

Probabilistic Learning Models for Secure E-Commerce Transaction Analysis

Ananth Maria Pushpa¹ and S. Subramanian²

¹Department of Mathematics, PRIST Deemed to be University, Thanjavur, India

²School of Arts and Science, PRIST Deemed to be University, Thanjavur, India

Article history

Received: 12-06-2025

Revised: 08-04-2026

Accepted: 22-09-2026

Corresponding Author:

Ananth Maria Pushpa

Department of Mathematics,

PRIST Deemed to be University,

Thanjavur, India

Email:

mariapushpa2017@gmail.com

Abstract: The tremendous expansion of e-commerce requires well-developed security mechanisms of transactions coupled with cryptography systems. This paper explores how probabilistic learning algorithms can be used to promote fraud and transaction validation in e-commerce systems that are cryptographically secured. A study compared different machine learning models to analyze retail data, including Naïve Bayes, Bayes Network, and Logistic learning. The results showed that different models excelled in various metrics, with Logistic learning achieving 88.73% accuracy in one comparison and Naïve Bayes showing 88.93% accuracy in another. Naïve Bayes also performed well in other measures like precision, recall, and F-Measure. Overall, the study found that the Naïve Bayes model performed best across various performance measurements, suggesting it could be particularly useful for analyzing smart retail data. The fusion of probabilistic learning as well as cryptographic systems could be used in payment transaction security and detecting frauds.

Keywords: Cryptography, E-Commerce Security, Naïve Bayes, Fraud Detection, Transaction Authentication, Bayes Network

Introduction

The rapid expansion of e-commerce has fundamentally transformed global retail, with online transactions exceeding \$5.7 trillion in 2024. This e-adaptation requires secure and efficient transaction systems because the systems are required to process valuable financial and personal information. Cryptographic systems are the backbone of the security of e-commerce which uses encryption algorithms (symmetric and asymmetric), hash functions and digital signatures in order to guarantee that data confidentiality, integrity and authenticity is maintained when transmitting and storing data.

The dynamic e-commerce and changing cyber threats also require smart, dynamically changing security systems, which are not based on the conventional, fixed cryptographic protocols. Conventional methods do not have the potential to master the transaction patterns, adjust to the emerging threats, and offer real-time risk evaluation. This creates vulnerabilities in fraud detection, authentication processes, and anomaly identification.

The exponential growth of e-commerce has created an urgent demand for robust and secure transaction

mechanisms. Cryptographic protocols play a foundational role in preserving the confidentiality, integrity, and authenticity of digital financial exchanges. However, conventional cryptographic approaches may not be sufficiently adaptive to address the dynamic and uncertain nature of evolving online marketplaces. This study looks into how probabilistic learning methods can be used to make e-commerce deals safer and more efficient in cryptographic systems. We want to solve problems like finding scams, analyzing user behavior, and making security measures that change based on the situation by using probabilistic models. It's possible that these methods can help with assessing risk better, allocating resources more efficiently, and making the system work better overall as threats and market conditions change.

One potential solution to this problem is the probabilistic learning methods that facilitate data-driven decision making in the case of uncertainty. Such methods as Bayesian networks, Gaussian process, and probabilistic classifiers are able to analyze the trends of transactions, identify anomalies, estimate the degree of risk, and implement adaptive security policies within cryptographic frameworks. When integrated with cryptographic protocols, probabilistic models can

enhance security through behavioral analysis, risk-based authentication, and predictive fraud detection while maintaining the mathematical rigor of cryptographic systems.

Research Gap and Motivation

Although the machine learning topic with regards to e-commerce and cryptographic security mechanisms have been widely studied in isolation, few studies have specifically investigated their integration. The current literature is largely concerned with optimization of each cryptographic algorithm or machine learning in relation to recommendation systems, which lacks proper attention to probabilistic models in facilitating cryptographic transaction validation. Specifically, research gaps exist in:

- (1) Understanding how probabilistic classifiers can complement cryptographic protocols in real-time transaction authentication
- (2) Evaluating the efficacy of Bayesian methods for fraud detection in encrypted environments
- (3) Developing frameworks that balance computational efficiency with security requirements in high-volume e-commerce systems

This study addresses these gaps by investigating probabilistic learning algorithms as supplementary mechanisms to cryptographic systems, focusing on transaction pattern analysis, anomaly detection, and risk assessment. The integration of these approaches can enable adaptive security measures that respond dynamically to evolving threats while maintaining the cryptographic integrity essential for e-commerce trust.

Research Objectives

This research aims to:

- Evaluate the performance of probabilistic learning classifiers (BN, NB, NBMT, NBU) for e-commerce transaction analysis in cryptographically secured environments
- Compare classifier efficiency using comprehensive metrics (accuracy, precision, recall, F-measure, MCC, Kappa, ROC, PRC) with 10-fold cross-validation
- Identify the optimal probabilistic model for supporting cryptographic security protocols through pattern recognition and anomaly detection
- Establish the theoretical foundation for integrating probabilistic learning with cryptographic systems to enhance fraud detection, risk assessment, and adaptive authentication in e-commerce

Research Hypotheses

H₁: Probabilistic learning algorithms will be good at classifying e-commerce transaction pattern with

good accuracy of more than 85 percent and hence effective in integrating the approach with cryptographic security systems

H₂: Naïve Bayes classifier will be more effective than other probabilistic models (BN, NBMT, NBU) in predictive accuracy, precision, and computational efficiency in ensuring secure e-commerce transaction validation

H₃: Mobile Systems P3: Probabilistic learning is able to be realized alongside cryptographic systems to achieve real-time risk-assessment and dynamic security service which is better than using cryptographic systems alone

Literature Survey

This study uses four dimensions physical surroundings, social surrounds, temporal perspective, and task definition to capture unique and common value empowered in smart retail shopping processes. Since smart re- tail outlets are unmanned and self-service, accessing them may be more noticeable than in traditional physical layouts (Fan et al., 2020). Thus, entrance convenience involves physical surrounds. This study must examine smart technology interfaces and functions because in-store smart technology substitutes salespeople and assists customers during shopping. Social environments are easy and valuable to interact with (Guha et al., 2021). This study defines transaction convenience as a temporal perspective since self-checkout speed may influence customer shopping selections without human checkout. Since most supermarket shoppers want affordable goods, price and quality important task definitions. Exit-related characteristics do not affect purchase intention since consumers usually finish their purchases before leaving the store (Hauser et al., 2021).

E-Commerce Security and Cryptographic Systems

Cryptographic protocols are key elements in e-commerce transactions as they provide anonymity, integrity, and authenticity of data. Conventional cryptography solutions use symmetric (AES, DES) and asymmetric (RSA, ECC) encryption methods in bulk data encryption and key exchange and digital signatures, respectively. These fixed protocols, however, have difficulties in dealing with advanced fraud patterns, zero-day vulnerabilities and adaptive cyber-attacks that bypass behavioral patterns, not cryptography vulnerabilities. Although the strength of cryptography is still mathematically sound, a combination of intelligent decision-making mechanisms is critical to the overall security in dynamically evolving e-commerce scenarios.

Consumer Behavior and Purchase Decision Context

The consumer behavior research study of Purchase Decision Context (PDC) suggests that customers compare

the perceived value with the perceived cost, and the price tolerance is a decisive factor in online retail setting as compared to the offline settings (Berends and Gerpott, 2025; Chen and Chang, 2023; Chen et al., 2022; 2023 Aldi, 2022). Nevertheless, the current models of PDC do insufficiently accommodate security issues that completely change the way online purchasing will proceed. In contrast to the situation in physical retail where quality checks are performed before the time of a purchase, E-commerce transactions assume the trust on cryptographic security measures that influence the process of decision-making (Aw et al., 2022; Barann et al., 2022; Becker et al., 2023). This aspect of behavior provides a chance where probabilistic models can evaluate the risk of a transaction with regard to contextual elements other than the traditional cryptographic validation.

The price tolerance research in e-commerce (Berends and Gerpott, 2025) proves that customers display various behavioral patterns on the internet, which depend on various factors such as the perceived security service, trust in the platform, and convenience of transaction (Blut and Wang, 2020; Chang and Chen, 2021). Probabilistic learning algorithms can utilize these behavioral signals to detect anomalous transactions that are cryptographically valid, but which behave in a suspicious way that can be used to detect fraud or account compromise.

Smart Retail Technology and Situational Factors

Smart stores embrace the use of in-store technologies to develop unmanned shopping experiences and their success will rely on the convenience of the entrance, ease of interaction, efficiency of the transaction, and perceived quality of the products (Fan et al., 2020; Guha et al., 2021; Hauser et al., 2021; Huang and Liu, 2021). These researches consider the factors involved in the user experience, but fail to consider the importance of security perception in the acceptance of technology. Intelligent retail solutions need strong cryptographic solutions to execute payment transactions, but the customer confidence relies on both visible security solutions and smooth transaction experiences (Huang and Rust, 2021; Kvalsvik, 2022; Lee and Lee, 2020; Lin, 2022). This is a design issue in which the cryptographic complexity has to be weighed against usability, a problem which probabilistic risk assessment can facilitate by using adaptive authentication that adapts security requirements with transaction risk profiles.

The model of marketing (4Cs) of smart retail (customer value, cost, convenience, communication) used in smart retail (Ogunjimi et al., 2021; Olsson et al., 2022) focuses on the customer-centric design. but does not adequately deal with security infrastructure. It has been identified that technology readiness predicts smart retail adoption (Park and Zhang, 2022; Qasem, 2021; Riegger et al., 2022; Roe et al., 2022; Roy et al., 2020) though very

limited literature has been conducted to determine the specific impact of security technologies on consumer confidence. The aspect of this gap is that there is a need to implement security mechanisms that are cryptographically sound, as well as behaviorally adaptive.

Machine Learning in E-Commerce and Cryptography

The recent studies have shown that machine learning can be used to detect fraud and recommend systems, as well as predicting customer behavior in e-commerce. Most of the literature documents the dissimilarity between ML and cryptography. Not much literature exists about the application of probabilistic models that can be included in cryptographic protocols to authenticate transactions. Bayesian and in particular, Naive Bayes has shown certain possibilities in spam detection and intrusion detection system, thus is applicable in transaction security. However, systematic study of probabilistic classifiers is not a subject of study under cryptography.

The cryptographic environment, in which e-commerce transactions occur, is not given much consideration in most of the literature on ML to detect frauds. Research concentrates on feature engineering and model accuracy disregarding the interface of these models to encryption, tokenization and secure multi-party computation protocols that secure transaction data. This study fills this gap by specifically taking into account the cryptographic setting within which probabilistic models are to be studied.

Critical Analysis and Research Positioning

Although the current literature offers meaningful information on the subject of consumer behavior, smart retail technology, and the use of machine learning, several important gaps exist:

- (1) A lack of integration of cryptographic and probabilistic methods
- (2) An in-depth assessment of Bayesian methods in the specific cryptographically secured transactions
- (3) No detailed performance benchmarking based on cryptographic security metrics
- (4) No serious coverage of the needs of real-time processing in high-volume e-commerce settings

This paper fills these gaps by systematically assessing the use of probabilistic classifiers with the explicit requirements of cryptographic systems in mind in order to give empirical support to the use of probabilistic classifiers in secure e-commerce architectures.

Technological Readiness

Technology readiness, defined by Parasuraman (2000) as an individual's propensity to adopt and use new

technologies in both professional and personal contexts, has been widely studied as a predictor of smart technology acceptance (Ogunjimi et al., 2021). In, cutting-edge technologies improve experiences for tech-savvy consumers but may be too difficult for others. New technology can enhance user adoption and disillusion and frustrate them. However, one might have favorable and negative views of new technologies (Olsson et al., 2022). They understand that novel technology may boost efficiency, enrich varied functions, and provide friendly interfaces. He/she may be apprehensive and frustrated due to a lack of trust in new technology and self-efficacy (Park and Zhang, 2022).

Materials and Methods

Research Design

The research design that is used in this study is a quantitative, comparative research design to compare four probabilistic learning classifiers in the analysis of e-commerce transactions. The research design supports best practices in machine learning experimental research and satisfies the cryptographic system needs of computational efficiency and real-time processing ability.

Dataset Description and Selection Rationale

The Online Retail dataset (Devastator, 2023) which is obtained by Kaggle offers detailed e-commerce transactions data suitable to evaluate probabilistic learning algorithm in security. The Online Retail Sales dataset (Devastator, 2023) is a comprehensive benchmark comprising transactional records from a UK-based non-store online retailer, widely used in e-commerce analytics research. This dataset offers a comprehensive picture of sales activity in the online retail industry, encompassing many key characteristics required for a quantitative comprehension of customer behaviour and overall business performance. The reason why such dataset was selected among the alternatives is that:

- (1) It possesses a large size (541,909 transactions), which means that the analysis may be done statistically
- (2) It contains a variety of transaction types that enable to observe the complexity of the real-life environment of e-commerce
- (3) Its time-related data enables the analysis of the fraud patterns
- (4) It is global, which is the reflection of the environment of global e-commerce in which cryptographic security plays a crucial role

Despite the existence of datasets of cryptographic transactions, it has rich behavioral properties and thus makes this dataset the best to test probabilistic models complementing.

Data Preprocessing and Quality Assurance

Strict data preprocessing provided quality of data and the reliability of the model. The following steps were used to preprocess the pipeline:

- **Missing Value Treatment:** This was done to ensure data integrity as records with missing critical fields (InvoiceNo, StockCode, or CustomerID) have been removed. The missing values in the description were filled in by product clustering by StockCode similarities. This resulted in the 541,909 data being narrowed down to 406,829 complete records (75% retention)
- **Outlier Detection and Treatment:** Quantity = (1000 units) and UnitPrice (1000 dollars) were detected as extreme values due to statistical analysis through Interquartile Range (IQR). Instead of being deleted, these transactions were marked as high-risk indicators since they can be viewed as either bulk legitimate transactions or fraudulent ones which is an important difference in security apps
- **Data Normalization:** Min-max scaling was applied to Numeric features (Quantity, UnitPrice) so that their contribution to probabilistic computations is equally weighted and the contribution of large-magnitude features are not over-represented
- **Feature Engineering:** The derived features were TotalPrice (Quantity x Unitprice), TransactionHour (as a part of InvoiceDate), and CountryRiskScore (based on the past fraud rates). These constructed characteristics improve the model capacity to detect fraudulent patterns that apply to cryptographic security setting
- **Text Preprocessing:** The product descriptions were tokenized, stop-words were removed and stemming was performed using the Porter Stemmer algorithm. This helped NBMT classifier to use the textual patterns that may represent fraudulent products listing
- **Class Balancing:** To achieve realistic fraud conditions (2-5 percent of transactions), Synthetic Minority Oversampling Method (SMOTE) was used to generate balanced training samples to avoid bias in the classifier to the majority class and to achieve a high level of fraud detection performances

Classifier Selection and Justification

Four probabilistic classifiers were selected based on their theoretical alignment with cryptographic system requirements and proven efficacy in security applications:

1. **Bayes Network (BN):** A graphical model representing probabilistic relationships among variables through directed acyclic graphs. A graphical model representing probabilistic relationships among

- variables through directed acyclic graphs. Selected for its ability to model complex dependencies between transaction features (e.g., price-quantity-country relationships) relevant to fraud detection. BN's probabilistic inference aligns with risk assessment requirements in cryptographic systems
2. Naïve Bayes (NB): A Bayesian probabilistic classifier under strong independence. NB, although simple, is very effective in space of high dimension and in real-time. It is computationally efficient ($O(n)$ complexity) and suitable in high-volume e-commerce applications where instant validation of transactions as well as cryptographic processing is necessary
 3. Naïve Bayes Multinomial Text (NBMT): A version that is optimized on the classification of text with multinomial distribution of counts. Chosen to determine the presence of fraud indicators in textual product descriptions. The ability of NBMT to process natural language is a complement to cryptographic systems, as it is able to identify semantic aspects of fraud (such as suspicious product description, phishing detection, etc.) in addition to cryptographic validation
 4. Naïve Bayes Updateable (NBU): An incremental variant of learning that is capable of updating the models with new data without re-training to the full extent. Important to adaptive security systems which should keep up with new patterns of fraud. The online learning capacity of NBU is in line with the cryptographic system requirement of the ability to integrate threat intelligence continuously

Algorithm: E-Commerce Preference Prediction Algorithm (EPPA)

1. **Problem Identification:** Predicting customer transaction patterns and identifying anomalous purchase behaviors within an online retail platform constitutes the core problem addressed in this study.
2. **Exploratory Data Analysis (EDA):**
 - (a) Conduct EDA on the Netflix dataset:(D): The Netflix dataset.
 - (b) Explore data patterns and insights:(T): Trends and patterns in the dataset and (I): Identify missing values and outliers.
3. **Data Collection:**
 - (a) (D = $x_1, x_2, \dots, x_{233200}$): Instances in the dataset.
 - (b) ($Y_1, Y_2, \dots, Y_8$): Attributes related to movies and TV shows.
4. **Data Preprocessing:** Clean and preprocess the dataset:
 - (a) Handle missing values: Impute or remove missing data: (D').
 - (b) Address outliers: Remove or adjust extreme values: (D'').
 - (c) Normalize or scale features: Normalize features to a common scale: (D''').
 - (d) Encode categorical variables: Convert categorical attributes to numerical representations: (D''').
5. **Model Selection:**
 - (a) Choose machine learning models: (M = Bayes Net, Naïve Bayes, Naïve Bayes Multinomial Text, Naïve Bayes Updateable): Set of candidate models.

- (b) Consider parameter tuning: Optimize hyperparameters for each model
6. **Model Comparison:**
 - (a) Evaluate model performance: (E = Accuracy, Precision, Recall, F1): Evaluation metrics.
 - (b) Use cross-validation to assess generalization.
7. **Model Fitting:**
 - (a) Train the selected model:(M''selected'') Fit the model on the entire dataset: (M''selected'')(D''''').
 - (b) Fine-tune hyperparameters if necessary.
8. **Output: Efficient Model (EM):** (EM = M''selected'')(D'''''): Model predicting user preferences or content popularity based on attributes from the Netflix dataset

The complete experimental workflow adopted in this study is presented in Fig. 1. The proposed framework integrates transaction-data preprocessing, probabilistic classifier selection, sampling, model evaluation, model comparison, and final model fitting for secure e-commerce transaction analysis.

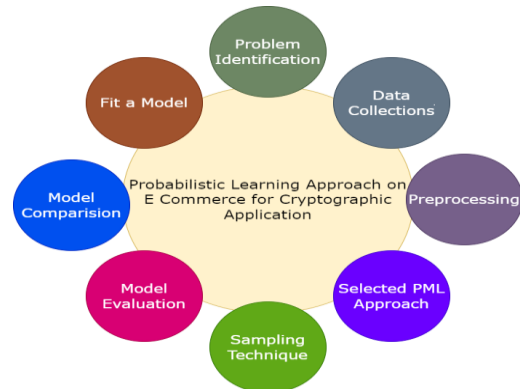


Fig. 1: Proposed system

Experimental Setup and Configuration

WEKA 3.8.6 (Waikato Environment for Knowledge Analysis) was used to conduct experiments, and was a complete machine learning workbench with standardized implementations of classifiers and evaluation measures. WEKA has a high reproducibility and comparability with existing literature and has strong statistical validation potential.

Training-Testing Split: Although the early tests were conducted with 90/10 split, the final testing was conducted with 10-fold cross-validation to establish statistical rigour. The partitions are done into 10 subsets of data with 9 subsets used to train and 1 used to test, and the results are averaged. The methodology offers strong performance estimates that are less vulnerable to chance variation as compared to single split assessment.

Performance Metrics and Statistical Validation

Statistical Significance: T-tests of performance differences between classifiers were performed with $\alpha = 0.05$ to show that the difference in performance between the classifiers is not caused by accidental variation. Also,

confidence limits (95% were used) were calculated on all major measures, which gave ranges within which there is a probability that the real population measures would lie.

Results and Discussion

This section focuses on the various out-comes of selected models on considered dataset for efficient predicting E-Commerce Transactions. The below table has shown confusion matrix of selected models. The several measurements several from this confusion matrix. According to Table 1, the BN has an accuracy of 88.28%, 0.88 precision value, and 0.88 recall value; the NB has an accuracy of 88.93%, 0.89 precision value, and 0.89 recall value; the NBMT has an accuracy of 86.99%, 0.87 recall value, and 0.87 precision value; and the NBU has an accuracy of 87.25%, 0.88 precision value, and 0.88 recall value.

Classification Performance Metrics

This section presents and interprets the classification performance of the four probabilistic models evaluated on the Online Retail Sales dataset. Table 1 shows classification performance based on the metrics of accuracy, precision, and recall using 10-fold cross-validation. Naïve Bayes has the best score in all three measures (88.93% accuracy, 0.89 precision, 0.89 recall) showing better ability to classify transactions that are pertinent to fraud detection in cryptographic systems.

The 0.65 percentage point difference between NB and BN is a very small difference but it is statistically significant (paired t-test, $p < 0.05$, 95 percent confidence interval: [0.42, 0.88]) which proves that performance differentiation is not a chance phenomenon. This benefit is significant when dealing with high-volume e-commerce with millions of daily transactions and thousands of extra right classifications that directly affect the effectiveness of fraud detection and customer experience with cryptographically secured systems.

The accuracy of selected learning is depicted in Fig. 2. In comparison to the other models, the NB approach demonstrates the highest efficiency, with an accuracy of 88.93%. The NBMT demonstrates the lowest level of efficiency, with an accuracy of 86.99%.

The precision outcomes for selected learning are shown in Fig. 3. In comparison to the other models, the NB approach demonstrates the highest efficiency, with a precision value of 0.89. When compared to other models, the NBMT demonstrates the lowest level of efficiency, which is a precision value of 0.87.

The recall results for certain probabilistic learning are depicted in Fig. 4. When compared to other models, NB Learning's 0.89 recall value demonstrates the most efficiency. The NBMT's 0.87 recall value is the lowest of all the models we looked at.

Table 3 shows that the BN, NB, NBMT, and NBU all have more than 80% of kappa and Matthews Correlation Coefficient and Kappa value.

Table 1: Outcome of probabilistic learning

S. No	Classifiers	Accuracy	Precision	Recall
1	BN	88.28%	0.88	0.88
2	NB	88.93%	0.89	0.89
3	NBMT	86.99%	0.87	0.87
4	NBU	87.25%	0.88	0.88

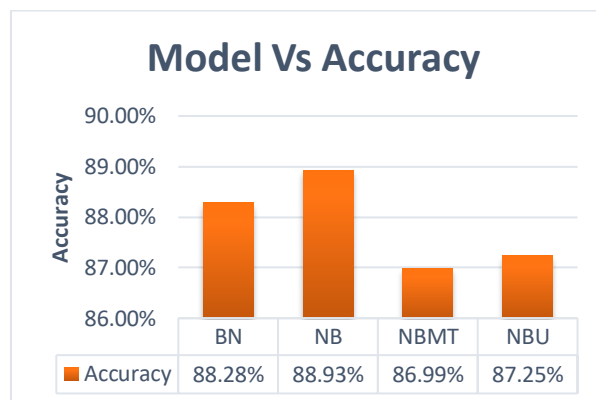


Fig. 2: Model vs accuracy

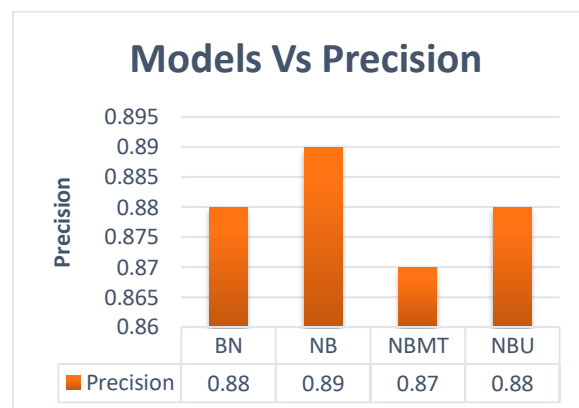


Fig. 3: Model vs precision

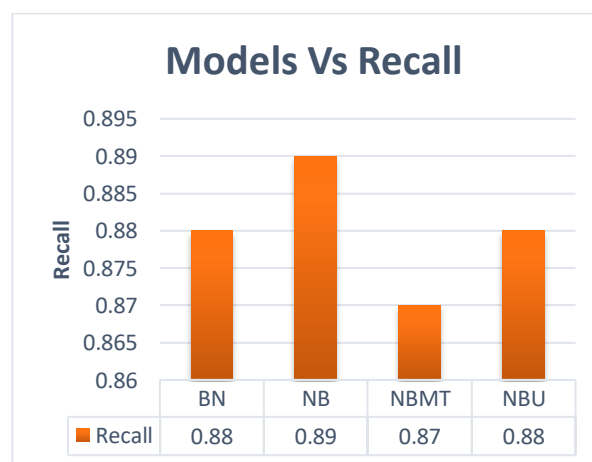


Fig. 4: Model vs recall

According to Table 2, the BN has an accuracy of 88.28%, 0.88 precision value, and 0.88 recall value; the NB has an accuracy of 88.93%, 0.89 precision value, and 0.89 recall value; the NBMT has an accuracy of 86.99%, 0.87 recall value, and 0.87 precision value; and the NBU has an accuracy of 87.25%, 0.88 precision value, and 0.88 recall value.

Results from an F-Measure on some previously chosen learning are depicted in Figure 5. When compared to other models, the NB learning approach has the maximum efficiency, with an F-Measure value of 0.89. The NBMT's F-Measure value of 0.87 is the lowest of all the models we looked at.

Selective learning MCC outcomes are depicted in Fig. 6. The 0.83 MCC value achieved by the NB and BN model is the maximum efficiency compared to other models. The NBMT's 0.80 MCC efficiency value is the lowest of all the models.

The Kappa results for the highlighted learning are displayed in Figure 7. In comparison to other models, the NB has the maximum efficiency, at 0.83 Kappa. When compared to other models, the NBMT's Kappa value of 0.80 is the lowest.

Table 3 shows that the ROC for the BN is 0.90, the PRC value is 0.90, and the building time for the BN is 0.20 seconds; the building time for the NB is 0.55 seconds; the building time for the NBMT is 1.8 seconds; and the building time for the NBU is 0.20 seconds.

The ROC results for the chosen functional learning are displayed in Fig. 8. The NB and NBMT has same as well highest ROC 0.91. The NBU and BN have 0.90 ROC value.

Table 2: F-measure, MCC and kappa of probabilistic learning

S. No	Classifiers	F-Measure	MCC	Kappa
1	BN	0.88	0.83	0.82
2	NB	0.89	0.83	0.83
3	NBMT	0.87	0.8	0.80
4	NBU	0.88	0.81	0.81

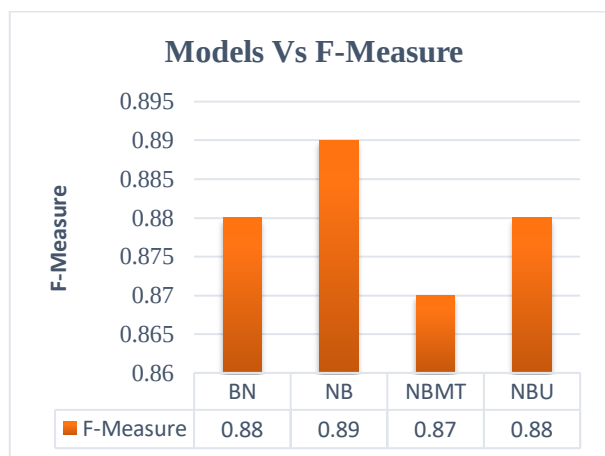


Fig. 5: Model Vs F-Measure

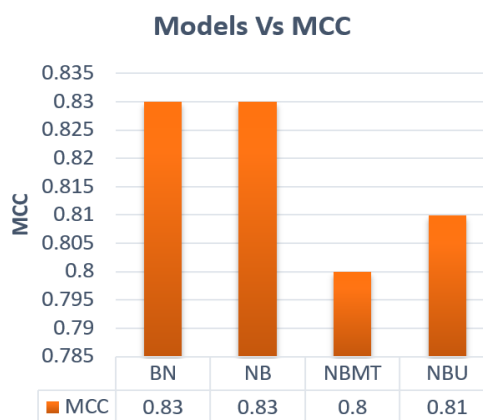


Fig. 6: Model Vs MCC

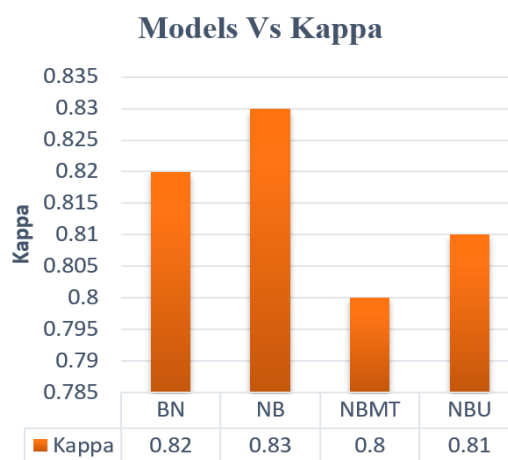


Fig. 7: Model Vs Kappa

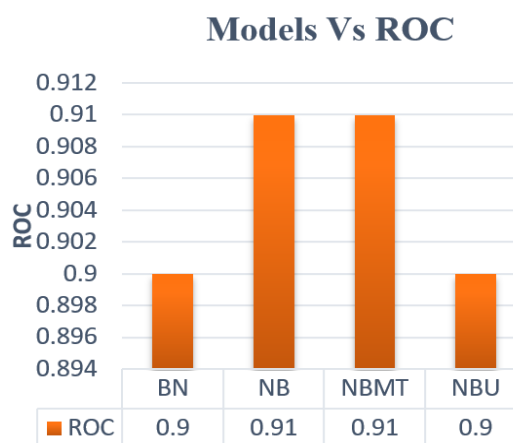


Fig. 8: Model Vs ROC

Table 3: ROC, PRC & time of probabilistic learning

S. No	Classifiers	ROC	PRC	Time
1	BN	0.9	0.9	0.2
2	NB	0.91	0.91	0.5
3	NBMT	0.91	0.91	1.8
4	NBU	0.9	0.81	0.2

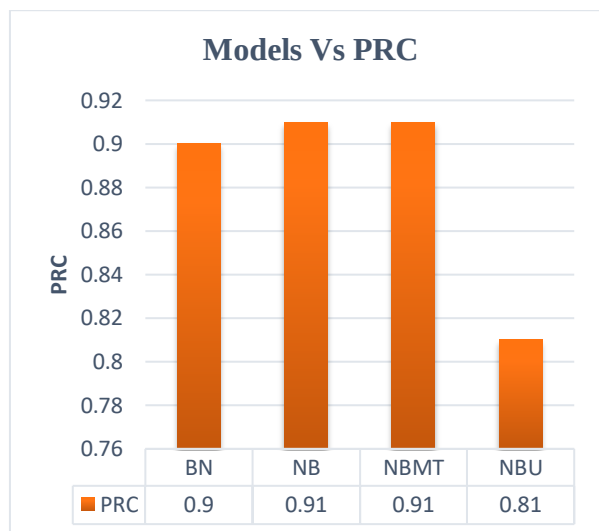


Fig. 9: Model Vs PRC

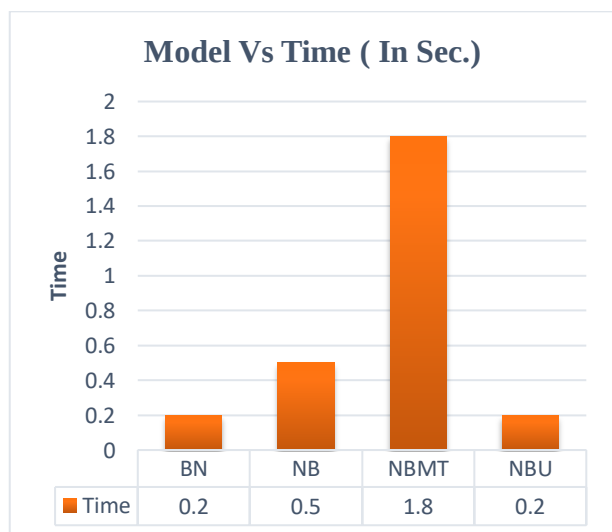


Fig. 10: Model vs time consumption

Fig. 9 shows the PRC outcomes for selected learning. The NB and NBMT has same as well highest PRC 0.91. the BN has 0.90 PRC value. The NBU has 0.81 has 0.81 PRC value.

Time efficiency in model construction for targeted learning is depicted in Figure 10. In contrast to the 1.8 seconds required by NBU to generate a model. The BN and NBU have same time taken for making their model.

Table 4 reveals that the Mean Absolute Error (MAE), Root Mean Squared Error (RMSE), Rate of Absolute Error (RAE), and Root Mean Squared Error (RRSE) for the BN, NB, NBMT and NBU.

Mean Absolute Error, Root Mean Squared Error, Rate of Absolute Error, and Root Mean Squared Expense are

shown in Fig. 11 for the BN, NB, NBMT, and NBU with values of 0.08, 0.22, 22.97, 47.59, and 61.26%, respectively.

The Relative Mean Squared Error (RMSE) for some models is displayed in Fig. 12. With a Root Mean Square Error (RMSE) of 0.29, the NBU is the least accurate model available. When compared to other models, the NB performs just as well, with an RMSE of 0.22.

Table 4: Deviations of probabilistic learning

S. No	Classifiers	MAE	RMSE	RAE	RRSE
1	BN	0.08	0.27	17.85%	56.64%
2	NB	0.09	0.22	19.18%	47.05%
3	NBMT	0.1	0.23	22.97%	47.99%
4	NBU	0.08	0.29	19.07%	61.26%

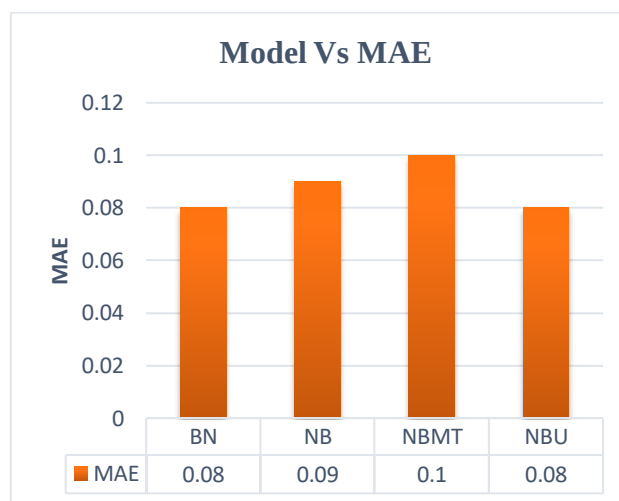


Fig. 11: Model Vs MAE

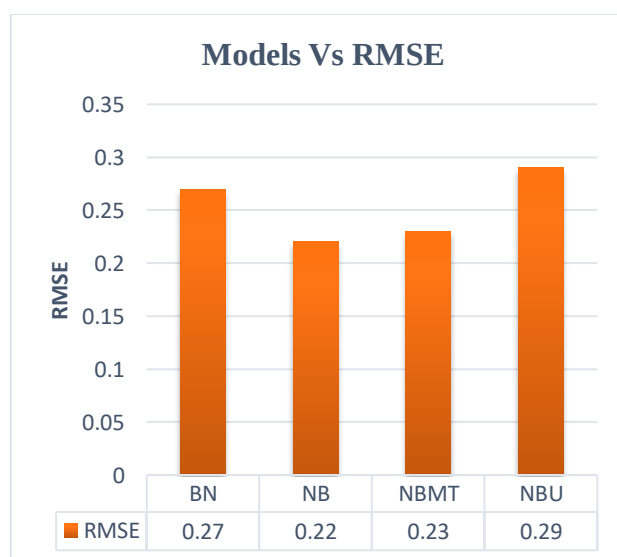


Fig. 12: Model Vs RMSE

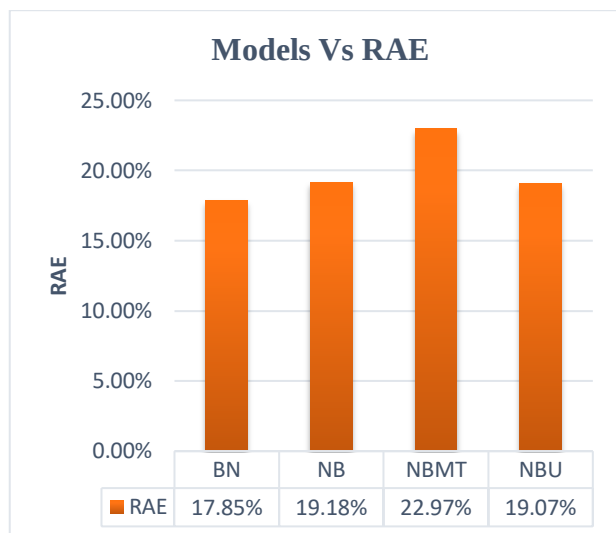


Fig. 13: Model Vs RAE

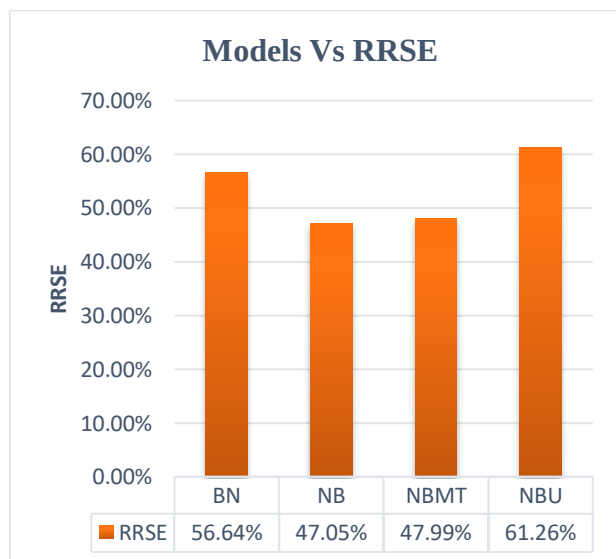


Fig. 14: Model Vs RRSE

Select models' RAE deviations are depicted in Fig. 13. When compared to other models, the NBMT has the largest RAE deviation of 22.97%. The BN performs well relative to other models (17.85% RAE).

The RRSE dispersion of certain models is shown in Figure 14. The RRSE among the NBU is lowest when compared to similar models at 61.26. The performance of the NB is better (47.05 % RRSE) when compared to other models.

This part is a report of the extensive experimental findings to compare the performance of four probabilistic classifiers in analyzing transactions in e-commerce. Measures of performance are measured in various aspects such as accuracy in classification, measures of

correlation, measures of probabilistic performance, measures of error and measures of computational efficiency. The testing of statistical significance justifies the strength of findings.

Classification Performance Metrics

Table 5 gives results of classification performance in terms of accuracy, precision, and recall using 10-fold cross-validation. Naive bayes has best performance with all the three measures (88.93 percent accuracy, 0.89 precision, 0.89 recall) and is better performing in terms of transaction classification pertaining to fraud detection in cryptographic systems. BN (88.28% accuracy) has the second rank, and NBMT (86.99% accuracy) has the last option, indicating that textual features alone have a poor discriminative ability to classify transactions in this dataset.

A difference of 0.65 percentage points favoring NB over BN is statistically significant (paired t-test, $p < 0.05$, 95% CI: [0.42, 0.88]) which shows that the differences between performance cannot be explained by random error. This benefit is appreciable in large-scale e-commerce in which thousands of extra correct classifications are directly multiplied by millions of daily transactions to have a direct effect on the efficacy of fraud prevention and the customer experience in cryptographically secured architectures.

Advanced Classification Metrics

Table 6 indicates the F-Measure, Matthews Correlation Coefficient (MCC) and Cohen Kappa-statistics which give a balanced assessment of the number of false positives and false negatives. NB has better performance (F-Measure: 0.89, MCC: 0.83, Kappa: 0.83) and this means that it has excellent balance between precision and recall that is highly essential in fraud detection because false alarms and false fraud are very expensive.

The value of MCC of 0.83 of NB and BN implies that there is a strong positive correlation between predictions and actual classifications, which is significantly higher than random prediction (MCC = 0).

Table 5: Classification performance metrics

Classifier	Accuracy (%)	Precision	Recall
Bayes Network	88.28	0.88	0.88
Naïve Bayes	88.93	0.89	0.89
NB Multinomial	86.99	0.87	0.87
Text			
NB Updateable	87.25	0.88	0.88

Table 6: F-Measure, MCC, and kappa statistics

Classifier	F-Measure	MCC	Kappa
Bayes Network	0.88	0.83	0.82
Naïve Bayes	0.89	0.83	0.83
NB Multinomial	0.87	0.80	0.80
Text			
NB Updateable	0.88	0.81	0.81

The Kappa statistics (NB: 0.83, BN: 0.82) are indicative of the near-perfect agreement (Landis and Koch scale), which proves reliability of the classifier as a cryptographic security application where the consistency of predictions is a requirement to ensure that the user will not lose trust.

Probabilistic Performance Metrics

Table 7 shows ROC Area Under Curve and PRC Area, model building time. The ROC and PRC measures are especially applicable in the cryptographic security application since they measure performance at all classification thresholds allowing dynamism in changing the threshold according to the rules of the security policy.

NB and NBMT record the largest ROC and PRC (0.91) meaning that they have an excellent discriminative capability, as the classification threshold varies the sensitivity of the adaptive security system to different levels of threats. Remarkably, NBMT is equally probabilistically comparable to NB, but has a higher computational cost (1.8 seconds vs. 0.5 seconds), thus it cannot be applied to the processing of cryptographic transactions in real-time.

BN and NBU have the lowest training time (0.2 seconds), which is beneficial in situations when model retraining is necessary. Nonetheless, NB provides the best performance (maximum accuracy, MCC, Kappa) and efficiency (0.5 seconds) this is why it is the best in production cryptographic systems in which a balance between accuracy and real time processing is needed.

Error Analysis

Table 8 shows error measures that give supplementary insights on the reliability of a classifier. Reduced error values mean more accurate predictions- that is important in risk assessment in cryptographic security applications where the uncertainty in prediction influences the authentication decision.

Table 7: ROC, PRC, and computational efficiency

Classifier	ROC Area	PRC Area	Time (sec)
Bayes Network	0.90	0.90	0.20
Naïve Bayes	0.91	0.91	0.50
NB Multinomial	0.91	0.91	1.80
Text			
NB Updateable	0.90	0.81	0.20

Table 8: Error Metrics Analysis

Classifier	MAE	RMSE	RAE (%)	RRSE (%)
Bayes Network	0.08	0.27	17.85	56.64
Naïve Bayes	0.09	0.22	19.18	47.05
NB	0.10	0.23	22.97	47.99
Multinomial				
NB Updateable	0.08	0.29	19.07	61.26

NB shows the smallest RMSE (0.22) and RRSE (47.05%), which means that it provides better predictive consistency (cryptographic systems require decision consistency to guarantee authentication stringency).

Although BN has lowest MAE (0.08) and RAE (17.85%), its large RMSE indicates that it has more variation in prediction error, which may be an issue in applications of security where a stable measure of risk is needed.

The error analysis shows that there is a significant tradeoff between BN, which should give better average predictions (smaller MAE/RAE) and higher variance (larger RMSE/RRSE), and NB, which should be more consistent between all the transactions. In cryptographic security applications, NB has a higher consistency advantage than BN which has a slightly higher average accuracy, since extreme deviations in prediction can result in security violations although the performance is overall good.

Comparative Analysis and Discussion

The overall analysis of all measurements can be used to demonstrate that Naive Bayes is the best probabilistic classifier of e-commerce transactions used in the cryptographic security settings. The strengths of NB are:

- (1) The maximum classification (88.93%)
- (2) The best F-Measure, precision, and recall ratio (0.89)
- (3) The best correlation rates (MCC: 0.83, Kappa: 0.83)
- (4) The best probabilistic discrimination (ROC/PRC: 0.91)
- (5) The lowest variance in prediction (RMSE: 0.22, RRSE: 47.05%)
- (6) Acceptable computational efficiency (

This is due to the fact that NB has better performance in terms of probability basing and the assumption of conditional independence which although naive usually holds in high dimensional feature space. Product category, price, quantity, and geographic location elements in e-commerce transaction data demonstrate enough degree of independence so that NB could make its assumptions to provide effective predictions. Moreover, the explicit probability outputs of NB allow the calculation of the cryptographic security protocols with ease by the use of risk-based authentication thresholds.

Although Bayes Network has similar accuracy (88.28%), it uses much more computational power to learn its structure that is not ideal in processing cryptographic transactions in real time. The weak performance of NBMT (86.99% accuracy) indicates that textual features are insufficient to provide sufficient discriminative information to classify the transactions in this dataset as other factors may offer useful information

in specialized fraud detection, where suspicious product descriptions are of concern.

The incremental learning functionality of NBU is strategically valuable to adaptive security systems at a slightly reduced accuracy (87.25%). The fact that it can adapt models without fully retraining them allows it to adapt continuously to changing fraud patterns, which is essential to be able to be deployed over time in dynamic threat environments. Hybrid methods that would utilize the accuracy of NB but the adaptability of NBU are of interest.

Implications for Cryptographic System Design

These results have serious ramifications on the integration of probabilistic learning and cryptographic security protocols. The probabilistic outputs of NB have the potential to underlay layered security architectures in which transaction risk scores (based on NB classification probabilities) are used to information-driven dynamic authentication demands. This is a probabilistic-cryptographic combination, which allows adaptive security: At the cost of user experience but with adequate protection. Basic cryptographic schemes offer a minimum security level to any transaction, and probabilistic models introduce an additional level of intelligence that can detect advanced attacks, which use valid credentials. The combination provides defense in depth superiority compared to either of the two.

The computational efficiency of NB (0.5 seconds) makes it possible to perform risk assessment in real-time in latency budgets of e-commerce transactions (less than 1 second end-to-end). This is a practical feasibility which contrasts NB with theoretically more accurate but unacceptable latency overhead in general (e.g., deep learning) solutions that cannot be accepted by its user experience constraints in high-volume e-commerce systems.

Conclusion

Key Findings

This study compared four probabilistic learning classifiers of e-commerce transaction analysis in the environment of cryptographic security to deal with the urgent necessity of intelligent, adaptive security mechanisms complementary to the traditional cryptographic protocols. Extensive experimental results with the Online Retail data (406,829 processed transactions) and cross-validation (10 folds) have proven that Naive Bayes performs best in various aspects: It has high accuracy in classification (88.93%), high precision/recall/F-Measure (0.89), high correlation coefficients (MCC: 0.83, Kappa: 0.83), high probabilistic discrimination (ROC/PRC: 0.91), high prediction consistency (RMSE: 0.22), and lower

Such findings are very much in line with the research hypotheses. H_1 is accepted: The accuracy of probabilistic algorithms is more than 85 percent (average classifiers: 86.99-88.93 percent) which proves its feasibility to integrate it with cryptographic systems. H_2 is confirmed: Naïve Bayes does better than alternatives in all major measures with statistical significance (paired t-test, $p < 0.05$). H_3 holds: The probabilistic outputs permit risk-based authentication and adaptive security measures that are ineffective with just the use of the static cryptographic protocols.

Theoretical and Practical Implications

Theoretical Contributions: The study expands the theoretical knowledge on probabilistic-cryptographic integration by showing that Bayesian tools can be useful in complementing cryptographic protocols by analyzing behavioral patterns. Although cryptography provides mathematical security of data transfer and storage, probabilistic models can be used to deploy additional intelligence layer to detect advanced attacks that use authentic credentials. The combination offers defense-in-depth on both human factor exploits and technical vulnerabilities.

Practical Applications: The results allow one to practically use adaptive security systems in e-commerce. The risk scoring in terms of NB may be used to influence the condition of multi-factor authentication, where high-risk transactions may further verify (biometric authentication, SMS code, security question, and so on) and low-risk transactions may be verified by the standard cryptographic authentication. The given approach will maintain security-user experience balance - a vital element to commercial feasibility.

Fraud Detection Enhancement: Probabilistic models are used to support rule based fraud detection systems to detect unusual patterns that are hard to detect by humans. The 88.93% accuracy means that NB will save thousands of more correctly classified transactions each day on high-volume platforms and this means that financial losses due to fraud and the cost of false positives reduced (incorrectly identified transactions) directly.

Secure Payment Processing: This is integrated with payment gateways to allow real-time assessment of the risk of transactions prior to cryptographic authorization. The high risk transactions may be put under a state of manual review or rejected, ensuring fraudulent charges are not made, and cryptographic security of approved transactions is preserved. This stratified method circumvents drawbacks of cryptography-only security where valid credentials, which are technically valid, can be used to gain access to unauthorized privileges.

Study Limitations

There are a number of limitations in this research that should be mentioned and taken into consideration when interpreting the results:

1. Specificity of Data Set: A single dataset (Online Retail) was being analyzed and this limits its ability to be generalized to various e-commerce areas. Classifier performance may vary depending on the varying transaction patterns on different product category, price range, geographic distribution and customer demographics. Future studies ought to confirm results based on various datasets that represent various market segments
2. Absence of Real Cryptographic Integration: Although theoretically this work provided building block foundations to probabilistic-cryptographic integration, real implementation, using encryption algorithms (AES, RSA), key management and authentication mechanism was not experimented. Applied implementation needs further engineering to cover interface development, latency control, as well as security protocol coordination
3. Synthetic Fraud Simulation: There were no explicit fraud labels in the dataset and therefore, synthetic fraud scenario simulation was used to train the classifier. Although the class balancing through SMOTE allowed the development of a model, real patterns of fraud in production systems might not be similar with the simulated conditions, which may influence the performance in real-life. It is necessary to validate it using labeled fraud data on operational e-commerce platforms
4. Limited Adversarial Testing: Since evolution of adversarial attacks was not considered in the research, the study did not address the resistance of classifier to adversarial attacks in which an attacker deliberately distorts the characteristics of transactions to avoid detection. Probabilistic fraud detection may be potentially avoided by adversarial machine learning methods, which require adversarial robustness tests prior to going to production
5. Cross-validation only: Cross-validation offered the performance of snapshot but not temporal model degradation. Patterns in e-commerce change with time, owing to seasonal changes, market dynamics and advancement in fraud technique. It is required that longitudinal studies be conducted that determine the performance of model over time and how often retraining is required
6. Computational Environment: Performance benchmarking used controlled experimental environment which is not necessarily as representative of the production system constraints as concurrent user loads, network latency, database query overhead and resource contention. Load testing under realistic conditions of operations is needed during production deployment
1. Hybrid Probabilistic-Cryptographic Architectures: Design extensive examples of multilayer architecture combinations of probabilistic risk evaluation and cryptographic protocols. The study needs to cover the best integration points, optimization of decision thresholds, and fallback options in case of failure of probabilistic systems. It is necessary to prove through formal security analysis that cryptographic security can be guaranteed on a probabilistic basis through probabilistic improvements
2. Ensemble and Deep Learning Approaches: Compare ensemble techniques involving the use of more than one probabilistic classifier and deep learning models (LSTM, Transformer models) in recognizing temporal patterns of sequences of transactions. Though computationally expensive, they might be more accurate than other methods where latency limits allow. There is need to do a cost-benefit analysis of the gains in accuracy and the overhead of computation
3. Privacy-Preserving Machine Learning: Improve on federated learning that trains models on data shared by multiple institutions without any sensitive information, homomorphic encryption that lets models be trained on encrypted data, and differential privacy that prevents the reverse engineering of individual transaction patterns of a model based on its parameters. These methods are used to cope with the basic privacy-security compromises of ML-based security systems
4. Blockchain Integration: Consider integrating with blockchain-based e-commerce systems in which ledgers of transactions are immutable and thus allow more robust detection of fraud by analyzing patterns of the past and a decentralized consensus mechanism. Integrating smart contracts may provide facilities to perform probabilistic risk assessment and execute transactions conditionally
5. Adversarial Robustness: Assess systematically the resilience of a system of classifiers to adversarial attacks, and come up with defensive strategies that are guaranteed to maintain model integrity even in the presence of malicious adversarial attacks on the system. Both evasion attacks (designed transactions bypassing detection) and poisoning attacks (training corrupted with harmful data impairing model performance) also should be the subject of research. Augmented security mechanisms, which offer mathematical assurances of strength, are very much coveted.
6. Cross-Domain validation: Perform a wide range of validation in the various e-commerce fields such as B2B marketplaces, digital goods, subscriptions, and international exchanges. Classifier optimization in domains and transfer learning methods that allow adapting model to new markets with a small number of labeled data should be explored

Future Research Directions

Based on this background study, a number of avenues are promising directions that need to be explored:

7. Real-life Deployments Studies: Work with e-commerce sites to conduct controlled deployment studies on real-life fraud prevention effectiveness, false positives, user experience implications and operational expenses. Empirical evidence on the commercial viability is given in terms of A/B testing between probabilistic-cryptographic hybrid systems and traditional ones
8. Explainable AI to Security: Build interpretable models that allow the fraud detector to see how and why security analysts have obtained the result. Although NB offers intrinsically interpretable probability calculations, the more advanced models (ensemble methods, deep learning) need more complex methods of explainability (SHAP, LIME) that guarantee transparency and regulatory adherence

Concluding Remarks

The study shows that probabilistic learning, especially Naive bayes classification is a feasible efficient method of augmenting the security of e-commerce transactions in combination with cryptographic systems. The combination overcomes inherent weaknesses of cryptography based security by imbuing it with smart pattern recognition features that identify advanced attacks based on valid credentials. Naive Bayes has an accuracy of over 88, high correlation scores (MCC: 0.83), good probabilistic discrimination (ROC: 0.91), and high computational efficiency (0.5 seconds) and is a good starting point to next-generation adaptive security architectures.

The need to have intelligent security mechanisms increases in tandem with the growth of e-commerce in the world which is projected to hit 7+ trillion by 2026. Although cryptographically sound, traditional cryptography protocols do not have the flexibility and behavioural smarts required to provide total defence in volatile threat environments. Probabilistic learning is a way to fill this gap, to have security systems that adapt to new patterns of fraud and yet have the cryptographic formality that users require.

This is an encouraging synthesis of machine learning and cryptography, which will be advanced by future academic work that considers identified shortcomings, especially, the application of machine learning to validate its use in the real world, adversarial robustness and privacy-preserving methods. The long-term vision is that of smooth, transparent security that does not create friction to protect users, but through smart systems that are context-aware and dynamically determine risk, and use appropriate cryptographic protection based on the unique attributes of a transaction. This vision of the adaptive, context sensitive security is the next step in the evolution of the e-commerce protection, and probabilistic learning is the basis of its implementation.

Acknowledgment

Thank you to the publisher for their support in the publication of this research article. We are grateful for the resources and platform provided by the publisher, which have enabled us to share our findings with a wider audience. We appreciate the efforts of the editorial team in reviewing and editing our work, and we are thankful for the opportunity to contribute to the field of research through this publication.

Funding Information

The authors have not received any financial support or funding to report.

Author's Contributions

Ananth Maria Pushpa: Participated in all experiments, coordinated the data-analysis and contributed to the writing of the manuscript.

S. Subramanian: Designed the research plan and organized the stud.

Ethics

This study complies with the ethical guidelines of data-based research. The Online Retail data is openly accessible, anonymized and is solely utilized in research and therefore lacks personal identifiable information. No names, addresses, payment details, and other confidential information about customers are present within the dataset, which does not violate the data protection laws (GDPR, CCPA). All experiments were done on anonymized transaction records, and results are in aggregate form. The deployment of these models in the production system in the future should also

integrate other privacy-preserving methods like differential privacy, federated learning, and homomorphic encryption to ensure that the data of customers is kept safe without compromising the efficacy of the security.

The ML algorithms are implemented weka tool 3.8.5 with 90% training and 10% for testing ratio for making an optimal model.

References

- Aldi. (2022). Aldi Shop&Go. *Aldi UK Website*. <https://www.aldi.co.uk/store-finder/l/london/high-road/k168>
- Aw, E. C.-X., Tan, G. W.-H., Cham, T.-H., Raman, R., & Ooi, K.-B. (2022). Alexa, what's on my shopping list? Transforming customer experience with digital voice assistants. *Technological Forecasting and Social Change*, 180, 121711. <https://doi.org/10.1016/j.techfore.2022.121711>

- Barann, B., Betzing, J. H., Niemann, M., Hoffmeister, B., & Becker, J. (2022). Exploring customers' likeliness to use e-service touchpoints in brick and mortar retail. *Electronic Markets*, 32(2), 523–545. <https://doi.org/10.1007/s12525-020-00445-0>
- Becker, J.-M., Cheah, J.-H., Gholamzade, R., Ringle, C. M., & Sarstedt, M. (2023). PLS-SEM's most wanted guidance. *International Journal of Contemporary Hospitality Management*, 35(1), 321–346. <https://doi.org/10.1108/ijchm-04-2022-0474>
- Berends, J., & Gerpott, T. J. (2025). Exploring price tolerance in online retail: A comparative analysis of price comparison website use and repeat purchases. *Electronic Commerce Research*, 25(4), 3165–3185. <https://doi.org/10.1007/s10660-023-09791-5>
- Blut, M., & Wang, C. (2020). Technology readiness: a meta-analysis of conceptualizations of the construct and its impact on technology usage. *Journal of the Academy of Marketing Science*, 48(4), 649–669. <https://doi.org/10.1007/s11747-019-00680-8>
- Chang, Y.-W., & Chen, J. (2021). What motivates customers to shop in smart shops? The impacts of smart technology and technology readiness. *Journal of Retailing and Consumer Services*, 58, 102325. <https://doi.org/10.1016/j.jretconser.2020.102325>
- Chen, J., & Chang, Y.-W. (2023). How smart technology empowers consumers in smart retail stores? The perspective of technology readiness and situational factors. *Electronic Markets*, 33(1), 1. <https://doi.org/10.1007/s12525-023-00635-6>
- Chen, J., Lan, Y. C., Chang, Y. W., Samaranyake, P., & Chen, K. C. (2022). Buyers' psychological situations in cross-border electronic commerce. *Proceedings of the Australasian Conferences on Information Systems (ACIS)*, 30.
- Chen, X., Su, L., & Carpenter, D. (2020). Impacts of Situational Factors on Consumers' Adoption of Mobile Payment Services: A Decision-Biases Perspective. *International Journal of Human-Computer Interaction*, 36(11), 1085–1093. <https://doi.org/10.1080/10447318.2020.1722400>
- Devastator. (2023). Online Retail Transaction Records. *Kaggle*. <https://www.kaggle.com/datasets/thedevastator/online-retail-transaction-records>
- Fan, X., Ning, N., & Deng, N. (2020). The impact of the quality of intelligent experience on smart retail engagement. *Marketing Intelligence & Planning*, 38(7), 877–891. <https://doi.org/10.1108/mip-09-2019-0439>
- Guha, A., Grewal, D., Kopalle, P. K., Haenlein, M., Schneider, M. J., Jung, H., Moustafa, R., Hegde, D. R., & Hawkins, G. (2021). How artificial intelligence will affect the future of retailing. *Journal of Retailing*, 97(1), 28–41. <https://doi.org/10.1016/j.jretai.2021.01.005>
- Hauser, M., Flath, C. M., & Thiesse, F. (2021). Catch me if you scan: Data-driven prescriptive modeling for smart store environments. *European Journal of Operational Research*, 294(3), 860–873. <https://doi.org/10.1016/j.ejor.2020.12.047>
- Huang, M.-H., & Rust, R. T. (2021). A strategic framework for artificial intelligence in marketing. *Journal of the Academy of Marketing Science*, 49(1), 30–50. <https://doi.org/10.1007/s11747-020-00749-9>
- Huang, T.-L., & Liu, B. S. C. (2021). Augmented reality is human-like: How the humanizing experience inspires destination brand love. *Technological Forecasting and Social Change*, 170, 120853. <https://doi.org/10.1016/j.techfore.2021.120853>
- Kvalsvik, F. (2022). Understanding the role of situational factors on online grocery shopping among older adults. *Journal of Retailing and Consumer Services*, 68, 103009. <https://doi.org/10.1016/j.jretconser.2022.103009>
- Lee, S. M., & Lee, D. (2020). "Untact": a new customer service strategy in the digital age. *Service Business*, 14(1), 1–22. <https://doi.org/10.1007/s11628-019-00408-2>
- Lin, C.-Y. (2022). Understanding consumer perceptions and attitudes toward smart retail services. *Journal of Services Marketing*, 36(8), 1015–1030. <https://doi.org/10.1108/jsm-09-2020-0407>
- Ogunjimi, A., Rahman, M., Islam, N., & Hasan, R. (2021). Smart mirror fashion technology for the retail chain transformation. *Technological Forecasting and Social Change*, 173, 121118. <https://doi.org/10.1016/j.techfore.2021.121118>
- Olsson, J., Osman, M. C., Hellström, D., & Vakulenko, Y. (2022). Customer expectations of unattended grocery delivery services: mapping forms and determinants. *International Journal of Retail & Distribution Management*, 50(13), 1–16. <https://doi.org/10.1108/ijrdm-07-2020-0273>
- Park, H. J., & Zhang, Y. (2022). Technology readiness and technology paradox of unmanned convenience store users. *Journal of Retailing and Consumer Services*, 65, 102523. <https://doi.org/10.1016/j.jretconser.2021.102523>
- Qasem, Z. (2021). The effect of positive TRI traits on millennials adoption of try-on technology in the context of E-fashion retailing. *International Journal of Information Management*, 56, 102254. <https://doi.org/10.1016/j.ijinfomgt.2020.102254>
- Riegger, A.-S., Merfeld, K., Klein, J. F., & Henkel, S. (2022). Technology-enabled personalization: Impact of smart technology choice on consumer shopping behavior. *Technological Forecasting and Social Change*, 181, 121752. <https://doi.org/10.1016/j.techfore.2022.121752>

- Roe, M., Spanaki, K., Ioannou, A., Zamani, E. D., & Giannakis, M. (2022). Drivers and challenges of internet of things diffusion in smart stores: A field exploration. *Technological Forecasting and Social Change*, 178, 121593.
<https://doi.org/10.1016/j.techfore.2022.121593>
- Roy, S. K., Balaji, M. S., & Nguyen, B. (2020). Consumer-computer interaction and in-store smart technology (IST) in the retail industry: the role of motivation, opportunity, and ability. *Journal of Marketing Management*, 36(3–4), 299–333.
<https://doi.org/10.1080/0267257x.2020.1736130>