**European Scholar Journal (ESJ)**
Available Online at: https://www.scholarzest.com
Vol. 1 No. 1, September 2020,
ISSN: 2660-5562

# INFORMATION SYSTEMS SECURITY IN FINANCE USING MACHINE LEARNING

**Gabriel Akhmedjanov,**
Tashkent State Technical University
September 2020

**Article history:**

**Received:** July, 10th 2020
**Accepted:** August 31st 2020
**Published:** September, 30th 2020

**Abstract:**

Machine learning has a long history in finance, dating back to the days before mobile banking apps, intelligent chatbots, and search engines. Few businesses are better suited for artificial intelligence than banking, with its enormous volume, accurate historical records, and quantitative character. Machine learning is being used in finance in more ways than ever before, thanks to the availability of more processing power and machine learning technologies. Financial services companies deal with a massive amount of client and transaction data that needs to be examined for fraud. Payments, in particular, are a hotbed for fraud, and treasury and finance professionals surveyed anticipate the pandemic will account for a large portion of the increase in 2020. To meet these demands, businesses must always explore for innovative ways to tighten fraud prevention and risk management practises.

**Keywords:** Artificial intelligence, Machine learning, information technology, financial analysis, knowledge discovery

## INTRODUCTION

Artificial intelligence (AI) is currently being debated in a variety of industries, including the financial sector. Deposit-taking, lending, asset management, and insurance broking are all services that financial institutions are contemplating using AI for. For example, utilising a chatbot to greet clients, anticipating market trends to provide client suggestions, and calculating a borrower's future earnings to extend loans are all considered useful AI applications for improving productivity and risk management. When introducing a new information technology (IT) like AI, it's critical to pay particular attention to the security concerns that come with it. In general, artificial intelligence (AI) refers to the use of computer systems and other methodologies to perform human-like intellectual tasks such as inference, recognition, and decision-making.

Machine learning is used to implement it (ML). Various research has revealed the risks and dangers that are unique to ML-based IT. Manipulation of such flaws results in serious security issues, such as the theft or manipulation of the machine learning model and/or its training data. It is vital to plan ahead of time in order to establish secure machine learning systems. In this work, we divide ML systems into twelve types based on the interactions between the entities that make up the system, and we examine the vulnerabilities and threats that each type faces, as well as the solutions that are available for each type. The research offered is important to financial organisations when deciding which security measures to employ since it allows them to identify potential attacks and responses for the type of machine learning system to be used.

## MACHINE LEARNING

Machine learning has a long history in finance, dating back to the days before mobile banking apps, intelligent chatbots, and search engines. Few businesses are better suited for artificial intelligence than banking, with its enormous volume, accurate historical records, and quantitative character. Machine learning is being used in finance in more ways than ever before, thanks to the availability of more processing power and machine learning technologies. Systems can detect unusual activities or behaviours ("anomalies") and flag them for security professionals using machine learning. The issue for these algorithms is to eliminate false-positives, which are circumstances in which "risks" are highlighted that were never actually risks. We spoke with a half-dozen fraud and security AI executives at Emerj, all of whom are sure that in the next five to ten years, really "learning" systems will be a must, given the incalculably large number of ways security may be exploited. Some of our readers in the banking and financial industries may find it challenging to persuade their colleagues or senior management to explore an AI solution to a current problem. It's worth noting that, while AI is causing waves of disruption throughout many industries, not all businesses will have the foresight to see how AI may aid them in the future. This lack of information, according to some experts, such as Ian Wilson, former head of AI at HSBC, is a significant obstacle to overcome when trying to identify the proper AI solution.

## TRAINING DATA MANIPULATION

The attacker tries to deduce training data from the supplier and then extract confidential information about individuals and organisations from the data. By manipulating the training data, the attacker also tries to get the model generator to build a malicious model.By transmitting enormous amounts of training data, the attacker attempts to disrupt the model generator's usual functions. The training-data supplier either uses non-confidential material as training data or adjusts the training data in such a way that it is impossible for the attacker to extract sensitive information as a countermeasure against the leakage of training data. The model generator either detects and removes malicious training data before the training process or employs an ML technique to lessen the effect of such data as a countermeasure against the production of a malicious model. The model generator uses services like a Content Delivery Network (CDN) or a network gateway to manage access requests from other networks as a denial-of-service countermeasure.

It is crucial to consider data leakage concerns while inferring training data and related information. Because the training data are not secret, the danger is minimised if the training data solely include public data such as financial market data and statistics data. If the training data, on the other hand, includes sensitive information such as customers' assets and financial transactions, the risk is considered high. In this instance, financial institutions should take extra security precautions to safeguard the training data. Financial institutions should focus on the risk of model leakage when inferring from ML models. Assume you're using a machine learning system to forecast financial markets. If the organisation considers the system to be a valuable asset, it should put in place security measures to safeguard it. If, on the other hand, an ML system is used to automatically respond to non-confidential client enquiries, the impact of model leaking is considered minor. The institution does not need to take any additional security measures in this circumstance.

## MANAGEMENT OF FRAUD AND RISK

Financial services companies deal with a massive amount of client and transaction data that needs to be examined for fraud. Payments, in particular, are a hotbed for fraud, and treasury and finance professionals surveyed anticipate the pandemic will account for a large portion of the increase in 2020. To meet these demands, businesses must always explore for innovative ways to tighten fraud prevention and risk management practises. Machine learning is being used by companies like PayPal to improve their fraud detection and risk management skills. PayPal's risk management engines can determine the level of risk connected with a customer in milliseconds using a combination of linear, neural network, and deep learning algorithms. Similarly, financial services firms can use machine learning algorithms to replace statistical risk management techniques. Several organisations employ software that automatically scans transactions for risk, moves flagged transactions to a risk queue, and investigates suspicious activities. Over time, computer programmes' capacity to identify fraud improves as their knowledge bases grow.

Machine learning can also assist lenders in determining a potential customer's creditworthiness. Machine learning could assist in determining how much credit should be offered to a certain consumer by studying historical spending behaviour and patterns. The solution would be particularly beneficial to new consumers with limited credit histories. Automating credit and risk rating processes on a large scale can help these companies improve their business models in general. The Bottom Line: Machine learning's applicability in financial services go much beyond these few examples. Machine learning has the potential to help the financial sector as a whole improve security and service.

## FINANCES FOR INDIVIDUALS

Machine learning-powered budget management apps give users with highly focused financial advice and guidance. Customers can use their mobile devices to track their spending on a regular basis with these apps. The data can then be analysed using machine learning to find expenditure trends that clients may not be aware of and places where they might save. One international bank used machine learning to identify troubled consumers and provide better solutions for meeting their needs. The bank found that certain client categories were experiencing financial hardship when the algorithm observed anomalous spikes in late-night credit card usage mixed with low savings rates. Customers who were flagged by the system were given automatic credit limit increases and free financial assistance to lessen the risk of defaulting.

Financial services companies deal with a massive amount of client and transaction data that needs to be examined for fraud. Payments, in particular, are a hotbed for fraud, and treasury and finance professionals surveyed anticipate the pandemic will account for a large portion of the increase in 2020. To meet these demands, businesses must always explore for innovative ways to tighten fraud prevention and risk management practises. Machine learning is being used by companies like PayPal to improve their fraud detection and risk management skills. PayPal's risk management engines can determine the level of risk connected with a customer in milliseconds using a combination of linear, neural network, and deep learning algorithms.

Similarly, financial services firms can use machine learning algorithms to replace statistical risk management techniques. Several organisations employ software that automatically scans transactions for risk, moves flagged transactions to a risk queue, and investigates suspicious activities. Over time, computer programmes' capacity to identify fraud improves as their knowledge bases grow. Machine learning gives actionable intelligence to financial services firms, which serves as a foundation for subsequent decisions. A machine learning software, for example, may use a variety of data sources to assign risk scores to loan applicants. Algorithms might then anticipate which consumers are more likely to fail on their loans, allowing the bank to personalise its services and terms to each individual. Machine learning can

also assist lenders in determining a potential customer's creditworthiness. Machine learning could assist in determining how much credit should be offered to a certain consumer by studying historical spending behaviour and patterns. The solution would be particularly beneficial to new consumers with limited credit histories. Automating credit and risk rating processes on a large scale can help these companies improve their business models in general.

## CONCLUSION

Machine learning has a long history in finance, dating back to the days before mobile banking apps, intelligent chatbots, and search engines. Few businesses are better suited for artificial intelligence than banking, with its enormous volume, accurate historical records, and quantitative character. Machine learning is being used in finance in more ways than ever before, thanks to the availability of more processing power and machine learning technologies. Financial services companies deal with a massive amount of client and transaction data that needs to be examined for fraud. Payments, in particular, are a hotbed for fraud, and treasury and finance professionals surveyed anticipate the pandemic will account for a large portion of the increase in 2020. To meet these demands, businesses must always explore for innovative ways to tighten fraud prevention and risk management practises. Artificial intelligence (AI) is currently being debated in a variety of industries, including the financial sector. Deposit-taking, lending, asset management, and insurance broking are all services that financial institutions are contemplating using AI for. For example, utilising a chatbot to greet clients, anticipating market trends to provide client suggestions, and calculating a borrower's future earnings to extend loans are all considered useful AI applications for improving productivity and risk management. When introducing a new information technology (IT) like AI, it's critical to pay particular attention to the security concerns that come with it.

## REFERENCES


1. Refsdal, Atle, Bjørnar Solhaug, and Ketil Stølen. 2015. "Cyber-Risk Management." In Cyber-Risk Management, edited by Atle Refsdal, Bjørnar Solhaug, and Ketil Stølen, 33–47. Cham: Springer International Publishing.
2. Reuvid, Jonathan. 2016. Managing Cybersecurity Risk: How Directors and Corporate Officers Can Protect Their Businesses. Legend Press Ltd.
3. Rohmeyer, Paul, and Jennifer L. Bayuk. 2018. Financial Cybersecurity Risk Management: Leadership Perspectives and Guidance for Systems and Institutions. Apress.
4. Ruan, K. 2017. "Introducing Cybernomics: A Unifying Economic Framework for Measuring Cyber Risk." Computers & Security. https://www.sciencedirect.com/science/article/pii/S0167404816301407.
5. Shetty, S., M. McShane, L. Zhang, and J. P. Kesan. 2018. "Reducing Informational Disadvantages to Improve Cyber Risk Management." Geneva Papers on Risk and Insurance Theory. https://link.springer.com/article/10.1057/s41288-018-0078-3.
6. Siegel, Carol A., Ty R. Sagalow, and Paul Serritella. 2002. "Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security." In Information Security Management Handbook, Volume 4, 357–80. Auerbach Publications.
7. Trim, Peter, and Yang-Im Lee. 2016. Cyber Security Management: A Governance, Risk and Compliance Framework. Routledge.