ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

SCIENTIFIC Research and Community

Review Article

Open Access

Fraud Detection using Cloud-Based ML

Venkata Soma

New York Mets, USA

ABSTRACT

The present research paper focuses on analysing the fraud detection processes by using the cloud-based ML system. The current business processes are shifting from traditional to digital business operations; hence, they fetch, use, and manage crucial information online. This study found that Amazon and Google use their personal cloud system to prevent data theft. Fraudsters conduct unauthorised access to financial information which leads one to face financial loss. Hence, each organisation needs to use cloud-based ML, as this algorithm can detect the pattern of issues and allows the cloud system to promote and use proper data protection strategies.

***Corresponding author**

Venkata Soma, New York Mets, USA.

Received: October 03, 2023; **Accepted:** October 20, 2023; **Published:** October 27, 2023

Keywords: Cloud System, Machine Learning (ML), Fraud Detection, Unauthorised Intrusion, Prevention, IoT, AI

Introduction

Fraud detection is very important to save the common people from any fraudulent attempts and activities. In that case, fraudulent activities need to be identified first. This detection is required for each individual and company to prevent their financial losses, resulting from such activities. Along with the advancement of digitalisation and online activities, such fraudulent activities increased in number. They trap the common people and businesspersons through banking information, identity usage, and unauthorised access to personal information. Unknowingly, these persons provide their personal information to the fraudsters and pave their way to financial loss. Identity theft, credit card fraud, phishing activities, and account takeover are some of the fraudulent activities which lead people to experience financial losses.

Aim

The research paper aims to navigate and analyse the overall efficacy of cloud-based machine learning (ML)systems in determining and preserving fraudulent activities in digital business activities.

Objectives

- To scrutinize the prevalent requirements and the approaches in the determination of fraud within the functioning of digital businesses.
- To investigate the extent to which based ML configurations are utilized through leading organizations such as Amazon and Google for preserving the loss or stealing of potential information.
- To recognize the shared patterns and tools required by the fraudster to grant accessibility of authority access to financial information.
- To offer potential recommendations for the commercial implementation regarding the cloud-based ML systems to exemplify the abilities regarding fraud determination.

Research Rationale

During the prompt movement of traditional to digital commercial activities, the mass of the online related transitions and the utilization of the information has a potential impact on the increased usage of the data. The transformation in the digital paradigm has set the ground for certain fraudulent activities, including theft of identity, fraud of credit cards, and attacks involving phishing.

Research Questions

- How effective are cloud-based ML systems for fraud detection?
- What are the main fraud detection techniques used by Amazon?
- How do Google's ML systems prevent financial information theft?
- What tools help identify unauthorized access to financial data?

Literature Review

Research Background

Cloud computing (CC) is one of the novel technologies which eases access to computer resources and network systems. This assists in robust data storage and data management systems; apart from that, it also eases cloud-provided services, which will be beneficial for the development of business processes through data security protocols. In that case, advanced technologies often need help to maintain proper service and resource management. Hence, the current business world and the confidential information of each person require improvement in cloud security services. Regular monitoring of services, networks, and resources can detect uneven and sceptical incidents in regular activities. The study of suggested that the "intrusion detection system" (IDS) is an advanced mechanism that controls network traffic to detect all abnormal activities [1]. Random forest (RF) and other featuring activities are the prime components of a cloud-based "intrusion detection model" and enhance accuracy rate. Hence, cloud-based

machine learning systems work through "platform as a service" (PaaS), "infrastructure as a service" (IaaS) and "software as a service" (SaaS).

Here, ML is used for feature engineering, while RF predicts and detects intrusions. A combination of these models can enhance the strength of cloud-based ML technology to detect doubtful activities and take necessary precautions. Cloud service, along with diverse ML detection techniques is beneficial for fraud-alerting technologies [2].

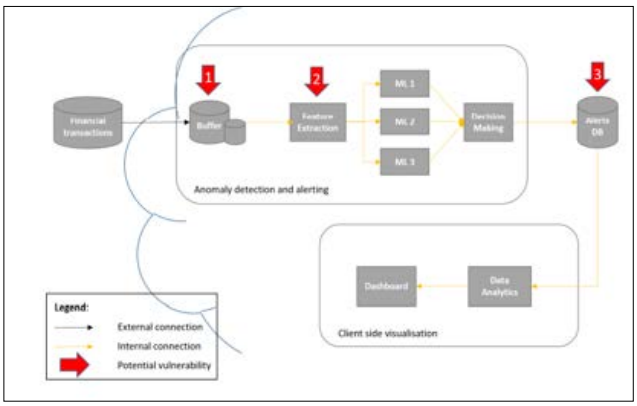

Figure 1: Financial Fraud Alerting System Depending on Parallel Anomaly Detector [2].

The report of mentioned that almost 10 million out of 12 billion transactions are fraudulent, which questions the strength of the fraud detection system. Again, a "semantic fusion of k-means" and "artificial bee colony" (ABC) algorithm improves two-level fraud detection for credit card fraud [3].

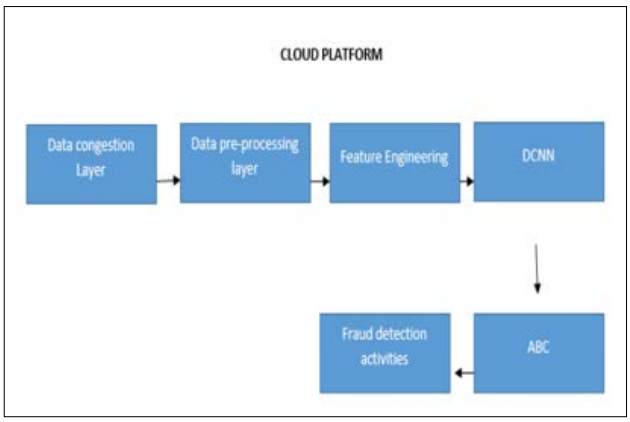

Figure 2: Recommended Cloud-Based Security System Architecture [3].

In that case, virtual technologies and cloud computing services become susceptible to diverse security problems; these problems may lead an organisation to compromise the integrity of information as well as the internal operational activities. Holes in the operational and security management activities are crucial to data security breaches [4]. Hence, it is essential to identify fraudulent activities and identification of malicious software to prevent data theft issues.

Critical Assessment

This is based on the best multicast tree which is available in the location of the path "taken by the bees that have the lowest value for the goal function" (p. 4534) [3]. The basic ABC algorithm can tackle the hurdles throughout the complete search space, and it assists in promoting a strong level of exploration. At most times, this algorithm fits all types of optimisation-based risks. It further investigates the workable solution to make the process time-efficient [mentioned in Figure 3]. ML algorithm needs to be implemented based on the needs and requirements of the authentication in the data achievement processes. Proper training is required to enhance cloud literacy among the industries [4].

Algorithm 1:ABC optimization

Set the population of solutions to start at xi,j, i = 1...SN,j = 1...D.
Assess the population
cycle=1
Repeat
Using (2), create new solutions vi,j for the working bees and assess them.
Use the avaricious selection procedure.
Utilizing (1), determine the probability values Pi, j for the solutions xi, j.
From the solutions xi, j chosen based on Pi, j, create the new solutions vi, j for the observers and assess them.
Use the avaricious selection procedure.
If an abandoned solution for the scout exists, identify it and substitute it with a fresh randomly generated solution, xi,j by (3)
Finally, the greatest answer found thus far: cycle=cycle+1 till cycle=MCN

Figure 3: "Artificial Bee Colony" (ABC) Algorithm [3].

The study of mentioned that the ML algorithm is an amalgamation of the Internet of Things (IoTs) and these are based on cloud applications the study of highlights different ML classifiers, which improve data protection and management processes [5-7]. J48, LMT, and RF are the decision trees and KNN classifiers are used. These classifiers focus on the development of business processes by increasing the detection of malware and improving accuracy in data management processes.

Figure 4: Monitoring Processes to Assess the Root Cause of Issues and Mitigation [8].

Artificial intelligence (AI) and machine learning (ML) algorithms are crucial for security issues. A combination of these two advanced technologies improves the "Intrusion Detection System" (IDS) and "Intrusion Prevention System" (IPS). as a result, the cyber-physical infrastructure and system nature are improved, and this combination of AI and ML comprises interconnected devices to assess the client information, needed dataset, and end-point

log records. ML algorithm, with proper use of AI, can conduct learning, analysis, and identification of security issues through cyber-attacks [8]. This monitors the cloud workloads, under which the end-point control can be measured to handle the hurdles of cyber threat issues [mentioned in Figure 4].

Linkage to Aim

Amazon uses machine learning (ML) algorithms in its fraud detection infrastructure. This is beneficial for the development of security in financial transaction processes. Its ML model can detect fraudulent activities efficiently and can flag doubtful or unfamiliar activities for review. Figure 5 presents the data protection and fraud detection algorithm that Amazon, an online business platform uses [9]. Those platforms increase data visualisation and ease in reporting through detailed analysis.

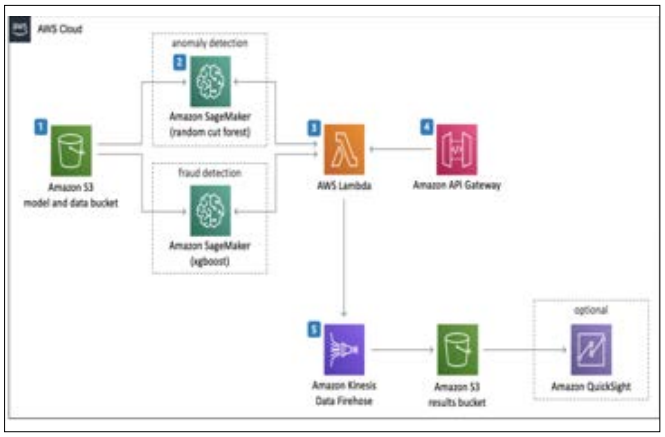

Figure 5: Fraud Detection Processes Based on ML Architecture [9].

Table 1: The Fraud Detection Elements of Amazon AWS and their Functions [9].

Elements	Functions
Amazon Simple Storage Service (Amazon S3)	Holds an example dataset of credit card transactions.
Amazon SageMaker notebook instance	Hosts various machine learning models to be trained on the dataset.
AWS Lambda Functions	Processes transactions from the example dataset and invokes two Amazon SageMaker endpoints to assign anomaly scores and classification scores to incoming data points.
Amazon API Gateway REST API	Uses signed HTTP requests to invoke predictions.
Amazon Kinesis Data Firehose Delivery Stream	Transfers the processed transactions to another Amazon S3 bucket for storage.
Amazon QuickSight in Amazon S3	Once transactions are stored in Amazon S3, use tools like Amazon QuickSight for visualization, reporting, ad-hoc queries, and detailed analysis.

Again, in the case of "new account fraud". In that case, the ML algorithm will look into the use of bots to detect an attack on the digital platform. Synthetic identities and generating multiple accounts can detect those fraudsters and AWS ML prevents their actions [10].

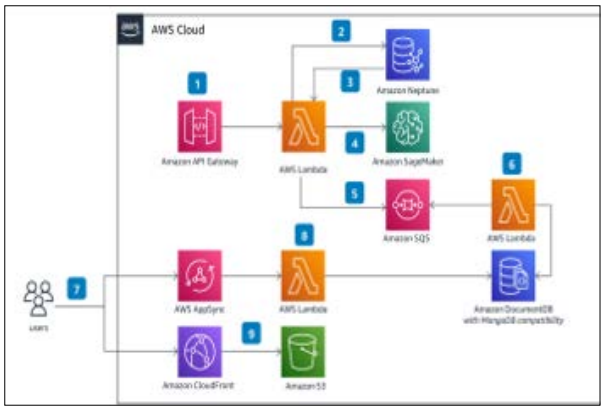

Figure 6: "Near Real-Time Fraud Detection" Model [11].

Encapsulation of Application

The study of mentioned that cloud system improves the data protection system through cloud computing [12]. Data privacy and scalable solutions are important for each organisation. This will be beneficial for the development of an internal security system. This article also mentioned the use of cloud AI for data protection; despite it can improve data protection and fraudulent detection activities through its complement solution, it is not enough to provide a riskless data protection system. In this concern, this study of supported the use of Cloud ML to strengthen the data protection system of any organisation [13]. Similarly, the study of assessed the IoT-based cloud system to manage cyber security threats and risks; however, IoT is also not effective enough to support the data protection and management system [14].

Methodology

Research Approach

The study undertakes adherence to the descriptive research design qualitative research approach to proactively illustrate the utilization of cloud-based machine learning systems in the determination of fraudulent activities. This configuration aids in the facilitation of the extensive scrutinization of the prevalent practices, benefits, and potential challenges regarding the incorporation of the mechanisms.

Research Design

A descriptive research approach is employed to proactively navigate the overall efficacy of the cloud-based ML systems and detection of fraud. The design aids in the in-depth analysis if the comprehensive factors and scrutinizes the complicated phenomenon that analyses the existing data and the theoretical insights.

Data Collection Methods

The research depends upon secondary data collection methods to collect the relevant information. The sources of the information involve academic journals and papers that elaborate and describe the aspects associated with fraud detection, cloud detection, and machine learning.

Ethical Considerations

Ethical considerations are a significant aspect of the research work, specifically in assuring the inclusivity and credibility of the sedentary sources of the data. It is crucial for the assurance that all the secondary sources of the data are specifically cited and complained to mitigate the extent of plagiarism. The information required to be gathered from authenticated sources and credible

sources to manifest the overall accuracy and reliability of the findings. Moreover, it is beneficial to stay reluctant the utilize data that might infringe on the privacy or the confidentiality of individuals or organizations. Openness regarding the restrictions of the secondary sources of the information, which involves potential inclinations of incompetency regarding the information, is further necessary to undertake the vertical consequences. Through the adherence to ethical norms and principles, the research potentially aimed to enhance the trustworthiness and valuable aspects regarding the devotion to comprehension of cloud-based ML systems in detecting fraud.

Results

Critical Analysis

The use of cloud-based ML in fraud detection technology is beneficial for the development of the organisational data security system. This increases the "deep generative intrusion detection system" and can promote high dimensionality, high redundancy, and high volume of network traffic. Hence, proper traffic management and detects threats. Hence, it can be said that this study on cloud-based ML for fraud detection strategies paves the way for further research on the difference between IoT-based cloud systems and AI-based cloud systems with the ML-based cloud system.

Findings and Discussions

Theme 1: Current Approaches in the Detection of the Fraud

The theme elaborates on the exploration of the prevalent methods and technologies utilized in fraud determination across various sectors. It further focussed on recognizing the standardized practices, mechanisms, and approaches presently employed to determine the prevalent operation regarding fraudulent activities. This theme aligns with the core objectives for the examination of the fraud determination activities within the operations of digital operations.

Theme 2: Incorporation of the Cloud Based ML Configurations

This theme scrutinizes the system configuration regarding cloud ML and incorporates the potential aspect of the company, that involves Amazon and Google for the detection of fraud. It bounds the models regarding the ML models and the potential algorithms and that indicates the cloud infrastructures utilized during the implementation procedures the theme potentially addresses the objectives regarding the scrutinization of the cloud-based ML systems through the leading companies for preserving the theft of the data sets.

Theme 3: Efficacy of the ML Algorithms in the Fraud Detection

Within the periphery of this theme, the crew determination regarding the evaluation of the efficacy of diversified Algorithms in determining and managing the operations concerning frauds. It further scrutinizes the performance of the metric, the overall success rates, and the restrictions of the pivotal algorithms This theme inclines with the potential objectives for gaining accessibility if the implementation of the cloud-based ML configurations to streamline the determination of the real-world implications. Moreover, the theme navigates the challenges encountered by the algorithms that involve manipulation of the imbalanced datasets, falsified providers, and the adaptability to fraudulent patterns. The themes are particularly aimed towards achieving the entire effectiveness of the cloud-based ML algorithms in streamlining the determination of fraud in the operations regarding the digital morphology of the business.

Theme 4: Challenges and Recommendations Regarding the Cloud-Based ML Systems

The theme determines the overall performance of certain machine learning programs in recognizing the mitigation of fraudulent activities. It scrutinizes the potential metrics regarding the accuracy of the mechanisms such as precision, recall value, and the F1q score, illustrating the success factors and the implications of the real-world scenarios Moreover, it navigates the potential drawbacks such as the manipulation of the imbalance datasets and the maintenance of the diversified positivity's, and the adaptation regarding the evolution of the fraudulent patterns.

Conclusion

This research paper highlighted that the use of cloud computing systems and their combination with machine learning (ML) algorithms is beneficial for the fraud detection system. ML algorithm is different and stronger than IoT and AI to strengthen the cloud computing system. This study mentioned that ML algorithms can detect the pattern of risk and unauthorised intrusion; as a result, an organisation can take necessary measures to promote prevention processes.

Recommendations

Hence, this is necessary to assess the organisations and their business operations. Intrusion detection and prevention systems are crucial for internal data security management. Furthermore, proper detection of data imbalance is crucial for detecting data theft and doubtful actions within online platforms. Amazon and Google also use their personal cloud system; Amazon AWS and Google Cloud focus on maintaining the issues of data theft and increasing data security. Smart cities also can use this cloud-based ML technology to improve the data security system; from healthcare organisations to online business platforms, each business process needs to use this technology to reduce the data protection issue and increase data safety. This system is crucial as online business requires using the personal credentials of stakeholders online.

Future Work

This research paper will provide vital insight into the reason for their organisation and business operations can use cloud-based machine learning algorithms. They will be able to use the cloud as an intrusion detection system to prevent unauthorised intrusion.

References

1. Kumar DA, Venugopalan S (2017) Intrusion detection systems: a review. Int J Adv Res Comput Sci 8: 356-370.
2. Zhang C, Yu M, Wang W, Yan F (2019) MArk: Exploiting cloud services for cost-effective, SLO-aware machine learning inference serving. In 2019 USENIX Annual Technical Conference (USENIX ATC 19) 1049-1062.
3. Mekterović I, Karan M, Pintar D, Brkić L (2021) Credit card fraud detection in card-not-present transactions: Where to invest?. Appl Sci 11: 6766.
4. Alzahrani L, Seth KP (2021) The impact of organizational practices on the information security management performance. Information 12: 398.
5. Alsharif MH, Kelechi AH, Yahya K, Chaudhry SA (2020) Machine learning algorithms for smart data analysis in Internet of Things environment: Taxonomies and research trends. Symmetry 12: 88.
6. Umer Ahmed Butt, Muhammad Mehmood, Syed Bilal Hussain Shah, Rashid Amin, Waqas Shaukat M, et al. (2020) A review of machine learning algorithms for cloud computing security. Electronics 9: 1379.

7. Aslan Ö, Ozkan Okay M, Gupta D (2021) Intelligent behavior-based malware detection system on cloud computing environment. IEEE Access 9: 83252-83271.
8. Li JH (2018) Cyber security meets artificial intelligence: a survey. Front Inf Technol Electron Eng 12: 1462-1474.
9. (2021) Amazon AWS. Fraud detection using machine learning. https://aws.amazon.com/solutions/implementations/fraud-detection-using-machine-learning/.
10. (2021) Amazon AWS. Identify fraudulent online activities. https://aws.amazon.com/machine-learning/ml-use-cases/fraud-detection/.
11. (2021) Amazon AWS. Guidance for near real-time fraud detection with graph neural network on AWS. https://aws.amazon.com/solutions/guidance/near-real-time-fraud-detection-with-graph-neural-network-on-aws/.
12. Kumar PR, Raj PH, Jelciana P (2018) Exploring data security issues and solutions in cloud computing. Procedia Comput Sci 125: 691-697.
13. Sivan R, Zukarnain ZA (2021) Security and privacy in cloud-based e-health system. Symmetry 13: 742.
14. Butpheng C, Yeh KH, Xiong H (2020) Security and privacy in IoT-cloud-based e-health systems-A comprehensive review. Symmetry 12: 1191.