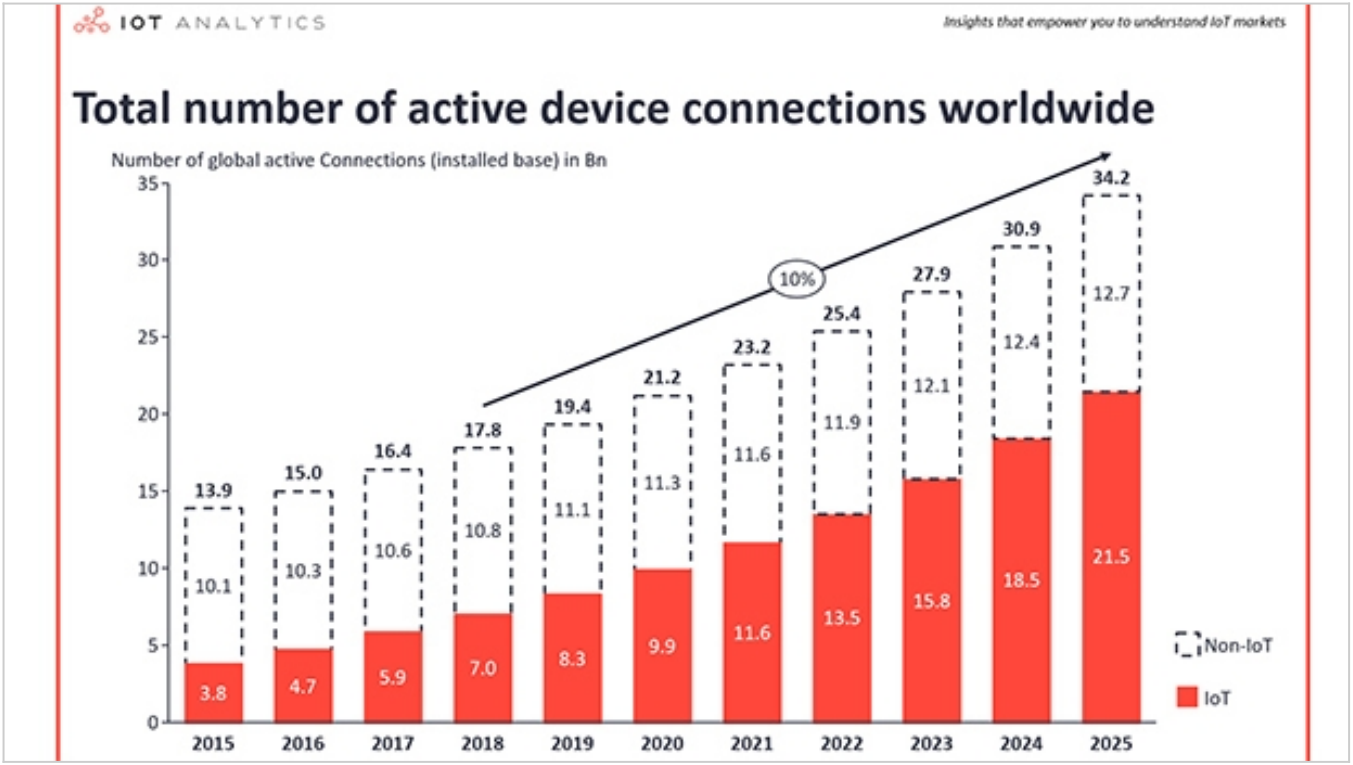
According to data collected from IOT Analytics, there are over 7 billion IOT devices in operation today, with this number set to triple over the next 6 years. The introduction and adoption of 5G, allowing a very high data rate, which is required by most IOT devices, is contributing to this rise, allowing for a wider range of IOT applications.

For the consumer, it's not just smart meters where we're seeing this optimization – it's everywhere. It's not uncommon to see personal assistants in the home, commonly used to play music or purchase goods on request, allowing for a streamlined user shopping experience, whilst the companies supplying these services benefit from increased knowledge, and ultimately more purchases from the user – simply because it's a more convenient way to shop.

The increase in IOT devices will lead to an exponential increase in the amount of data that is collected and processed. Providing great opportunities for business optimization through an up-to-date view of the data, enabling machine learning technologies to make automated decisions based on the current trends. This will become integral to success for companies employing IOT devices, as it will allow for greater automation opportunities and more agile processes. Physical systems with IOT monitoring and ML will gain additional benefit, such as prediction capabilities for supply and demand, faults and much more.

IOT devices are also improving shopping experiences for many purchases made in person. We are approaching the age of the staff-less store; there are a number of these across the globe already and they rely on an advanced system of cameras to identify the shopper, and their shopping, to ensure they are charged the correct amount on check-out, in turn enabling a more streamlined experience due to the removal of the queue and check out process. One space where this is happening faster than others is on the fuel forecourt. Most forecourts now offer 'pay at pump' functionality, enabling the driver to avoid the queues once they have finished fuelling.

Fuel businesses are taking this further by increasing the number of unmanned sites, as many of the services offered at service stations can now be automated, driving increased profits for these businesses. However, convenience often comes at a cost, and sadly in this age of large-scale cyber-attacks, IOT devices are now becoming targets for fraudsters to either steal information or use the devices themselves as part of larger scale attacks, for example in Distributed Denial of Service (DDoS) attacks.



Non-IoT includes all mobile phones, tablets, PCs, laptops, and fixed line phones. IoT includes all consumer and B2B devices connected. |

Recently there have been reports of internet connected fuel pumps being attacked, as well as in-depth technical guides published on the dark web with details on how to perform a device takeover. In the case of fuel pumps, devices are being manipulated, so that attackers receive cut price fuel. In some cases, the device is being used like a card skimmer, sending payment card information directly to the attacker to sell on the dark web. Because these devices are connected to the internet with very little security, large numbers of pumps can be attacked at once, without the attacker needing to be present.

Fortunately, most of these hacks can be avoided with relative ease – a change of the default access password (with a strong password) is enough to prevent the large-scale attacks. But what about protecting the terminal itself? These attacks are more difficult to prevent, especially on unmanned sites. Since these sites do not have any staff present to deter fraudsters, they become an obvious target for this type of attack. My team and I have recently undertaken an exercise into preventing even this type of attack. Where members of our fraud team visited several unmanned sites. We determined that basic security measures, such as installing CCTV security cameras, pointed at each fuel pump payment terminal, would be enough to deter many fraudsters.

Following our advice, those unmanned sites have seen a marked drop in fraudulent activity and the fuel supplier is now looking to roll out our recommendations across its network. Not only will this reduce the amount of fraudulent activity; the overall cost of managing unmanned sites will decrease and the customer is now more likely to roll out further unmanned sites to increase optimization further.

IOT devices are a powerful tool for automation and improving business insight but require some basic security measures to ensure they remain safe for businesses to use. It is very exciting to imagine where this technology will lead in the coming years, but without security improvements, they could become one of the best targets for the fraudsters of the future. If your business employs IOT devices, ensure they conform to strict security policies and always be alert to hardware modification as well as remote attacks to protect your business.

Oliver Tearle is Head of Research at The ai Corporation (ai), a company trusted around the world for developing innovative technology that allows our customers to take control and grow profitably. Founded in 1998, they have a long track record of providing solutions to some of the world's largest financial/payment institutions and international merchants. Through our relentless focus on these tools, we constantly strive to help our customers create highly profitable returns.

