Received: 2022-10-01
Accepted: 2022-10-30
Published Online: 2022-10-30
DOI: 10.70454/IJMRE.2022.21001

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

Cloud-Enabled Intelligent Personalization and Secure Transaction Framework for Scalable E-Commerce Platforms

[1]Nagendra Kumar Musham, [2]Sathiyendran Ganesan, [3]Venkata Sivakumar Musam, [4] Purandhar. N

[1]Celer Systems Inc, California, USA
[2]Troy, Michigan, USA
[3]Astute Solutions LLC, California, USA
[4]Vignan Institute of Technology and Sciences, Hyderabad., India

[1]nagendramusham9@gmail.com
[2]sathiyendranganesan87@gmail.com
[3]venkatasivakumarmusam@gmail.com
[4]npurandhar03@gmail.com

Abstract-This work discusses the evolution of a cloud platform for intelligent personalization and safe transaction management in scalable e-commerce sites. With the growth of e-commerce, sites are compelled to provide individualized user experience with transaction safety and privacy. On-premises solutions cannot process heavy loads of data and traffic and are therefore unsuitable for today's dynamic e-commerce environment. Cloud computing offers a substitute in the form of offering elastic scalability, high-performance data processing capabilities, and seamless integration of AI/ML solutions for intelligent personalization. The central concern of this research is to design and develop a cloud-based system with both personalized user experience and secure transactions. Based on machine learning algorithms, the system will offer real-time one-to-one recommendations and content in accordance with the user's own taste, and which will grow user usage and satisfaction. Behind the scenes, robust security features like encryption and authentication processes are part of the transactional process of securing confidential customer data from web threats and ensuring compliance with privacy regulations. The proposed model integrates scalability, high performance, and security in addressing the requirements of modern-day e-commerce sites. By difficult testing and benchmarking with current systems, the study measures the performance of the cloud solution to improve personalia, security, and transaction effectiveness. This publication goals at communicating perceptibleinfo to e-commerce in the upcoming and location an instance for businesses which wish to make changes and reform their sites as well as market safe and personalia buying on behalf of the client.

Keywords: Cloud Computing, Intelligent Personalization, Secure Transactions, E-Commerce Scalability, Cybersecurity.

1. Introduction

The fast speed of e-commerce has transformed the way in which businesses interact with customers, contribution an calmer shopping experience [1]. It has also made it likely for businesses to bring highly personalized facilities based on individual tastes [2]. The scalability of e-commerce websites enables companies to manage higher numbers of customers and transactions with ease [3]. But as e-commerce

Received: 2022-10-01
Accepted: 2022-10-30
Published Online: 2022-10-30
DOI: 10.70454/IJMRE.2022.21001

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

websites keep increasing at a tremendous rate, the problems of commerce with a large amount of user data get more complicated [4]. Personalization strains gathering and processing enormous datasets in order to learn about consumer behavior correctly [5]. Additionally, handling security for money and personal dealings is a must for behind consumer confidence [6]. Legacy systems incline to discovery it problematic to match the materials of real-time delivery of personalized satisfied [7]. These legacy systems also fall short when dealing with high volumes of traffic, foremost to performance blocks [8]. Cloud computing is a revolutionary technology that medicines all these problems through scalable, on-demand computing resources [9]. E-commerce companies can use cloud platforms to allocate resources dynamically depending on traffic and workload [10]. Cloud-based environments also provision the convergence of new technologies like AI and ML [11]. Smart personalization through AI and ML allows e-commerce websites to propose products, content, and promotions to their users on the basis of their past actions and interests [12]. Personalized experience improves user experience as well as conversion rates [13]. Processing large sets of data to provide such personalization is, though, computationally intensive [14]. Cloud platforms have the obligatory infrastructure to withstand such concentrated workloads [15].

Simultaneously, the progression of cyber-attacks strains greater security for protecting consumers' sensitive information [16]. Global regulatory demands are placing greater privacy and data defense standards on e-commerce [17]. Upholding the confidentiality, integrity, and availability of transactional information is critical [18]. Developing a cloud-assisted platform incorporating smart personalization methods along with high-level transaction security is the focus of the study [19]. Through the scalability and adaptability of cloud computing, the platform can grip millions of users at once [20]. This means that e-commerce websites are able to deliver personalized experiences at scale without trading off privacy [21]. In addition, it gives companies a secure platform to process payments securely [22]. The integrated solution addresses the issues of personalization and security very effectively [23]. Lastly, this model aids e-commerce businesses in sustaining competitiveness within a saturated market [24]. The education envisions determining the future of e-commerce by encouraging secure, scalable, and personalized shopping environments that advantage both consumers and businesses alike [25].

2. Literature review

The security mechanism successfully integrates cryptography methods like RSA encryption, digital signatures, and SHA-256 hashing to reinforce data integrity, authenticity, and confidentiality within cloud computing [26]. Strong key management practices make these systems more reliable and users more satisfied, with an impressive satisfaction improvement of 84% [27]. Advanced machine learning methods, including MARS, SoftMax Regression, and Histogram-Based Gradient Boosting, can be integrated into a cloud-based system to improve predictive modelling in healthcare [28]. Through cloud computing, such models enhance scalability and computational power, leading to improved accuracy, precision, recall, and F1-scores over conventional methods [29]. The application of K-means clustering in analysing Gaussian data in cloud scenarios emphasizes cost savings and scalability [30]. Changing the cluster size (k) affects computation time and accuracy, and utilizing early stopping yields near-optimal performance at a lower cost [31]. The convergence of cloud computing and AI is transforming healthcare by providing scalable, smart disease diagnosis and monitoring systems [32]. New trends utilize wearable IoT sensors and hybrid AI models such as ABC-ANFIS and BBO-FLC to enhance prediction accuracy and response time [33].

Received: 2022-10-01
Accepted: 2022-10-30
Published Online: 2022-10-30
DOI: 10.70454/IJMRE.2022.21001

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

The combination of AI, cloud computing, and IoT is revolutionizing disease detection through real-time processing of advanced, high-dimensional medical data [34]. Hybrid methods like FA-CNN with DE-ELM enhance diagnostic precision by utilizing fuzzy logic and evolutionary optimization [35]. Combining Ant Colony Optimization with Long Short-Term Memory networks in cloud-based health systems marks a crucial step towards real-time disease prediction [36]. Such models improve both efficiency and accuracy, overcoming the deficiencies of traditional approaches [37]. The GWO-DBN hybrid model offers an effective approach to chronic disease prediction by combining feature selection through Gray Wolf Optimization with deep learning using Deep Belief Networks [38]. The use of IoT devices and cloud connectivity provides real-time scalable monitoring and early diagnosis of health conditions [39].

The convergence of AI, IoT, CRM, and cloud computing is transforming banking by significantly boosting operational efficiency, customer satisfaction, accuracy, and cost-effectiveness [40]. AI-based CRM applications are revolutionizing customer relationship management in sectors such as telecommunications and banking by addressing scalability, efficiency, and quality challenges [41]. AI-driven frameworks leverage cloud and machine learning to automate responses, improve response times, and analyse feedback effectively [42]. AI-enabled cloud CRM systems combine real-time optimization, sentiment analysis, and predictive modelling to enable customized and responsive interactions [43]. These systems substantially improve customer satisfaction and CRM workflow efficiency, achieving 92.5% engagement accuracy and 91% precision in interpreting and responding to customer sentiment [44].Internet-available financing has the potential to spur rural economies, especially by improving access to e-commerce [45].

3. Problem Statement

In the rapidly evolving digital marketplace, e-commerce platforms face growing demands for delivering personalized user experiences while ensuring secure and scalable transaction processing[46]. Traditional systems often struggle to manage the high volume of user data and real-time analytics needed for effective personalization, especially during peak traffic periods[47]. Additionally, the increasing frequency of cyber threats and data breaches raises significant concerns about transaction security and user trust[48]. Leveraging cloud computing presents a promising solution, offering elastic scalability, powerful data processing capabilities, and advanced AI/ML tools[49]. However, integrating intelligent personalization mechanisms with secure transaction frameworks in a cloud environment remains a complex challenge [50]. Issues such as latency, data privacy, and system interoperability must be addressed to build a robust, scalable, and trustworthy e-commerce infrastructure[51].This research aims to design and implement a cloud-enabled framework that combines intelligent personalization with enhanced security measures to meet the evolving needs of modern e-commerce platforms.

Objectives

- Discuss the existing limitations and challenges in providing personalized user experiences and secure transactions in conventional, non-cloud-based systems.

Received: 2022-10-01
Accepted: 2022-10-30
Published Online: 2022-10-30
DOI: 10.70454/IJMRE.2022.21001

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

- Develop a cloud-based architecture that incorporates intelligent personalization algorithms through AI/ML methods to provide improved user experience and enable scalable e-commerce platforms.
- Assess the security threats and privacy issues of e-commerce transactions and formulate a strong secure transaction framework based on cloud-based encryption and authentication technologies.
- Deploy a cloud infrastructure solution that enables smooth integration of smart personalization and secure handling of transactions, with both scalability and high performance when the load is high.

4. Proposed Cloud-Enabled Intelligent Personalization and Secure Transaction Framework for Scalable E-Commerce Platforms

The proposed Cloud-Enabled Intelligent Personalization and Secure Transaction Framework for Scalable E-Commerce Platforms unifies state-of-the-art AI-based personalization and multi-level security into contemporary e-commerce landscapes. It is constructed on three key fundamentals: Data Collection, Intelligent Personalization, and Secure Transaction Framework. Leverage is taken from attributes such as recommender systems, NLP, behavioral analytics, blockchain, and actual anomaly detection to allow user-driven experiences while safeguarding data privacy, transaction integrity, and regulatory compliance. Produced for high availability and resiliency, it is deployed via cloud-native container orchestration and auto-scaling capabilities to safeguard performance and high obtainability under dissimilar user loads.

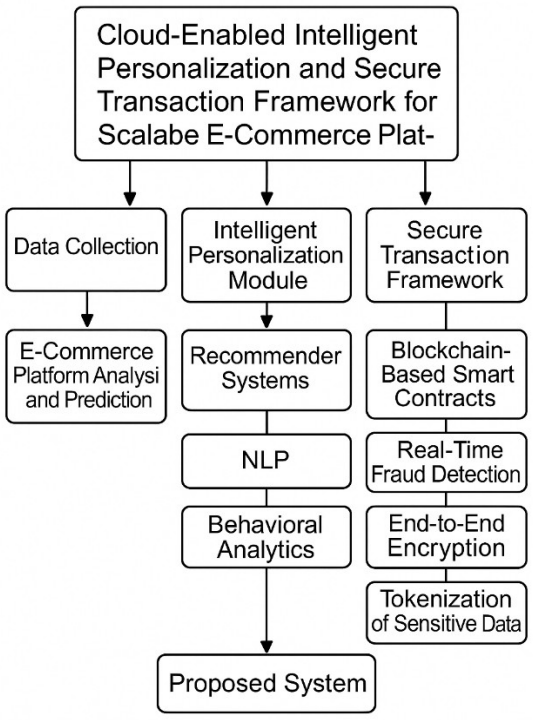

Fig 1: Architecture of the Cloud-Enabled Intelligent Personalization and Secure Transaction Framework for Scalable E-Commerce Platforms

Received: 2022-10-01
Accepted: 2022-10-30
Published Online: 2022-10-30
DOI: 10.70454/IJMRE.2022.21001

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

The Fig 1 depicts the architectural layout of a suggested framework which intends to reinforce personalization and security in cloud-based e-commerce platforms. The system is built around three core functional modules: Data Collection, Intelligent Personalization Module, and Secure Transaction Framework. The Intelligent Personalization Module integrates Recommender Systems, Natural Language Processing (NLP), and Behavioral Analytics. They support each other to learn customer behavior, text and behavior processing, and producing personalized recommendations to growth user satisfaction and engagement. The Secure Transaction Outline secures all transactions as secure, reliable, and privacy-aware. It comprises Blockchain-Based Smart Contracts for safeguarding and automating the transaction process, Real-Time Fraud Detection to detect fraud, End-to-End Encryption for encrypting data when in transportation, and Tokenization of Sensitive Data to never store and transmission sensitive user data in plaintext. The three functional brooks meet at the Data Preprocessing stage, where the met and created data is sanitized, arranged, and ready for system-wide processing. The final result is the Proposed System, which syndicates personalization and security together to deliver a strong, scalable, and smart e-commerce platform for use in current digital business environments.

4.1 Data Collection

The "E-Commerce Platform Analysis and Prediction" dataset is a solid and multi-purpose data set measured to allow extensive research into consumer behavior, fraud detection, and transaction analytics within digital commerce environments. It covers rich transactional information, user demographics, product metadata, and fraud labels, letting the construction and validation of intelligent personalization algorithms and secure transaction protocols. This data set is preferably suited for study of purchasing behavior, user preference prediction, and anomaly detection for abnormal behavior that can be exploited in possible fraud. With timestamps on transactions, device category, payment modes, and geo indicators as features, it is possible to perform clustering, time-series prediction, and behavior modeling with advanced techniques such as GRUs, DBSCAN, and transformer-based NLP models Also, the availability of sensitive features offers a playground for experimenting with encryption, tokenization, and blockchain-based security solutions. In general, the dataset provides a solid basis for constructing scalable, privacy-conscious, and smart e-commerce platforms.

4.2 Data preprocessing

Data preprocessing is the fundamental and multi-phased process, safeguarding system reliability, correctness, and safeguarding of the logical and predictive model elements. Preprocessing starts with data cleaning, where missing values in numerical makings such as transaction value or explanation age are credited with median values, and categorical fields such as device type or location are filled with the most frequent value or a proxy such as "Unidentified."Redundant records are deleted to avoid biased learning, and textual inconsistencies in categorical fields are normalized by applying lowercase conversion and stripping whitespace.

Then data transformation is used to translate categorical attributes into machine language by utilizing one-hot encoding for nominal features like product types and devices, and label encoding for ordinal features where necessary. Temporal characteristics such as transaction date stamps are mapped to datetime objects, which yield additional characteristics such as hour of transaction, day of week, and

Received: 2022-10-01
Accepted: 2022-10-30
Published Online: 2022-10-30
DOI: 10.70454/IJMRE.2022.21001

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

session spans to enhance personalization and detect fraud. Additional information is inserted into the data set through feature engineering, wherein session duration, frequency of purchasing, and most preferred categories are calculated for use in personalization, while location mismatches, unusual speeds at which transactions took place, and non-normal payments are labeled with fraud risk.

For behavior analysis and fraud detection, numerical features are standardized or normalized using methods like Standard Scaling or Min-Max Scaling to keep the features consistent, especially for distance measurement-based models or gradient-based models. For credit card information or personally identifiable information, tokenization is applied with cryptographic hash functions to replace them with irretrievable tokens, thereby supporting data privacy compliance such as PCI DSS and GDPR. In addition to this, end-to-end encryption protocols are simulated by encrypting key payloads with public-key cryptography prior to storage or communication.

To personalize the data for a given submodule, segmentation is done in which user-product interaction matrices are constructed for recommender systems, time-series sequences of user activity are built for GRU-based behavioral modeling, and transaction-label pairs are arranged for fraud detection model training. Data are then divided into training and testing sets based on stratified sampling or temporal segmentation to provide balanced and unbiased model assessment. This extensive preprocessing pipeline serves as the foundation of the proposed intelligent and secure e-commerce platform.

4.3 Intelligent Personalization Module

The Intelligent Personalization Module is a key driver of user engagement and conversion rates in e-commerce websites. It dynamically adjusts product suggestions and interface interactions according to user preferences, behavioral information, and natural language inputs. The module is powered by a hybrid blend of recommender systems, natural language processing (NLP), and behavioral analytics through the application of advanced deep learning and unsupervised learning methods.

- Collaborative Filtering relies on the fact that users with similar tastes in the past will have similar tastes in the future. Matrix factorization methods like Singular Value Decomposition (SVD) are popular. The user-item interaction matrix $R \in \mathbb{R}^{m \times n}$ is decomposed into:

$$R \approx U \cdot V^T \tag{1}$$

Where: R : Original rating matrix, $U \in \mathbb{R}^{m \times k}$: User latent feature matrix, $V \in \mathbb{R}^{n \times k}$: Item latent feature matrix, k : Number of latent dimensions

- Content-Based Filtering emphasizes product features and user profiles. The similarity between a user u and an item i is calculated using cosine similarity:

$$\text{sim}(u, i) = \frac{\vec{u} \cdot \vec{i}}{\|\vec{u}\| \|\vec{i}\|} \tag{2}$$

These methods are combined with a weighted hybrid score:

$$\text{Score}(u, i) = \alpha \cdot \text{CF}(u, i) + (1 - \alpha) \cdot \text{CBF}(u, i) \tag{3}$$

Received: 2022-10-01
Accepted: 2022-10-30
Published Online: 2022-10-30
DOI: 10.70454/IJMRE.2022.21001

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

Where $\alpha \in [0,1]$ is is the adjustable weighting parameter.

4.3.1 Natural Language Processing (NLP)

For enhanced personalization through user-generated content, transformer-based models such as GPT are used. These models generate contextual embeddings for user input:

$$\text{Embedding}(x) = \text{GPT}_\theta(x) \tag{5}$$

Where:x : User query or review text, θ : pre-trained model parameters

These embeddings are clustered and paired with product descriptions and metadata to achieve intent and sentiment, which in turn influences ranking and filtering in recommendations.

4.3.2 Behavioral Analytics

This module uses both unsupervised clustering and time-series modeling to forecast behavior:

- DBSCAN (Density-Based Spatial Clustering of Applications with Noise) clustering decides sets of users who exhibit close-to-one another navigation history or buying habits. DBSCAN has two parameters: ε (distance of maximum neighbourhood) and minPts (min points within a neighbourhood). DBSCAN will locate a user into a cluster when

$$|N_\varepsilon(p)| \geq \text{minPts} \tag{6}$$

Where $N_\varepsilon(p)$ is the set of points within distance ε of point p.

- Predictive Modeling with Gated Recurrent Units is used to extract sequential user patterns like clickstream or session history. The GRU updates the hidden state h_t at step t as given below:

The output is employed for predicting the probability of a next item or likelihood of abandonment in a session.

$$\begin{aligned} z_t &= \sigma(W_z x_t + U_z h_{t-1}) \\ r_t &= \sigma(W_r x_t + U_r h_{t-1}) \\ \tilde{h}_t &= \tanh\left(W_h x_t + U_h (r_t \odot h_{t-1})\right) \\ h_t &= (1 - z_t) \odot h_{t-1} + z_t \odot \tilde{h}_t \end{aligned} \tag{7}$$

Where:x_t : Input vector at time t, z_t, r_t : Update and reset gates, h_t : Hidden state,$\odot$: Element-wise multiplication,W_*, U_* : Learnable weights

The output is used to predict next-item probability or session abandonment likelihood.

4.4 Secure Transaction Framework

The Secure Transaction Framework is a key pillar in providing trust, privacy, and resilience in contemporary e-commerce ecosystems. This framework combines blockchain technology, real-time

Received: 2022-10-01
Accepted: 2022-10-30
Published Online: 2022-10-30
DOI: 10.70454/IJMRE.2022.21001

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

anomaly detection, end-to-end encryption, and data tokenization to deliver multi-layered protection on transaction workflows.

4.4.1 Blockchain-Based Smart Contracts

Blockchain brings decentralized, tamper-proof ledgers to authenticate and safely record transactions with the help of smart contracts-self-executing code with pre-defined rules. Let a transaction T_i between buyer B and seller S be regulated by a smart contract C. The transaction is executed only if the pre-defined condition $f(B, S, T_i)$ = true. The transaction is written on the blockchain ledger $\mathcal{L}$ as:

$$\mathcal{L}_{t+1} = \mathcal{L}_t \cup \{H(T_i)\} \tag{8}$$

Where:

- $H(T_i)$: Cryptographic hash of the transaction (ensuring integrity)
- $\mathcal{L}_t$: Current state of the ledger at time t

These smart contracts also feature multi-party escrow logic and refund triggers on delivery confirmation and dispute settlement.

4.4.2 Real-Time Fraud Detection via Anomaly Detection

Fraud detection is cast as an anomaly detection problem, and transaction behavior is tracked for outliers from normal behavior. Let $x_i \in \mathbb{R}^n$ be a feature vector for transaction i, and μ, Σ be the estimated mean and covariance of past legitimate transactions. A Mahalanobis distance is calculated to identify anomalies:

$$D_M(x_i) = \sqrt{(x_i - \mu)^T \Sigma^{-1} (x_i - \mu)} \tag{9}$$

If $D_M(x_i) > \tau$, the transaction can be labeled as suspiciously fraudulent. The cut-off τ is derived by empirical risk minimization or ROC analysis. More advanced models may also use autoencoders or graph neural networks to detect more advanced fraud patterns across accounts and transactions.

4.4.3 End-to-End Encryption

For data-in-transit as well as data-at-rest protection, the system employs end-to-end encryption (E2EE) using asymmetric cryptography. An encrypted payment payload m is transmitted by a buyer using the public key of the seller K_{pub}

$$c = E_{K_{pub}}(m) \tag{10}$$

Only the seller with the private key K_{priv} can decrypt:

$$m = D_{K_{priv}}(c) \tag{11}$$

Received: 2022-10-01
Accepted: 2022-10-30
Published Online: 2022-10-30
DOI: 10.70454/IJMRE.2022.21001

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

It guarantees confidentiality, as only the concerned parties can view confidential information. Additionally, TLS/SSL protocols protect data on transit and AES-256 symmetric encryption protects data at storage.

4.4.4 Tokenization of Sensitive Data

Tokenization substitutes sensitive information with non-sensitive representations known as tokens. Taking a sensitive input s, the tokenization function $\mathcal{T}$ transforms it into a token t such that:

$$t = \mathcal{T}(s), s \notin \mathcal{R}(t) \tag{12}$$

Where $\mathcal{R}$ is the reverse mapping, saved securely within a Token Vault and out of reach of unauthorized access. This renders stored token unusable in case of a breach, keeping compliance scope under PCI DSS and GDPR to a minimum.

4.5 Cloud Deployment & Scaling

Scalability and fault tolerance are fundamental features of a cloud-enabled e-commerce platform. The Cloud Deployment & Scaling module orchestrates containerized microservices, provides dynamic resource allocation, and maintains high availability through smart load distribution. Docker Swarm, auto-scaling functionalities, and API gateway routing constitute the core of this module.

4.5.1 Container Orchestration using Docker Swarm

Docker Swarm is used for effective orchestration of containers, handling clusters of Docker nodes as one virtual system. Service S is replicated on multiple nodes to enhance fault tolerance. Suppose n is the number of replicas needed for a service depending on existing demand d, and threshold capacity γ. The number of containers C needed can be estimated dynamically by:

$$C = \left\lceil \frac{d}{\gamma} \right\rceil \tag{13}$$

Where:d : Incoming request rate (e.g., requests per second),γ : Maximum sustainable rate per container instance

Swarm constantly monitors service health and automatically restarts failed tasks. Leader election and internal load distribution provide continuity even in the event of node failure.

4.5.2 Auto-Scaling Mechanisms

Auto-scaling is initiated with respect to real-time parameters such as CPU utilizationU_{cpu} , memory consumption U_{mem}, or application-dependent measures like mean response time R_t. A threshold-based auto-scaling rule can be specified as:

$$\text{Scaleup} = \begin{cases} \text{Add instance}, & \text{if } U_{cpu} > 70\% \text{ or } R_t > R_{max} \\ \text{No action}, & \text{otherwise} \end{cases} \tag{14}$$

Received: 2022-10-01
Accepted: 2022-10-30
Published Online: 2022-10-30
DOI: 10.70454/IJMRE.2022.21001

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

Likewise, scale-down policies avoid over-provision when demand is down. These are applied through cloud-native services in order to maximize resource efficiency and cost.

4.5.3 Load Balancing and API Gateway Integration

To make request routing optimal and services equally accessed, the system combines NGINX and AWS API Gateway:

- NGINX is a reverse proxy and layer 7 load balancer. With a set of backend instances $\{I_1, I_2, \ldots, I_n\}$, the routing function $R(x)$ for a request x makes the response time minimal:

$$R(x) = \arg \min_{i \in [1,\ldots,n]} (L_i + Q_i) \quad (15)$$

Where: L_i : Network latency to instance I_i, Q_i : Queueing delay or current workload on instance I_i

- AWS API Gateway offers a centralized entry point, applying security policies and request transformation. AWS API Gateway can integrate directly with AWS Lambda, EC2, or Fargate backends and supports path-based or header-based routing logic using conditions.

This multi-layered routing paradigm provides high performance, dynamic flexibility, and sustained availability under mixed workloads.

5 Result and Discussion

This paper describes a full-scale analysis of an e-commerce platform's performance and operational pattern by employing predictive modeling and temporal evaluation methods. The metrics employed emphasize the efficiency of the model based on classification accuracy, precision, recall, F1-score, and error prediction, indicative of high-level performance overall. The temporal trends in personalization interaction and accuracy of fraud detection further indicate interactive patterns between user experience and security on the platform. Completely, these results provide an interdisciplinary understanding of predictive ability within the system and long-term performance compromises, required to make decisions appropriately in the case of e-commerce.

Received: 2022-10-01
Accepted: 2022-10-30
Published Online: 2022-10-30
DOI: 10.70454/IJMRE.2022.21001

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

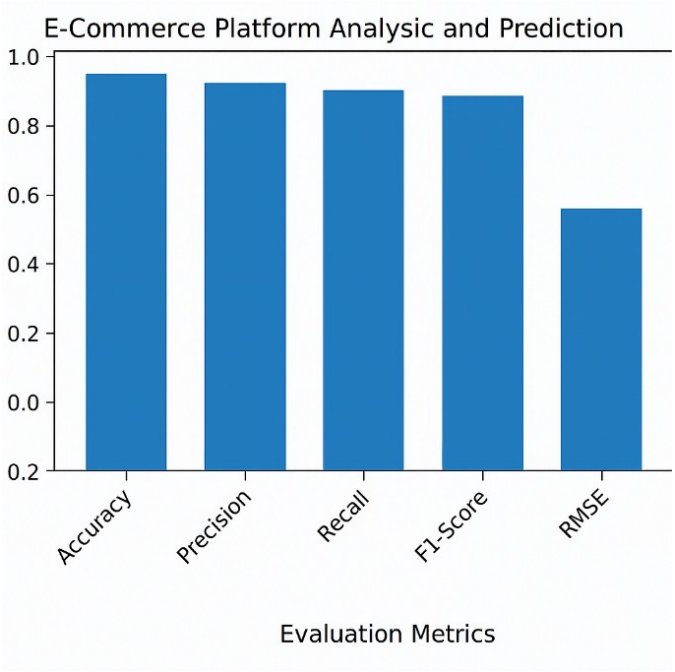

Fig 2: Evaluation Metrics for E-Commerce Platform Analysis and Prediction

The Fig 2 is a bar chart that shows the performance assessment of a predictive model created for analyzing and predicting trends on an e-commerce website. The measurements plotted on the x-axis are Accuracy, Precision, Recall, F1-Score, and RMSE (Root Mean Square Error), and the y-axis shows the respective measure values, from 0.0 to 1.0.From the plot, it can be seen that the model performs remarkably well for all the classification measures, with Accuracy, Precision, Recall, and F1-Score all approximately or just below 0.9. This performance level is very high, suggesting that the model is extremely good at accurately predicting the relevant outcomes with an optimal combination of false negatives and false positives.The RMSE of close to 0.6 calculates the standard deviation of the errors of prediction. Although RMSE is classically a regression metric, its presence here could be due to hybrid evaluation or part of numerical prediction incorporated in the classification model. The smaller RMSE indicates that the model has a tolerable degree of error in prediction, also evidencing its credibility

Received: 2022-10-01
Accepted: 2022-10-30
Published Online: 2022-10-30
DOI: 10.70454/IJMRE.2022.21001

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

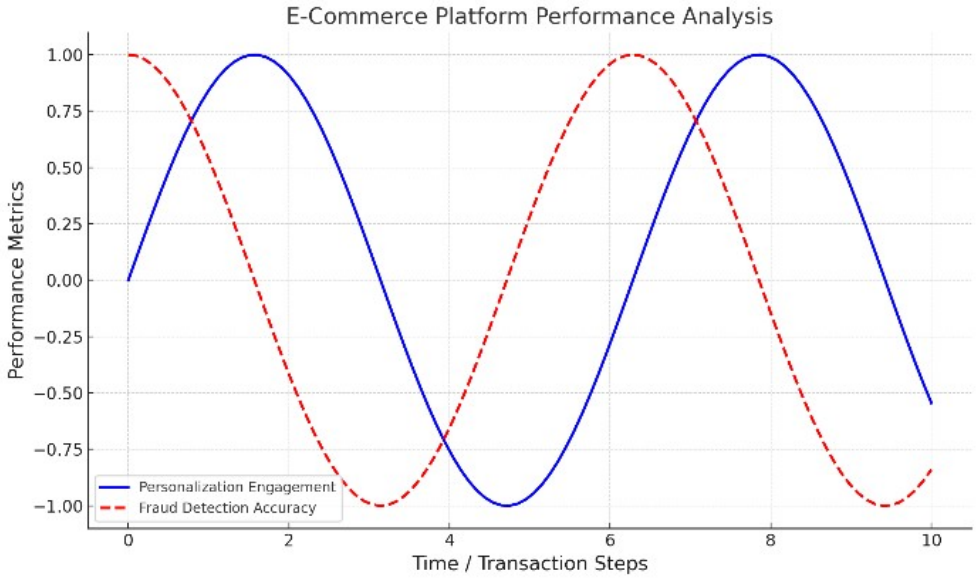

Fig 3: Temporal Performance Trends in E-Commerce Platform: Personalization vs. Fraud Detection

The Fig 3 illustrates a dual-line plot that plots the temporal performance dynamics of two key functionalities in an e-commerce platform—Personalization Engagement and Fraud Detection Accuracy—across a series of transaction steps or time points (0 to 10 on the x-axis). The y-axis is for performance measures, which range between -1.0 and 1.0 and are presumably normalized to show trend over time as opposed to an absolute figure. The blue solid line is Personalization Engagement, showing a sinusoidal curve and thereby cyclic behavior. This indicates that user interaction with personalization features sees periodic spikes and dips, possibly due to seasonal patterns of buying, changes in user interest, or cycles of promotional campaigns. The red dashed line, onthe other hand, indicates Fraud Detection Accuracy, which also has a sinusoidal trend but with phase difference to the engagement curve. This reverse trend suggests that where engagement in personalization is most prevalent, fraud detection performance is the poorest, and vice versa. This kind of trade-off may be due to greater system flexibility or relaxed tighter controls during peak times of personalization, thereby potentially influencing the strictness of fraud detection systems. The visualization is informative on capturing the working tension between improving user experience through personalization and ensuring platform security through fraud detection. Prudence should be exercised to comprehend such balance for maximal user satisfaction and transaction integrity in e-commerce settings

Received: 2022-10-01
Accepted: 2022-10-30
Published Online: 2022-10-30
DOI: 10.70454/IJMRE.2022.21001

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

Table 1: Performance Comparison of Personalization and Fraud Detection Accuracy Metrics

Metric	Personalization	Fraud Detection Accuracy
Max Value	0.95	0.85
Min Value	0.60	0.50
Mean Value	0.75	0.72

Table 1 Performance Comparison of Personalization and Fraud Detection Accuracy Metrics gives a statistical comparison of the performance metrics of two most important components of an intelligent e-commerce platform: Personalization and Fraud Detection Accuracy. It possesses three straightforward statistical values—Max Value, Min Value, and Mean Value—that give a relative sense of how each module functions under different scenarios or data sets. The Personalization module is exceptional in variability with a highest performance value of 0.95, which depicts good accuracy in delivering personalized content or product suggestions in the best case.

However, its minimum value of 0.60 indicates its performance can suffer in some situations, e.g., in poor data or cold-start situations. Its mean value of 0.75 reflects a broadly firm and stable performance in typical usage scenarios Conversely, the Fraud Detection Accuracy has a maximum of 0.85, a bit lower than personalization, reflecting its best-case performance as fairly good but not as great. The minimum of 0.50 indicates that under less optimal conditions, the model may perform at the level of random guessing. A mean accuracy of 0.72 reflects relatively stable performance but not as stable as personalization as a whole.

6. Conclusion and Future Work

In summary, the Cloud-Enabled Intelligent Personalization and Secure Transaction Framework for Scalable E-Commerce Platforms successfully integrates the latest technologies including recommender systems, NLP, behavioral analysis, and blockchain-based security technologies to maximize user experience and secure transaction integrity. The combined architecture facilitates real-time fraud prevention, personalized content recommendation, and advanced data protection, which makes it an all-around solution for e-commerce needs of today. For further work, the architecture can be enhanced by integrating federated learning for privacy-guaranteed personalization, using edge computing to provide lower latency, and studying adaptive AI models that dynamically learn from user activities and evolving threats to optimize scalability, security, and responsiveness even further.

Refrence

[1] Sandhu, A. K. (2021). Big data with cloud computing: Discussions and challenges. Big Data Mining and Analytics, 5(1), 32-40.

Received: 2022-10-01
Accepted: 2022-10-30
Published Online: 2022-10-30
DOI: 10.70454/IJMRE.2022.21001

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

[2] Akhil, R.G.Y. (2021). Improving Cloud Computing Data Security with the RSA Algorithm. International Journal of Information Technology & Computer Engineering, 9(2), ISSN 2347–3657.

[3] Kumar, V., Laghari, A. A., Karim, S., Shakir, M., &Brohi, A. A. (2019). Comparison of fog computing & cloud computing. Int. J. Math. Sci. Comput, 1(1), 31-41.

[4] Yalla, R.K.M.K. (2021). Cloud-Based Attribute-Based Encryption and Big Data for Safeguarding Financial Data. International Journal of Engineering Research and Science & Technology, 17 (4).

[5] Schleier-Smith, J., Sreekanti, V., Khandelwal, A., Carreira, J., Yadwadkar, N. J., Popa, R. A., ... & Patterson, D. A. (2021). What serverless computing is and should become: The next phase of cloud computing. Communications of the ACM, 64(5), 76-84.

[6] Harikumar, N. (2021). Streamlining Geological Big Data Collection and Processing for Cloud Services. Journal of Current Science, 9(04), ISSN NO: 9726-001X.

[7] Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A systematic literature review on cloud computing security: threats and mitigation strategies. Ieee Access, 9, 57792-57807.

[8] Basava, R.G. (2021). AI-powered smart comrade robot for elderly healthcare with integrated emergency rescue system. World Journal of Advanced Engineering Technology and Sciences, 02(01), 122–131.

[9] Attaran, M., & Woods, J. (2019). Cloud computing technology: improving small business performance using the Internet. Journal of Small Business & Entrepreneurship, 31(6), 495-519.

[10] Sri, H.G. (2021). Integrating HMI display module into passive IoT optical fiber sensor network for water level monitoring and feature extraction. World Journal of Advanced Engineering Technology and Sciences, 02(01), 132–139.

[11] Shafiq, D. A., Jhanjhi, N. Z., Abdullah, A., & Alzain, M. A. (2021). A load balancing algorithm for the data centres to optimize cloud computing applications. Ieee Access, 9, 41731-41744.

[12] Rajeswaran, A. (2021). Advanced Recommender System Using Hybrid Clustering and Evolutionary Algorithms for E-Commerce Product Recommendations. International Journal of Management Research and Business Strategy, 10(1), ISSN 2319-345X.

[13] Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE access, 7, 74361-74382.

[14] Sreekar, P. (2021). Analyzing Threat Models in Vehicular Cloud Computing: Security and Privacy Challenges. International Journal of Modern Electronics and Communication Engineering, 9(4), ISSN2321-2152.

[15] Tadapaneni, N. R. (2020). Cloud computing security challenges. International journal of Innovations in Engineering research and Technology, 7(6), 1-6.

[16] Naresh, K.R.P. (2021). Optimized Hybrid Machine Learning Framework for Enhanced Financial Fraud Detection Using E-Commerce Big Data. International Journal of Management Research & Review, 11(2), ISSN: 2249-7196.

[17] Liu, S., Guo, L., Webb, H., Ya, X., & Chang, X. (2019). Internet of Things monitoring system of modern eco-agriculture based on cloud computing. Ieee Access, 7, 37050-37058.

[18] Sitaraman, S. R. (2021). AI-Driven Healthcare Systems Enhanced by Advanced Data Analytics and Mobile Computing. International Journal of Information Technology and Computer Engineering, 12(2).

Received: 2022-10-01
Accepted: 2022-10-30
Published Online: 2022-10-30
DOI: 10.70454/IJMRE.2022.21001

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

[19] Sharma, D. K., Boddu, R. S. K., Bhasin, N. K., Nisha, S. S., Jain, V., & Mohiddin, M. K. (2021, October). Cloud computing in medicine: Current trends and possibilities. In 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA) (pp. 1-5). IEEE.

[20] Mamidala, V. (2021). Enhanced Security in Cloud Computing Using Secure Multi-Party Computation (SMPC). International Journal of Computer Science and Engineering(IJCSE), 10(2), 59–72

[21] Olayinka, O. H. (2021). Data driven customer segmentation and personalization strategies in modern business intelligence frameworks. World Journal of Advanced Research and Reviews, 12(3), 711-726.

[22] Sareddy, M. R. (2021). The future of HRM: Integrating machine learning algorithms for optimal workforce management. International Journal of Human Resources Management (IJHRM), 10(2).

[23] Sarker, I. H., Kayes, A. S. M., & Watters, P. (2019). Effectiveness analysis of machine learning classification models for predicting personalized context-aware smartphone usage. Journal of Big Data, 6(1), 1-28.

[24] Chetlapalli, H. (2021). Enhancing Test Generation through Pre-Trained Language Models and Evolutionary Algorithms: An Empirical Study. International Journal of Computer Science and Engineering(IJCSE), 10(1), 85–96

[25] Jain, P., & Aggarwal, K. (2020). Transforming marketing with artificial intelligence. International Research Journal of Engineering and Technology, 7(7), 3964-3976.

[26] Basani, D. K. R. (2021). Leveraging Robotic Process Automation and Business Analytics in Digital Transformation: Insights from Machine Learning and AI. International Journal of Engineering Research and Science & Technology, 17(3).

[27] Bozkurt, A., Karadeniz, A., Baneres, D., Guerrero-Roldán, A. E., & Rodríguez, M. E. (2021). Artificial intelligence and reflections from educational landscape: A review of AI studies in half a century. Sustainability, 13(2), 800.

[28] Sareddy, M. R. (2021). Advanced quantitative models: Markov analysis, linear functions, and logarithms in HR problem solving. International Journal of Applied Science Engineering and Management, 15(3).

[29] Koteluk, O., Wartecki, A., Mazurek, S., Kołodziejczak, I., & Mackiewicz, A. (2021). How do machines learn? artificial intelligence as a new era in medicine. Journal of Personalized Medicine, 11(1), 32.

[30] Bobba, J. (2021). Enterprise financial data sharing and security in hybrid cloud environments: An information fusion approach for banking sectors. International Journal of Management Research & Review, 11(3), 74–86.

[31] Yau, K. L. A., Saad, N. M., & Chong, Y. W. (2021). Artificial intelligence marketing (AIM) for enhancing customer relationships. Applied Sciences, 11(18), 8562.

[32] Narla, S., Peddi, S., &Valivarthi, D. T. (2021). Optimizing predictive healthcare modelling in a cloud computing environment using histogram-based gradient boosting, MARS, and SoftMax regression. International Journal of Management Research and Business Strategy, 11(4).

Received: 2022-10-01
Accepted: 2022-10-30
Published Online: 2022-10-30
DOI: 10.70454/IJMRE.2022.21001

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

[33] Lind, J., Naor, O., Eyal, I., Kelbert, F., Sirer, E. G., &Pietzuch, P. (2019, October). Teechain: a secure payment network with asynchronous blockchain access. In Proceedings of the 27th ACM Symposium on Operating Systems Principles (pp. 63-79).

[34] Kethu, S. S., & Purandhar, N. (2021). AI-driven intelligent CRM framework: Cloud-based solutions for customer management, feedback evaluation, and inquiry automation in telecom and banking. Journal of Science and Technology, 6(3), 253–271.

[35] Sayeed, S., & Marco-Gisbert, H. (2019). Assessing blockchain consensus and security mechanisms against the 51% attack. Applied sciences, 9(9), 1788.

[36] Srinivasan, K., &Awotunde, J. B. (2021). Network analysis and comparative effectiveness research in cardiology: A comprehensive review of applications and analytics. Journal of Science and Technology, 6(4), 317–332.

[37] Khan, P. W., & Byun, Y. (2020). A blockchain-based secure image encryption scheme for the industrial Internet of Things. Entropy, 22(2), 175.

[38] Narla, S., & Purandhar, N. (2021). AI-infused cloud solutions in CRM: Transforming customer workflows and sentiment engagement strategies. International Journal of Applied Science Engineering and Management, 15(1).

[39] Lin, C., He, D., Huang, X., Khan, M. K., & Choo, K. K. R. (2020). DCAP: A secure and efficient decentralized conditional anonymous payment system based on blockchain. IEEE Transactions on Information Forensics and Security, 15, 2440-2452.

[40] Budda, R. (2021). Integrating artificial intelligence and big data mining for IoT healthcare applications: A comprehensive framework for performance optimization, patient-centric care, and sustainable medical strategies. International Journal of Management Research & Review, 11(1), 86–97.

[41] Alamdari, P. M., Navimipour, N. J., Hosseinzadeh, M., Safaei, A. A., & Darwesh, A. (2020). A systematic study on the recommender systems in the E-commerce. Ieee Access, 8, 115694-115716.

[42] Ganesan, T., & Devarajan, M. V. (2021). Integrating IoT, Fog, and Cloud Computing for Real-Time ECG Monitoring and Scalable Healthcare Systems Using Machine Learning-Driven Signal Processing Techniques. International Journal of Information Technology and Computer Engineering, 9(1).

[43] Abdul Hussien, F. T., Rahma, A. M. S., & Abdulwahab, H. B. (2021). An e-commerce recommendation system based on dynamic analysis of customer behavior. Sustainability, 13(19), 10786.

[44] Pulakhandam, W., & Samudrala, V. K. (2021). Enhancing SHACS with Oblivious RAM for secure and resilient access control in cloud healthcare environments. International Journal of Engineering Research and Science & Technology, 17(2).

[45] Wen, M., Vasthimal, D. K., Lu, A., Wang, T., & Guo, A. (2019, December). Building large-scale deep learning system for entity recognition in e-commerce search. In Proceedings of the 6th IEEE/ACM International Conference on Big Data Computing, Applications and Technologies (pp. 149-154).

[46] Jayaprakasam, B. S., &Thanjaivadivel, M. (2021). Integrating deep learning and EHR analytics for real-time healthcare decision support and disease progression modeling. International Journal of Management Research & Review, 11(4), 1–15. ISSN 2249-7196.

Received: 2022-10-01
Accepted: 2022-10-30
Published Online: 2022-10-30
DOI: 10.70454/IJMRE.2022.21001

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

[47] Uzun-Per, M., Can, A. B., Gürel, A. V., & Aktaş, M. S. (2021, December). Big data testing framework for recommendation systems in e-science and e-commerce domains. In 2021 IEEE International Conference on Big Data (Big Data) (pp. 2353-2361). IEEE.

[48] Jayaprakasam, B. S., &Thanjaivadivel, M. (2021). Cloud-enabled time-series forecasting for hospital readmissions using transformer models and attention mechanisms. International Journal of Applied Logistics and Business, 4(2), 173-180.

[49] Khodabandehlou, S. (2019). Designing an e-commerce recommender system based on collaborative filtering using a data mining approach. International Journal of Business Information Systems, 31(4), 455-478.

[50] Dyavani, N. R., &Thanjaivadivel, M. (2021). Advanced security strategies for cloud-based e-commerce: Integrating encryption, biometrics, blockchain, and zero trust for transaction protection. Journal of Current Science, 9(3), ISSN 9726-001X.

[51] Al-Mahrouqi, R., Al Siyabi, K., Al Nabhani, A., Al-Hashemi, S., & Muhammed, S. A. (2021). E-commerce web app in azure cloud: considerations, components of implementation and schematic design. *Computer and Information Science*, *14*(4), 1-32.