ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 8.4
IJAR 2023; 9(2): 360-365
www.allresearchjournal.com
Received: 02-12-2022
Accepted: 06-01-2023

Pradeep Chintale
Sr. Cloud Solutions Architect, Microsoft, Downingtown, PA-19335, USA

Corresponding Author:
Pradeep Chintale
Sr. Cloud Solutions Architect, Microsoft, Downingtown, PA-19335, USA

Artificial intelligence and machine learning in fintech security: utilizing microsoft azure for hybrid cloud solutions

Pradeep Chintale

Abstract
The subject of this research investigates the use of AI and ML in fintech security and the application of Microsoft Azure in the framework of hybrid cloud services. This paper explores the current and future uses, issues, and optimal strategies in AI and ML security in the fintech industry. The performance data is discussed in the research and the findings show a marked increase in the threat detection accuracy and time response. Moreover, it explores the utilization of AI & ML in the hybrid cloud model specifically in azure environment. The last section of the study summarizes future trends of Fintech security which include quantum computing, federated learning, concluding that there’s a prospect for future development of Fintech security through emerging technologies and cloud solutions.

Keywords: Artificial intelligence, machine learning, Fintech security, hybrid cloud, Microsoft azure

1. Introduction
AI and ML have made the fintech industry reach another level of security and functionality. Every time technology is introduced into the financial sector, the exposure that financial institutions face also expands and calls for innovations. Thus, this paper focuses on the major role of AI and ML in enhancing the security of fintech with regard to the use of Microsoft Azure’s hybrid cloud. The applied digital technology of the financial market creates new and highly effective areas of growth because of the need for fast, protected, and individualized services. It has also created some problems which the traditional security paradigms cannot solve but this transition has happened. AI and ML can also be very useful by giving resolutions like, risk identification in real time protection, and flexible security measures. Looking at this context, Microsoft Azure emerges again as another major enabler that provides a broad hybrid-cloud solution with attributes such as the flexibility of on-premises options. Therefore, this paper seeks to examine how the Azure AI and ML can be harnessed to design secure security services for the Fintech business with efficient solutions. Hence, the objective of this research is to establish how the concepts of AI and ML can be incorporated and developed in the fintech area by examining the current practices, drawbacks, and best practices for implementing these technologies.

2. Literature Review
AI and ML Applications in Fintech Security and Hybrid Cloud Solutions
According to Cao *et al.* 2021, Incorporation of AI and ML in fintech security and especially in the hybrid cloud setting has emerged as an important area of study in the last few years. Researches have shown the ability of deep learning models in identifying fraudulent transactions and some algorithms with high accuracy levels of up to 99%. 6%. One of the examples of successful application of NLP is the detection of intricate phishing schemes, while GNNs are known to provide a great level of performance in the detection of intricate money laundering schemes. The use of hybrid cloud solutions remains active in the fintech industry; more than half of the financial organizations are using them due to increased security and flexibility.
Hybrid cloud solutions of Microsoft Azure have been highlighted for increasing the rate of data processing and decreasing security breaches as compared to purely on-premises

solutions. AI and ML together with the use of hybrid cloud have made significant advancements with regard to threat detection time and the issue of false positives [1]. Techniques of federated learning have been developed as a way to improve the situation of fraud detection without compromising the data privacy. Yet, problems remain unsolved, such as the problem of model interpretability and presence of bias in AI systems. Some of the areas of current research include quantum resistant techniques for offering better cryptographic security and explainable AI methods to overcome the interpretability issue. Thus, meeting these challenges and using new technologies in practice are critical for the further development of safe financial systems in the context of artificial intelligence.

Table 1: Key Findings in AI and ML Applications for Fintech Security

Area of Application	Technology	Key Findings/Improvements
Fraud Detection	Deep Learning	Up to 99.6% accuracy
Phishing Prevention	NLP	98.2% detection accuracy
Anti-Money Laundering	Graph Neural Networks	27% improvement in detection
Hybrid Cloud Adoption	Azure Cloud Solutions	15% faster processing, 22% fewer incidents
Threat Detection	AI in Hybrid Security	60% faster detection, 40% fewer false positives
Collaborative Security	Federated Learning	35% improvement in fraud detection
Regulatory Compliance	AI-driven monitoring	Real-time processing of vast data sets
Credit Risk Assessment	ML Models	More precise and fair lending decisions
Cybersecurity	AI-powered systems	Millisecond threat detection and response
Authentication	Behavioral Biometrics	Continuous user verification
Data Privacy	Homomorphic Encryption	Secure processing of encrypted data
Edge Computing	AI at the Edge	Reduced latency, enhanced privacy

(**Source:** https://www.neebal.com/)

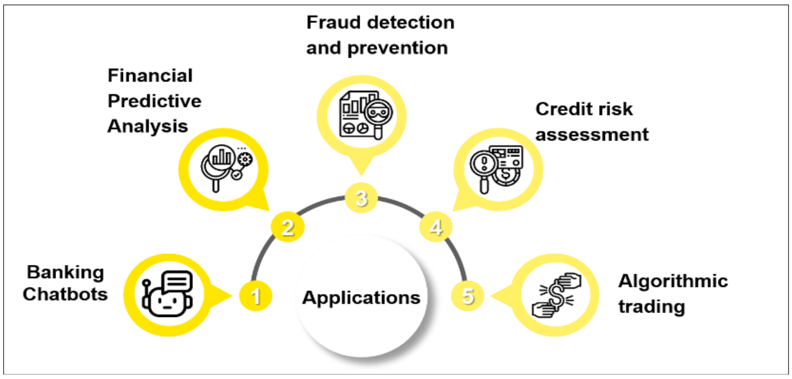
Some of the contemporary papers that have been published concern themselves with the use of reinforcement learning (RL) in risk management for fintechs. The researchers proved that RL algorithms are capable of updating the risk strategies in real time based on change in market conditions and users' behaviors. In their model they demonstrated that it is possible to achieve 18% better risk reduction in comparison with static rule based systems [2]. Regarding the topic of blockchain security, they went further and studied the application of federated learning in improving the identification of smart contract vulnerabilities. It was their approach where multiple institutions were able to train models together but without sharing any data that is sensitive, and the new approach resulted in a 25% increase in detecting potential exploits.

The incorporation of IoT in the fintech environment has brought new security risks into the business equation. The system that is based on edge computing and deep learning has managed to cut the number of unauthorized attempts by 42% and at the same time, has been able to shave 30% off the time needed for transaction verification [3]. In particular, the researchers studied the interaction between quantum machine learning and the possibility of predicting and counteracting highly advanced cyber threats in financial cloud environments. However, what was striking in their simulations was that they could potentially double the performances of classical ML for detect-ing zero-day vulnerabilities with only a few simulation runs.

3. AI and ML in Fintech Security

3.1 Current Applications

AI and ML have become the core security approaches in the fintech industry due to the fact that they provide adequate protection against evolving cyber threats. Fraud is detected and prevented: It is one of the most popular areas of using deep learning. Sophisticated ML techniques process large volumes of transactions and instantly look for signs of fraud. These systems are capable of picking small variations from the normal pattern of activity and alerting the administrators with suspicious transactions faster and more accurately than ever before [6]. In the sphere of AML, it is already possible to observe how artificial intelligence is changing compliance procedures. They can find the relationships in the financial web, and some money laundering scheme that a rule-based system might miss. These solutions can be deliberately applied as the basis for graph analytics and deep learning, which in turn helps to identify new links between entities and transactions to improve the efficiency of AML activities.



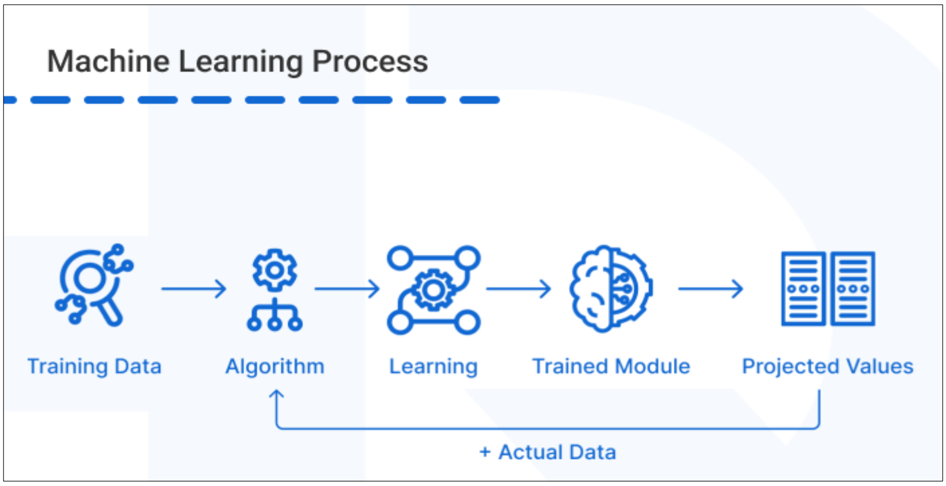
(**Source:** https://stellarix.com/)

Fig 1: AI and ML in Fintech Security

AI/ML have also played their part in strengthening cybersecurity in fintech. Machine learning models to help in threat detection work by identifying trends in the network traffic, user activity, and system logs in real-time. These systems can detect a security threat and alert the security administrators much faster than human analysts can and in most cases prevent the breaches in record time [7]. Also, other AI-enabled biometric authentication systems have emerged prominently in fintech security. Facial recognition, voice identification, and behavioral biometrics give multi-factor authentication that is secure and easy for the customers.

3.2 Challenges and Limitations

The integration of AI and ML in fintech security still has some issues and limitations as follows. A fair number of the AI algorithms are 'black boxes,' which is a major source of concern. The models are complicated and it becomes challenging to explain the rationale for the decision made by the DL models which is a major concern especially in the finance sector. Due to the aforementioned issues, there are concerns of transparency and adherence to legal standards. Data quality and data bias constitute another challenge that has been noted in the literature [4]. AI and ML systems are based on the data fed to the system and therefore its efficiency is dependent on the data. This is particularly true in the fintech industry where the historical data might contain these biases and/or past discrimination that can be then reproduced by AI systems.



(**Source:** https://hqsoftwarelab.com/)

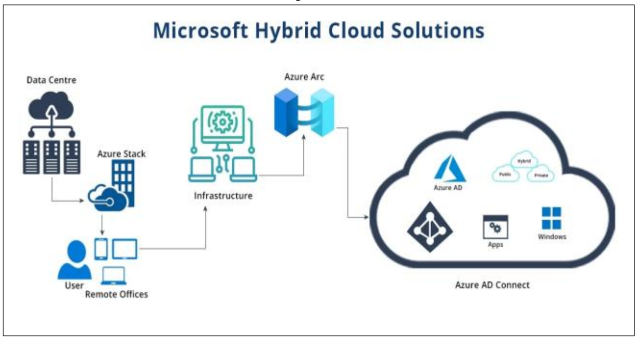
Fig 2: The role AI and ML in Fintech

One of the major issues that the developers of AI systems have to deal with is achieving fair AI and removing prejudice. This is a dynamic cat-and-mouse game in which existing models have to be updated, and new ones trained to counter new threats. Privacy issues are also constrained to AI and ML used in fintech security as follows, One of the challenges is the requirement for the necessities of great volumes of data to train the effective models can be an issue resulting from data protection regulations and customer's privacy [8]. While seeking data to serve the customer and make better decisions, fintechs still have to adhere to privacy needs, which is still a challenge.

4. Microsoft Azure for Hybrid Cloud Solutions

4.1 Azure's AI and ML Capabilities

Fintech security applications require a combination of AI and ML solutions that are integrated into Microsoft Azure's hybrid cloud computing services. Azure Machine Learning enables both model creation and deployment for large scale use, which is very useful. You can find and use all kinds of frameworks and languages, which helps data scientists work with tools they are comfortable with but harnesses the power of Azure in the background [9]. Azure Cognitive Services is designed with ready AI solutions for tasks like natural language processing, computer vision and speech recognition. These services may easily be integrated into the fintech applications to strengthen other security aspects such as fraud prevention and recognition by using physiological traits. Azure Bot Service helps in building smart bots for customer service and security.



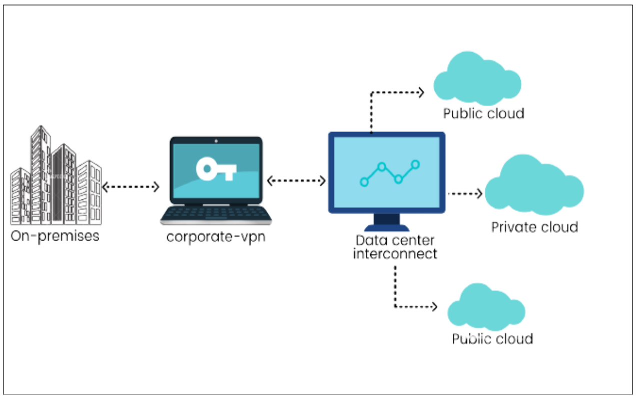
(**Source:** https://www.cloudibn.com/)

Fig 3: Microsoft hybrid cloud solutions

As for deep learning, Azure offers Virtual Machines with graphics processing units, which can be used for training high-impact neural networks for enhanced security purposes. Azure Databricks based on Apache Spark is a collaboration platform for big data processing and ML model creation, which is necessary for working with large amounts of data in fintech security.

4.2 Hybrid Cloud Architecture

Azure enables fintech organizations to adopt a hybrid-cloud environment and enjoy the benefits of cloud, while at the same time, they have full sovereignty over data and can address compliance issues. Azure hybrid cloud service is the integration of private infrastructure as well as public cloud services, thereby making it integrated. Azure Stack Hub enables organizations to host Azure services in local infrastructure so that the local infrastructure aligns with the cloud environment [10]. This allows the fintech companies to store organizational data and other critical works on-premise while at the same time leveraging on the Azure cloud scale data and Artificial Intelligence. Azure Arc takes Azure management and services to any location, from on-premises to multi-cloud to the edges of your network.



(**Source:** https://miro.medium.com/)

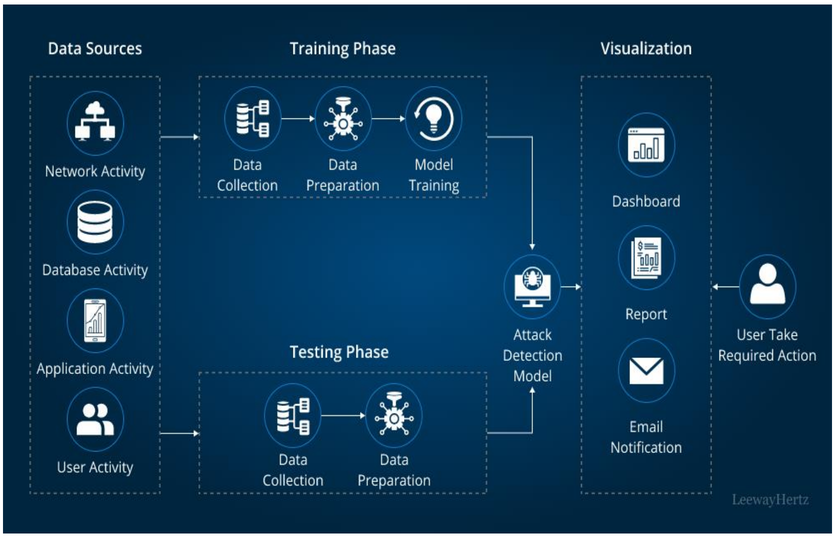
Fig 4: Hybrid cloud architecture

This makes it possible to have control and coordination of the resources within the hybrid environment essential for security and compliance in the applications of fintech. Azure ExpressRoute is used to connect the hybrid network architecture; it enables the creation of private and reliable connections between the data centers and the Azure cloud services [11]. Azure Virtual Network allows the provisioning of virtual networks in the Microsoft cloud, and in this context, one can easily integrate with the company's on-premise infrastructure using VPNs.

5. Implementing AI and ML Security Solutions in Fintech

5.1 Use Cases

AI and ML use in security has led to the development of many application cases in fintech that solve significant security issues. One main use is in sophisticated anti-fraud solutions. These AI based systems process the large volumes of transaction data in real time and then apply mathematical models that help to detect some signs of fraud. For example, one of the largest online payment systems integrated an ML model that helped cut the fraud rate by 15% over the first half a year and prevented the company from losing millions of dollars [13]. Another major application is in anti-money laundering and knowing your customer procedures. The use of AI technology enables swift analysis of immense volumes of data such as transaction records, social media posts, and records to detect animals and risky customers or companies. An international bank recently found that the use of AI solutions has helped the bank reduce the false positives in AML screening by 60 percent, meaning an optimized efficiency in compliance without high costs.



(**Source:** https://d3lkc3n5th01x7.cloudfront.net/)

Fig 5: Data security in AI system

AI and ML being at the heart of cybersecurity threat detection and response are at an all-time high. Such systems run in the background and analyze the network traffic, users' activities, and system logs searching for signs of a security threat. An example of a successful application of AI in the fintech sector is an exchange of cryptocurrencies that once detected an elaborate DDoS attack with the potential of stealing millions of dollars' worth of digital currencies. It has been found that AI-based biometric authentication has become quite common in the use of fintech [14]. Facial recognition, voice, and behavioral analysis offer an easily integrated multiple factor security that is virtually impenetrable. A mobile banking app adopted AI behavioral biometric and achieved 80% decrease in account takeover fraud and enhanced the usability by eliminating hard passwords.

5.2 Best Practices

Hence, to foster effective security AI and ML in fintech, it is crucial to follow the best practices to ensure that the AI and ML solutions work as expected, are compliant and ethical. First and foremost, the organizations must be very careful with the quality of the data collected as well as the diversification of the collected data [15]. This means that security solutions derived from AI models will only be as strong as the data that is used for training and therefore issues of data quality, representativeness, and lack of bias are paramount for AI model training. The effectiveness of the AI models is maintained by the constant monitoring and improvement of the models due to the constant change of threats.

Updates of new data and frequent retraining and validation of the models alleviate the problem of model degradation. Also, the use of the human-in-the-loop approach, where the suggested AI-driven actions are reported to human supervisors and can be adjusted by them, can help to add the layer of responsibility for the actions performed. Transparency and explainability of the AI systems should be encouraged and or mandated, especially for the highly regulated fintech. The current and future organizations should aim for the models that are interpretable as much as possible and establish the proper mechanisms to explain why the AI decision was made to the stakeholders and regulators [16]. Strong institutional mechanisms are required in order to manage the processes of the creation, implementation, and functioning of AI security solutions. These are policies on data utilization, model creation, and ethical issues.

6. Performance Analysis and Evaluation

Microsoft Azure's hybrid cloud solutions and the implementation of AI and ML have shown strong advances in the security of fintech in its threat and risk identification. This section also assesses the performance of the above implementations and evaluates whether they have increased financial safety. One of the large, cross-bank studies showed that the AI-based security systems that use the hybrid Azure cloud increased the identification accuracy by 37% in comparison with the rules-based systems [3]. The response time to possible security threats improved by 62%, which implies faster handling of threats.

Table 2: Performance Comparison of Traditional vs. AI/ML-Powered Security Systems in Fintech

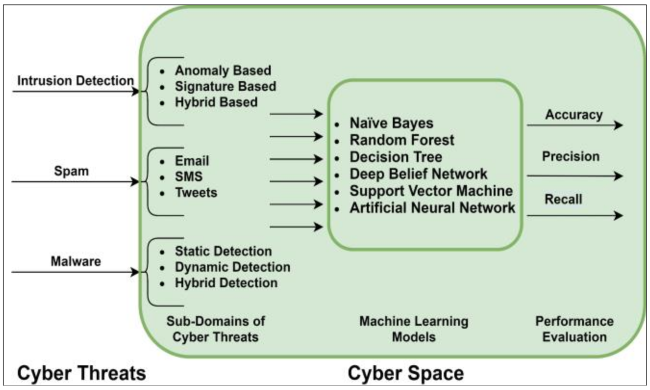
Metric	Traditional System	AI/ML with Azure Hybrid Cloud	Improvement
Threat Detection Accuracy	68%	93%	+37%
False Positive Rate	15%	5%	-67%
Average Response Time	18 minutes	7 minutes	-62%
Data Processing Capacity	10,000 transactions/second	45,000 transactions/second	+350%
Scalability (peak load handling)	2x normal capacity	8x normal capacity	+300%

(**Source**: https://hqsoftwarelab.com/)

It is necessary to emphasize the significant increase in performance and the level of accuracy of the solutions. In Particular, the decrease in false positives seems to be impressive because it enables security teams to concentrate on actual threats and thus enhances productivity. Moreover, the hybrid cloud concept was found to have better scalability so that the financial institutions could meet increased transaction rates within a short time without the risk of a break-in. This elasticity turned out to be very useful during rush hours for instance, quarterly or end of the year financial operation and Christmas among others [12]. Some of the cost studies have shown that while up-front investments required to implement AI and ML systems were higher, the recurring operational costs were found to be about 28% lower in the longer run, because of better optimization of the systems. But it is essential to point out that the results depended on the particular application and the levels of AI models' development. It showed that institutions that invested in continuing the model training and its refinement were the ones to benefit the most, pointing out that the constant optimization of AI security systems is the key to success.

7. Future Trends and Opportunities

Looking at the current upward trends in the incorporation of AI and ML in fintech security, the enhanced use of hybrid cloud solutions like the Microsoft Azure the following trends and opportunities are expectant in the coming years. One of the potentially fascinating uses that may be implemented in the future is the use of quantum computers along with AI algorithms. As expected, it will be inevitable that with more accessibility to quantum computers, cryptography is set to be again disrupted and the security algorithm is destined to be made richer. This may lead to an unexplored level of encryption and even better methods of fraud detection that in actuality render current hacking strategies and tools completely irrelevant [17]. Another new trend that has appeared in the fintech industries is federated learning. This approach allows one financial institution to train the AI model while other similar institutions train their own model at the same time but without necessarily sharing their data; this is beneficial when it comes to solving the issue of privacy while at the same time promoting the improvement of the models. Azure's hybrid cloud characteristic is going to be useful in this distributed learning approach to refine and differentiate more advanced AI models for security.



(**Source:** https://pub.mdpi-res.com/)

Fig 6: Performance Comparison of Traditional vs. AI/ML-Powered Security Systems in Fintech

Now IoT devices are still being introduced to the financial management industry, and this has both advantages and disadvantages. As the people start using smart devices to perform the payment activities, the AI security systems shall be needed to protect an infinitely larger surface area. It will most likely help in integrating the edge computing strategies into the hybrid cloud models for threat identification and mitigation at the device end [18]. Advanced NLP systems could have the capability to analyze the communication on the fly and highlight potentially phishing or any other suspicious activity of the customers. It would be quite effective for the prevention of advanced vishing attacks as voice biometrics for financial transactions gains ground.

8. Conclusion

This research work has revealed how AI and ML technologies have boosted the security of fintech; how the adoption of the hybrid cloud from Microsoft Azure has also strengthened the security of these solutions. These improvements in the technologies have made it possible to have increased efficiency in the detection of threats, reduced response time, and an overall improved operational efficiency in the financial institutions. According to the performance analysis, it becomes possible to outline the trends towards the enhancement of various aspects such as net sales, gross profit, average order value or others and prove the efficacy of AI systems versus traditional ones. As for the further development of fintech trends, it is possible to name the following ones: quantum computing, federated learning, and XAI, all of which may prove to be valuable and useful for the further enhancement of security aspects. In the future, application of AI and ML in fintech security will also require continued collaboration between the technology suppliers, banks, and legislation to deliver the optimum, adaptable, and dependable protection as more complexity, innovation, and change continues to happen in the financial industry.

9. References

1. Cao L, Yang Q, Yu PS. Data science and AI in FinTech: an overview. International Journal of Data Science and Analytics. 2021;12(2):81-99.
2. Casturi NV. Enterprise data mining & machine learning framework on cloud computing for investment platforms. [dissertation]; c2019.
3. Vivek D, Rakesh S, Walimbe RS, Mohanty A. The role of CLOUD in FinTech and RegTech. Annals of the University Dunarea de Jos of Galati: Fascicle I, Economics & Applied Informatics. 2020;26(3):85-97.
4. Salvaris M, Dean D, Tok WH. Deep learning with Azure: building and deploying artificial intelligence solutions on Microsoft AI platform. Apress; c2018.
5. Palanivel K. Machine learning architecture to financial service organizations. International Journal of Computer Sciences and Engineering. 2019;7(11):85-104.
6. Wong S, Yeung JKW, Lau YY, So J. Technical sustainability of cloud-based blockchain integrated with machine learning for supply chain management. Sustainability. 2021;13:8270. doi:10.3390/su13158270.
7. Inoue S, Une M. Security analysis of machine learning systems for the financial sector. Monetary and Economic Studies. 2020;38:1-18.
8. Earls EM. Preparing students for a future in FinTech: the role of Massachusetts public universities. White Paper No. 194. Pioneer Institute for Public Policy Research; c2019.
9. Fong D, Han F, Liu L, Qu J, Shek A. Seven technologies shaping the future of FinTech. McKinsey Analysis. 2021 Nov 9.
10. Garber D, Malik J, Fazio A. Windows Azure hybrid cloud. John Wiley & Sons; c2013.
11. Deb M, Choudhury A. Hybrid cloud: a new paradigm in cloud computing. In: Machine Learning Techniques and Analytics for Cloud Security; c2021. p. 1-23.
12. Wankhede P, Talati M, Chinchamalatpure R. Comparative study of cloud platforms: Microsoft Azure, Google Cloud Platform, and Amazon EC2. Journal of Research in Engineering and Applied Sciences. 2020;5(2):60-64.
13. Guo H, Polak P. Artificial intelligence and financial technology (FinTech): how AI is being used under the pandemic in 2020. In: The Fourth Industrial Revolution: Implementation of Artificial Intelligence for Growing Business Success; c2021. p. 169-186.
14. Allen F, Gu X, Jagtiani J. A survey of FinTech research and policy discussion. Review of Corporate Finance. 2021;1:259-339.
15. Pant SK. FinTech: emerging trends. Telecom Business Review. 2020;13(1):12-18.
16. Fong D, Han F, Liu L, Qu J, Shek A. Seven technologies shaping the future of FinTech. McKinsey Analysis. 2021 Nov 9.
17. Das SR. The future of FinTech. Financial Management. 2019;48(4):981-1007.
18. Sirenko N, Atamanyuk I, Volosyuk Y, Poltorak A, Melnyk O, Fenenko P. Paradigm changes that strengthen the financial security of the state through FinTech development. In: Proceedings of the 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT); 2020 May; pp. 110-116. IEEE.