Fig 1. “Machine Learning and Artificial Intelligence.” *Sophos* Accessed 30 Jun. 2020.

AI in Banking

A Guide to Feed Data-Hungry AI with Healthy Data

ABSTRACT

Artificial Intelligence (AI) crosses electronic frontiers to develop its services in many industries including the financial industry. Single sourcing the available data is a more affordable and more reliable way to feed AI. As the population of online and mobile service users grows across the world, the possibility of single sourcing information and creating a digital identity system becomes more realistic. In this brief, the researcher reviews how digital ID systems can contribute to the AI industry and empower financial technology.

Ava Taresi

Information Technology TCN705

TABLE OF CONTENTS

TABLE OF FIGURES

1. Introduction: Independent and Accurate Data Is Essential for AI in Banking

Data availability is the backbone of successful Artificial Intelligence (AI) technologies. AI technologies in the banking industry can consume a lot of data to learn and improve itself. AI needs as much data as possible to improve its accuracy and reliability in banking. That is why feeding AI technology a steady and healthy flow of data is crucial for the future of banks, businesses, and customer experience.

The Financial Technology (FinTech) industry uses technology and AI solutions to automate and deliver financial solutions. FinTech defines the way AI collects, shares, and uses data to improve user experience in the financial industry (Arjunwadkar, 27-28). Financial institutions (FI) create and retain their access to the user's financial data, income, credit cards, assets, mortgages, liabilities, transactions, and demographic data, which makes the industry highly regulated.

FIs and banks are not the only recipients of such sensitive data. Every entity that collects, processes, and analyzes users' data is responsible for prioritizing users' privacy.

2. Challenges: From Data Collection to Data Governance

Improving and utilizing AI for innovation in the banking industry involves a great amount of data collection, storage, sharing and governance (Fig. 2). Many parties are involved in this complicated process. Bank customers, governments, researchers, tech-companies, FIs, and academic organizations are only a part of this circle.

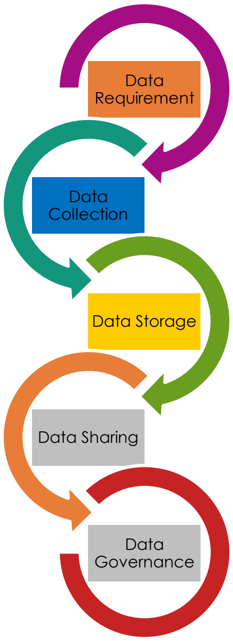

Fig 2. AI Learning Life Cycle

2.1. Data-Ownership and Data Sharing

Each party involved in the banking industry has obligations to preserve and to keep data private. Each party also has policies in relation to other parties, whether the other parties are rivals or cooperators. Such relationships weigh on the parties' decisions to share parts of data or data as a whole.

When a bank uses the FinTech industry to benefit the latest innovations, the bank interacts with FinTech in three ways (Fig. 3):

- In-House Development of New Tools: Banks have an in-house FinTech department or employ a subsidiary company.
- Partnership with FinTech Companies: Banks partner with or invest in a FinTech company for a specific project.
- Collaboration with the FinTech Community: Banks collaborate with FinTech companies as trusted channel to stimulate innovative ideas ("Technology-led innovation in banking").

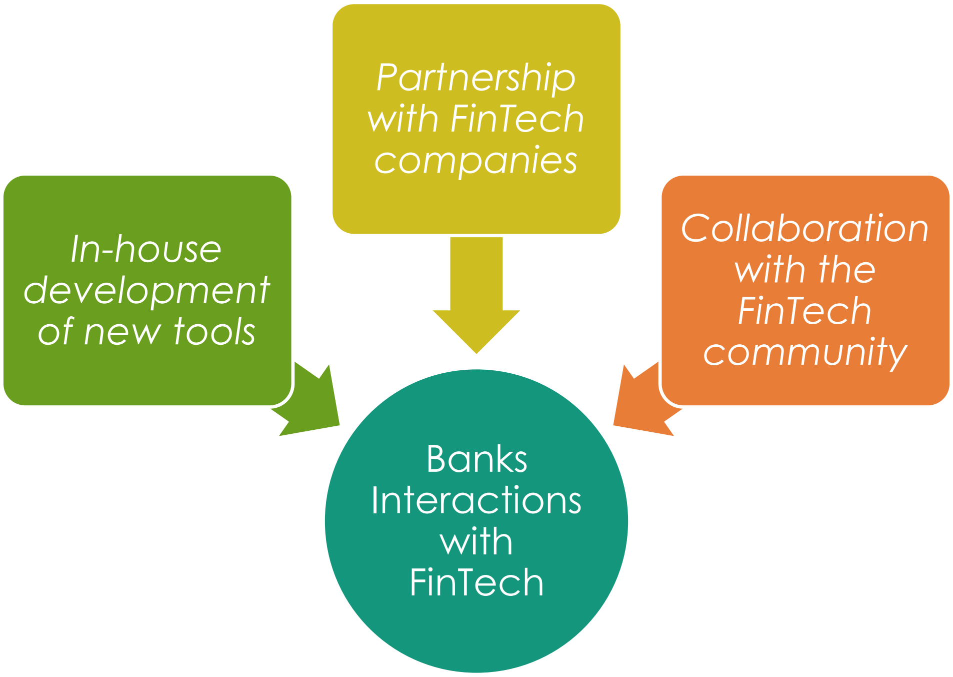
Partnership with FinTech companies
In-house development of new tools
Collaboration with the FinTech community
Banks Interactions with FinTech

Fig 3. Banks' Interactions with FinTech

When banks choose to partner with an external FinTech company, they must take measures to ensure they do not compromise customers' privacy and data.

AI needs sensitive financial data collected from the highly regulated banking industry to launch a service or product that millions of clients will use on daily basis.

3. Solution: E-Governments Build AI Backbone

AI is data hungry but feeding AI data from numerous sources and eliminating repetitive data from the source of data is costly and time consuming. In FIs, different systems will register and save users' data and the final extraction of data contains duplicated and redundant data. Customers often have an account and receive services for multiple products such as a credit card, a mortgage, and treasury services. Different systems within the same bank register each product. Merging the data and creating unique data from the bank is a challenge which makes creating a single source of truth very costly.

It takes a strong, steady, and healthy data pool to educate and advance AI. A supply of trusted, good-quality information under the strict supervision of an independent governing body can only help AI if its accessibility is guaranteed and its flow is never interrupted.

3.1. Digital Identification

An independent party must regulate the process of data sharing. The independent party must monitor the flow of data from the AI technology point of view, free of financial or political biases.

Data collection in banking begins when a bank asks customers to bring a piece of government-issued ID with them to a branch. If the government issues a digital ID, the bank must accept it rather than asking for a physical ID. An official digital ID identifies the customer electronically and is as valid as a physical document.

Since 2002, Estonia uses digital IDs and digital signatures to build its national data backbone, called X-Road and to form its e-government. Digital ID cards and signatures give the citizens (also known as users in AI) universal access to the Estonian government and private sector's services. The services include everything citizens need, from health care to banking services. Since the launch of X-Road, citizens submitted more information in the national database and has made the national database stronger (Anthes 18-20).

While Estonia initiated its plan in 2002, Finland had already started a similar plan two years earlier to collect bank customers' data via a digital ID; they would charge each customer 10 euros for this service. The plan was not a national plan as an industry was seeking to profit from people by to collecting their data and improving its AI database. Not all bank customers opted in and eventually the plan failed to become a national strategy to build the e-government (Heller 1-25).

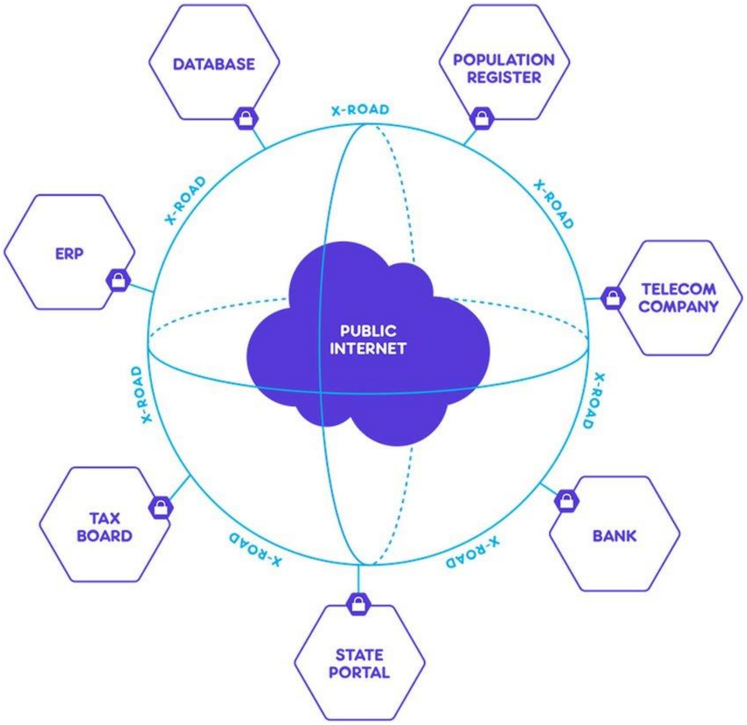

Fig 4. Estonia's X-road from: Soe, Ralf-Martin & Drechsler, Wolfgang. "Agile local governments: Experimentation before implementation." ***Government Information Quarterly*** **1 December 2017**

The Estonian government regulated and passed legislations to ensure that the digital IDs are incorporated in both the government and in private sectors. The government regulated the X-Road and built the skeleton of the e-government (Fig. 4). Such a platform allowed various industries to use and develop the X-Road and allowed citizen to have control over the data they are sharing with the business in question (Anthes 18-20).

The architecture of digital ID services includes a main server and a processing capacity. The server authenticates the digital ID by verifying sensitive data like users' biometrics and then routes the authenticated requests downstream to destination businesses (such as the healthcare system, FIs, and energy companies) for further processing (Camacho et al.).

3.2. Digital Authorization

AI in the FinTech industry needs a single source of data and a single format in its systems when it is dealing with multiple levels of information. The identification and authorization process can contribute to creating a single format of reliable data.

Digital authorization is different than digital identification. Digital identification assures that the users' credentials match the ones that they present during registration at their FIs. Digital authorization is the limited power that users give to a third-party application for their services.

OAuth is a universal online authorization standard that helps users access a third-party application without sharing their credentials. OAuth is a time-bound temporary privilege that applies to a defined purpose.

There are three players in an OAuth transaction:

- the user
- the consumer
- the service provider

Each player takes a step to ensure users' privacy.

1. Users show their intent to use a third-party web application (such as a web game) via a service provider (such as Facebook).
2. Facebook prompts users to authenticate their ID.
3. Facebook requests consent from users to give the third-party web application permission to post on users' Facebook wall.
4. The provided token is good to only post messages to the user's Facebook wall for a limited period (Siriwardena).

Nowhere within these four steps are users' IDs shared with the third-party application. This authorization is not enough to send a friend request or to delete images. The users gave online authorization to the third-party web application through the service provider, who already had access to their identification.

A reliable and trusted service provider can collect data and identify users without sharing any information with third party application. The service provider can be the source of data that collects and protects users' data while they try to use different services and platforms in FIs.

In 2017, the US's Securities Industry and Financial Markets Association (SIFMA) and the Financial Industry Regulatory Authority (FINRA) recommended that FIs use application programming interfaces (APIs) or protocols to enable users to use "safe and hygienic methods" (SIFMA) like OAuth to communicate with FIs. They suggested that such protocols or software components would avoid unnecessary credential sharing and help FIs and FinTech companies to collect and share data with users' consent. According to FINRA and SIFMA such methods gives users control to withdraw their consent and stop sharing information with the involved FinTech company.

4. Call-to-Action: Reliable and Single Source of Data for AI

Feeding AI from one source of information and securing the authenticity of a single source of information by creating digital IDs at national levels can benefit governments and many businesses in the private sector. If AI has one reliable source, FinTech can contribute to solutions for larger problems such as money laundering or terrorist funding acts.

Digital and online authentication through an independent and nationally supervised service provider can limit businesses' access to users' digital IDs. The OAuth standard can protect users' IDs from being shared by a third-party business.

In traditional government, citizens and businesses must visit a government office physically to finish their regulated inquiry. Such a traditional interaction poses less threat to paper-based information asset (Karokola et al.). To guarantee an e-government's data security, the AI must address data confidentiality, integrity, availability, and accountability. Such security objectives are the future challenges that e-governments must address in the process of shaping their road map (Wangwe et al.).

Countries must invest in their educational system to guarantee every generation's political engagement. Education about democracy and open data creates more political involvement, which will strengthen the e-government and citizens' trust in sharing more data for the future of AI.

5. WORKS CITED

Anthes, Gary. *Estonia: A Model for e-Government*. Communications of the ACM, vol 58, no. 6, *2015, pp.* 18-20. https://doi.org/10.1145/2754951. Accessed 23 June 2020

Arjunwadkar, Parag Y. *FinTech: The Technology Driving Disruption in the Financial Services Industry.* Auerbach Publishers, Incorporated, 2018, https://ebookcentral-proquest-com.libaccess.senecacollege.ca/lib/senecac/detail.action?docID=5352233. Accessed 18 June 2020.

Camacho, Luz, et al. *Method and apparatus for reducing on-line fraud using personal digital identification*. US: Patent WO2001067201A3. 13 September 2001. https://patentscope.wipo.int/search/en/detail.jsf?docId=WO2001067201. Accessed 23 June 2020

Canadian Bankers Association. *Basic Banking*, 2019, https://cba.ca/technology-innovation-banking. Accessed 19 June 2020.

Heller, Nathan. *Estonia, The Digital Republic*. The New Yorker, 2017, pp. 1-25. https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic Accessed 23 June 2020.

Karokola, Geoffrey, et al. *Secure e-government services: a comparative analysis of e-government maturity models for the developing regions-the need for security services*. 2012, http://dx.doi.org.libaccess.senecacollege.ca/10.4018/jegr.2012010101. Accessed 30 June 2020.

Machine Learning and Artificial Intelligence. 30 April 2019. Image. 30 June 2020. <https://home.sophos.com/en-us/security-news/2019/artificial-intelligence.aspx>.

SIFMA. *Special Notice: Financial Technology Innovation*. 30 July 2018. *SIFMA*. 19 June 2020. <https://www.sifma.org/wp-content/uploads/2018/10/SIFMA-Comment-Letter-re-Financial-Technology-Innovation-Special-Notice-10-18-18.pdf>.

Siriwardena, Prabath. "OAuth 2.0 Fundamentals." *Advanced API Security: OAuth 2.0 and Beyond*. 2nd ed. Apress, 2019. https://learning-oreilly-com.libaccess.senecacollege.ca/library/view/advanced-api-security/9781484220504/A323855_2_En_4_Chapter.html. Accessed 23 June 2020.

Soe, Ralf Martin and Wolfgang Drechsler. "Agile local governments: Experimentation before implementation." 2017. https://www.researchgate.net/figure/The-X-road-Source-Information-System-Authority-of-Estonia_fig3_322038966. Accessed 30 June 2020

Wangwe, Carina Kabajunga, et al. "A Sustainable Information Security Framework for e-Government - Case of Tanzania." *Technological and Economic Development of Economy,* vol. 18, no.1, 2012, pp. 117–131. *Vilnius Gedinimas Technical University,* doi: 10.3846/20294913.2012.661196. https://www.bjrbe.vgtu.lt/index.php/TEDE/article/view/4682. Accessed 30 June 2020.