ISSN: 2754-6705

Journal of Mathematical & Computer Applications

SCIENTIFIC Research and Community

Review Article

Open Access

Audit Trails and Logging Biometric Authentication for Data Security in Banking Using Reporting Tools

Pranay Mungara

USA

ABSTRACT

Many sectors, including government, consumer electronics, and business security systems, are beginning to see the potential benefits of biometric authentication. More and more businesses, organisations, and individuals are turning to biometric security measures to keep cyberspace safe from malicious actors. Cybersecurity is the practice of protecting computer systems, networks, data, and software from intrusion and other forms of cyberattack. The provision of banking services through electronic means is known as "cyber banking." The rise of online banking is a reflection of the general shift in consumer spending habits. Despite its many advantages, online banking has been plagued by security breaches. Biometric security ensures the identity of individuals by confirming their behavioural and physical characteristics. It is the gold standard of physical security when it comes to verifying identities. Biometric authentication holds that individuals can be uniquely identified by their intrinsic physical or behavioural characteristics. To combat these difficulties, a plethora of security safeguards have been integrated across the entire online banking service. A major danger to the occurrence of criminal or terrorist behaviour, cybercrime has deep roots globally. These threats can jeopardise both internal and external security if no one in charge takes them seriously. Money and personal information are at risk if cybercrime goes undetected. Attacks on the Internet and its supporting infrastructure have happened before. Every single day, crimes involving computers occur, such as hacker attacks and online fraud. In order to combat the threat of cybersecurity and offer the banking industry with a high level of safety and security, the study delves into the essential characteristics of biometric systems in both conventional and Islamic banking.

***Corresponding author**

Pranay Mungara, USA.

Received: May 03, 2023; **Accepted:** May 09, 2023, **Published:** May 16, 2023

Keywords: Data Security, Biometric Authentication, Banking

Introduction

A more specialised definition of illegal behaviour that is centred on the internet and information technology is referred to as cybercrime. Particularly for nations that are still in the process of growing their economies, cybercriminals' attacks present an increasingly challenging dilemma. Acquiring sensitive information with the intention of utilising it to obtain complete control and major advantages is the objective of international cyber terrorism. In recent years, the banking industry has been impacted by a worldwide economic crisis, which has resulted in the industry being obliged to undergo reorganisation, notably in some countries. In addition, consumers on both the individual and industrial levels have lost faith in the financial system, which has suffered significant damage. It is particularly challenging for financial institutions to acquire new customers in the fiercely competitive business environment that exists today [1].

The term "biometric" refers to the distinctive physical characteristics of an individual, such as fingerprints, finger scans, and facial geometry, that are used to identify one person from another. The majority of the time, this technology is utilised for the purposes of identification, access control, and the identification of those subject to surveillance. When it comes to security systems, biometrics are most commonly utilised in environments where physical security is of utmost importance and theft is a concern. During the global financial crisis, banks were under to a great deal of pressure to maintain their levels of liquidity. In general, empirical data reveals that banks that have sufficient liquidity are able to fulfil their payment commitments, but banks that do not have sufficient liquidity are unable to follow through with their obligations. The Global Financial Crisis (GFC) highlighted how quickly liquidity risk may spread, as it occurred when funding sources were decreasing and concerns about asset value and capital sufficiency were emerging [2].

Critical financial data ought to be safeguarded by an artificial intelligence-based access control system that is both scalable and flexible. This is because the majority of banking and finance services and information are now stored on the cloud. Encryption, two-factor authentication, and authorization are all built-in security elements that can be utilised by financial institutions through the utilisation of systems. Access controls, on the other hand, are more significantly important than infrastructure and property when it comes to securing the information of customers and businesses. Banks that make the decision to develop their noninterest revenue businesses are confronted with more interbank rivalry as a consequence of the significant financial liberalisation and globalisation expansion. This is done in order to expand, achieve efficiency, and reduce idiosyncratic risk [3, 4].

There is a close connection between cybercrime and cybersecurity. The security managers of a firm are responsible for ensuring that the organisation's environment remains secure by enhancing the security layers and protecting the information infrastructure. Cybercrimes either involve the use of computers as the target of the crime or as a medium for the storage of the criminal activity. It is possible for computers to function as both a target and a storage device, in accordance with the manner in which the information that they store is altered or accessed. The ability of computers to store information that can be used to commit a crime is essential. ICT has resulted in unanticipated consequences, which have lead to an increased awareness of a variety of cybercrimes. There have been a variety of businesses that have been affected by cybercrime, and one of those areas is the banking industry. This industry has been the target of a variety of cybercrimes, including phishing, identity theft, ATM fraud, and denial of service assaults [5, 6].

In addition, certain financial institutions make use of a mix of biometrics. The conclusion that can be drawn from this is that the combination of multi-factor authentication and biometrics verification results in the creation of a layer of protection that is nearly impossible to breach. Data mining tools are utilised by numerous banking sectors for a variety of purposes, including but not limited to client segmentation and productivity, advertising, credit ratings and authorization, non-payment of payments, and fraudulent transactions. Cybercrime is a risk that is greater than it has ever been. When compared to traditional crimes, cyber fraud and criminal conduct that is carried out through the use of electronic equipment such as mobile phones, computers, and other network devices are classified as a type of crimes that are transitional in nature. In order to achieve their goals, cybercriminals adopt a wide range of strategies, which are determined by their skill set, desires, and aims. The exponential rise in the number of cybercrimes is the most significant challenge facing financial institutions in the twenty-first century, and the protection of the internet is currently more crucial than it has ever been [7, 8].

Literature Review

The Islamic finance and capital markets are one of the segments of the global financial markets that is increasing at the quickest rate. Due to recent developments in Islamic finance and the stock market, the environment in which the financial industry operates has undergone a tremendous transformation. Investors and depositors all over the world now have the opportunity to consider Islamic banking as a viable choice as a result of its spectacular growth. The expansion of Islamic banking is occurring at a rate that has not been seen in the past twenty years, despite the fact that the current financial framework and business methods are not compatible with one another. At the end of 2008, the total amount of Islamic banking reached $951 billion, with activities taking place in more than fifty countries. In spite of the fact that Islamic banking is confronted with a multitude of obstacles, there are three that are essential to the continued existence of the sector. The first of these challenges is Sharia compliance in the operations of Islamic banking in an environment where interest-based practices are dominant, particularly in Muslim cultures [9].

It is also important to consider how professionals working in the financial sector evaluate the system's performance and how well it can fulfil all of the requirements that are imposed by industry and commerce. Third, the number of Muslims who believe that the operations that are now being carried out in Islamic banking are Sharia-compliant or are simply duplicates of Western procedures that are being shrouded under the name of Sharia. Together, the fields of finance and technology are referred to as FinTech. Clients of Islamic finance is provided with financial services in accordance with the laws and guidelines that are described in Shariah for Islamic finance. In the same way that Islamic finance has expanded fast over the past two decades, FinTech has experienced significant growth over the previous ten years. The primary objective of Islamic finance is to utilise financial mechanisms that are in accordance with Shariah in order to hasten the process of social and economic development. "FinTech is technologically enabled financial innovation that could result in new business models, applications, processes, or products with an associated significant effect on financial markets and institutions and the provision of financial services," according to the definition provided by the Financial Stability Board (FSB) [10].

Audit Trail – Purpose, Importance and Best Practices

There is a register that records every action, event, or activity that a user or a system did with your data. This is known as an audit trail. As a result, it may be associated with the creation, alteration, or deletion of records, or it may be a series of automatic system operations (Syslog). Naturally, the daily amount of audit logs can range from hundreds for smaller organisations to hundreds of thousands for larger organisations, which makes it extremely difficult to keep track of each and every one of them. Because of this, having a technology that allows for automated tracking is not only beneficial but also required [11]. In addition, figure 1 illustrates the process of comprehending the inspection trail.

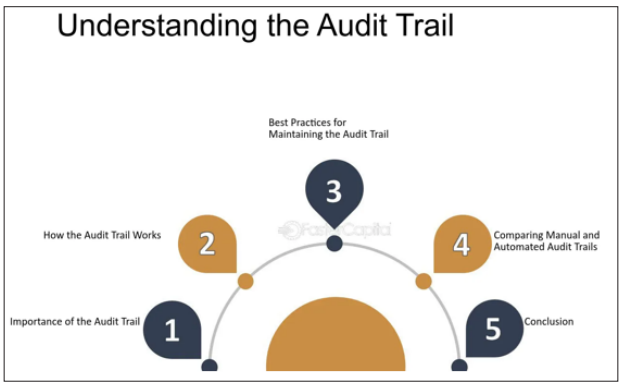

Figure 1: Understanding the Audit Trail

An organization's audit trail is essential because:
Compliance - It is actually mandatory that you maintain an audit trail.

Internal Fraud - your data is being accessed by an excessive number of systems or individuals. Whatever the situation may be, keeping track of everything is a major challenge due to the time and energy it consumes, the resources it consumes, and the hidden risks that can result from improper execution.

Data Breach - The level of activity and innovation displayed by cybercriminals is increasing year after year. There is a nearly 30% chance of a data breach occurring if you deal with sensitive data-and personal data is quite sensitive.

What are the Different Solutions for Audit Trail

It is the responsibility of each business to choose how audit trails will be stored and monitored. Some potential approaches to this problem are as follows:

1. Make use of your software's pre-existing features and capabilities to monitor data usage. Aside from the time and manpower needed, the complexity of making use of the audit trail data increases as an organization's size or number of

software applications grows. Not only are many rules and security standards requiring this method, but it also makes it exceedingly difficult to observe everything at once and conduct correlation analysis [12].

2. In order to aggregate your logs, give insights, and detect risks, you should use security information and event management (SIEM) software, which is the most prevalent corporate logging solution. The SIEM data structure could be difficult to achieve without a great deal of knowledge and experience, and this varies from product to product.
3. Companies frequently employ generic log collectors, which are generally open-source products. This solution is great for app developers, but it won't work for audit trails. When it comes to collecting access logs and organising data, these log collectors are top-notch. But it wasn't intended to be an audit trail.
4. A generic system that incorporates all of the aforementioned features (such as SIEM, general log collector, IoT, etc.) is a security platform all-in-one; nevertheless, it has limited options for an audit trail. The audit logs' security is also uncertain. As with any software-for-all solution, this platform's management can eat up a lot of internal resources.
5. Personalised solutions—created in-house or by contracting with an expert firm. This is the most labour-intensive and potentially expensive choice. Integrity assurances are appropriate for a purpose-built, dedicated audit trail solution. Both big and small businesses can benefit from this service.

Compliance and Regulatory Landscape

During this period of time, when digital transformation is the dominant force in the financial landscape, the most important issues for banking institutions all over the world are assuring compliance with regulatory standards and protecting themselves against fraud. Monitoring, logging, and analysing client activity requires sophisticated systems [13]. This is because the complexity of current financial transactions and the growing sophistication of cyber threats necessitate the need for such solutions. For the purposes of both compliance and investigation, audit logging, which is an essential component of banking security frameworks, is of utmost importance since it provides a comprehensive record of transactions and interactions that can be analysed. Within the context of the fight against money laundering, terrorist funding, and other types of financial misbehaviour, regulatory agencies all over the world have tightened their grip on compliance requirements, enforcing stringent audit trails and transparent reporting methods. Large data analytics is becoming increasingly popular among banks and other financial organisations as a powerful tool that may help them improve their audit recording capabilities. Big data technologies, which are distinguished by their capacity to handle and analyse enormous amounts of data in real time, provide opportunities that have never been seen before for recognising patterns, locating uncommon occurrences, and reacting to potential dangers with an astonishing degree of speed and precision.

The incorporation of large amounts of data into the audit logging process is in accordance with the requirements of regulatory authorities and greatly strengthens the security precautions taken by banks. Through the utilisation of intricate algorithms and machine learning models, financial institutions are able to sift through massive information in order to unearth concealed risks, fraudulent activity, and compliance violations [14]. It is essential to possess this skill in order to fulfil legal and regulatory requirements, preserve the trust of customers, and guarantee the integrity of the financial system. For the purpose of ensuring the integrity, transparency, and stability of the banking system, the financial sector functions within a regulatory structure that is notoriously complicated and constantly evolving. Financial organisations are required to build thorough audit logging systems in order to comply with key regulatory mandates. These mandates include the Bank Secrecy Act (BSA), the Anti-Money Laundering (AML) regulations, and the General Data Protection Regulation (GDPR) in the European Union, amongst others. In order to support efficient monitoring, reporting, and analysis, these systems need to accurately record transactions, interactions with customers, and any other activities that are pertinent.

The major purpose of these legislation is to discourage criminal activity in the financial sector, the protection of consumer information, and the promotion of a financial market that is both fair and transparent. Compliance requires the acquisition of enormous volumes of data as well as the ability to analyse and comprehend this data in the context of the requirements imposed by regulatory agencies [15]. Consequently, the difficulty for financial institutions resides in their capacity to adjust to the requirements imposed by regulatory agencies. This involves making certain that their audit logging and data management procedures are resilient and flexible enough to meet new regulations and standards as they come into existence.

Banking Security Challenges

Protecting financial assets, personal information, and the integrity of transactions from theft, fraud, and other security breaches is the goal of banking security, which involves a variety of different techniques. The advent of the digital age has brought up considerable security challenges, despite the fact that it has made financial operations more convenient and efficient. Phishing, malware, and advanced persistent threats (APTs) are just some of the increasingly complex methods that cybercriminals use to get around standard security measures as they evade detection.

By providing a comprehensive and tamper-proof record of all transactions and system access, audit logs are able to address these difficulties. Detecting unauthorised activity, conducting investigations into security events, and presenting evidence for judicial processes are all key functions that they perform. When it comes to audit logging operations, however, the sheer amount and complexity of the data provide considerable hurdles. The analytical capabilities of traditional systems are frequently restricted and they are generally compartmentalised; therefore, these systems require assistance in order to keep up with the requirements of modern banking security [16]. The application of big data technologies, which provide new opportunities for improving the efficacy and efficiency of audit recording methods, comes into play at this point.

Role of Big Data in Audit Logging

Technologies that deal with big data have completely altered the way in which financial institutions conduct audit logging for the purposes of compliance and security. By utilising the power of big data analytics, financial institutions are able to process and analyse massive datasets in real time or near real time. This gives them the ability to identify and respond to possible problems with a level of speed and precision that has never been seen before. For the purpose of giving a comprehensive perspective of activities that can be mined for insights on compliance and security issues, big data platforms incorporate data from a variety of sources, such as transaction records, customer interactions, and external databases. In addition, it was presented in figure 2.

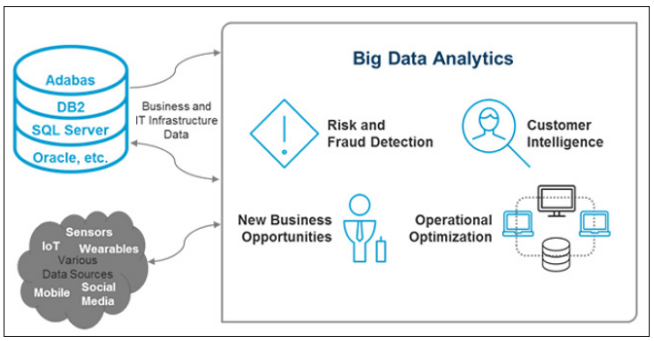

Figure 2: Cyber Risks on Big Data Analytics

Data Ingestion and Storage

The ingestion of many sorts of data from a variety of sources, such as transaction logs, customer interactions, and data feeds from third parties, can be accomplished in real time or very close to real time through the use of big data ecosystems. Technologies such as Apache Kafka, which is a distributed streaming platform, make it possible to handle high-volume data streams in an effective manner. This ensures that data is collected quickly and without any interruptions, and that it is immediately available for processing. When it comes to storage, systems such as the Hadoop Distributed File System (HDFS) or cloud-based data lakes make it possible to store petabytes of data at a cost-effective rate. A versatile foundation for comprehensive audit logging systems is provided by these storage solutions, which are designed to handle structured, semi-structured, and unstructured data respectively.

Data Processing and Analytics

Big data processing frameworks such as Apache Spark and Apache Flink come into play after the data has been ingested and stored. When it comes to processing massive datasets, these frameworks have the ability to perform complicated data processing operations in memory, which dramatically reduces the amount of time needed. Spark, for instance, enables organisations to perform batch processing, stream processing, and machine learning, which in turn enables them to analyse audit logs in a variety of dimensions. In order to recognise patterns, anomalies, and trends within the audit logs, machine learning (ML) and artificial intelligence (AI) play a crucial role. To discover risk trends in real time, machine learning algorithms can learn from historical data to make predictions about fraudulent transactions, identify anomalies, and detect anomalies. TensorFlow and PyTorch are examples of tools that make it easier to design and deploy these models. These models may then be integrated into the audit logging process, which increases the effectiveness of decision-making and risk management.

Visualization and Reporting

The visualisation and reporting of audit logs, which are essential for compliance and operational supervision, are also included in the scope of big data technology. Tools such as Apache Superset and Tableau are able to combine with various sources of big data in order to generate interactive dashboards and reports. These visualisation tools make it possible to view audit logs in real time, providing a quick and easy way to gain insights into transaction patterns, security threats, and compliance status.

Security and Compliance

Large data systems employ sophisticated security safeguards to safeguard sensitive data contained inside audit logs. This is accomplished on the technical front. Compliance with regulatory standards such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) can be ensured through the utilisation of technologies such as encryption, access control, and data masking [17]. Additionally, big data solutions have the capability to automate compliance reporting, which may include the generation of essential papers and alerts in order to efficiently satisfy regulatory deadlines and requirements.

Further enhancement of audit logging capabilities can be achieved through the implementation of machine learning and artificial intelligence (AI) capabilities inside big data frameworks. These technologies have the ability to recognise trends and irregularities that may be indicative of fraudulent behaviour, compliance violations, or other security concerns. As an illustration, machine learning models can acquire knowledge from previous transaction data in order to identify transactions that depart from established patterns, so indicating the possibility of fraudulent activity. In a similar vein, analytics that are driven by artificial intelligence can automate the process of compliance monitoring, thereby decreasing the workload of human analysts and minimising the possibility of errors caused by humans.

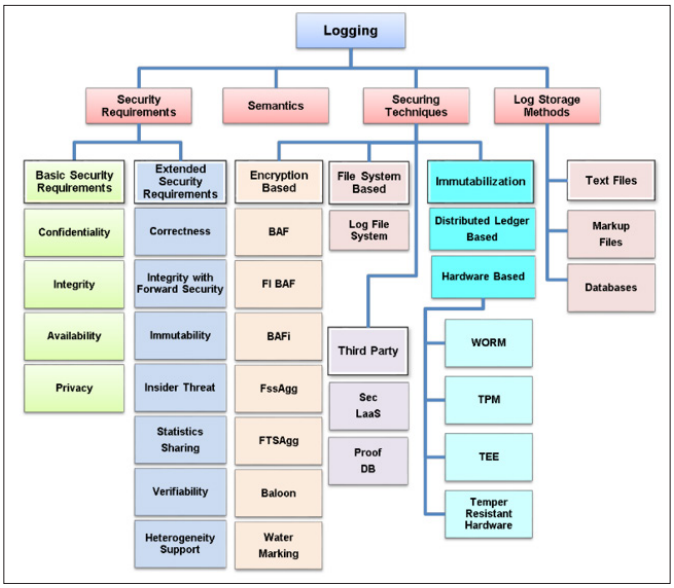

Figure 3: Audit Log Management – Taxonomy

The "Non-Repudiation" factor is the most critical aspect of information security in computer forensics. This factor can be maintained by logging each sensitive activity that a user engages in within the system. The following are significant challenges that arise in log storage and analysis methods, in addition to some handling issues such as real-time storage, accessibility, and alert generating depending on a particular occurrence. At this point in time, a logging scheme is considered to be an all-encompassing resource for capturing important events. In terms of security, these needs can be divided into two categories: basic security requirements and extended security requirements. There is a taxonomy of log management that can be found in Figure 3. Confidentiality, Integrity, Availability, Non-Repudiation, and Privacy are regarded to be fundamental security needs for a logging scheme that is both secure and trusted. In order to maintain confidentiality, it is necessary to restrict unauthorised access. When it comes to protecting data from being manipulated or even deleted, integrity is absolutely necessary. The assurance and promise that data will be accessible when it is needed in the form in which it was saved is what we mean when we talk about availability. One of the properties that must be had in order to offer proofs that contain adequate data on the existence of an activity is non-repudiation.

Conclusion

A significant step forward in the continuous efforts of the banking industry to meet regulatory compliance criteria and improve security measures is represented by the use of big data technologies into client audit logging methods. It has become increasingly important for financial institutions to be able to properly track, monitor, and analyse the behaviours and transactions of their customers as they negotiate an increasingly complex regulatory landscape. Big data analytics provides a powerful tool that enables financial institutions to process enormous volumes of data in real time, recognise trends and abnormalities that may be suggestive of fraud or non-compliance, and take preventative efforts to address these concerns. The issues that are involved with banking security and compliance are diverse. These challenges include the technological aspects of data management and analysis, as well as the more general regulatory and ethical considerations of consumer protection and privacy. Big data technologies supply a means to strike a compromise between both objectives by providing greater visibility into transactional data while simultaneously preserving sensitive information. This is made possible by the powerful analytics capabilities that these platforms possess. In addition, the implementation of machine learning and artificial intelligence within audit logging procedures has the potential to revolutionise the way in which financial institutions identify and respond to possible security issues. Through the automation of transaction data analysis, these technologies have the potential to drastically reduce the amount of time and resources necessary for compliance monitoring and fraud detection. This enables financial institutions to concentrate on their main business activities and provide better service to their customers. The implementation of big data in audit logging, on the other hand, creates important problems regarding data governance, data security, and data privacy. In order to successfully traverse these difficulties, financial institutions need to adopt comprehensive data management processes and ensure compliance with rules governing data protection. Continuous coordination between regulatory agencies, technology suppliers, and banking institutions will be necessary in order to fully exploit the potential of big data in audit logs while also protecting the interests of consumers and maintaining the integrity of the financial system. This will be the case as technology continues to advance.

References

1. M Castelli, L Manzoni, A Popovič (2016) An artificial intelligence system to predict quality of service in banking organizations. Comput. Intell. Neurosci 7.
2. F Gideon, M A Petersen, J Mukuddem Petersen, B De Waal (2012) Bank liquidity and the global financial crisis. J. Appl. Math 27.
3. L Sun, S Wu, Z Zhu, A Stephenson (2017) Noninterest income and performance of commercial banking in China. Sci. Program 8.
4. K Riad, M Elhoseny (2022) A blockchain-based key-revocation access control for open banking. Wireless Commun. Mobile Comput 14.
5. L Ali (2019) Cybercrimes-A constant threat for the business sectors and its growth (a study of the online banking sectors in GCC). J Developing Areas 53: 267-279.
6. M Button, J Whittaker (2021) Exploring the voluntary response to cyberfraud: From vigilantism to responsibilisation. Int. J. Law, Crime Justice 66.
7. Warjiyono S Aji, Fandhilah N Hidayatun, H Faqih, Liesnaningsih ((2019) The sentiment analysis of FinTech users using support vector machine and particle swarm optimization method. In Proc. 7th Int. Conf. Cyber IT Service Manage. (CITSM) 7: 1-5.
8. M R Rabbani, Y Abdulla, A Basahr, S Khan, M A M Ali (2020) Embracing of FinTech in Islamic finance in the post COVID era. In Proc. Int. Conf. Decis. Aid Sci. Appl. (DASA 1230-1234.
9. Q A Kester and E J Afoma (2021) Crime predictive model in cybercrime based on social and economic factors using the Bayesian and Markov theories. In Proc. Int. Conf. Comput., Comput. Model. Appl. (ICCMA 165-170.
10. D Y Kao (2019) Cybercrime countermeasure of insider threat investigation. In Proc. 21st Int. Conf. Adv. Commun. Technol. (ICACT) 413-418.
11. A Mahmud (2023) Application and criminalization of artificial intelligence in the digital society: Security threats and the regulatory challenges. J. Appl. Secur. Res 18: 1-15.
12. Naheem Mohammed A (2019) Saudi Arabia's Efforts on Combating Money Laundering and Terrorist Financing. Journal of Money Laundering Control 22: 233-246.
13. Michael (2023) Rising to the Challenge - How AI Revolutionizes Fraud Detection. Any Drum http://anydrum.com/2023/rising-to-the-challenge-how-ai-revolutionizes-fraud-detection/.
14. Allant Group (2020) Privacy Affects Every Aspect of a Business https://allantgroup.com/news/privacy-affects-every-aspect-of-a-business.
15. Lassila T (Tuomas) (2020) Towards Better Organizational Analytics Capability: A Maturity Model https://core.ac.uk/download/344912645.pdf.
16. Workshop Review: Virtual Workshop on AI and Machine Learning in Geophysics Draws Global Audience. The Leading Edge https://chooser.crossref.org/?doi=10.1190%2Ftle41120872.1.
17. Caprian Iu (2023) The Use of Machine Learning for the Purpose of Combating Bank Fraud. Business Inform 7: 140-145.