Using AI can make your business fraud-free and safer

By Rob Lith

4 Feb 2019

When it comes to AI, virtual assistants and chatbots are an immediate association for many. However, despite the growing importance of intelligent, programmed systems in relation to customer-facing interactions and hyper-personalised marketing, AI has other important uses for companies too - in fighting fraud.

Rob Lith, Chief Commercial Officer at Connection Telecom

The South African context

Although there's no question that fraud and corruption is a global issue – the UN chose 9 December as International Anti-Corruption Day back in 2003 – the topic has special significance in South Africa. PWC's 2018 Global Economic Crime and Fraud Survey identified our country as having the highest rate of reported economic crime in the world, at 77% as opposed to the global average of 49%. Building on that, fraud committed by the consumer is the second-most reported crime in South Africa.

Apart from significant financial losses, repercussions for companies can include devastating reputational damage if their systems are compromised. Making local news right now, for example, is a case of R3.1m SIM-swap fraud, and mass debit order fraud that may have affected up to 750,000 bank accounts. The latter has South African banks scrambling to implement a new DebiCheck system before further scams strike their customers and impact their own revenue.

AI's greatest benefit – detecting unusual patterns

Fraud thrives in complex transactional environments like those found in the finance, insurance and telecoms industries. Millions of banking transactions and call records make it incredibly difficult to spot suspicious behaviour using traditional, manual methods.

By contrast, AI, or, more pertinently, Deep Learning can, through programmed and continually evolving algorithms, scan the massive volumes of data for expected behavioural patterns and immediately alert human operators to investigate any anomalies. These investigators can then apply their own initiation and experience to the case for the greatest accuracy.

#BizTrends2019: Smarter chatbots to a seamless multi-cloud environment

Rob Lith 7 Jan 2019

Further to this, the more exposure the AI has to fraud patterns, the better it becomes at predicting future attacks. Within the telephony sphere, for example, AI is being used to great effect in proactively combatting the problem of toll or VoIP fraud, where hackers access phone systems and make calls from that account to high-expense, long-distance destinations. With AI examining global trends, it becomes possible to predict the next flare-up location and safeguard against it.

Sentiment analysis

AI is stepping up to combat fraud in other areas too. Although still a bit too expensive for widespread use (as yet), sentiment analysis tools like IBM's Watson and Google's Cloud Natural Language API can be integrated into cloud-based solutions used by call centres.

With access to millions, if not billions, of call records, these smart systems have the potential to detect the vocal nuances of deceit-related stress on the part of callers and alert the customer agent. This would help counter the widespread problem of fraudulent insurance claims and credit applications.

Real-time sentiment analysis may sound more like futuristic sci-fi than a useful business tool right now, but AI in telephony products is already at the point of live, increasingly accurate, transcription. Such technology enables instant search of written records, removing the time-consuming need to listen to recordings in the event of an investigation.

Your best defence today

AI is becoming increasingly sophisticated, but admittedly should not be treated as the be-all and end-all of business protection. The best anti-fraud and general cybercrime strategy for any company is a Defence in Depth approach, where multiple security measures are combined and layered to ensure that, should one measure be overcome by cybercriminals – themselves often using increasingly sophisticated AI tools – the others will still provide redundancy protection, slowing the attacker.

Smart firewall protection, password-strengthening, anti-virus products and compliant-handling-and-storage of business data all contribute to greater business defence. Here, cloud-based software is especially beneficial as the flexible, subscription-based products are continually improved and updated by the provider to protect against the latest vulnerabilities, with no on-premise hardware or upgrade costs required on your part.

#BizTrends2019: South African cybersecurity trends for 2019

Brian Pinnock 21 Jan 2019

Also, by using a giant cloud service platform, like AWS or Azure, whichever machine learning tools you're using can access a world of Big Data and computing power to extend their analytical capabilities – and develop a more nuanced understanding of how humans behave and think.

In today's volatile business environment, exposing your company to fraud and corruption can have severe consequences. Looking at ways to bring cloud-based AI on board in this crucial role will have major benefits for your organisation. Many South African CIOs are now driving the move to cloud services for this reason, and as part of a greater future-proofing strategy for their organisations. It's something for any business decision-maker to start adopting and integrating now.

ABOUT ROB LITH

Rob Lith is the director of Connection Telecom. ICT Industry aficionado and internet specialist, he has been involved in the industry for the last 20 years. Email him at rob@connection-telecom.com.

- Using AI can make your business fraud-free and safer - 4 Feb 2019
- #BizTrends2019: Smarter chatbots to a seamless multi-cloud environment - 7 Jan 2019
- SA needs to prioritise STEM education - 22 Aug 2018
- Contemporary ICT insights for South African companies - 5 Jun 2018
- Could the humble phone call be the future of digital CX? - 31 Oct 2017

View my profile and articles...