International Engineering Journal For Research & Development
Vol.4
Issue 1
E-ISSN NO:-2349-0721
Impact factor : 6.549

ROLE OF ARTIFICIAL INTELLIGENCE IN COMBATING CYBER THREATS IN BANKING

Vishal Dineshkumar Soni
Department of Information Technology, Campbellsville University, Campbellsville, Kentucky

ABSTRACT

With the advances in information technology, various cyberspaces are used by criminals to enhance cybercrime. To mitigate this cybercrime and cyber threats, the bank and financial industry try to implement artificial intelligence. Various opportunities are provided by AI techniques, which help the banking sector to increase prosperity and growth. To maintain trust in artificial intelligence, it is important to maintain transparency and explain ability. Information about customer's behavior and interest is provided by artificial intelligence techniques. Robo-advice is an automated platform that is maintained by AI. Artificial Intelligence is also involved in protecting personal data. Proper design provided by AI towards the banking sector, by which they are able to identify fraud in transactions. AI directly linked with the domain of cyber security. Various kinds of cybercrimes are prevented and identified by AI-based fraud detection systems. However, implementation and maintenance of artificial intelligence consist of the high cost. Along with this unemployment rate is increased by AI techniques.

Keywords: Artificial intelligence, cyber threats, financial services, data security, Risk assessment

INTRODUCTION

Artificial Intelligence has been developed as a concept to mimic human brain as AI is able to investigate a huge number of problems with a holistic human approach. Important questions about information privacy and security are raised due to the increase of internet computing and complex distribution. The cyber infrastructure contains vulnerable encroachment and other threats. Due to this problem physical devices such as detectors and sensors are not able to protect or monitor these infrastructures. High performing, flexible, robust, and adaptable cyber defense system is needed in this case. Banking sectors have been using Artificial Intelligence for several years. In the banking industry, artificial intelligence techniques are implemented rapidly for a new range of applications. This paper has been described about implementation of AI in the banking sector to mitigate cyber-attacks. Artificial intelligence is involved in various activities of the financial industry or bank. AI consists of several advantages and disadvantages which is also included in this paper.

UNDERSTANDING ARTIFICIAL INTELLIGENCE

Artificial intelligence is a typical technique that is able to perform in various functions; these functions are associated with human minds such as reasoning, learning, interacting with the environment, exercising creativity, perceiving, and problem-solving. According to Kaya et al. (2019), advanced computation technologies are mainly combined with artificial intelligence that varies with degrees of maturity. Large volumes of structured and unstructured data are maintained by artificial technology. This technology is treated as a cognitive technology, which controls the cognitive activities of humans. Useful pattern an actionable insight of large dataset is extracted by a set of algorithms, principles, processes, and problem definitions of Artificial

Intelligence. Individual human behavior, interference method, and knowledge representation is controlled by the classic Artificial Intelligence approach.

An explosion of AI is involved in the execution of various tasks such as planning, moving, social and business transactions, speaking, creative, object, and sound recognition. Few important methods are helped to perform tasks; these methods are text mining, recommendation system, machine, and deep learning, natural language processing, predictive and prescriptive analysis. These methods are also utilized to solve problems related to cyber security with the observation in Artificial Intelligence techniques. Text information generated from data in Natural language generation is the mainframe by AI technologies. Data properly interpreted in the Natural Language generation process. Deep learning and procurement learning process is a structure, focus of machine learning is moved towards a process of experience-driven and sequential decision making from pattern recognition with the observation of deep learning and procurement learning processes.

CYBER SECURITY IN BANKS

A survey reveals that, in 2016, the cost of cybercrime in the global economy was $450 billion with Asian organizations accounting for more than $81 billion. Denial-of-service attacks, infrastructure attacks, and other issues around data protection are a major part of high profiling cyber-attacks (Vieira and Sehgal 2018). Approximately 70% of CEOs of the capital market and banks consider cyber security a threat to their development. Security incidents left an impact on financial service organizations 300 times more frequently compared to the business in various industries. On the other hand, the financial service industry is targeted by 33% large attacks. In this position, it is important to develop a few security programs to protect cyber threats in banking. Global banking and financial industry claim that cyber-attack consists of approximately $360 billion in costs in a year. In recent years, global ransomware attacks have an impact on financial institutions. To combat hackers many nails are trying to implement artificial intelligence.

CYBER SECURITY THREATS IN BANKS

Rapid development of commuting technology consists of many positive factors; however, these new technologies introduce a few difficult issues. Siddiqui et al. (2018) stated that, common issues such as fraud and theft are attained in new forms of cybercrime through information technology. The number and variety of cybercrimes are increasing day by day. These crimes are facilitated by information technology, which erases all country borders and globalizes cybercrime. This factor makes it harder to motor, control, detect, and prevent. Information technology is used as a tool for committing cybercrime. Few cyber-attacks directly have an impact on enterprise systems such as phishing. This kind of attack is difficult to detect, to mitigate this problem AI software tries to identify the behavioral pattern for all user accounts or devices.

Advancement of security automation is analyzed as well as integration and diverse products are able to profile key advantages. Response time is identified properly, along with these scarce resources are involved in enhancement of productivity of the talented security engineers. Artificial intelligence is implemented by human development and cutting edge research, which is able to maintain all kinds of threats. To identify, mutating, and counter evolving all threats inside the network advanced defensive capabilities are used increasingly. Artificial intelligence labs can detect all threats. Responses of banks towards cybercrime are analyzed, the concentration of single malicious agents, and a single point of attack can evolve this response towards cybercrime. As per Crisanto and Prenio (2017), the unprecedented command is provided by machine learning as well as artificial

intelligence to maintain unlimited budgets. To provide high-quality cyber security in banks it is important to analyze implementation of artificial intelligence.

USE OF ARTIFICIAL INTELLIGENCE

A multitude of reality and flavor is maintained by Artificial Intelligence techniques. Use cases of artificial intelligence are classified into three categories, these categories can provide information about potential areas of opportunities for the banking sector. These three categories are classified below:

- Enhancing customer interaction and experience: Examples are customer service improvement, voice banking, Robo-advice, biometric authentication, targeted customer offers, customer segmentation, and chatbots.
- Improving efficiency of banking processes: Examples are, predictive maintenance in IT, complaints management, automated data extraction, KYC, credit scoring, process automation/optimization, document classification, etc.
- Developing security and risk control: Examples are, AML (Anti-Money Laundering) detection and monitoring, enhanced risk control, support of data quality assurances, cyber risk prevention, compliance monitoring, payment transaction monitoring, fraud prevention, system capacity limit prediction, etc.

Figure 1: Use of AI in banking sector
(Source: Hasham2019, p.218)

- On the other hand, creation of new business opportunities and the generation of new sources of revenues is treated as a major opportunity of implementation AI in banking sector examples are investment analysis, personal finance management, asset allocation, lead generation, etc.

ARTIFICIAL INTELLIGENCE IN BANKING

Now, financial services industries can use Artificial Intelligence techniques widely, which becomes more popular in customer-facing digital challenges. Hasham et al. (2019) stated that, ability of machines as well as human thinking, reasoning, and decision making are maintained by artificial intelligence techniques. Innovation and lower costs are improved by the bank to handle apparatus and information stockpiling, due to this factor AI are developing in money related administration. However, in Technology Review Nanette Byrnes stated that counterfeit design acknowledgment, picture acknowledgment, common dialect handling, and theory age among

others is treated as a regardless of quick advance in the innovation. It is easy to state that credit scoring is not a new application; credit scoring is one of the first applications of statistical modeling in financial sectors.

On the other hand, banks are trying to gather statistical analysis, decision trees, regression, and transactional data; these factors can maintain credit risk of customers and provide proper methods by which customers can repay their loan. Improvised access and accurate scoring are enabled by artificial intelligence techniques. This technique is implemented to mitigate risk and the number of false negatives and false positives. The most suitable debit plan is selected by banks with the observation of artificial intelligence (Kose 2019). Artificial intelligence can ensure banks about the maintenance of credit risk; this factor directly has an impact on financial stability. This process is important because several supervisory requirements are present in this area; including the European Banking Authority Regulatory Technical Standards in Assessment Methodology for an internal rating based Approach. Consistency in model outputs and comparability of risk-weighted exposures are targeted by targetted standards.

AI FOR CUSTOMER INTERACTION: THE EXAMPLE OF ROBO-ADVICE AND HANDLING OF CUSTOMER COMPLAINTS

Robo-advisor is an automated system that provides investment advice and algorithm-driven financial advice. Robo-advice can collect information from individuals. Robo-advice can provide suggestions towards possible investment solutions, tailored to the client's expectations and need. This process is conducted with a combination of different technologies such as machine learning and natural language processing, artificial intelligence algorithms, and cognitive systems. Hakala (2019) stated that, great consumer experience is enabled by this technology, especially those customers who are helped by this technology who prefer digital interaction and do-it-yourself approach. Investment advice is provided by financial institutions, which help to respect an array and horizontal and sector legislation. Along with this financial market and wealth management related information is provided by Robo-advice.

7.1 Customer Complaints

Credit or financial institutions provide information about customer service for customers based on the correct regulatory framework. This process can solve complaints of customers within a specific timeframe. If customers are not satisfied with the provided response, then customers can appeal to National Competent Authorities (NCAs). Jakšič and Marinc (2019) stated that, this process is created due to large volume data that is present in this case to reply to complaints of customers. Large volumes of unstructured text documents and many queries are classified by banks into types with the help of AI techniques. This process ensures that banks are routed to the right team for resolution. Faster resolution of complaints, the national competent authority, the financial industry, and benefiting the consumer which made the complaints are maintained and solved by AI techniques. Consistency in responses to the complaints of the financial industry is evaluated by AI technologies. This process is more acceptable than the traditional manual classification process.

7.2 AI for security purpose: Fraud Prevention

Artificial intelligence is involved in the identification of fraud and other negative activities that are directly linked with financial crime generally. Fraud is classified into two categories such as external fraud and internal fraud. Attack on banks or clients for money transfer, online payment, identification fraud, etc. are considered as an external fraud. On the other hand, malevolent action from employees is considered an internal fraud. Feature

engineering, adaptive learning, supervised, and unsupervised is helpful to implement a Fraud Detection System. Collecting, analyzing, and learning from traditional data are involved in the Fraud Detection System.

Along with this, interacting with FDS maintainers is an important aspect. Suspicious events are easily identified by the Fraud Detection System, on the other hand, FDS can control fraudulent activities by suspending or blocking mentioned activities. Fraud Detection System works authentically during the time of the profile creation of customers. Financial institutions can save money with the observation of Artificial Intelligence applications. Fight of money-laundering and terrorism-financing is considered a crucial factor and other types of financial crime. Anomaly Detection is an important aspect of artificial intelligence which is involved in the prevention of fraud and cyber attack.

EXAMPLE OF USING AI TO COMBAT CYBER SECURITY

Before development of chatbots, chatbots for Customer Suppport Mapa research was conducted successfully. To break down their utilization over the managing of any account part and different enterprise ventures of customers is targeted widely. Therefore, it is observed that chatbots are dispatched by Bank of America, American Express, and MasterCard, due to the helping customers explore applications all the more viable, customer questions speedier and providing help to consumers more cost viable. In addition, in the case of computerized reasoning, it is observed that this process is rotated around client support. Both in money related administration and past are presented with a large number of illustrations; these are not completely falsely insightful. According to Castelli et al. (2016), chatbots are conducted with the choice of trees; along with this acknowledge questions are unable to provide frequent replies toward the band's FAQs (Kanabolo and Gundeti, 2019). A few important managed learning processes are implemented; however, it is a long way from conscious robots of sci-fi. The property innovation process is introduced by banks that can maintain destination outsider edge (Facebook Messenger), application (for example, Barclays Launchpad, for instance) and destination, on the other hand, chatbots, are propelled by Facebook.

ADVANTAGES OF ARTIFICIAL INTELLIGENCE FOR THE BANKING SECTOR

The Expense pattern of customers is easily evaluated by AI techniques for banking authorities. Banks can introduce customized investment plans which directly have an impact on customer budgeting plans. Customers are informed by the bank about their expenses and investment based on data. To understand customer's behavior and preferences, AI technology helps to track traditional data and other data sources, this factor can enhance the experience of employees (Cidon et al. 2019).

Artificial intelligence processes are conducted with the presence of a huge number of data and identify patterns that might elude human observers. Artificial intelligence is able to play an important role in fraud prevention. Many financial service providers are involved in the development of artificial intelligence and machine learning solutions to identify fraud in real-time.

Online banking or mobile banking becomes popular as this process provides 24/7 transactions, in this case, banks can access customer data with the help of artificial intelligence techniques. Along with these detailed demographics, records of online and offline transactions and website analytics are integrated and analyzed properly by the machine learning process.

Risk assessment process is a very complex and critical process, both accuracy and confidentiality required while providing loans. Agarwal (2019) stated that, artificial intelligence can handle the risk assessment process easily and relevant data of customers is analyzed by AI technologies. Information related to the latest transaction,

financial activity, and market trends is analyzed and combined by AI techniques, by which AI evaluates the potential risk of providing loans. Artificial intelligence is involved in protecting personal data that can control various kinds of cyber threats. Banking sectors are trying to implement Artificial Intelligence to compose high-quality security. Banks and financial sectors can collect information about the user's behavior (Sindhu and Namratha 2019). AI is involved in reducing the cost of appointing additional employees to handle all kinds of customer-oriented operations. Artificial Intelligence converts task humans to AI, which increases speed of the task and reduces cost-related issues. Customer experience and employee effectiveness are enhanced by AI techniques. Artificial intelligence can find out various kinds of suspicious activities, fraud, and support investigators. The fraud prevention process is implemented by AI to enhance financial security.

DISADVANTAGES OF AI FOR BANKING SECTOR

To maintain and conduct artificial intelligence it is important to invest huge costs, this technique is conducted with very complex machines. According to Kurode (2018), Artificial Intelligence is conducted with advanced software programs; to meet the need of the changing environment it is important to update this software regularly. Artificial intelligence cannot make any judgment call, this technique only helps to learn and improve. AI can provide a lot of power to individuals who control this system. Due to this factor, it is stated that AI carries the risk and takes control away from humans while dehumanizing action in several ways. If employees are unable to control artificial intelligence, then this technique can leave a negative impact on the bank and financial industry (Dimitrios 2019). Artificial intelligence replaces humans in the workforce with machines, and wide-reaching unemployment is increased due to AI.

CONCLUSION

Artificial intelligence techniques are used widely in banks and financial institutions. Based on this paper it is concluded that artificial intelligence was introduced as a concept to mimic human brains. AI technology is used to enhance customer interaction and experience, enhance the efficiency of banking processes, and develop security and risk control. The importance of artificial intelligence in the banking sector is concluded in this paper. Information About cyber-attack and the prices of solutions is provided by AI towards banks and financial institutions. Various issues related to fraud and data breach are identified by artificial intelligence techniques.

REFERENCES

1. Agarwal, P., 2019, March. Redefining Banking and Financial Industry through the application of Computational Intelligence. In *2019 Advances in Science and Engineering Technology International Conferences (ASET)* (pp. 1-5). IEEE.
2. Castelli, M., Manzoni, L. and Popovič, A., 2016. An artificial intelligence system to predict quality of service in banking organizations. Computational intelligence and neuroscience, 2016.
3. Cidon, A., Gavish, L. and Perone, M., Barracuda Networks Inc, 2019. System and method for ai-based anti-fraud user training and protection. U.S. Patent Application 15/693,353.
4. Crisanto, J.C. and Prenio, J., 2017. Regulatory approaches to enhance banks' cybersecurity frameworks. Financial Stability Institutions (FSI) Insights on policy implementation, (2).
5. Dimitrios, K., 2019. Can artificial intelligence replace whistle-blowers in the business sector?. International Journal of Technology Policy and Law, 3(2), pp.160-171.
6. Hakala, K., 2019. Robo-advisors as a form of artificial intelligence in private customers' investment advisory services.

7. Hasham, S., Joshi, S. and Mikkelsen, D., 2019. Financial Crime And Fraud In The Age of Cyber Security. McKinsey & Company.
8. Jakšič, M. and Marinč, M., 2019. Relationship banking and information technology: The role of artificial intelligence and FinTech. Risk Management, 21(1), pp.1-18.
9. Kanabolo, D. and Gundeti, M.S., 2019. The Role of Artificial Intelligence (AI) in Medical Imaging: General Radiologic and Urologic Applications. Medical Imaging: Artificial Intelligence, Image Recognition, and Machine Learning Techniques, p.27.
10. Kaya, O., Schildbach, J., AG, D.B. and Schneider, S., 2019. Artificial intelligence in banking. Artificial intelligence.
11. Kose, U., 2019. Using artificial intelligence techniques for economic time series prediction. In Contemporary Issues in Behavioral Finance. Emerald Publishing Limited.
12. Kurode, T., 2018. Review of Applicability of Artificial Intelligence in Various Financial Services in India. Journal of Advance Management Research, 6.
13. Siddiqui, M.Z., Yadav, S. and Husain, M.S., 2018. Application of artificial intelligence in fighting against cyber crimes: A REVIEW. International Journal of Advanced Research in Computer Science, 9(Special Issue 2), p.118.
14. Sindhu, J. and Namratha, R., 2019. Impact of Artificial Intelligence in chosen Indian Commercial Bank-A Cost Benefit Analysis. Asian Journal of Management, 10(4), pp.377-384.
15. Vieira, A. and Sehgal, A., 2018. How banks can better serve their customers through artificial techniques. In Digital marketplaces unleashed (pp. 311-326). Springer, Berlin, Heidelberg.