UDC 004.852

VULNERABILITIES OF DEEP LEARNING BIOMETRIC VOICE APPLICATIONS IN BANKING AND FINANCIAL SERVICES

S.N. PETROV, O.S. ELSAYED, T.A. PULKO

The Belarusian State University of Informatics and Radioelectronics, Republic of Belarus

Submitted 8 November 2020

Abstract. The analysis of the market of virtual digital voice assistants is carried out. It is established that the popularity of such applications in the fintech industry is growing, especially starting in 2019. Made a review of the most popular voice assistants used in banks. The main vulnerabilities and threats are analyzed.

Keywords: speech recognition, neural network, voice technologies, biometric technologies, voice spoofing, virtual voice assistants.

Introduction

The usage of biological measurements or Biometrics' traits as key values for smartly identifying someone or verifying their claim of being a certain person, increasingly through means of Artificial Intelligence and Deep Learning methods, is enthusiastically being propagated as other remote technologies in the post-coronavirus pandemic are, abruptly being introduced into the lives of the ordinary people within their regular interactions and daily activities, and gradually obtaining popularity as the «New Normals» among both consumers and services providers across multiple different areas and applications, such as Automotive, Healthcare, Education, Governmental & Public Services, Legal & Forensic, Military & Defense, Consumer Electronics & IoT Gadgets, and Retail, E-Commerce and the Banking and Financial Services and Insurance .

Speech and Voice Recognition market is expected to grow between the years 2019–2025 almost 17,2 % CAGR (Compound Annual Growth Rate) reaching an estimated 26,8 billions dollars by 2025. And the selected Biometric measures when ranking by Consumer Preference was: voice recognition (32 %), fingerprints (27 %), facial scan (20 %), hand geometry (12 %), and iris scan (10 %), where high preference to most convenience and familiarity when choosing the biometric technology.

This growing is contributed equally by the consumers themselves and by driver and orchestrated by the Authorities i.e. both the Service Regulators & Service Providers in the Fintech (Financial Technology) sector to comply with such mandatory, caused by number of interconnected reasons pushing both parties to participate in this cycle of pushing forward towards further broader adoption of advanced smart voice-based technologies and solutions; Governments and Regulators are both strictly obliged to comply with the anti-money-laundry and criminal funding acts like the American KYC regulation or the European PSD2 regulation both with punitive compensations of multi million dollars for the entities that fall short of fulfilling them.

On the other hand, voice-enabled devices are driving the interest of several well established banking and ICT market players and start-ups equally towards developing consumer-centric solutions for this market highlighted by the convince and none-intrusive features of the technology. Voice recognition technologies are increasingly being considered as relatively cost-effective and convenient mechanisms to gain access or exercise control over different types of connected devices that are part of smart homes, connected cars, and other smart technology segments in the Internet of Things Ecosystem.

However, it is very important to keep in mind no system is perfect and the same applies to Machine or Deep-Learning-based systems, which in themselves are based on statistical and mathematical methods with scientifically forecasted margins of errors.

Smart voice-based Biometrics technologies in Fintech services

Specially with the COVID-19 era, when due to the various degrees mobility restrictions of individuals that ranged from simple social distancing measures and guideline to be followed strictly by people and businesses in their daily work-habits, to partial or full local and regional lockdowns.

The person themselves being the password or key of access is not new and as technology is spreading it is being used more and more in the daily lives of ordinary including their daily interactions and activities. Banking and financial services being a daily activity for people it was not very far behind in the following of the trend, this was specially capitalized and with the outbreak of the Coronavirus pandemic and the consequent lockdowns that followed. To meet the minimum requirements of banks and monitory and in the need to authenticate and identify their customers/clients.

Speech technologies are widely used in the Fintech sphere. There are several main areas of use for biometrics systems.

1. Speaker Identification. Automatically verify and authenticate speakers in seconds by using their voice as a highly accurate biometric identifier and provide every client with a truly immersive call experience.

2. Fraud Detection. Prevent yourself from fraudsters hiding behind someone else’s identity with a speaker verification system running in the background marking suspicious speakers whose voices don’t match.

3. Defense and Security. Identify and quickly search for speakers in the large quantities of audio recordings to stay ahead of crime and perform detailed forensic voice analyses faster with the help of AI-powered technology.

A large and fast-growing market is the use of virtual voice assistants, which greatly simplifies the management of a Bank account, making this process similar to normal communication with a human operator. Company «Tractica» defines a virtual digital assistant as an automated software application or platform that assists humans through understanding natural language in written or spoken form and leverages some form of artificial intelligence in doing so [1]. According to their research, the virtual digital assistant market will grow rapidly further (Fig. 1).

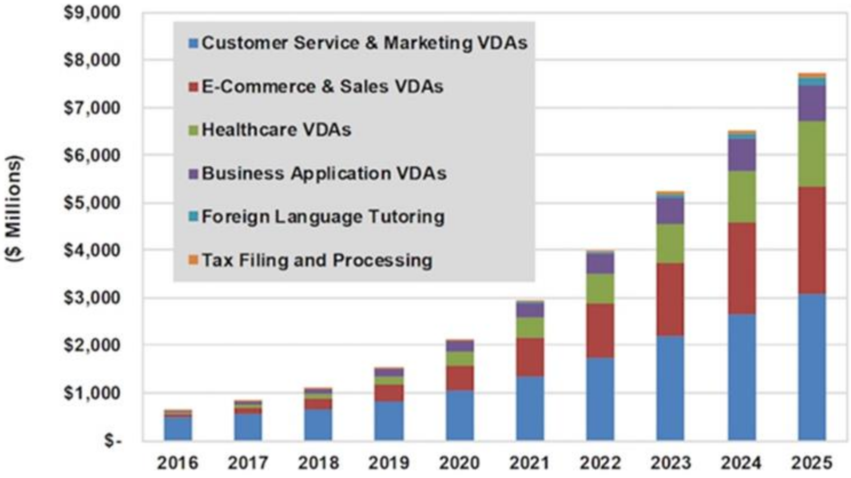

Fig. 1. Enterprise virtual digital assistant software revenue by use case, 2016–2025

Many financial organizations, mainly in the US, are already using voice-activated virtual assistants to access accounts and make payments. Under the Alexa skills category of «banking and finance» (such as YNAB, Business Voice Apps, Create My Voice, Marketplace, Commercial Trends and others) more than 3000 results come up, including American Express, Capital One, PayPal and US Bank.

Some banks have also integrated Apple’s Siri, including Mashreq Bank in the UAE. In 2016, Mashreq started allowing customers to transfer payments of up to Dh500 using Siri. Mashreq Bank customers can tell Siri how much they want to transfer and to whom, but have to authenticate by using either their pin or touch ID fingerprint recognition.

In 2017, UK bank Barclays rolled out a similar concept, allowing customers to ask Siri to make a payment and then authenticate it with Apple’s touch ID.

OCBC Bank in Singapore has offered voice banking through Google Assistant on a smartphone or Google Home device since April 2018. Customers can mainly inquire about the bank's services and plan their financial future; for example, they can calculate the mortgage loan amount they can afford.

Bank of America, which serves more than 65 million consumer and clients, created its own virtual assistant Erica in June 2018.

Biometrics' voice recognition systems vulnerabilities

However, such systems have certain disadvantages. Many challenges connected with accuracy level. Voice-based systems have very high error rates, especially false rejections.

Another problem is speaker verification spoofing. According to [2] most biometric systems are vulnerable to imposture. Spoofing attacks are performed on a biometric system at the sensor or acquisition level to bias score distributions toward those of genuine clients, increasing the False Acceptance Rate (FAR) [3].

The most common options for implementing spoofing today are:

1. Impersonation. Impersonation refers to spoofing attacks with human-altered voices and is one of the most obvious forms of spoofing.

2. Replay attacks, using speech recordings of a genuine client, or concatenation of shorter segments. The equal error rate (EER) of 1 % can increase to 70 % using replayed spoof attacks.

3. Voice conversion, which is a technique that electronically converts one speaker's voice towards that of another.

4. Speech synthesis. In this approach a speech synthesizer is used which is adapted to the voice of genuine clients. Using an HMM-based speech synthesizer, the FAR can rise up to 91 %.

Conclusion

Virtual voice assistants are widely used in the banking sector. The integration of such systems allows you to reduce customer service time, increase security, but at the same time, these solutions currently have the disadvantages inherent in all probabilistic technologies (FAR and FRR), and are also subject to targeted attacks such as voice spoofing.

References

1. Virtual Digital Assistant Software to Reach $7.7 Billion and 1 Billion Users in 2025 [Electronic source]. URL: https://voicebot.ai/2018/02/01/virtual-digital-assistant-software-reach-7-7-billion-1-billion-users-2025/.

2. Spoofing countermeasures for the protection of automatic speaker recognition from attacks with artificial signals, F. Alegre, R. Vipperla and N. Evans, INTERSPEECH 2012, 13th Annual Conference of the International Speech Communication Association [Electronic source]. URL: http://www.eurecom.fr/en/publication/3731/download/mm-publi-3731.pdf.

3. Spoofing and countermeasures for automatic speaker verification, N. Evans, T. Kinnunen, J. Yamagishi, INTERSPEECH 2013, 14th Annual Conference of the International Speech Communication Association [Electronic source]. URL: https://www.researchgate.net.