PAPER • **OPEN ACCESS**

Weighted naïve bayes multi-user classification for adaptive authentication

Journal of Physics Communications

OPEN ACCESS

RECEIVED
29 May 2024

REVISED
10 October 2024

ACCEPTED FOR PUBLICATION
22 October 2024

PUBLISHED
1 November 2024

PAPER

Weighted naïve bayes multi-user classification for adaptive authentication

Prudence M Mavhemwa[1,*], **Marco Zennaro**[2], **Philibert Nsengiyumva**[3] **and Frederic Nzanywayingoma**[4]

[1] African Centre of Excellence in Internet of Things, University of Rwanda, Kigali, Rwanda
[2] Science, Technology, and Innovation Unit, ICTP, Trieste, Italy
[3] Department of Electrical and Electronic Engineering, University of Rwanda, Kigali, Rwanda
[4] Department of Information Systems, University of Rwanda, Kigali, Rwanda
[*] Author to whom any correspondence should be addressed.

E-mail: pmavhemwa@gmail.com, mzennaro@ictp.it, nsenga_philibert@yahoo.com and f.nzanywayingoma@ur.ac.rw

Keywords: adaptive-authentication, multi-user classification, naive bayes, risk-calculation, security, weighted

Abstract

Machine learning classification algorithms have been extensively utilized in addressing user authentication challenges. Nonetheless, a majority of solutions categorize users into three classes, whereas adaptive authentication scenarios necessitate classification beyond this threshold. The rationale behind this limitation has not been thoroughly explored. The current study leveraged the Naive Bayes theorem for user authentication endeavors to assess the risk associated with login attempts. The Naive Bayes Machine Learning algorithm, along with its variations such as Gaussian, Categorical, and Bernoulli, was applied on both weighted and unweighted datasets to ascertain risk levels and categorize them into six classes. Additionally, the classification task was executed using alternative algorithms. The outcomes of cross-validation and comparative analyses revealed that the performance was commendable for up to three classes, after which a decrease was observed in certain Naive Bayes and SVM classifiers. Among the Naïve Bayes family, the Bernoulli NB algorithm exhibited superior performance but was surpassed by Decision Trees, SVM, XGB, and Random Forests. Notably, the weighted dataset consistently outperformed the unweighted counterpart, with the allocation of weights significantly influencing algorithmic efficacy. The 80:20 split strategy yielded the most favorable outcomes in contrast to the 70:30 and 60:40 splits, albeit no significant variances were detected during cross-validation. Non-Naïve Bayes algorithms demonstrated superior performance compared to Naïve Bayes algorithms. For Naïve Bayes, optimal performance is achieved with three classes, highlighting its utility in conditional risk calculation, while non-Naïve Bayes multi-classification algorithms are more suitable for classification tasks due to the problem's inherent compatibility with conditional probabilities. In conclusion, it is imperative to acknowledge that the characteristics of the data, the use of weights, and the data splitting methodology significantly influence the accuracy of machine learning algorithms in multi-class user classification.

1. Introduction

The Internet of Medical Things (IoMT) has profoundly reshaped the medical sector by facilitating remote resource access and enabling seamless online interaction between healthcare providers and patients. The global health crisis caused by the COVID-19 pandemic has expedited the implementation of intelligent health technologies such as cloud computing, big data, and machine learning [1]. The Internet of Things (IoT) plays a pivotal role in revolutionising healthcare by offering various advantages [2, 3]. These emerging computational frameworks are intricately woven into all aspects of human existence, underscoring the critical need for robust security measures [4]. Ensuring security is paramount in mitigating unauthorised access and the potential misuse of sensitive data exchanged between patients and healthcare professionals. Thorough research focusing

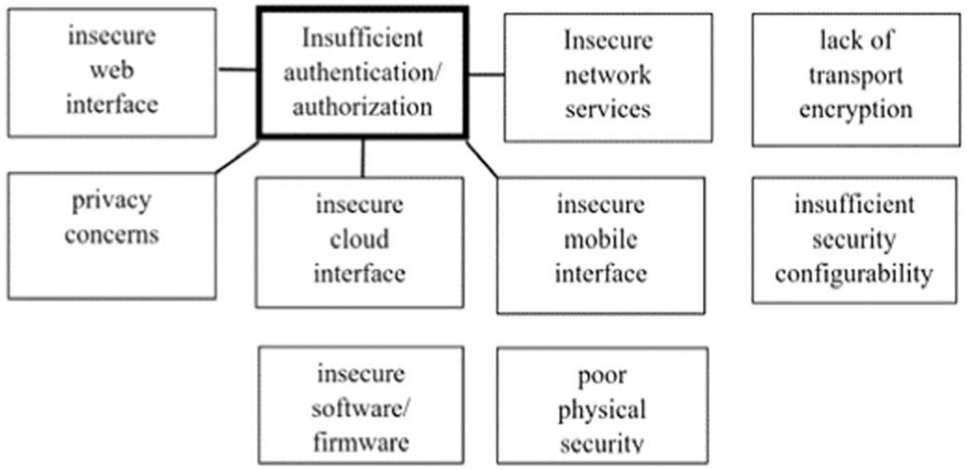

insecure web interface
Insufficient authentication/ authorization
Insecure network services
lack of transport encryption
privacy concerns
insecure cloud interface
insecure mobile interface
insufficient security configurability
insecure software/ firmware
poor physical security

Figure 1. Top Ten IoT vulnerabilities. Reproduced with permission from [5]. CC BY-NC 4.0.

on the usability and security of user authentication is imperative to ensure that IoT devices are designed with user-centric principles. The examination ought to pinpoint prevalent vulnerabilities in IoT systems, as detailed in the work by [5] and visually depicted in figure 1.

The highlighted vulnerability is linked to other vulnerabilities, as illustrated in the figure. Most IoT devices encounter numerous security challenges [6, 7] and many IoMT devices lack the required security [8, 9]. However, developing secure authentication protocols is challenging owing to device limitations that limit their ability to perform complex computations, diverse IoMT devices made using different platforms and protocols, their decentralised nature, which makes them vulnerable to exploitation [1] and the distinct threat landscape and malicious intentions prevalent in IoMT environments compared to traditional IoT devices [4, 10–13]. Authentication methods differ across devices, often utilizing a uniform approach, notwithstanding the more effective strategy of tailoring treatment to individual users based on their level of risk. The integration of Riskscore could improve the user experience during authentication by imposing greater challenges on suspicious users while easing the process for less suspicious ones. This, in turn, supports compliance with the IoMT, enhancing overall health and well-being, and contributing to the achievement of Goal 3 outlined in the Sustainable Development Goals (SDG3) aimed at ensuring universal access to healthcare [14]. Various techniques have been amalgamated with machine learning for authentication purposes which leverage techniques such as multi-factor authentication, implicit authentication, and behavioral biometrics, to enhance security and usability in shared environments. However, challenges remain in balancing security with user experience, particularly in dynamic environments where future research may focus on refining these models to enhance adaptability and robustness against emerging threats.

According to [15–17], there are several limitations in problem classification, primarily due to issues like imbalanced data, computational constraints, and inadequate training data where addressing these challenges is crucial for enhancing the effectiveness of ML applications. On the other hand, although these constraints provide difficulties, they also provide room for creativity in machine learning techniques, promoting the investigation of hybrid strategies and cutting-edge algorithms to improve classification precision. Therefore, it is recommended to conduct controlled experiments to determine the most suitable algorithm. Furthermore, the assessment of classification and predictive modelling algorithms predominantly hinges on their outcomes and typically falls into either binary or multi-class categories.

1.1. Main contributions

Previous studies used binary classifiers to categorize users as valid or illegitimate using standard NB, ensuring individuals face the same level of verification difficulty. Our proposed method is part of ongoing work that aims to authenticate users based on their actual risk scores by decoupling user classification. Considering the aforementioned, we plan to develop a hybrid algorithm that incorporates feature and contextual weights in the Naive Bayes algorithm to cater for the conditional independence bias in login risk calculation. The novelty of our work is on incorporating the weighted features in the risk probability calculation where the deviation from the known context will increase the risk score. We plan to go beyond binary classification as a way of ensuring authentication based on risk score for improved usability of the authentication process. Risk scores will be categorised into several classes. We will compare our weighted scheme with other classification models

Table 1. Our proposed work against previous work.

Item	Previous work	Our proposed work
Usable-Security	The cybersecurity industry regards usability as a trade-off on security rather than as a security enhancing component [18–20]. Works by [18] acknowledge that bridging the usability/security gap has not been satisfactory and offer a theoretical and practical perspective that they assume will hold in the cybersecurity domain.	We propose to use Risk score to enhance the usability of the authentication process by increasing the burden on more suspicious users and decreasing it on less suspicious ones. Our work is part of ongoing authentication research that seeks to address some of the issues identified in [1] which include adjustability, re-authentication and user-friendly authentication.
Adaptive authentication	Current authentication techniques impose what users must use [21].	We aim to enable adaptive user authentication by assigning suitable authenticators based on Risk score and user profile.
Applying Machine learning on classification problems	There are several limitations in ML classification problems where addressing these challenges is crucial for enhancing the effectiveness of ML applications[15–17].	We carry out controlled tests to find the optimal algorithm.
Naïve Bayes accuracy	General Naïve Bayes approach has been found to perform poorly and is less accurate when attribute independence is violated [22–25].	We introduce attribute and context weighting where we assign weights to predictors in riskscore calculation for authentication.
Weighted Naïve Bayes accuracy	Research shows that the feature weighting approach outperforms standard NB in many of the examined datasets[26, 27].	We propose to show how w_i affects the final risk score testing different weights.
Multi-class classification	Previous studies used binary classifiers to categorize users as valid or illegitimate, ensuring individuals face the same level of verification difficulty.	The proposed method aims to decouple user classification extending up to six classes.

observing model behaviours as more classes are added. The summary of previous work and our proposed work is as shown in table 1 below.

1.2. Structure of paper

This paper presents related work in section 2, introduces the proposed architecture and research method in section 3, and presents the results in section 4. Discussion of research findings is in section 5. Section 6 concludes and gives future work.

2. Related work

2.1. Naïve Bayes algorithm

The Naive Bayes (NB) conditional probability theory has been extensively utilised in the realm of classification tasks, yet its assumption of conditional independence hinders its competitiveness in comparison to alternative algorithms. This theory, as delineated in [28], encompasses a set of classification algorithms based on Bayes theorem, aimed at categorising data into distinct groups under the presumption of predictor independence, irrespective of their quantity [29]. According to the theory, each predictor is posited to independently and conditionally influence the outcome for a particular class [8]. Nevertheless, this methodology has demonstrated inefficacy and reduced accuracy in cases where attribute interdependence is breached [22]. Author [29] provides an analysis of the advantages and disadvantages of Naive Bayes with notable challenges according [22] as including the learner's inability to obtain potential hidden forms from the data and reduced efficiency when the NB is applied without without considering feature dependency.

2.1.1. Types of Naïve Bayes classifiers

The Python sci-kit learn library offers various classifiers, including multiple options below [30]:

1. Multinomial Naïve Bayes: The system operates on multinomially distributed categorized data. Documents are categorized into foreign news, sports, politics, and religion. It arranges texts based on how frequently certain terms are used as characteristics.
2. Bernoulli Naïve Bayes: One of the most widely used models, it functions similarly to a multinomial classifier and uses Boolean variables with a 'Yes' or 'No' value as its predictors. Its main purpose is document classification.
3. Gaussian Naïve Bayes: The model assumes continuous data, rather than discrete values, which are samples from the Gaussian distribution, based on the normal distribution.
4. Complement Naïve Bayes: This Multinomial NB modification is designed to handle imbalanced data by determining model weights based on the complement of each class.
5. Categorical Naïve Bayes: This works best when the features are categorically distributed.
6. Weighted Naïve Bayes: The method employs domain-based weights to assign varying weights to different attributes based on their prediction ability, based on expert knowledge [27].

Author [31] proposed a method to improve attribute weighting for Naive Bayes text classifiers using the improved distance correlation coefficient. Their model incorporated deep attribute weighting by combining measurement of inverse document frequency and distance correlation coefficient, demonstrating that their attribute weighting method achieves an effective balance between classification accuracy and execution time. Their work, however, did not address multi-class classification. In [32] researchers proposed a universal Domain Adaptation (UniDA) method called Adaptive Unknown Authentication by Classifier Paradox (UACP) to adaptively identify target unknowns based on paradoxical predictions. A composite classifier was jointly designed with two types of predictors: a multi-class and a binary predictor. A weight adaptive multi-factor authorization technology to enhance network security is described in [33]. In their work, two adaptive weight algorithms were designed to meet more precise authority control in complex network security scenarios and through construction and testing of the actual prototype system, the utility and advantages of multi-factor and weight adaptation in authorization were verified. Their work, however, mainly focused on multi-factor authentication. A weighted Naive Bayes classification algorithm with an Adaptive Genetic algorithm (AGA_WNB) to improve image classification accuracy using initial weights of features as the initial population and adjusted crossover and mutation probabilities based on fitness functions to optimise classification accuracy was proposed in [34]. Results showed that (AGA_WNB) outperformed other models, but their work, however, did not address multi-class classification. An adaptive multi-factor authentication system that selected multiple authentication modalities based on trustworthiness values in different environments, employing a multi-user permission strategy to dynamically select approvers based on the sensitivity of the requested information and the user's work environment, was proposed in [35]. Their work mainly focused on authentication in general. A feature weighting-based Naive Bayesian microblog user classifying method to distinguish between normal microblog and malicious microblogs users was proposed in [36], where the prior probability, the conditional probability, and the information gain of each feature were calculated. Their classification, however, was binary. [37] introduced an adaptive user authentication system that verifies user identity using different authentication steps based on a risk score. The adaptive user authentication system implemented a sequence of authentication steps based on a risk score to verify user identity. They did not address multi-class classification. An adaptively evidential weighted classifier combination method using basic probability assignment (BPA) modelling was proposed in [38]. They determined weights for individual classifiers based on the uncertainty degree of the corresponding BPA measured by belief entropy. Their work illustrated the effectiveness of the proposed weighted combination method through numerical experimental results.

2.2. Feature-based classification and prediction

Authors [27] highlighted that not all medical symptoms are equally effective in predicting a specific disease and introduced the Weighted Naive Bayes Classifier (WNBC) framework, which assigns different weights to attributes based on their predictive abilities, consulted with domain experts. Their experiment shows that the weighted Naïve Bayes method outperforms the Naïve Bayes method. Author [28] utilised contextual factors such as money, location, MAC address, and successful attempts to identify fraudulent activities in their Naive Bayes-based mobile banking security system. Their algorithm accurately identified the behaviour of a new transaction and classified it as either normal or unusual. In [39], Naive Bayes and Mean of Horner's Rule were used to classify users based on their keystroke dynamics, discovering that this method yielded more precise outcomes than Naïve Bayes alone. In [40] the Naive Bayes classifier was used to estimate the likelihood of a digital identity characteristic being real based on the reliability of the sources used. They utilised various digital identifying sources, such as phone numbers, email addresses, first and last names, addresses, and account numbers, and demonstrated that the Naive Bayes theorem effectively predicts the reliability of an identity source. In [41] certainty factors and the Naive Bayes classifier were used to develop an expert system that could classify stroke illnesses with 96% accuracy. A 76% accuracy rate in user face detection for an attendance system using the Naïve Bayes algorithm was achieved in [42] but background light impacted their prototype's accuracy. Because different qualities have different levels of relevance, [43] proposed an Attribute and Instance Weighted Naive Bayes (AIWNB) that blends attribute and instance weighting. They estimated the weights directly using training data. The same authors in [44] proposed an attribute-weighted, fine-tuned NB model, emphasizing the importance of accurate conditional probability estimates and eliminating the implausible attribute conditional independence assumption. For multi-class classification [45] conducted a comparative study of different classification algorithms on early diagnosis of heart diseases and could only classify data into three categories: ”Normal,” ”Suspect,” and ”Pathological”. Based on these findings, they concluded that Random Forests had the best accuracy and F-Score. A similar experiment in [46] on breast cancer and iris datasets found that Random Forest algorithm outperformed Decision Tree in binary-class classification, with CTree outperforming in multi class classification. Their research underscored the importance of considering dataset characteristics and training-testing partitions in model evaluation for a specific task. Using Browser fingerprints [47], attempted to solve the adaptive authentication problem employing Bayes theory and weighting observing that weighting improves the accuracy of their algorithm. Authors [26] argue that despite numerous studies examining Naive Bayes' robustness, no one has proven a necessary and sufficient condition for its behavior. They contend that while conditional independence is a prerequisite for maximum performance, it is not sufficient. This review highlighted the potential for other researchers to utilize the Naive Bayes technique so in the next section we will look at the research methods.

3. Research methods

This section delineates the proposed methodology, data aggregation, preprocessing, sampling, and construction of machine learning models, encompassing the proposed user classification technique based on Naive Bayes. The probability of a login attempt being illegitimate is computed considering various contextual data, and the selection of Naive Bayes was predicated on the conditional aspect of the issue and its expeditious problem-solving capabilities in classification. The Bayes theorem is shown below

Table 2. Contextual Factors and their weights.

Contextual factor	Weight
Mobile Device	3
Other Device	1
Network	2
Location	3
Habit	1
Total	10

$$P(c|a) = \frac{P(a|c) \cdot P(c)}{P(a)}, \tag{1}$$

where 'c' represents a class, 'a' represents attributes, $P(c|a)$ is the posterior probability, P(a) is the prior probability, P(c) is the prior probability of the class and $P(a|c)$ is the probability of the predictor based on the class. The weighted NB introduced to overcome the conditional independence bias is represented as equation (2)

$$P(Y = y|X = x) = \hat{P}(Y = y) \prod_{i=1}^{n} \hat{P}(X = x_i|Y = y)^{w_i}, \tag{2}$$

with w_i denoting each feature weight. Since we believe contextual factors influence the final risk likelihood, we want to show how w_i affects the final risk score. Since research shows that the feature weighting approach outperforms standard NB in many of the examined datasets [26, 27], we need to see how the weighting in equation (2) affects user classification beyond binary. We conducted a comparative analysis between several variations of Naive Bayes and alternative multi-class classification approaches to assess its efficacy. To mitigate inherent biases in traditional Naive Bayes, we allocated weights to our contextual variables informed by scholarly works [27, 43] and domain expertise. These weights serve as coefficients for contextual factors, which were then multiplied based on the deviation of a feature from known values. The weights, displayed in table 2, along with a 10-point scale, would subsequently undergo normalisation to a range between 0 and 1.

The following example demonstrates how each contextual factor's contribution would be calculated. It is assumed that there is a one-to-one mapping between a user and a mobile device; hence a user is associated with one mobile device. Also, GPS or cell data provides location information for the user and the mobile device, along with the network that connects their device. As a result, if only for instance, the device changes, the probability of the user being illegitimate based on weight only is $3/10 = 0.3$ and if location also changes, contribution becomes $3/10 + 3/10 = 6/10 = 0.6$. The full weighted classifier now consists of weighted data assigned to each pair of {attribute, value} giving each tuple a set $\{a_i, v_i, w_i\}$ where an attribute a_i has a value v_i and a weight w_i where $1 <= wi <= 10$, for instance, for Mobile Device Change context which has Operating System and Browser as attributes is expressed as follows:

$$\{a_i, v_i, w_i\} = \{\text{Mobile Operating System, Android, } 1.5\} \tag{3}$$

$$\{a_i, v_i, w_i\} = \{\text{Mobile Browser, Opera, } 1.5\} \tag{4}$$

$$\Rightarrow \{a_i, v_i, w_i\} = \{\text{Mobile Device Change, Yes, } 3\} \tag{5}$$

The proposed solution was tested on a Windows 11 computer with an Intel Core i7@1.30 GHz processor and 16 GB RAM using Python 3.10.9 and Jupyter 6.5.2. Synthesised data was merged from various sources including Datasets [48–50] due to the scarcity of datasets related to adaptive authentication. Following equation (2) our work employed the chain rule derived from [50] which can be expressed as equation (6):

$$P(A_1, A_2, \ldots, A_n) = P(A_1)P(A_2|A_1)P(A_3|A_1, A_2)\ldots P(A_n|A_1, A_2, \ldots, A_{n-1}) \tag{6}$$

In equation (6), we have the formula for the joint probability of events $A_1, A_2, \ldots, A_n$. where our predictors were Mobile Device, Other Device, Location Change, Network Change, and Habit Change with a change in any of these weighted predictors affecting the risk probability. The risk score or probability, is the dependent variable, as depicted in figure 2.

We used feature weightings to apply several Naive Bayes variants based on the dataset, and we compared the outcomes with other multi-class classification techniques.

3.1. Data collection

We used synthesised data, as previously described, which included 15 features with 3,000 records. The description of the data is in table 3 below.

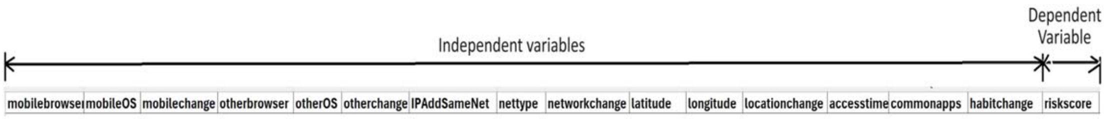


Figure 2. Independent and dependent variables in risk calculation.

Table 3. The risk calculation dataset attributes detailed information.

S no	Attribute	Description	Values/Range
1	Mobile Browser	Mobile phone browser	0 for Chrome, 1 for Opera,2 for DuckDuckGo, 3 for Firefox, 4 for Microsoft Edge
2	Mobile OS	Mobile phone Operating System	0 for Android, 1 for Tizen,2 for iOS, 3 for Windows
3	Mobile Device Change	Mobile Device Change	0,1 for No and Yes
4	Other Browser	Other device browser	0 for Google Chrome, 1 for Brave, 2 for Apple Safari ,3 for Firefox, 4 for Microsoft Edge
5	Other OS	Other Device Operating System	0 for Windows 10, 1 for Linux Ubuntu, 2 for Windows 11, 3 for Mac OS, 4 for Windows 8
6	Other Change	Other Device Change	0,1 for No and Yes
7	IP Add Same Network	Known IP Address	0,1 for No and Yes
8	Network Type	Network Type	0,1 for WiFi and Mobile
9	Network Change	Change in user's devices network	0,1 for No and Yes
10	Latitude	Describes latitude	0,1 for known latitude and unknown latitude
11	Latitude	Describes latitude	0,1 for known latitude and unknown latitude
12	Location Change	Change in location	0,1 for No and Yes
13	Common Apps	Apps commonly used by user on device	0 for TikTok, 1 for Facebook, 2 for SnapChat, 3 for Instagram, 4 for WhatsApp, 5 for Telegram
14	Access Times	Usual time apps are accessed by user	0 for 2:00, 1 for 6:00 ,2 for 8:00, 3 for 9:00, 4 for 10:00, 5 for 11:00, 6 for12:00, 7 for 14:00, 8 for 18:00
15	Habit Change	Change in user habits	0,1 for No and Yes
16	Target	Categories/classes of risk	0 for Accept, 1 for Very Low, 1 for Low, 2 for Medium, 3 for High, 4 for Deny

3.2. Data pre-processing

Data pre-processing is essential to prevent misleading results due to outliers, redundant values, or missing values, and must be completed before analysis [51, 52]. This guarantees that a reliable machine learning model is tested. Different sources' data may not be suitable for analysis due to variations in formats, missing values, or outliers. Consequently, we examined the dataset for any missing values, noisy data, or outliers, and eliminated them. We employed tools like scalers to eliminate outliers from numerical data and hot encoders to encode categorical data, which we then replaced with encoded data.

3.2.1. Data merging

We combined multiple datasets to create a single dataset that combines weighted and non-weighted risk calculations for authentication.

3.2.2. Data cleaning and handling

This step involves removing, altering, or replacing problematic data from a dataset or record, as well as identifying incomplete, erroneous, incomplete, or irrelevant data portions [51]. Our instance had categorical and numerical data that required multiple strategies, despite no missing data.

3.3. Feature selection

The initial cleaning phase involved removing irrelevant features, such as MAC Addresses to maintain 15 features.

3.4. Data splitting

The study utilized stratified sampling to divide data into two sets: a training set and a testing set. The initial 80:20 ratio was utilized, with 3,000 records used, where 2,400 were for training and the remaining 600 for testing.

Table 4. Security meanings of the 6 risk classes.

Probabilities	$0.0 \leqslant x < 0.1$	$0.1 \leqslant x < 0.2$	$0.2 \leqslant x < 0.4$	$0.4 \leqslant x < 0.8$	$0.8 \leqslant x < 0.9$	1
Meaning	Allow	Very Low	Low	Medium	High	Deny

Table 5. Risk probability classes.

Probability range	Classes	Numbers
'0' if $0.0 \leqslant x < 0.5$ else '1'	0, 1	2 Classes
'0' if $0.0 \leqslant x < 0.1$, '1' if $0.1 \leqslant x < 0.9$, else '2'	0, 1, 2	3 Classes
'0' if $0.0 \leqslant x < 0.1$, '1' if $0.1 \leqslant x < 0.5$, '2' if $0.5 \leqslant x < 0.9$, else '3'	0, 1, 2, 3	4 Classes
'0' if $0.0 \leqslant x < 0.1$, '1' if $0.1 \leqslant x < 0.3$, '2' if $0.3 \leqslant x < 0.6$, '3' if $0.6 \leqslant x < 0.9$, else '4'	0, 1, 2, 3, 4	5 Classes
'0' if $0.0 \leqslant x < 0.1$, '1' if $0.1 \leqslant x < 0.2$, '2' if $0.2 \leqslant x < 0.4$, '3' if $0.4 \leqslant x < 0.8$, '4' if $0.8 \leqslant x < 0.9$, else '5'	0, 1, 2, 3, 4, 5	6 Classes

The Naive Bayes classifier and its variations were used to classify the outcome. The study also utilized different splitting ratios of 60:40 and 70:30 and compared the results.

3.5. Classification

The research performed user multi-class classification for authentication using Naïve Bayes classifier and its variations on the weighted and unweighted datasets. Other multi-class classification algorithms, that include Decision Trees, ADABoost, Random Forest, XGBoost and Support Vector Machine were also employed in testing the classification model. The experiment assessed the algorithm's ability to categorise risk probabilities into the six classes listed in table 4 below.

Normal scores are defined as 0-0.1, requiring no further authentication, while scores between 0.9-1 are considered unacceptable and rejected. A single authenticator can be used for low-risk probability authentication, but as the risk probability increases, the difficulty of authentication shifts from single to multi-factor. Table 5 presents a detailed risk classification for scores between 0 and 1 in the proposed multi-class classification.

4. Results

The study evaluated various classifier types, including Gaussian, Categorical, Bernoulli, Hybrid, and other multi-class classification algorithms. Weighted and unweighted datasets were used to execute classification algorithms, and the outcomes were compared and evaluated using weighting and unweighting method. Figure 3 displays a risk score graph based on various weightings, with *RiskScore3* being a result of unweighting contextual factors.

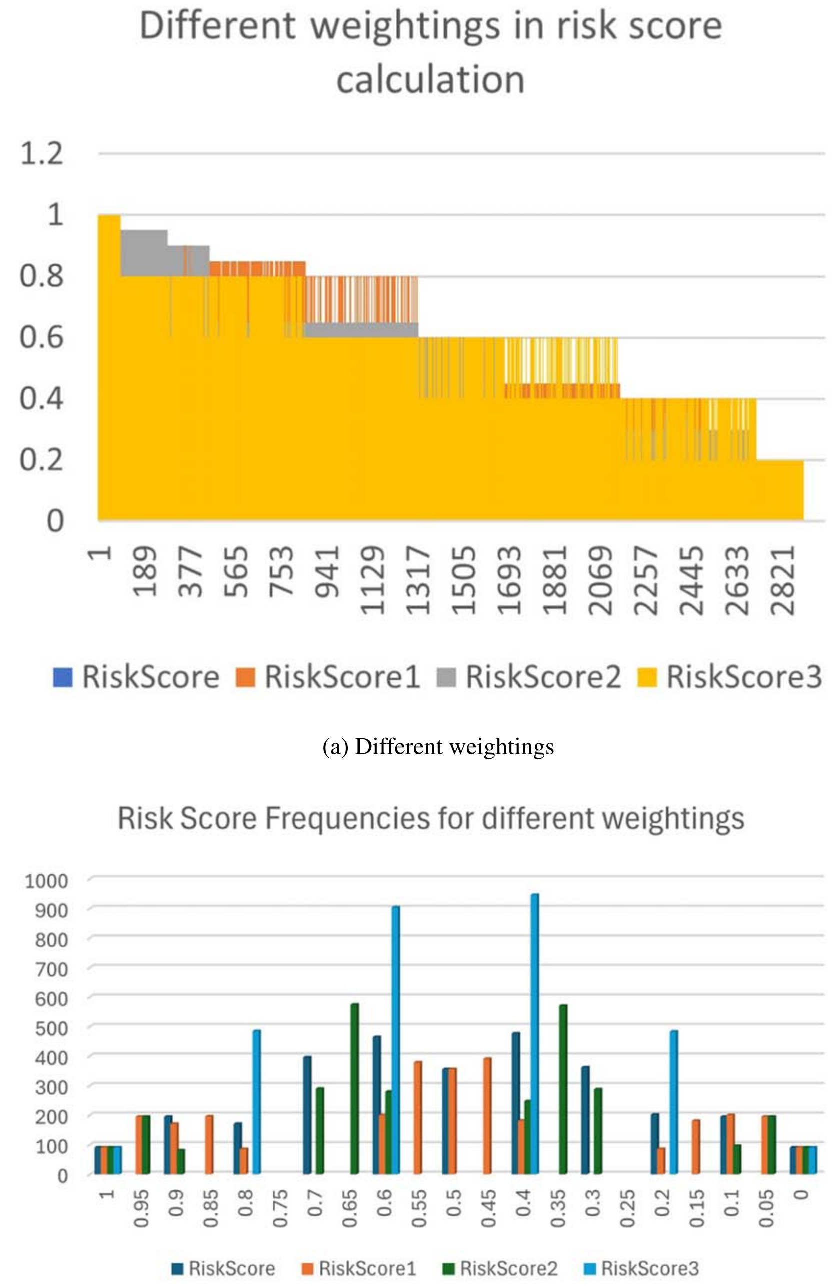
As shown, the graphs' shapes vary with weights, and the unweighted risk score leads to generalised outcomes, introducing bias, which we aim to minimise. The unweighted approach may have adverse effects on user classification and handling during authentication, potentially resulting in their grouping together. A correlation matrix with a dendrogram overlay was created to demonstrate the similarity in correlation between contextual factors and results across weighted and unweighted datasets. Figure 4 shows the matrix.

The data reveals minimal negative correlations, indicating that despite their weak nature, these correlations do not consistently recur, hence they cause minimum problems. Figure 5 displays the evaluation results of our algorithms' performance on weighted contextual features using the Gaussian NB and Categorical NB classifiers.

It can be observed that there is a decrease in accuracy as classes go beyond three. Figure 6 below shows the performance of the Bernoulli NB and the first mixed approach where Gaussian and Categorical NB were mixed at once.

A decrease in performance accuracy can also be observed as classes go beyond three. Figure 7 below shows the weighted mixed second approach. This method involves using both approaches separately and performance can be observed to degrade starting at three classes.

Results demonstrate that the Bernoulli model exhibits a slightly superior performance than the Gaussian and Categorical models for up to four classes with accuracy rate as low as 83%. The same observation extends to metrics such as precision, recall and F1-score. Conversely, the mixed methodologies yielded reduced accuracy in classification tasks relative to the aforementioned techniques. The evaluations took into account the premise that the suitability of algorithms is contingent upon the nature of the dataset. The preference of a weighted



(a) Different weightings

(b) Risk Score frequencies

Figure 3. Weighted and unweighted context for risk score calculations.

approach was justified by its consistently enhanced outcomes compared to the unweighted approach. Results of their comparisons are shown in figure 8 below.

Methodologies that combine different approaches showed decreased effectiveness compared to using individual methods, wherein Gaussian, Categorical, and Bernoulli strategies demonstrated similar levels of performance. The slight variations observed could potentially be linked to the inherent characteristics of the dataset, given that each algorithm presents unique strengths over the others. Overall performance tended to decrease as the number of categories increased. The investigation juxtaposed the outcomes of Naive Bayes multi-classification techniques against alternative algorithms, as illustrated in figure 9.

Decision Trees and Support Vector Machines (SVM), followed by Random Forests and XGBoost (XGB), demonstrated strong performance across all metrics when compared to Gaussian, Categorical, and Bernoulli algorithms. Conversely, ADA yielded lower performance than the other models. Despite exhibiting acceptable accuracy, Naïve Bayes algorithms did not perform as well as the alternative multi-class algorithms. A five-fold cross-validation was conducted to evaluate the model's performance across different data splits. The model's

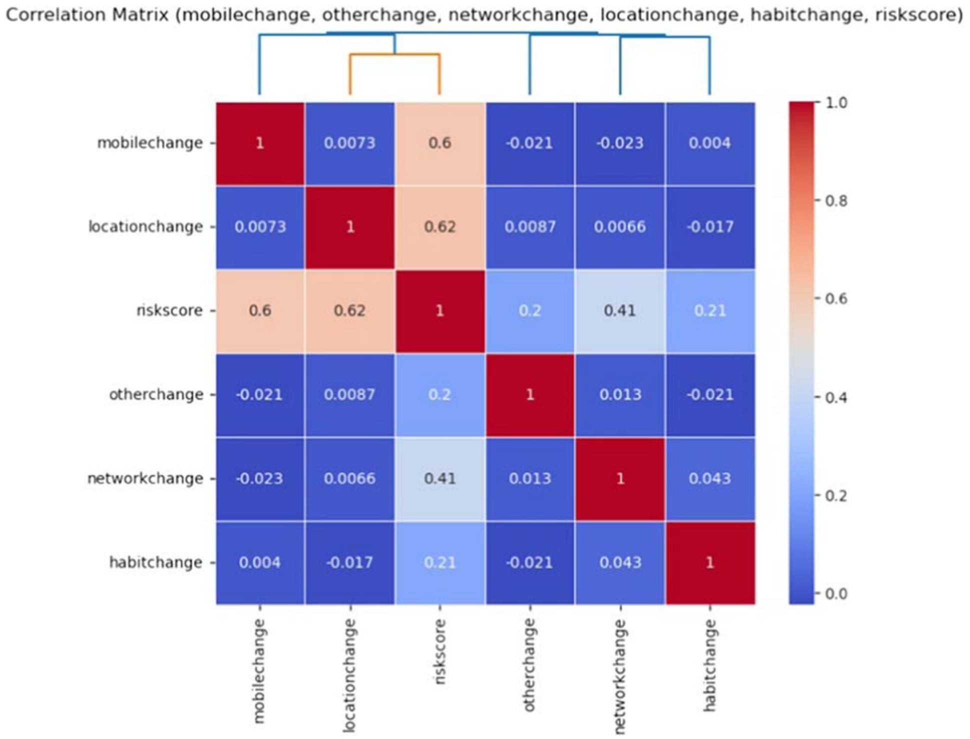


Figure 4. Correlation matrix of contextual factors contributing to final risk score.

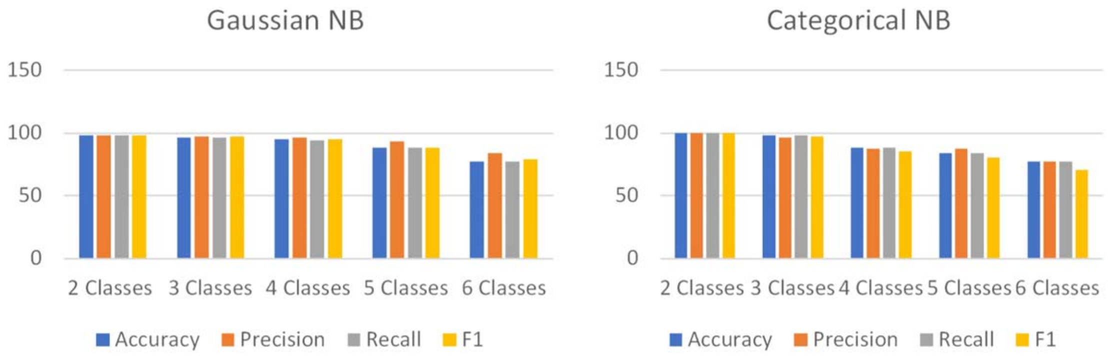


Figure 5. Weighted Bernoulli NB and Mixed approach.

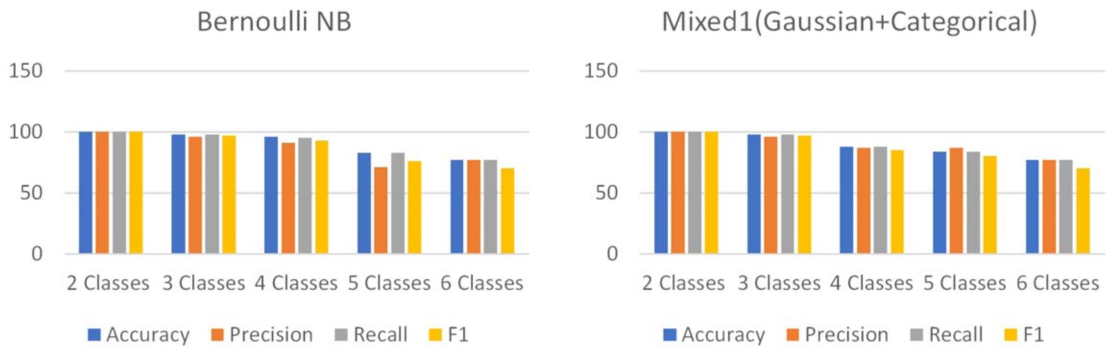


Figure 6. Weighted Bernoulli NB and Mixed approach.

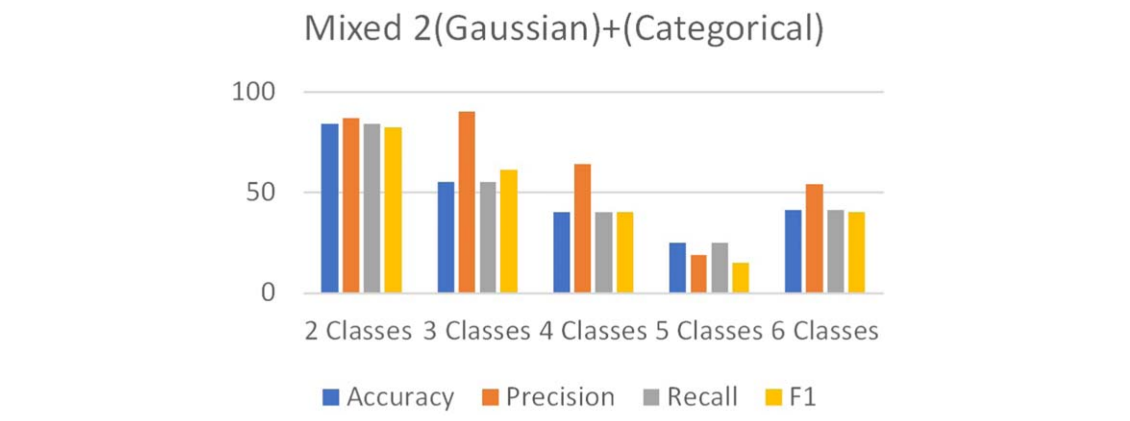


Figure 7. Weighted second mixed approach.

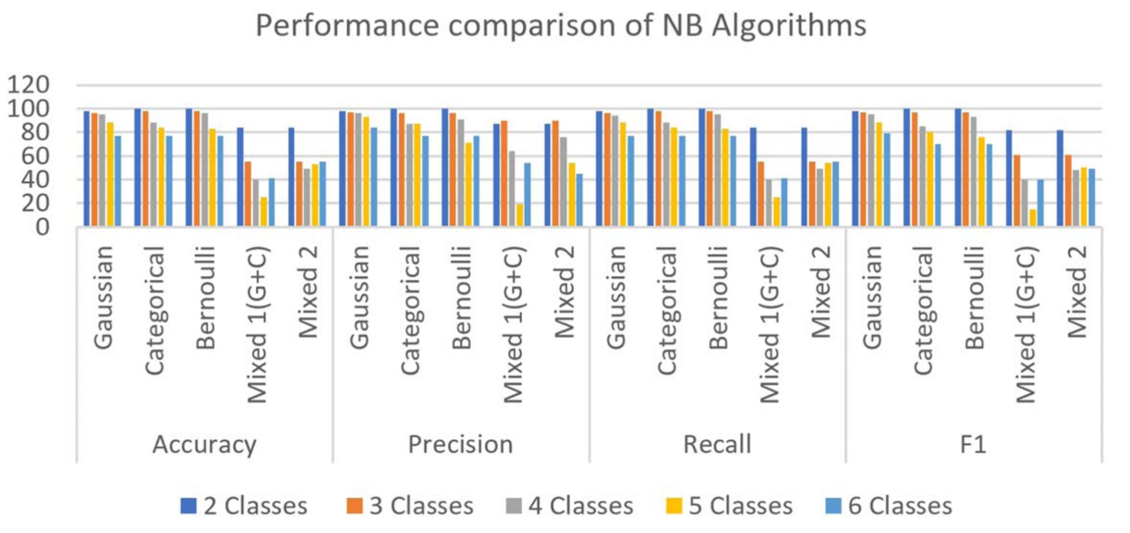


Figure 8. Comparison of NB algorithms on weighted dataset.

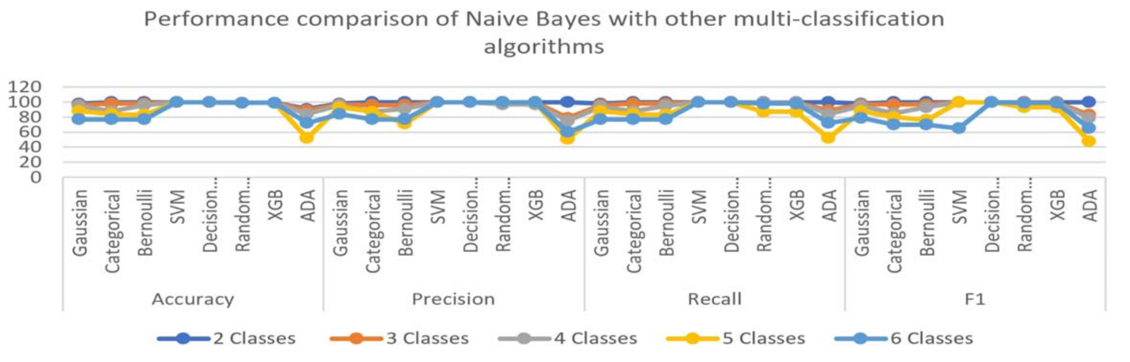


Figure 9. Performance evaluation of different multi-class classification algorithms.

performance was assessed using 80:20, 70:30, and 60:40 data splits. The performance of the model in various machine learning multi-class classification scenarios using these splits is illustrated in figure 10 below.

We created figure 11 to illustrates how our algorithms' performance varies with changes in the number of classes in order to assist explain the discrepancies.

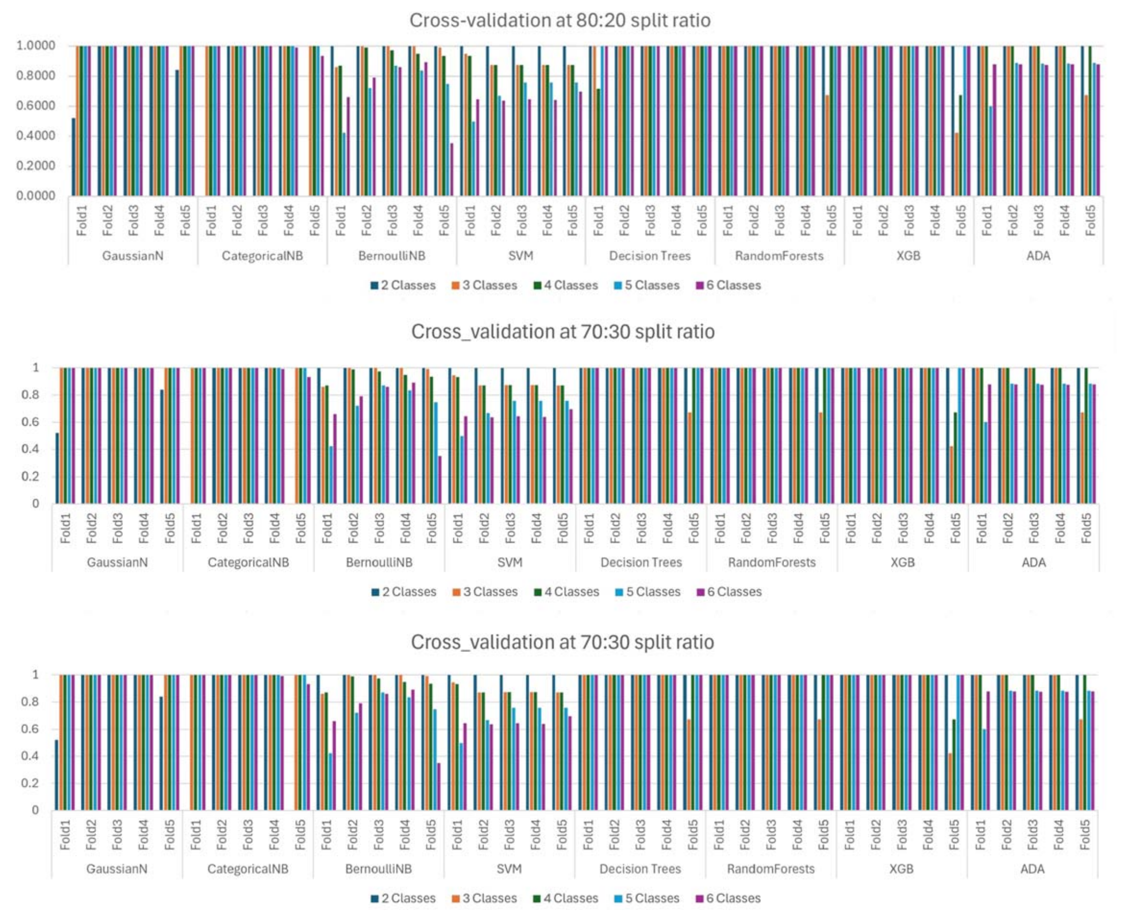


Figure 10. Performance evaluation of different multi-class classification algorithms.

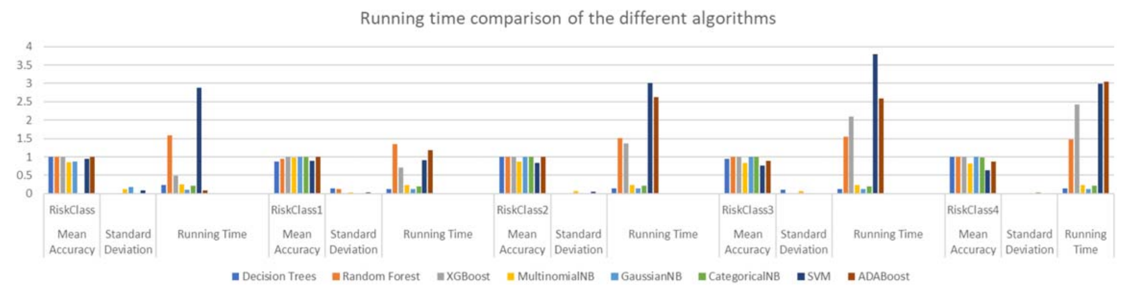


Figure 11. Running time evaluation of different algorithms.

4.1. Discussion

The weighting in table 2 proved to significantly impact the overall risk score and classes, thus enhancing the accuracy of classification models. The study tested various Naive Bayes classification methods using both weighted and unweighted training data, confirming the findings in [43]. The study aimed to evaluate the performance of both methods beyond three classes, and the heatmap reveals a positive correlation between variables, except for mobile device and habit changes. Positive correlations have advantages that include increased risk prediction accuracy, enhanced authentication decision-making, improved usability, reduced false positives/negatives, and better adaptation to dynamic environments [53]. It is, however, worth noting that the correlation does not imply causation [54].

The study classified authentication into six classes, but there was degradation beyond four classes, which may explain why previous studies focused on models for three classes. The accuracy of NB variants and ADA increased up to three classes before declining. When more than four classes were involved, Naïve Bayes classifiers were found to produce less accurate results than other multi-class algorithms that did not depend on the number of classes. Algorithms like Decision Trees, Random Forests, and Support Vector Machines can flexibly model dependencies and interactions between variables, do not assume feature independence, have greater flexibility in model structure and parameterization, are robust to imbalanced data, and have performance optimisation capabilities [55]. The Non-Naïve Bayes algorithms outperform other classification algorithms up to six classes. The (80:20) partition outperformed the other (70:30) and (60:40) partitions, confirming a claim by [46] that partitions significantly influence algorithm accuracy. The weighted version outperformed the unweighted version in confirming assertions made in [22, 26, 27, 43, 46]. The hybrid Naive Bayes method, which combined continuous and categorical data for training, produced more accurate results on weighted data but generally had poor performance. The study therefore concludes that weighting enhances performance. The unweighted approach assumes equal weights for all attributes, leading to biases in risk scores, with odd numbers 0.3,0.45 being omitted. Researchers [45] indicate that the type of data significantly impacts the performance of an algorithm. For example, if the data is categorical, CategoricalNB will obviously outperform other algorithms, and vice versa. The ADA Boost algorithm performed poorly, with an average accuracy of 74.25%, but tuning could potentially improve its performance. On the other hand, the cross-validation using splits did not show a significant effect on the performance of our model, as can be observed in figure 10. BernoulliNB, SVM, and ADA performed significantly lower than the rest as classes increased. Decision Trees, Random Forests, and Naive Bayes variations GaussianNB and Categorical NB performed well above three classes thereby cementing our conclusion on the suitability of the non-Naive Bayes algorithms for multi-user classification. When mean accuracy was compared, as shown in figure 11, the tree-based models (Decision Trees, Random Forest, and XGBoost) surpassed the others with perfect accuracy for binary and three classes holding up well in several risk categories. However, several models show a decline in accuracy for five and six classes suggesting that the classification issue for these categories might be more complicated, either as a result of feature scarcity or class overlap. Efficiency-wise, AdaBoost is a great option when efficiency is crucial because it stands out for having a shorter running time while retaining a high level of accuracy. The Naive Bayes variants show low running times compared to other models indicating speed and probably simplicity. The study supports [15] claim that there's limited theory for mapping algorithms to different problem types, suggesting controlled tests as the most effective approach in classification predictive modelling evaluation. The Naive Bayes method even though it performed worse than alternative algorithms is frequently used because of its simplicity and speed as demonstrated in figure 11 by low running time, validating [55, 56], usefulness as it worked well in our case, thereby supporting [57, 58], interpretability which comes from the ease of understanding the model and result, and efficiency measured from a running time point of view, which is what we desire.

5. Conclusion and future work

Our research primarily focused on implementing Naïve Bayes to address user classification problems in risk-based authentication. Binary user classification is frequently used to categorise users as valid or not, and other multi-class classifications go up to three classes [45]. However, two or three classes of users can only generalise authentication, limiting the usability of security solutions. The study proposed categorising user risk scores into six classes, with extreme classes indicating zero and one and the remaining four classes occupying the middle. The multi-class classification aims to contribute to improved usable security by adjusting authentication difficulty based on risk score. We tested both weighted and non-weighted features on various Naive Bayes algorithms on a synthetic dataset, and the weighted technique outperformed the unweighted technique, which was the overall finding across all experiments. Generally, Naïve Bayes classification algorithms' effectiveness peaks at three classes, and as class sizes increase, accuracy declines. The study also compared Naïve Bayes with other machine learning algorithms for multi-class classification, finding that SVM, Decision Trees, Random Forests, and XGB outperformed Naïve Bayes. Evaluating an algorithm using appropriate data is crucial, as different algorithms perform differently with different data, as per [30]. The Gaussian, CategoricalNB, and Bernoulli algorithms performed almost similarly in the general comparison, but upon five-fold cross-validation, the BernoulliNB performed poorly. In conclusion, when compared to other multi-class algorithms, our model properly categorises users with a higher level of precision when utilising non-Naïve Bayes algorithms, namely DT and RF. GaussianNB and categoricalNB also performed well in both general comparison and cross-validation. Cross-validation gave us an insight into the performance of our model as it complimented the initial performance comparison that we made, thereby reducing bias. Since not all iterations of the classification algorithm perform poorly, it is acceptable to say that some of the shortcomings of the Naive Bayes algorithm are reached from a generalised point of view. The results indicate that the Naïve Bayes rule can be used for risk calculation while other machine learning algorithms can be employed for user classification. As illustrated in figures 5 to 9, the Naïve Bayes algorithms did not perform as well as the alternative multi-class algorithms despite displaying acceptable accuracy, but these findings explain the algorithm's interpretability and simplicity, as it can be understood on a modular level shown in figure 4, and table 3 to 5, demonstrating how each feature contributes to a class prediction. The probablistic model is easy to explain and understand. Because of the Bayes theorem and the feature independence assumption, this algorithm is simpler to implement than other algorithms that are more complicated because of their underlying mathematical models, optimisation procedures, or architectural designs. Particularly during training, the algorithm runs quite quickly and because of the fact that it simply needs to calculate probabilities from the training data, the Naive Bayes algorithm is fast and computationally efficient,supporing [55, 56]. Large datasets, however, are where its speed is most noticeable [59]. Its efficiency is shown in figure 10 where the Gaussian NB and CategoricalNB compete with other Machine Learning multiclassification algorithms. The Naive Bayes doesn't need to store a lot of data in memory and has less computational overhead. Because it believes that features are independent of one another, the Naive Bayes method performs poorly in situations where the features are heavily correlated. It is therefore most appropriate for classification problems involving categorical features [60]. As can be observed in figure 4, there is little correlation, indicating that the algorithm performs well in our multi-classification scenario.

Based on results in figure 11 future work may involve looking at the characteristics that lead to the incorrect classifications in five and six classes through examining the models' feature relevance. Feature engineering may also be tried in the future to distinguish between classes where performance is lower. It is also necessary to try an ensemble approach that combines several models predictions to increase robustness. Fine-tuning attributes and weighted techniques in Android app construction, detecting context through device sensors, and assigning authenticators based on risk scores is also our future work. The app's deployment aims to collect complete data on user context and authenticators, as complete data is challenging to obtain.The solution's usability is expected to enhance security adherence, and full deployment will evaluate the model's viability for diverse users with diverse medical conditions that affect their use of authenticators.

Acknowledgments

This work was jointly supported by the African Centre of Excellence in Internet of Things (ACEIoT) from the College of Science and Technology, University of Rwanda, the Centre for Connected Intelligence (CCI) from the Department of Electrical, Electronic, and Computer Engineering, University of Pretoria, and the Regional Innovation Scholarship Fund (RSIF).

Data availability statement

All data that support the findings of this study are included within the article (and any supplementary files).

Conflict of interest

The authors have declared that no competing interests exist.

ORCID iDs

Prudence M Mavhemwa https://orcid.org/0000-0002-8140-7114

References

[1] Alsaeed N and Nadeem F 2022 Authentication in the internet of medical things: taxonomy, review, and open issues *Applied Sciences (Switzerland)* **12** 1–3

[2] Zakaria H, Azaliah N, Bakar A, Hassan N H and Yaacob S 2019 Iot security risk management model for secured practice in healthcare environment *Procedia Comput. Sci.* **161** 1241–8

[3] Chebib K 2021 Iot applications in the fight against covid-19 *GSMA Mobile for Development*

[4] Kermani M M, Azarderakhsh R and Mirakhorli M 2016 Multidisciplinary approaches and challenges in integrating emerging medical devices security research and education *2016 ASEE Annual Conference & Exposition*

[5] Coll L and Simpson R 2016 The internet of things and challenges for consumer protection *Consumersinternational* 1–122

[6] Aneela K M D G, Anusha I A and Aneela R 2017 Research trends of network security in iot *International Journal of Innovative Studies in Sciences and Engineering Technology* **3** 6–10

[7] M A R, Gill S H, Qureshi M A and Ullah S 2017 *International Journal of Advanced Computer Science and Applications* **8**

[8] Sagar P 2019 Top 8 iot market trends to look out for in 2019 *SSRN Electronic Journal* 1–4

[9] Tot I, Lalović K and Brzaković M 2017 Security mechanisms in iot *The IX International Conference on Business Information Security* 2017

[10] Oranski S 2019 Why strong healthcare iot security requires specialised solutions *Tech. Rep., Cybermdx*

[11] Mehran M-K, AzarderakhshReza, Kui R and Jean-Luc B 2016 Introduction to the special section on emerging security trends for biomedical computations, devices, and infrastructures: guest editorial *IEEE/ACM Trans. Comput. Biol. Bioinformatics* **13** 399–400

[12] Mozaffari K M, Reza A and Xie J 2016 Error detection reliable architectures of camellia block cipher applicable to different variants of its substitution boxes *2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST)* pp 1–6

[13] Anita A, Mehran M K and Reza A 2017 Fault diagnosis schemes for low-energy block cipher midori benchmarked on fpga *IEEE Trans. Very Large Scale Integr. VLSI Syst.* **25** 1528–36

[14] 2015 17 goals to transform the world for persons with disabilitiesTech. Rep. United Nations Enable

[15] Brownlee S 2016 Master machine learning algorithms: discover how they work and implement them from scratch *A-Tour-of-Machine-Learning-Algorithms*

[16] Abokadr S, Azman A, Hamdan H and Amelina N 2023 Handling imbalanced data for improved classification performance: Methods and challenges *Conference: 2023 3rd International Conference on Emerging Smart Technologies and Applications (eSmarTA)*

[17] Subasi O, Ghosh S, Manzano J, Palmer B and Marquez A 2024 Analysis and benchmarking of feature reduction for classification under computational constraints *Machine Learning: Science and Technology* **5** 1–2

[18] Nocera F D and Tempestini G 2022 Getting rid of the usability/security trade-off: a behavioral approach *Journal of Cybersecurity and Privacy* **2** 245–56

[19] Fallatah W, Furnell S and He Y 2023 Refining the understanding of usable security *HCI for Cybersecurity, Privacy and Trust: V International Conference, HCI-CPT 2023, Held as Part of the XXVHCI International Conference, HCII 2023* (Springer) pp 49–67

[20] Karamahmutoglu I and Gokturk M 2024 A systematic approach to measure usability and security trade-off. in 2024 International Congress on *Human-Computer Interaction, Optimization and Robotic Applications (HORA)* pp 1–4

[21] (Ucsc) 2019 Choosing a default authentication method *Information Technology Services*

[22] Frank E, Hall M and Pfahringer B 2012 Locally weighted naive bayes *Physica* A 249–56

[23] Zaidi N A, Cerquides J, Carman M J and Webb G I 2013 Alleviating naive bayes attribute independence assumption by attribute weighting *Journal of Machine Learning Research* **14** 1947–88

[24] Prabha D, Aswini J, Maheswari B, Subramanian R, Nithyanandhan R and Girija P 2022 A survey on alleviating the naive bayes conditional independence assumption *2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)*

[25] Subramanian R, Girija P, Sudha K, Aswini J, Sivakumar S and Nattesan N V S 2023 Alleviating the naive bayes assumption using filter approaches *2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India*

[26] Wickramasinghe I and Kalutarage H 2021 Naive bayes: applications, variations and vulnerabilities: a review of literature with code snippets for implementation *Soft Comput* **25** 2277–93

[27] Kharya S and Soni S 2016 Weighted naive bayes classifier: a predictive model for breast cancer detection *International Journal of Computer Applications* **133** 32–7

[28] Kumar G, Chaudhary A R and Kumar K 2019 Internet banking security enhancement using naïve bayes algorithm *International Journal of Innovative Technology and Exploring Engineering* **8** 79–82

[29] Vadapalli P 2022 Naive bayes classifier: pros & cons, applications & types explained

[30] Ray S 2017 Naive bayes classifier explained: applications and practice problems of naive bayes classifier

[31] Ruan S, Chen B, Song K and Li H 2021 Weighted naïve bayes text classification algorithm based on improved distance correlation coefficient *Neural Computing and Applications* **34** 1–10

[32] Yunyun Wang Y L and Chen S 2022 Towards adaptive unknown authentication for universal domain adaptation by classifier paradox *Mach. Learn.* **2207** 1–20

[33] Zeng R, Lin L and Zhao Y 2023 A novel weight adaptive multi factor authorization technology *Neural Computing and Applications* (Springer)

[34] Velasco C N 2023 *A Weighted Naive Bayes for Image Classification Based on Adaptive Genetic Algorithm* (Springer Nature)

[35] Adaptive multi-factor authentication system with multi-user permission strategy to access sensitive information 2019

[36] Feature weighting-based naive bayesian microblog user classifying method 2018

[37] Mcdougall A P, Simmons M J and Landman G J 2021 Adaptive user authentication *Adaptive User Authentication* United States of AmericaUS Patent 11,575,670

[38] Fei L, Kang B, Huynh V-N and Deng Y 2017 Adaptively evidential weighted classifier combination *Artificial Intelligence* **1712** 1–9

[39] Sari Z, Chandranegara D R, Khasanah R N, Wibowo H and Suharso W 2022 Analysis of the combination of naïve bayes and mhr (mean of horner's rule) for classification of keystroke dynamic authentication *Jurnal Online Informatika* **7** 62–69

[40] Blue J, Condell J and Lunney T 2019 It is probably me: a bayesian approach to weighting digital identity sources *Proceedings of the 2019 International Symposium on Networks* pp 1–6

[41] Ain K, Hidayati H B and Nastiti O A 2017 Expert system for stroke classification using naive bayes classifier and certainty factor as diagnosis supporting device *J. Phys. Conf. Ser.* **1445** 1–8

[42] Rahman R F and Suharjito 2023 Crowd face detection with naive bayes in attendance system using raspberry pi *E3S Web of Conferences* (EDP Sciences) (https://doi.org/10.1051/e3sconf/202338802010)

[43] Zhang H, Jiang L and Yu L 2021 Attribute and instance weighted naive bayes *Pattern Recognit* **111** 2–3

[44] Zhang H and Jiang L 2022 Fine tuning attribute weighted naive bayes *Neurocomputing* **488** 402–11

[45] Akkaya N C B 2019 Comparison of multi-class classification algorithms on early diagnosis of heart diseases *y-BIS 2019 Conference: ISBIS Young Business and Industrial Statisticians Workshop on Recent Advances in Data Science and Business Analytics* pp 1294–8

[46] Jha A, Dave M and Madan S 2019 Comparison of binary class and multi-class classifier using different data mining classification techniques *SSRN Electronic Journal Proceedings of International Conference on Advancements in Computing & Management (ICACM)* 894–903

[47] S A A, Yu I A and M R V 2021 Application of the user's digital footprint in the adaptive authentication problem *International Siberian Conference on Control and Communications (SIBCON)* pp 1–5

[48] Acien A, Morales A, Vera-Rodriguez R and Fierrez J 2020 Smartphone sensors for modeling human-computer interaction: general outlook and research datasets for user authentication *2020 IEEE XLIV Annual Computers, Software, and Applications Conference (COMPSAC)Proceedings of International Conference on Advancements in Computing & Management (ICACM) 2019* pp 1273–8

[49] DataHub. IPv4 geolocation 2018

[50] Wolfgang, Mobile application user statistics 2018

[51] Finan M B 2012 A probability course for the actuaries *A Probability Course for the Actuaries A Preparation for Exam P/1* **1** 1–4

[52] Obasi C B I C 2023 Evaluating the effectiveness of machine learning techniques in forecasting the severity of traffic accidents *Heliyon* **9** 1–12

[53] Hayes A 2023 Positive correlation: definition, measurement, examples

[54] Muncaster J and Turk M 2006 Continuous multimodal authentication using dynamic bayesian networks 1–4

[55] Veziroğlu M, Veziroğlu E and Bucak İ Ö 2024 *Performance Comparison between Naive Bayes and Machine Learning Algorithms for News Classification* (IntechOpen)

[56] Kumar R, Goswami B, Mhatre S M and Agrawal S 2024 Naive bayes in focus: a thorough examination of its algorithmic foundations and use cases *International Journal of Innovative Science and Research Technology* **9** 2078–81

[57] Azizah M F and Paramitha A T 2024 Predictive modelling of chronic kidney disease using gaussian naive bayes algorithm *International Journal of Artificial Intelligence in Medical Issues* **2** 125–35

[58] Garba M, Usman M and Gulumbe A M 2024 Improving breast cancer detection with naive bayes: a predictive analytics approach *Computer Science and Information Technology* **14** 185–96

[59] Askari A, d'Aspremont A and Ghaoui L E 2023 1. naive feature selection: a nearly tight convex relaxation for sparse naive bayes *Math. Oper. Res.* **49** 278–96

[60] Zhou H 2023 *Naive Bayes Classification* (Apress) pp 143–59