International Journal of Computer Applications Technology and Research
Volume 13–Issue 02, 01 - 07, 2024, ISSN:-2319–8656

DOI:10.7753/IJCATR1302.1001

Machine Learning Approach to Determine the Impact of Hate Speech Based on Public Opinions

Obilikwu Patrick
Benue State University
Makurdi, Nigeria

Charles Obekpa
Benue State University
Makurdi, Nigeria

Aamo Iorliam
Benue State University
Makurdi, Nigeria

Abstract: In an era dominated by online communication, the prevalence of hate speech has emerged as a significant societal concern. This paper presents a comprehensive study utilizing machine learning techniques to assess the detrimental effects of hate speech on public opinions. Utilizing a varied dataset encompassing public sentiments, we utilize advanced machine learning algorithms to categorize the adverse effects of hate speech. This study employs a combination of quantitative, qualitative, and experimental research methodologies. The experimentation phase involved training and testing the models using Logistic Regression (LR), Decision Tree (DT), and Random Forest (RF). The resulting model demonstrates high accuracy and precision, with LR achieving (0.96, 0.97), DT showing (0.99, 100), and RF exhibiting (100, 100). Our findings reveal compelling insights into the negative impact of hate speech. By classifying the negative repercussions, this research not only advances our understanding of online discourse but also provides a valuable foundation for the development of strategies to combat hate speech and cultivate a more inclusive digital environment.

Keywords: Hate Speech, predictive modeling, opinion mining, machine learning

1. INTRODUCTION

In an era characterized by unprecedented connectivity and information dissemination, the rise of hate speech has emerged as a pressing concern for both online. The pervasive nature of digital platforms has provided a fertile ground for the proliferation of harmful and discriminatory language, amplifying its potential to inflict profound societal harm [1]. Addressing this complex challenge requires a multifaceted approach, with machine learning presenting a promising avenue for automated detection and analysis [2].

This paper delves into the intersection of technology and societal well-being, aiming to harness the power of machine learning algorithms to classify the negative impact of hate speech. By leveraging machine learning techniques, we endeavor to shed light on the impact of hate speech on the victims and to equally decode the predominant hate rhetoric and sentiment in a given location. The objective of this study is to develop robust machine learning models capable of classifying hate speech [3]. Through these endeavors, we hope to contribute to the development of informed, data-driven strategies for mitigating the adverse effects of hate speech.

In this pursuit, we navigate a landscape where linguistic nuance, context, and evolving cultural norms play pivotal roles. This necessitates a nuanced approach to algorithmic design, one that balances accuracy with adaptability in the face of ever-changing forms of expression. By harnessing the power of natural language processing, we endeavor to equip our models with the capacity to decipher the intricacies of language, discerning between legitimate discourse and expressions laden with hate [4].

In the following sections, we will delve into the foundational concepts, methodologies, and empirical findings that underpin our approach. Through a synthesis of cutting-edge machine learning techniques and a deep dive into the intricate landscape of hate speech, we endeavor to illuminate the path forward in our collective pursuit of a safer, more inclusive digital sphere.

2. LITERATURE REVIEW

Study by [5], shows compelling evidence of online hate speech which has assume different dimensions. People and organization perpetrate hate speech which target individuals, groups, community or race for several reasons such as; intimidating, shaming, discrediting, and incite violence etc. [6] supported the above assertions and that online hate speech have become pervasive due to the presence of internet which has brought about the opportunities for disseminating hate speech. And defined Hate speech as bias-motivated, hostile, malicious speech aimed at a person or a group of people because of some of their actual or perceived innate characteristics and that the main motivation is to expresses discriminatory, intimidating, disapproving, antagonistic, prejudicial attitudes toward the targets. The study advocates the need for collective responsibility to tackle online hate speech.

With the rise of hate speech phenomena in the Twittersphere and social media in particular, significant research efforts have been undertaken in order to provide automatic solutions for detecting hate speech, varying from simple machine learning models to more complex deep neural network models [7].

The study by [8] developed a model using linear support vector machine and Naïve bayes to identify offensive language in social media tweet, the study obtains the following results for accuracy and recall for Naïve Bayes (92%, 95%), and Linear SVM (90%, 92%).

Another study by [9] developed machine learning algorithms such as Logistic Regression, Decision Tree, Random Forest, Multinomial Naïve Bayes, Stochastic Gradient Descent to classify suspicious text in Bengali text documents, feature extraction and selection techniques such as TF-IDF and BOW were used in the work. The five classifiers were trained using the feature extracted datasets for TF-IDF and BOW and gave different results. For the BOW feature extraction techniques Random Forest gave the highest accuracy of 83.21%, while Stochastic Gradient Descent gave the highest precision with 83.79%. Whereas for the TF-IDF feature extracted datasets, the Stochastic Gradient Descent gave accuracy of 84.57% and a precision of 83.78%. Comparison of the two feature extracted techniques shows TF-IDF outperforms the BOW techniques in terms of the overall results obtained in the study.

In a similar study by [10] to detect offensive content in code-mixed dataset of Dravidian languages, machine learning models were equally trained using different features such as n-gram, character n-gram, combined word and custom word embedding. Using the TF-IDF weights of word and character n-gram features they trained Machine learning classifiers. The model for Malayalam language got the official rank of 2nd and obtained an F1-score of 0.77, while Tamil language Model got the official rank of 3rd and F1 score of 0.87 from the results.

A study by [11] developed eight Machine Learning models with three selected feature engineering techniques to detect hate speech in text. The experiment shows that bigram features and TF-IDF gave a better result compared to word2Vec and Doc2Vec feature engineering techniques. Amongst the models trained SVM (79%) gave better results compared to the rest of the models while KNN gave the least result.

Another study by [7] developed deep learning model using CNN, GRU, CNN + GRU, and BERT to classify hate speech into hate and non-hate. They used annotated data to train the models and out-domain (secondary) data for testing to see how well the model generalize to unseen datasets. From the results of the experiment, both the annotated and an out-domain dataset showed that the CNN model gave the best performance, with an F1-score of 0.79 and area under the receiver operating characteristic curve (AUROC) of 0.89.

From the literature review by [12] various approaches are already in used to detect hate speech ranging from rule based, Machine Learning and deep learning and Hybrid techniques which lend credence to the fact that several studies have been adduce to detect hate speech from existing literature.

Most of the literature review shows extensive progress in detecting the presence of hate speech and also classifying hate speech from non-hate using machine learning and deep learning techniques. However, gap still exist in the literature as to the negative impact of hate speech on the victims and predominant hate rhetoric in a given geolocation. This work intends to close the above gap by classifying hate speech based on its impact on the victims and also identify the predominant hate-based rhetoric in a given geolocation.

3. METHODOLOGY

This research employed quantitative, qualitative, and experimental research methods. The study involved conducting experiments to train and test supervised machine learning models, utilizing Logistic Regression (LR), Decision Tree (DT), and Random Forest (RF). The model with the highest accuracy was chosen for deployment, and algorithm performance was assessed using Confusion Matrix and classification reports.

3.1 Multi-class Logistic Regression

Multi-class logistic regression, also known as multinomial logistic regression or SoftMax regression, is a classification algorithm used to model the relationship between a set of input features and multiple classes. It extends binary logistic regression to handle problems where there are more than two classes. The goal is to estimate the probability of each category for a given set of predictor values [13].

The mathematical theory behind multi-class logistic regression involves several key concepts:

3.1.2 Linear Combination of Features

In multi-class logistic regression, each class has its set of weights associated with the input features. For a given class j (where j ranges from 1 to C, where C is the number of classes) the linear combination of features X can be represented as:

$$Z_j = \theta_{0j} + \theta_{1j}\chi_1 + \theta_{2j}\chi_2 + \dots + \theta_{nj}\chi_n \qquad (1)$$

Here, Z_j is the linear combination for class j, xi represents the i-th feature, and θ_(0j) is the weight associated with i-th feature for class j.

3.1.3 SoftMax Function

In multi-class logistic regression, the SoftMax function is used to transform the linear combinations Z_j into class probabilities. The SoftMax function for class j is defined as:

$$\mathrm{P}(\Upsilon = j|\mathrm{X}) = \frac{e^{zj}}{\sum_{k=1}^{C} e^{zk}} \qquad (2)$$

Here, P (Y= j | X) is the probability of the input belonging to the class j, and C is the total number of classes. The exponential function e^{zj} ensures that the probabilities are non-negative, and the denominator sums over all classes to normalize the probabilities to add up to 1.

3.1.4 Multi-class Loss Function

The loss function used in multi-class logistic regression is typically the cross-entropy loss, which measures the dissimilarity between the predicted probabilities and the true class labels. The loss for a single training example is defined as:

$$L(\Upsilon, \mathrm{P}) = -\sum_{j=1}^{C} y_j \; log(P(\gamma = j \mid X)) \qquad (3)$$

Here, L (Y, P) is the loss for the training example, yj is an indicator variable (1 if the true class is j, 0 otherwise), and

P (γ = j | X) is the predicted probability for class j.

3.1.5 Optimization

The goal of training in multi-class logistic regression is to minimize the overall loss across all training examples. This is typically done using optimization techniques like gradient descent.

The gradients of the loss with respect to the model parameters θ (0j) are computed, and the parameters are updated iteratively to minimize the loss.

3.1.6 Algorithm

1. Input
   Training dataset D with features X and corresponding labels Y
   Learning rate (α), regularization parameter (λ), number of iterations
2. Data Preprocessing
   Encode categorical variables (if any) and normalize/standardize the feature values.
3. One-hot Encoding of Labels
   Convert the multi-class labels (Y) into a one-hot encoded matrix $Y_{one-hot}$ with C
   columns, where C is the number of classes
4. Initialize Parameters
   Initialize weight matrix W and bias vector b with random or zero values.
5. Training
   Function Train_Multinomial_Logistic_Regression (X, Y, one_hot, α, λ, num_iterations):
   For i in range num_iterations:
   Calculate the linear scores $Z = XW + b$
   Calculate the SoftMax probabilities P for each class:
   $P = softmax(Z)$
   Calculate the loss using the cross-entropy loss function:
   $$J = -\frac{1}{M}\sum_{j=1}^{C} Y_{ij}\,log(P_{ij}) + \frac{\lambda}{2m}\sum_{k=1}^{n}\sum_{j=1}^{C} W^2\ k_j$$
   Calculate the gradient of the loss w.r.t W and b
   $$dW = \frac{1}{m}X^T.(P - Y_{one-hot}) + \frac{\lambda}{m}W$$
   $$db = \frac{1}{m}\sum_{i=1}^{m}(P - Y_{one-hot})$$
   Return W and b
6. Prediction
   Function Predict_Multinomial_Logistic_Regression (X, W, b):
   Calculate the linear scores $Z = XW + b$
   Calculate the SoftMax probabilities P for each class:
   $P = soft\max(Z)$
   Return the class with the highest probability for each sample.

3.2 Decision Tree

Decision tree algorithms comprise trees that categorize data by looking at feature values. Every node in a decision tree depicts a feature that has to be classified, and the branches depict values that are considered by such a node, [14]. A decision tree is a popular machine learning algorithm used for both classification and regression tasks. It works by recursively partitioning the dataset into subsets based on the values of input features, ultimately leading to a tree-like structure where each leaf node represents a class label (in classification) or a numerical value (in regression).

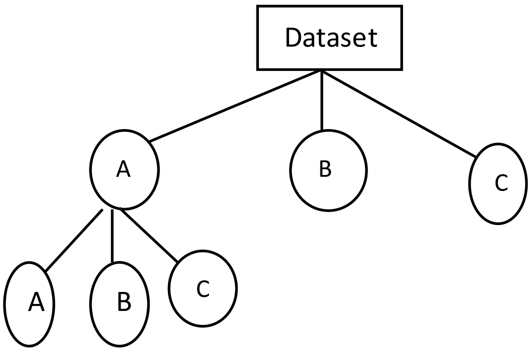


Figure 1: Multiclass Decision Tree

3.2.2 Entropy

Entropy is a measure of disorder or impurity in a set of data. In the context of decision trees, it's used to quantify the impurity of a dataset before a split. Mathematically, entropy is defined as:

$$H(S) = -\sum_{i=1}^{c} pi\ log_2(pi) \tag{4}$$

Where c is the number of classes and pi is the probability of an instance belonging to class i.

3.2.3 Information Gain

Information Gain is the reduction in entropy or impurity achieved by partitioning a dataset based on a specific attribute (feature). It helps in deciding which attribute to split on. Mathematically, Information Gain is calculated as:

$$IG(S,A) = H(S) - \sum_{v \epsilon Values(A)} \frac{|S_v|}{|S|}.H(S_v) \tag{5}$$

Where S is the dataset, A is the attribute being considered for the split, Values (A) are the possible values of attributes A, S_v is the subset of S where attributes A takes the value v.

3.2.4 Gini Impurity

Gini Impurity is an alternative to entropy for measuring impurity. It quantifies the probability of a randomly chosen element being misclassified. For a dataset S with c classes, Gini Impurity is calculated as:

$$Gini\ (S) = 1 - \sum_{i=1}^{c}(P_i)^2 \tag{6}$$

3.3 Random Forest Classifier

A Random Forest classifier is an ensemble learning method that combines the predictions of multiple decision trees to improve the accuracy and robustness of a classification task. It is based on the idea that a collection of weak learners (individual decision trees) can come together to form a strong learner. Random Forest is a supervised machine learning algorithm that uses a group of decision tree models for classification and making predictions, [15]. As the name indicates, a forest will be created from a group of decision trees and then will be randomized.

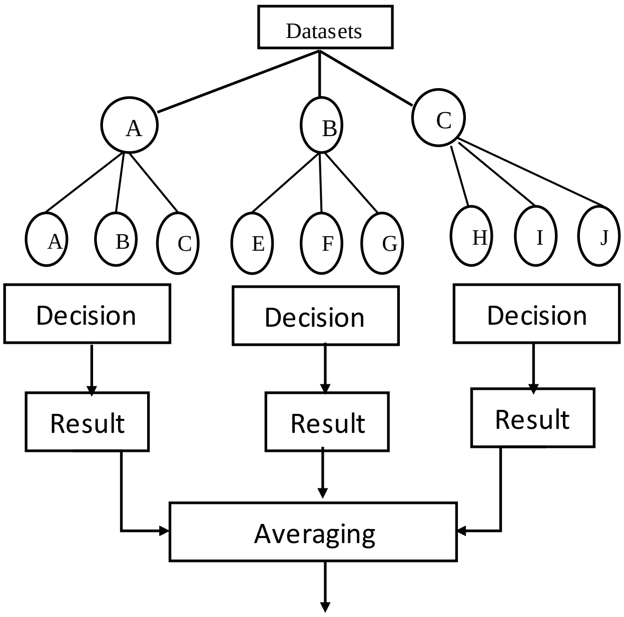


Figure 2: Random Forest

3.4 Data Pre-processing

To construct a comprehensive dataset for training and evaluation. We sourced data from social media platforms such as Facebook [16]. Prior to training, we subjected the dataset to extensive preprocessing [17]. This involved tasks such as lowercasing, punctuation removal, and tokenization.

To facilitate supervised learning, we engaged a team of human annotators proficient in understanding and categorizing hate speech [8]. Annotations were carried out using a multi-class labeling system, distinguishing between non-offensive language, offensive language, and hate speech to ensure inter-annotator agreement [18]. The dataset was split into training and test sets with the training set accounting for 70% while the test set 30% of the data.

The input variables are the hate motivated public comments express on social media platform. Because of freedom of expression, social media users are allowed to post and express their opinions freely. The data labeling was done by the annotators.

Table 1. Annotated data with labels

Labels	Comments
Violence	their people have ruined the country
discrimination	make sure you don’t admit them in our institution
positive	are you coming for the wedding?
harrassment	you don’t belong here

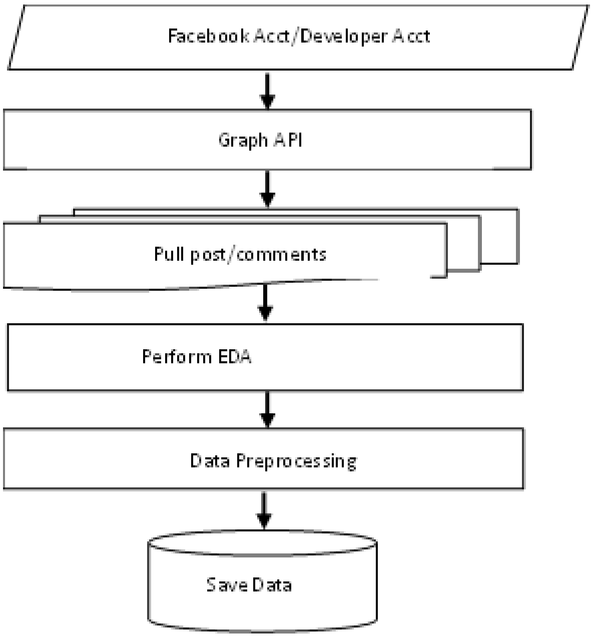


Figure 3: Data Collection Techniques

The target variable or the labels are the negative impact of a given comments or post from the public.

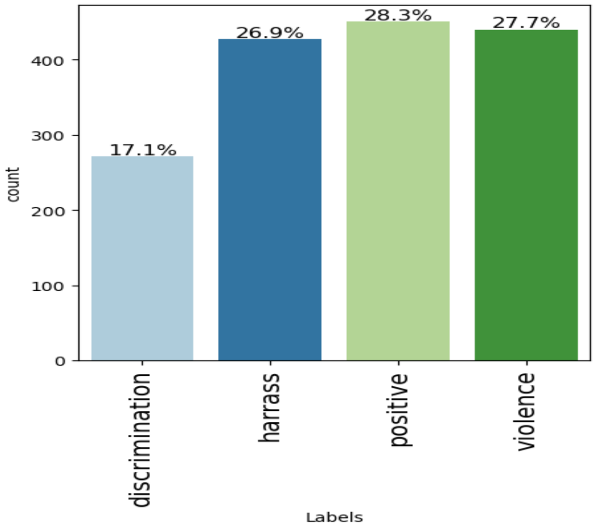


Figure 4: Distributions of labels in the datasets

We experimented with a range of machine learning models such as Logistic Regression, Decision Tree and Random Forest. To assess the efficacy of our models, we conducted rigorous evaluation using standard metrics such as precision, recall, F1-score, and accuracy.

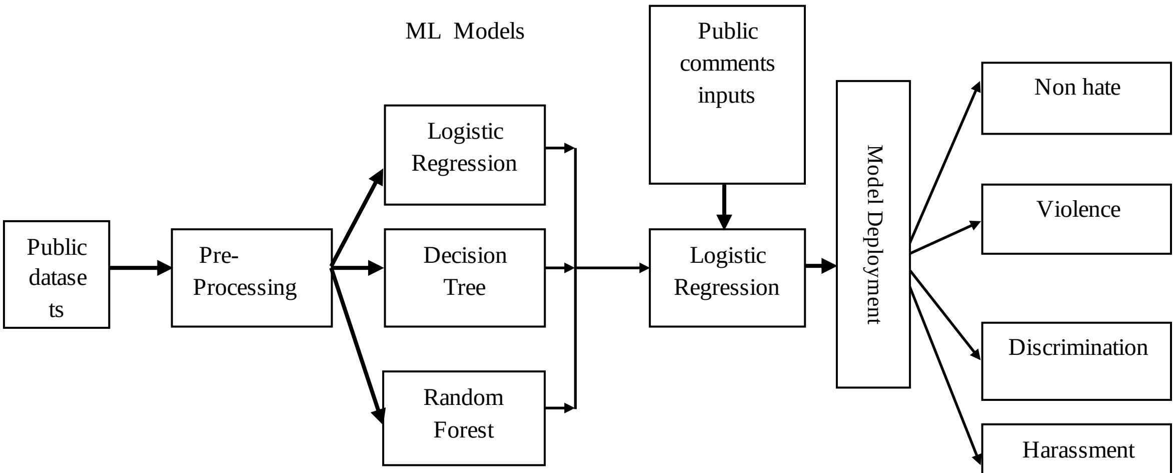


Figure 5. Flowchart showing the flow of activities in implementing the machine learning model for hate speech classification

To determine the impact of hate speech on public sentiment, we conducted sentiment analysis on the annotated dataset. We employed established sentiment lexicons and machine learning-based approaches to classify the emotional trajectory of the text.

3.5 Model Training and Evaluations

The three models were trained using the above datasets. The data was split using the 7:3 ratio i.e., 70% of the data were used to train the model while the remaining 30% for testing. The accuracy of the models was evaluated and the model with the highest accuracy was used for deployment. The codes were written using Python programming Language and the Visual Studio Code Integrated Development Environment (IDE) bundled with Anaconda.

A confusion matrix is a table used in machine learning to evaluate the performance of a classification algorithm. It summarizes the predictions of a model on a set of data for each class and compares them with actual labels. The matrix typically includes four values: true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN). These values are used to calculate various performance metrics such as accuracy, precision, recall, and F1 score, which help assess the model’s classification performance.

Accuracy: In machine learning, accuracy is a metric that measures the correctness of the predictions made by a model. It is defined as the ratio of correctly predicted instances to the total instances in the dataset.

Accuracy = (TP +TN) / (TP + TN + FP + FN)

Precision: Precision is a metric in machine learning that assesses the accuracy of the positive predictions made by a model. It is defined as the ratio of true positive predictions to the total number of positive predictions

Precision = TP / (TP + FP)

Recall: Recall, also known as sensitivity or true positive rate, is a metric in machine learning that measures the ability of a model to capture and correctly identify all the relevant instances of a particular class, out of all the instances that truly belong to that class in the dataset.

Recall = TP / (TP + FN)

F1 score: The F1 score is a metric in machine learning that combines both precision and recall into a single value. It is particularly useful when there is an imbalance between the classes or when both false positives and false negatives need to be considered.

F1-score = 2 * (Precision * Recall) / (Precision + Recall)

The model with the highest accuracy will be save for deployment. Joblib library was used to save the model. Joblib is a library that help to save and export machine learning models to production environment.

4. RESULTS

The following table and figures below show the performance evaluation of the models.

Table 2: Model performance and results

Trained model	Test Accuracy	Precision	Recall	f1-score
Logistic Regression	0.9657	0.97	0.96	0.96
Decision Tree	0.9981	1	1	1
Random Forest	1	1	1	1

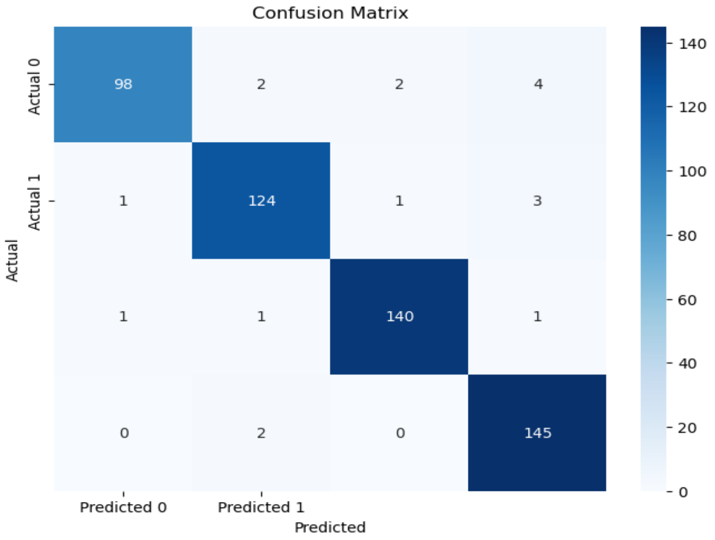


Figure 6: Logistic regression confusion matrix

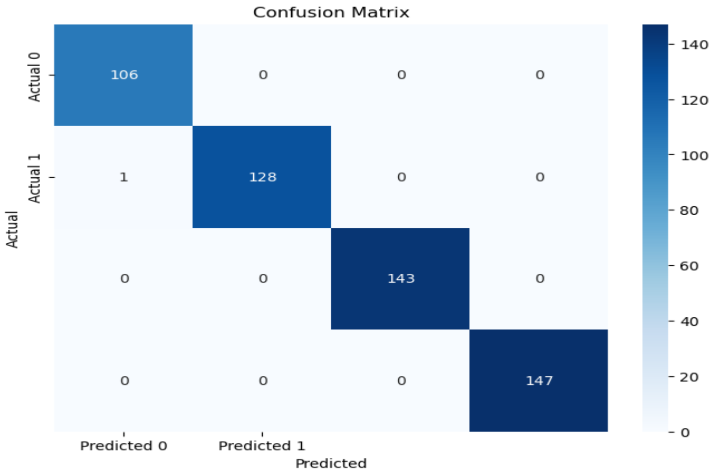
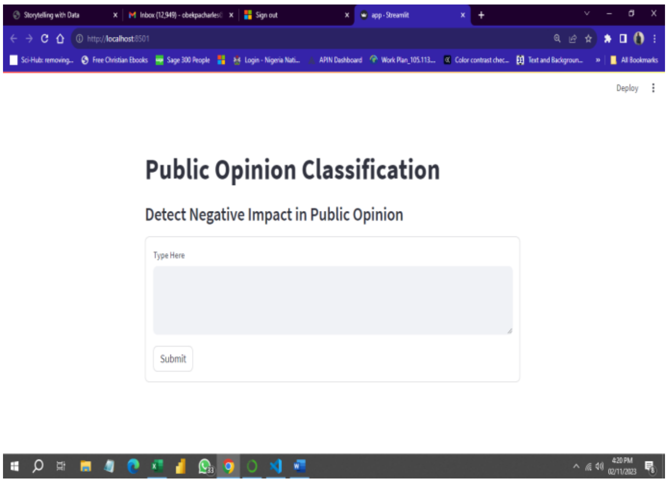


Figure 7: Decision Tree Confusion Matrix

5. DEPLOYMENT

After deploying the model register users can access the user interface in the form of html text field and type their comments and then submit using the submit button as is no Deployment ensures our model is made available for public use; the selected model (Logistic regression) was deployed locally using the open source Streamlit Python library.

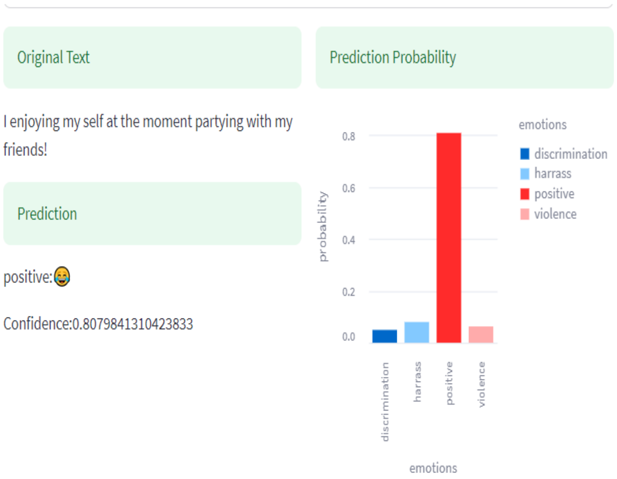
Streamlit is an open source, light weight Python library that is used to deploy machine learning models to production [19]. It lets you create and share amazing data apps with fewer efforts and lines of code.



Public Opinion Classification

Detect Negative Impact in Public Opinion

Figure 8: User interface to the deployed model



I enjoying my self at the moment partying with my friends!

positive:😀

Confidence:0.8079841310423833

Figure 9: Final prediction from the model

The above experiments demonstrated promising results in classifying hate speech. Decision Tree and Random Forest classifiers tends to overfit the data while the Logistic regression classifier provided a nuanced and improved results during testing informing the decision to use the classifier for deployment.

6. CONCLUSIONS

In the face of an increasingly interconnected digital landscape, the identification and mitigation of hate speech emerges as a critical imperative for the preservation of inclusive and constructive public discourse. This study has embarked on a journey at the intersection of technology and societal well-being, leveraging machine learning approach to dissect and classify the detrimental impact of hate speech on public sentiment.

Through an extensive empirical investigation, we have demonstrated the efficacy of our machine learning models in discerning and classifying the impact of hate speech and also isolating the predominant hate rhetoric in an area.

Furthermore, our analysis reveals the profound impact of hate speech on public sentiment. This not only highlights the emotional toll borne by affected individuals and communities but also underscores the potential for polarization and division within society.

However, our work is not without its limitations. Challenges persist in discerning subtle linguistic constructs, and the ever-evolving nature of hate speech demands continued vigilance and refinement in model training. Furthermore, the dynamic nature of online discourse necessitates ongoing efforts to adapt and refine our approach.

In summary, this study advances a multifaceted approach to addressing the impact of hate speech on public opinion and identify the hate sentiment in a given location. By harnessing the power of machine learning, we have endeavored to illuminate the intricate dynamics of hate speech, contributing to a safer, more inclusive digital sphere. As we look to the future, our hope is that this research serves as a catalyst for continued innovation and collaboration in the pursuit of a more empathetic and understanding online community.

7. ACKNOWLEDGMENTS

I express my profound and sincere gratitude to the post graduate coordinator Dr. Adeyelu Adekunle, Ekle Francis Adoba and my supervisors for tremendous support in this research and to my family for the financial and moral support accorded me.

8. REFERENCES

[1] Lutfiye S, M, A. 2019. Identification of Offensive Language in social media.

[2] Zafer A, Amr, T. (2019).p *Automatic hate speech detection using killer natural language processing optimizing ensemble deep learning approach*. Springer-Verlag GmbH Austria.

[3] Dewa, A, N, T, Ketut, G, D, P. 2021. Hate Speech Classification in Indonesian Language Tweets by Using Convolutional Neural Network.

[4] Sattam. A. (2018). *A lexicon based method to search for extreme opinions*. PLOS | ONE.

[5] Steiger, K. R. (2020). Online hate: Introduction into motivational causes, effects and regulatory contexts.

[6] Raphael, C. (2011). Fighting Hate and Bigotry on the Internet. Policy & Internet.

[7] Raghad, A, Hend, A. (2020). A Deep Learning Approach for Automatic Hate Speech Detection in the Saudi Twittersphere. Applied Sciences.

[8] Gabriel, A, De, S, Marjory, Da, C. (2019). Automatic offensive language detection from Twitter data using machine learning and feature selection of metadata. http://alt.qcri.org/semeval2019.

[9] Omar, S, Mohammed M, H, Kayes, R, N, Iqbal, H, S. (2020). Detecting Suspicious Texts Using Machine Learning Techniques. Applied Sciences.

[10] Varsha, P, Manish, J, Prasad, A, Joshi, M, M, Tanmay J. (2020). Using Machine Learning for Detection of Hate Speech and Offensive Code-Mixed Social Media text.

[11] Sindhu, A, Sarang, S, H, K, Zafar, A, Sajid, K, Ghulam, M. (2020). Automatic Hate Speech Detection using Machine Learning: A Comparative Study. International Journal of Advanced Computer Science and Applications.

[12] Mohiyaddeen, S, S. (2021). Automatic Hate Speech Detection: A Literature Review. International Journal of Engineering and Management Research.

[13] Williams, R. (2021). Multinomial Logit Models - Overview.

[14] Lior Rokach, Oded, M. (2015). Data Mining with Decision Trees Theory and Applications.

[15] Jonathan, K, A, Kassim T, Wilhemina, A, P, Sandra, A, Harriet, A, D, Emmanuel, O, O, Samuel, A, A, John, E. (2023). A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. doi: https://doi.org/10.1016/j.dajour.2023.100163

[16] Taherdoost, H. (2021). Data Collection Methods and Tools for Research; A Step-by-Step Guide to Choose Data Collection Technique for Academic and Business Research Projects. International Journal of Academic Research in Management.

[17] Anubha Parashar, Apoorva, P, Weiping, D, Mohammad, S, Imad, R. (2023). Data Preprocessing and Feature Selection Techniques in Gait Recognition: A Comparative Study of Machine Learning and Deep Learning Approaches. Elsevier.

[18] Teodor, F, David, I, M, J, Helena, H. (2021). Data Labeling: An Empirical Investigation into Industrial Challenges and Mitigation Strategies. DOI: 10.1007/978-3-030-64148-1_13.

[19] Arul S, Muskaan, D, Kowsigan, M. (2022). Indian Crop Production: Prediction And Model Deployment Using Ml And Streamlit .

[20] Spector, A. Z. 1989. Achieving application requirements. In Distributed Systems, S. Mullender

International Journal of Computer Applications Technology and Research
Volume 13–Issue 02, 08 - 16, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1302.1002

An APN Authentication Model for a Secure Enterprise Wireless Local Area Network

Robert Mwenda
Department of Computer Science
Chuka University, Kenya

Dr. Lucy Waruguru
Faculty of Computer Science
KCA University, Kenya

Dr. Joseph Mbugua
Department of Information Science
Garissa university, Kenya

Abstract

The Use of Wireless Networks is on the rise and many organizations are deploying WLANs to support their critical business applications. With the rising demand and use of wireless local area networks and the subsequent implementation of these networks by organizations, enterprises have been exposed to a lot of challenges and we have seen an increase in cybercrime and most of these attacks have been launched from wireless networks. Therefore, in this paper we will investigate the security threats and vulnerabilities that are there due to the inherent open nature of wireless communications and come up with an effective defense mechanism that will improve the wireless network security. The open system authentication architecture will be subjected to penetration tests and the results will be compared with those from other schemes like the pre- RSN and RSN methods to select the best model for WLAN authentication. The results inferred that the proposed model of authentication that is achieved by adding a nonce to the access point and therefore referred to as access point nonce (APN) authentication scheme is more effective and offer better security.

Keywords: WLAN, wireless security, APN, Authentication model IEEE 802.11, PMK

1. INTRODUCTION

A WLAN is a network that allows devices to connect and communicate without the use of cables and is heavily reliant on radio frequencies for the purpose of data transmission. The devices that are in communication broadcast data frames over a radio frequency interface. A WLAN uses access points and routers to make a connection between devices. All devices that have WLAN enabled on them and are within range are able to receive data frames. Wireless networks are very popular because they have the advantage of client mobility and thus avoid the cost of cabling that would otherwise be incurred by wired networks. The emergence of mobile devices such as laptops, tablets and smartphones that are portable has contributed largely in making WLAN very popular. The paper will measure and test the strengths of IEEE.802.1X EAP authentication and other variables that will be manipulated under the test-bed experiment. There is an effort to build other models like the Pre-Robust Security network designed by IEEE 802.11(1997) Pre-RSN architecture requires a wired equivalent protocol (WEP) is implemented first. This mechanism was expected to provide reasonable security strength that could match the security of wired network. This security solution seemed to have met its goal but it has been found that the security features are very weak. Even with its weaknesses pre-RSN is widely implemented and deployed by users to allow connectivity to hotspots. Pre-RSN models allow the selection of RC4 as their confidentiality protocol and CR-C32 enciphered as their integrity protocol. Wireless implementers are therefore left with the option of selecting either an open or pre-shared key this makes it limited in scope because it focuses on securing the wireless path between a client device and an access point.

The other model which is the robust security network architecture, provides a system of enhanced authentication mechanism for the access point and client station. It has a session specific key derivation and management framework and it also implements an enhanced data encryption. RSN requires that all the client stations on wirelesses network to be configured with TKIP or CCMP cipher suites and that also the stations create a pre-shared master key (PMK). RSN insists on the selection of EAP method for IEEE 802.1X authentication, but there are many EAP methods with varying weaknesses and strengths. RSN fails by not having a guideline to be followed when selecting an EAP method for IEEE.802.1X authentication and this creates a problem of either having a likelihood of choosing a weak authentication method or even implementing a strong authentication method wrongly. RSN has the limitation of lacking a way of selecting or configuring security of important components.

These previous approaches therefore lack important components and they are not comprehensive enough to address the many security issues that are related to authentication and access control in wireless local area network. Again while the use of these approaches has enabled security implementers choose between suitable and unsuitable authentication methods, none of these approaches has been able to provide a tool that can enable an implementer to visualize the security level that is expected from implementing a set of security features and configurations. The rest of the paper is structured as follows, first we present the literature review, then materials and methods, then we discuss the results obtained from the lab experiments and then discussion and conclusion.

2. RELATED WORK

There have been past efforts by researchers in trying to solve poor implementation of authentication mechanisms and poor access control methods in WLANs. A number of models have been implemented and these are: Pre-Robust Security Network (Pre-RSN) Model was designed by IEEE 802.11(1997). It’s the first security implementation approach. Pre-RSN architecture requires a wired equivalent protocol

(WEP) is implemented first. This mechanism was expected to provide reasonable security strength that could match the security of wired network. This security solution seemed to have met its goal but it was later established that the security features are very weak. Even with these weaknesses Pre-RSN WLANs are widely implemented and deployed in organizations like universities to allow users connect to hotspots.

Pre-RSN models allows the selection of RC4 as their confidentiality protocol and CR-C32 enciphered as the integrity protocol that they use. Implementers are left with the choice of selecting from two authentication mechanisms and access control methods; which are open and pre-shared key. It is therefore limited in scope because it focuses on securing the wireless path between a client device and access point.

Robust Security Network (RSN) Architecture this provides a system of enhanced authentication mechanism for the access point and client station. It introduced a session specific key derivation and management framework and it also enhanced data encryption. RSN requirement is that all the client's devices on a wireless Network be configured with TKIP or CCMP cipher suites and they be able to create a pre-shared master key (PMK)

Even though RSN insists on the selection of EAP method for IEE 802.1X authentication, there are many EAP methods with varying weaknesses and strengths. RSN does not have a guideline to be followed when selecting an EAP method for IEEE.801.1X authentication and this creates a possibility of choosing weak authentication method or implementing strong authentication method wrongly. RSN is limited because it lacks a mechanism of selecting/or configuring security features of important components like user databases, client drivers or client utility.

3. MATERIALS AND METHODS

The materials and methods used in this paper include a comprehensive literature search, data extraction, and analysis. The literature search was conducted using various online databases, including Google Scholar, IEE Explore, ACM digital library, and Science Direct.

The inclusion criteria for selecting article for this review paper was that they should be published in peer-reviewed journals, conference proceedings, or book chapters and be related to the wireless security and networks. The exclusion criteria were articles that did not meet the inclusion criteria or were not related to the research question. After conducting the literature search, the articles were screened base on their titles and abstracts. The selected articles were then reviewed in full and data extracted from them. The data extraction process included information on the authors, publication year, research methods, study objectives, key findings and limitations.

The data extracted from the articles was analyzed using a thematic analysis approach.

Data from the selected articles will be extracted using a standardized form that includes the following information: authors(s), year of publication, title, research question, study design, sample size, data sources, data analysis methods, key findings and analysis.

The limitations of this paper include the possibility of missing relevant articles due to the exclusion criteria and the potential bias in the selection and interpretation of the articles. To mitigate these limitations, we used a comparative literature search, screened the article based on strict inclusion criteria, and used a systematic approach to data extraction and analysis.

3.1 The problem formulation

Before setting a penetration testing lab, a lot of considerations must be made to include all the threats to be tested for; this will require some planning. A properly done penetration testing can provide very important information to security implementers about the areas lacking in security within their network. A good penetration testing would use the following process.

1. Reconnaissance- at this stage the attacker gathers as much data about the target network as possible. This would be done by a number of tools and techniques, but it is also possible to obtain information available publicly on the internet.
2. Enumeration-The initial step in attack on the network. This is where the attacker successfully establishes a connection to the target node. At the end of enumeration, the attacker will have obtained important data such as domain name, operating system version, user accounts, access port numbers and many others.
3. Exploitation- at this stage the actual attack based on the information acquired is carried out. The objective being to gain unlimited access to the network if possible.
4. Documentation- the vulnerabilities that were exploited are documented and a record kept.
5. Mitigation- when a solution is found based on vulnerabilities identified is found
6. Documentation- the mitigation steps are recorded and maintained

3.2 Setting up a penetration test-bed

This paper, we will use a test bed that will simulate an enterprise network. A selection of the required hardware and software will be afore mentioned. The section below will discuss this.

3.2.1 Required Resources

Wireless access points. The network to be attacked is a WLAN so the access point is of critical importance in identifying flaws.

- Targets with Wi-FI (Wireless Fidelity) compliant network cards to simulate an ideal enterprise WLAN environment, a number of nodes will connect to an access point to simulate a standard network activity and so they will be required to have a wireless network card on them
- Attack Computer the computer of the attacker will have a wireless network adapter which is able to do sniffing and packet injection. It should also be compatible to kali Linux which will be used to carry out the attack.
- Kali Linux –Kari Linux is a UNIX based operating system used for carrying out penetration tests and digital forensics. The operating system is equipped with all soft wares that are needed to carry out the

tests. It has tools like Air crack, Kismet, N-map, Wire shark, wids.py that are used for reconnaissance and infiltration.

3.2.2 Attacks to be carried out

The following attacks will be carried out. DOS (Denial of Service attack) and in this will use MDK3, a dos tool that is normally included in Kali Linux (Linux) and it will be used to carry out denial of service attacks through de-authentication WPA (WIFI Protected Access) Hacking- attacks against WPA2, which is a protocol that normally secures wireless communication, will be carried out using two tools- the air crack suite and pyrite. These tools will be installed in the back box operating system.

Phishing attacks-in this attack an evil twin access point will be set up and a de-authentication attack will be done and also vulnerable users will be tricked into divulging their password. This paper proposes a method of authentication that is achieved by adding a nonce to the access point and therefore referred to as access point nonce (APN) authentication scheme. This will improve on the existing open system authentication scheme.

3.2.3 Design implementation

A Simulation model, mimicking an enterprise WLAN network has been configured. Access points using WPA2 security, will be tested with different levels of protocol ability. There will be a web server on the network which will be subjected to denial of service attacks.

3.2.4 Attacking WLANs

The WPA2 protocol can have two modes, we focus on WPA-2 PSK (pre-shared key), and WPA enterprise. We will conduct a dictionary attack against WPA2-PSK, and then a brute force attack. However, because of limitations due to resources a full scale brute force attack will not be possible and thus only a proof of concept will be provided.

3.2.5 Attacking WLAN authentication

WPA2-PSK is widely deployed especially in home, and coffee shop networks as the standard authentication scheme. WPA2-PSK authentication is by a key known as PTK (Pairwise Transient Key) that encrypts sessions between the client and access point. The PTK is made up of the pre shared key, and these parameters: SSID (service set identifier), the A Nonce (a random number sent by the AP to the device to connect) the S Nonce (a random integer but generated by the client in response to the A Nonce), the client MAC address and BSSID (Basic service set Identifier) this is called a four-way handshake.

The WPA2 authentication process and the steps involved are as follows:

1. The AP sends an A Nonce to the client when it receives a connection request.
2. The client node sends a S Nonce+ a random integer
3. The AP constructs a GTK (Group Temporal Key) from this, and sends it with another randomly generated integer.
4. The Client responds with an acknowledgement of this value

An attacker eavesdropping on the network can be able to obtain all four parameters mentioned, leaving only pre shared key unknown. A dictionary attack will try a range of words included in a previously compiled list and tries against the captured file till there is a match.

4. WLAN VULNERABILITIES

A WLAN that is seen to be secure must have; confidentiality, integrity availability and access control and authentication. (Sheila et al, 2017) confidentiality ensures that all data frames before and after authentication are not accessed by any entity that is not authorized and integrity ensures that alterations are not made on data frames by entities that have no authority. Availability makes sure that at all times a legitimate client or individual user can access a WLAN resource uninterrupted. Access control prevents client devices or even users from accessing a WLAN resource when they have not been duly authenticated

Authentication proves that the device or individual trying to associate with the AP is who it claims to be (P Sathish, 2017).

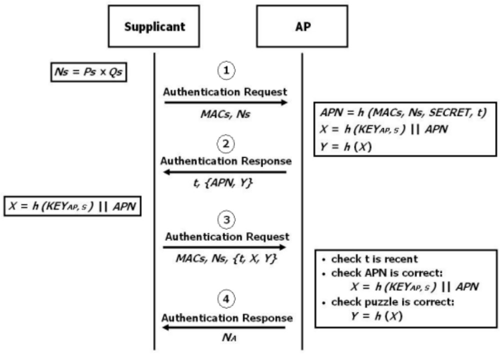
For an intruder to launch an attack on a WLAN, they must be near and within the range of the coverage of the access point, unlike in wired networks where an attacker must gain physical entry. The access rights of a client station to the wireless network are denied until proper and secure authentication has taken place. The WLAN must also guarantee that a secure authentication takes place. There are a number of attacks that affect WLANs and the mainly exploit weaknesses in the authentication mechanisms that are in place. These attacks compromise the availability of a WLAN, and its Confidentiality and Integrity of the authentication and access control traffic

4.1 The APN authentication procedure

This paper has proposed a method of authentication that is achieved by adding a nonce to the access point and therefore referred to as access point nonce (APN) authentication scheme. This will improve on the existing open system authentication scheme. This method is of the assumption that there is existence of a temporary secret key and that this key is shared between the client stations and the AP. the reason why there is this pre shared key between these devices is so that a trust relationship is initially created between the client station and the access point with which it will associate with and with which it will later exchange the identity tokens

The shared key that is generated can only be used for a limited period of time because after the two entities conduct a successful mutual authentication, the key will be dynamically updated. Because of this these dynamic keys do not require to be proof to active attacks and they are made to be easy to implement and very simple

The APN method that is being proposed by the research will use the client machine which is the supplicant will in normal circumstances trigger the APN authentication once the discovery phase is complete and where the MAC address of the target AP has been discovered from the probe responses that the AP sends. the Supplicant will then generate two large primes (Ps and Qs) and then goes forward to compute its identity token (Ns=PsxQs) and from there the client will send the initial authentication request to the AP. to connect the management frame from the client will encapsulate the MAC address of the client and its identity token Ns as shown



4.2 The proposed authentication procedure

Once the target AP receives the authentication request, it will scan to find out if there is an existence of an AP nonce that has been attached to this request. If the request that was received to authenticate from the station lacks the nonce, then the AP will generate a nonce and this nonce will be derived from a cryptographic hash function that is computed using the client station MAC address, its identity token and a secret that can only be known by AP and the current timestamp.

A secret that is known to the AP only and the current time tamp. The secret is very important because it will help prevent the forgery of the nonce by a third party. The reason for this is because it is practically not possible for an attacker to be able to generate a nonce that is acceptable by the AP, while not knowing the value of this secret. Replay attacks are prevented by including a time stamp on the secret. The APN can be generated as shown below

APN=h (MACs Ns, SECRET,t)…………………1

The next step is that the AP will bind the nonce and the identity of the client, so that the MAC address of the client cannot be trusted alone since MAC addresses can easily be spoofed. This is done by the AP validating the client by challenging it with a puzzle constructed in such a way that only a legitimate client that knows the shared key(KEYap,s) can easily solve it. This is achieved by the AP fist generating a pre-image through hashing the clients shared key and joining the output with the APN, then a puzzle image Y is computed by hashing the pre image

Pre- image: x=h (KEYaps) ||APN…………………………2

Image y=h(x)……………………………………….…..3

The puzzle is meant to be difficult and this is achieved by removing the first 128 bits of X, this means that the access point nonce itself is used as part of the image that is used to form the puzzle but alongside Y. once the puzzle has been successfully constructed, the access point will attach a timestamp and the constructed puzzle to the authentication frame response which is sent to the STA. The authentication response frame contains a field called status code and this code is used to display the results of authentication request that were done previously.

The puzzle challenge will be required by the client station device when making the initial authentication request. If the APN puzzle solution is not attached to this request, the status code is set to a reserved code for that response. When on reserved code mode, it means that an APN puzzle challenge is needed and so the AP will terminate the session and will not store any information

The client station will obtain the puzzle from the probe response and it will go ahead to compute the puzzle solution for the challenge by hashing the shared key. Only legitimate clients know the secret key. To solve the puzzle then, the client is only required to generate the key digest and because of this only a single hash operation is required to be carried out at the client station.

Illegitimate stations that do not have access to the shared key and want to solve the puzzle, must conduct a brute force attack and search all of the 128 bits' key space and this is practically infeasible

The shared key must be refreshed each time the mutual authentication process is complete. The refresh update is done after every 400 milliseconds once the key digest is produced, this action protects against an attacker who manages to discover the 128-bit hash and obtains the key.

Upon the successful solving of the puzzle by the client, it will transmit another authentication request that has the similar identity token and time stamp and the puzzle solution (X and Y).

To ensure that the requests that come from the AP are legitimate the following checks are made:

- **TIME STAMP**

The access point looks at the timestamp attached to the frame to compare with the current time to ensure that it is recent. This checks against replay attacks and any attempt of reusing the puzzle.

- **APN**

Using a computation method, the AP will re compute an APN. For APN to be proved as valid, the computed APN must match with the last 128 bits of X. an APN that is not valid means that the nonce was forged or could also mean that the request was changed. All frames that have their APN as invalid are terminated immediately.

The Access point nonce, allows for the binding of the clients MAV adder together with its identity token. But since the MAC address cannot be trusted in the WLAN for fear of mac address spoofing, this binding requires another layer of protection that will make certain the identity token is mapped to the legitimate identity.

- **Puzzle Verification**

A client is considered legitimate only when they have the correct puzzle solution. In this puzzle the client identity token is bound with the trusted shared key. For this reason, when the client supplies a puzzle solution and the correct identity token that was attached to it, it is verified as a legitimate client.

When the client passes all the three checks above it is then viewed to be a legitimate device and it can be allowed to associate and access the upper layer authentication

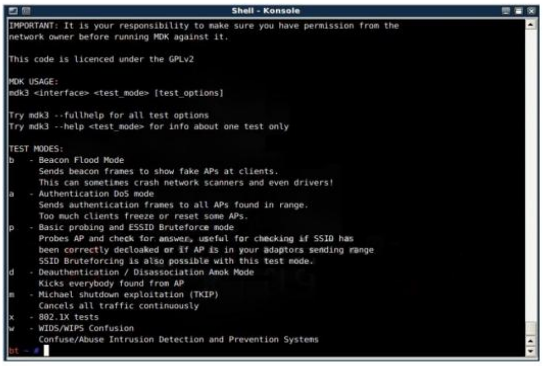
5. RESULTS AND ANALYSIS FROM THE LAB EXPERIMENTS

This section will analyses the effect of attacks carried out on WLAN from the simulation. Attacks carried out were, WLAN DoS attacks like De- authentication flooding and association flooding. The results are then briefly presented.

The researcher used MDK3 which is available free on open source to perpetrate the attacks on the access point station.

MDK3 has several flooding modes available as shown by the figure below

The first attack is carried out when de-authentication frames have been spoofed with the access point (AP) real MAC address, are repeatedly sent to the client that is legitimately associated to the AP, from the attacker fake AP



```
IMPORTANT: It is your responsibility to make sure you have permission from the
network owner before running MDK against it.

This code is licenced under the GPLv2

MDK USAGE:
mdk3 <interface> <test_mode> [test_options]

Try mdk3 --fullhelp for all test options
Try mdk3 --help <test_mode> for info about one test only

TEST MODES:
b   - Beacon Flood Mode
      Sends beacon frames to show fake APs at clients.
      This can sometimes crash network scanners and even drivers!
a   - Authentication DoS mode
      Sends authentication frames to all APs found in range.
      Too much clients freeze or reset some APs.
p   - Basic probing and ESSID Bruteforce mode
      Probes AP and check for answer, useful for checking if SSID has
      been correctly decloaked or if AP is in your adaptors sending range
      SSID Bruteforcing is also possible with this test mode.
d   - Deauthentication / Disassociation Amok Mode
      Kicks everybody found from AP
m   - Michael shutdown exploitation (TKIP)
      Cancels all traffic continuously
x   - 802.1X tests
w   - WIDS/WIPS Confusion
      Confuse/Abuse Intrusion Detection and Prevention Systems
bt ~ # 
```

Figure. 1 Example of an image with acceptable resolution

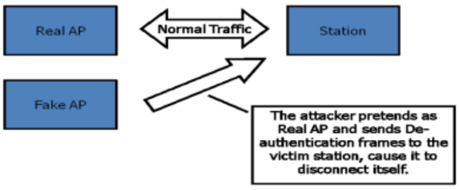
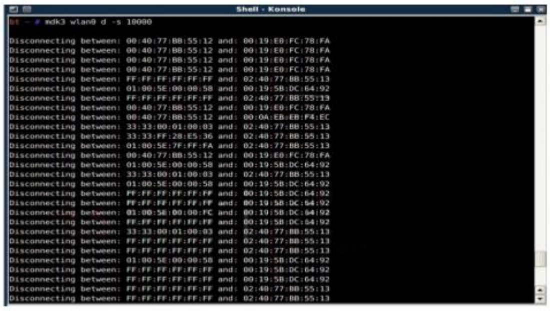

Real AP
Normal Traffic
Station
Fake AP
The attacker pretends as Real AP and sends De-authentication frames to the victim station, cause it to disconnect itself.

Figure 2. De-authentication Flooding attack**.**

The diagram shown below, shows the de-authentication flooding attack being perpetrated using MDK3. The client MAC addresses are on the left hand column and the MAC addresses of the AP are on the right hand side. All the clients on the network associated to the AP are thrown out of the network and disconnected from the network up until when the attack is halted

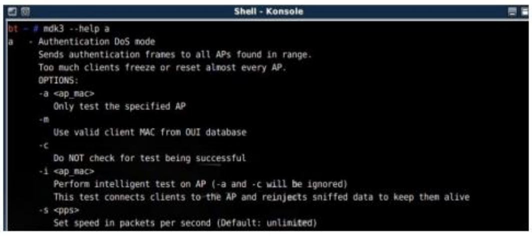


```
bt ~ # mdk3 wlan0 d -s 10000

Disconnecting between: 00:40:77:BB:55:12 and: 00:19:E0:FC:78:FA
Disconnecting between: 00:40:77:BB:55:12 and: 00:19:E0:FC:78:FA
Disconnecting between: 00:40:77:BB:55:12 and: 00:19:E0:FC:78:FA
Disconnecting between: 00:40:77:BB:55:12 and: 00:19:E0:FC:78:FA
Disconnecting between: FF:FF:FF:FF:FF:FF and: 02:40:77:BB:55:13
Disconnecting between: 01:00:5E:00:00:58 and: 00:19:5B:DC:64:92
Disconnecting between: FF:FF:FF:FF:FF:FF and: 02:40:77:BB:55:13
Disconnecting between: 00:40:77:BB:55:12 and: 00:19:E0:FC:78:FA
Disconnecting between: 00:40:77:BB:55:12 and: 00:0A:EB:EB:F4:EC
Disconnecting between: 33:33:00:01:00:03 and: 02:40:77:BB:55:13
Disconnecting between: 33:33:FF:28:E5:36 and: 02:40:77:BB:55:13
Disconnecting between: 01:00:5E:7F:FF:FA and: 02:40:77:BB:55:13
Disconnecting between: 00:40:77:BB:55:12 and: 00:19:E0:FC:78:FA
Disconnecting between: 01:00:5E:00:00:58 and: 00:19:5B:DC:64:92
Disconnecting between: 33:33:00:01:00:03 and: 02:40:77:BB:55:13
Disconnecting between: 01:00:5E:00:00:58 and: 00:19:5B:DC:64:92
Disconnecting between: FF:FF:FF:FF:FF:FF and: 00:19:5B:DC:64:92
Disconnecting between: FF:FF:FF:FF:FF:FF and: 00:19:5B:DC:64:92
Disconnecting between: 01:00:5E:00:00:FC and: 00:19:5B:DC:64:92
Disconnecting between: FF:FF:FF:FF:FF:FF and: 00:19:5B:DC:64:92
Disconnecting between: 33:33:00:01:00:03 and: 02:40:77:BB:55:13
Disconnecting between: FF:FF:FF:FF:FF:FF and: 02:40:77:BB:55:13
Disconnecting between: FF:FF:FF:FF:FF:FF and: 02:40:77:BB:55:13
Disconnecting between: 01:00:5E:00:00:58 and: 00:19:5B:DC:64:92
Disconnecting between: FF:FF:FF:FF:FF:FF and: 00:19:5B:DC:64:92
Disconnecting between: FF:FF:FF:FF:FF:FF and: 00:19:5B:DC:64:92
Disconnecting between: FF:FF:FF:FF:FF:FF and: 02:40:77:BB:55:13
Disconnecting between: FF:FF:FF:FF:FF:FF and: 02:40:77:BB:55:13
```

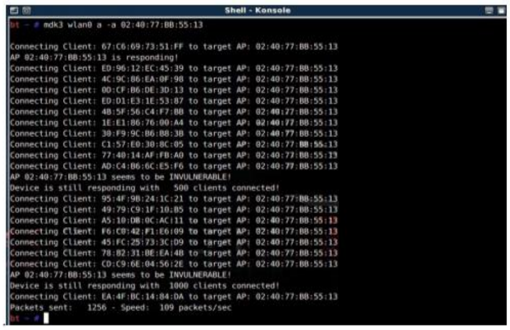
Fig 3. De-authentication/ Disassociation Attack Mode

From this experiment it is depicted that even at a very low rate, for example a transmission of a frame per second flooding, can be able to block the attacked client from associating to the AP. Whenever the client tries to re-establish a connection, the attacker sends another spoofed DE authentication frame that immediately ends the new connection. Because of this activity the throughput of the client drops to the lowest which in this case is zero during the attack duration MDK3 tool is also able to run in an Authentication DoS mode that enables it to generate a series of spoofed authentication requests that are continuously targeted to the AP being attacked. The attacked AP under this circumstance gets too busy processing fake requests in an attempt to provide normal service to legitimate clients. Figure 17 below illustrates the available options in the MDK3 Authentication DoS mode.



```
bt ~ # mdk3 --help a
a   - Authentication DoS mode
      Sends authentication frames to all APs found in range.
      Too much clients freeze or reset almost every AP.
      OPTIONS:
      -a <ap_mac>
         Only test the specified AP
      -m
         Use valid client MAC from OUI database
      -c
         Do NOT check for test being successful
      -i <ap_mac>
         Perform intelligent test on AP (-a and -c will be ignored)
         This test connects clients to the AP and reinjects sniffed data to keep them alive
      -s <pps>
         Set speed in packets per second (Default: unlimited)
```

Under normal circumstances, when the client request to authenticate, these authentication requests are sent to the specified AP (MAC address shown with the –an option in the shell command line) and when it's at the maximum rate that is possible. A report on the AP status is done after each 500 packets are transmitted. On the launch of the first attack, the AP is still be able to respond to new connections that are legitimate. When the attack is continued for a further five minutes, due to the many clients that are connected, the AP is forced freeze. A reboot of the AP station is then necessary to bring the AP back to its normal operating state even after the attack had long been stopped. Figure 18 below shows the Authentication DoS attack in action



```
bt ~ # mdk3 wlan0 a -a 02:40:77:BB:55:13

Connecting Client: 67:C6:69:73:51:FF to target AP: 02:40:77:BB:55:13
AP 02:40:77:BB:55:13 is responding!
Connecting Client: ED:96:12:EC:45:39 to target AP: 02:40:77:BB:55:13
Connecting Client: 4C:9C:86:EA:0F:98 to target AP: 02:40:77:BB:55:13
Connecting Client: 0D:CF:B6:DE:3D:13 to target AP: 02:40:77:BB:55:13
Connecting Client: ED:D1:E3:1E:53:87 to target AP: 02:40:77:BB:55:13
Connecting Client: 4B:5F:56:C4:F7:88 to target AP: 02:40:77:BB:55:13
Connecting Client: 1E:E1:86:76:00:A4 to target AP: 02:40:77:BB:55:13
Connecting Client: 30:F9:9C:B6:88:3B to target AP: 02:40:77:BB:55:13
Connecting Client: C1:57:E0:30:8C:05 to target AP: 02:40:77:BB:55:13
Connecting Client: 77:40:14:AF:FB:A0 to target AP: 02:40:77:BB:55:13
Connecting Client: AD:C4:B6:6C:E5:F6 to target AP: 02:40:77:BB:55:13
AP 02:40:77:BB:55:13 seems to be INVULNERABLE!
Device is still responding with   500 clients connected!
Connecting Client: 95:4F:9B:24:1C:21 to target AP: 02:40:77:BB:55:13
Connecting Client: 49:79:C9:1F:10:85 to target AP: 02:40:77:BB:55:13
Connecting Client: A5:10:DB:0C:AC:11 to target AP: 02:40:77:BB:55:13
Connecting Client: F6:C0:42:F1:E6:09 to target AP: 02:40:77:BB:55:13
Connecting Client: 45:FC:25:73:3C:D9 to target AP: 02:40:77:BB:55:13
Connecting Client: 78:82:31:BE:EA:48 to target AP: 02:40:77:BB:55:13
Connecting Client: CD:C9:6E:04:56:2E to target AP: 02:40:77:BB:55:13
AP 02:40:77:BB:55:13 seems to be INVULNERABLE!
Device is still responding with  1000 clients connected!
Connecting Client: EA:4F:BC:14:84:DA to target AP: 02:40:77:BB:55:13
Packets sent:   1256 - Speed:  109 packets/sec
bt ~ # 
```

Fig. 4 Authentication DoS in Acton

For the purpose of measuring the effect of attack on the WLAN throughput, continuous TCP packets are generated by the station, and sent to the mobile clients. The moment the client station associated to the AP receives the spoofed de authentication frame, the client is immediately disconnected and it becomes unauthenticated, therefore disconnecting from the network. Figure 19 below shows how the through put of the client under attack remains at zero for whole attack period.

Immediately the attack is stopped, however the throughput returns to normal and the client node is reconnected back to the AP. There is similarity on a pair of results obtained when the network is subjected to authentication flooding, and its shown that during the process of authentication flooding attack (from the10th to 25th second) only a few of the legitimate packet are transmitted against a huge amount of flooding packets. This is the case because when traffic is flooded, it consumes most of the AP resources and this makes the completely very busy trying to respond to spoofed frames.

The AP through put then drops to as little as ten percent (10%)of its normal operating capacity during the fifteen (15) seconds its under attack and its through put remains low for a few seconds after the attack is stopped. When the attack duration is prolonged for a long period of time, the AP will then ultimately freeze and must then must be rebooted. Flooding with association

requests attack using void11, gives results that are similar to the figure below.

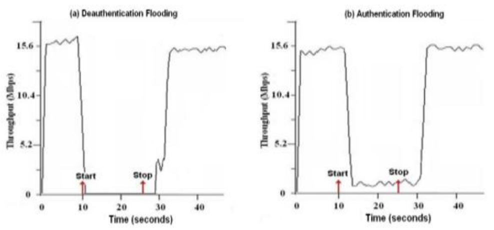
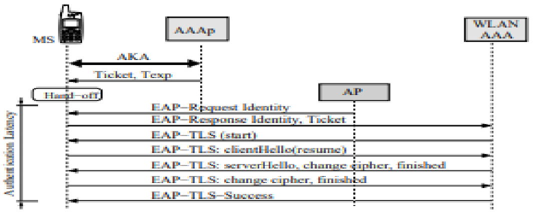


FIG 5. De-authentication and Authentication flooding

From this result, it is clear that a DE authentication flooding attack on WLAN is its most effective attack that causes most damage to the attacked WLANs throughput than damage that can be caused by authentication flooding and association flooding. When WLAN is under attack, the introduced Spoofed DE authentication frames can totally bring down the wireless network such that users who are legitimate are completely denied access to the network. The experiment carried out has demonstrated that it is easy to launch and attack WLANs by subjecting it to DoS attacks and when such WLAN are not properly protected, the WLAN becomes very vulnerable to many attacks and flooding attacks

5.1 Discussion of results

The 802.1x framework put in RSN allows for the exchange of the credentials of the client in a secure way. By this action any unauthorized access to the network is stopped because in this scheme, authentication of the devices is performed before a client is assigned with a network IP address. The standard ensures that the decision to allow authentication are made by the RADIUS server and this removes the need of configuring passwords in every station or Access point. This method therefore allows stations to be authenticates with credentials other than their MAC Address. The credentials of the supplicant (client station) are passed securely to the Access point (authenticator) through a secure EAP method. They are then channeled to the authentication server through EAP that is in RADIUS.


MS
AAAp
WLAN AAA
AKA
Ticket, Texp
Hand-off
AP
Authentication Latency
EAP–Request Identity
EAP–Response Identity, Ticket
EAP–TLS (start)
EAP–TLS: clientHello(resume)
EAP–TLS: serverHello, change cipher, finished
EAP–TLS: change cipher, finished
EAP–TLS–Success

By use of proactive context transfer and ticket forwarding, the network latency is reduced to 36.8% and EAP-TLS latency to 23.1%.

Several previous research studies have proposed that to secure WLANs against DoS attacks, a way of authenticating management frames using the various cryptographic techniques be found. With such solutions there are a number of limitations because the only focus is on improving security with additional cryptographic methods and operations, but they lack the details on the possible overheads to security that come as a result of meeting the required quality of service for real time applications.

These solutions might also not be able to protect the networks against the high rate of flooding attacks and cannot also enable the visualization of the security features and their selection to a safer more, efficient WLAN implementation.

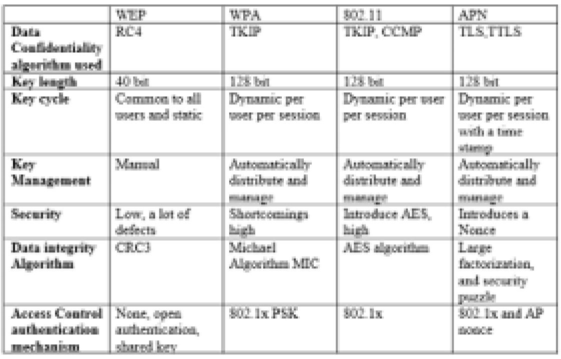
For implementers to enhance security of enterprises WLANs, and mitigate against many attacks like the DoS, a protection link layer, against attacks is necessary. Such protection should happen before the Access point gives any resources that can enable an establishment of a connection.

Denial of Service attacks are able to succeed primarily because they can be carried out before the 802.11x authentication completes. When there is a possibility of a lightweight authentication taking place prior to the process of association, all of the attacks mentioned earlier cannot occur, but the challenge is that to provide this link-layer protection.

It’s unfortunate that a majority of the providers of WLAN services and wireless internet service providers do not implement link layer security, but instead relies on proprietary solutions that are based on web authentication.

5.1.1 Comparison with traditional results

A comparison between the three aspects of data confidentiality, Integrity and access control was done on the major kinds of wireless LAN security mechanisms as shown on table below



	WEP	WPA	802.11	APN
Data Confidentiality algorithm used	RC4	TKIP	TKIP, CCMP	TLS,TTLS
Key length	40 bit	128 bit	128 bit	128 bit
Key cycle	Common to all users and static	Dynamic per user per session	Dynamic per user per session	Dynamic per user per session with a time stamp
Key Management	Manual	Automatically distribute and manage	Automatically distribute and manage	Automatically distribute and manage
Security	Low, a lot of defects	Shortcomings high	Introduce AES, high	Introduces a Nonce
Data integrity Algorithm	CRC3	Michael Algorithm MIC	AES algorithm	Large factorization, and security puzzle
Access Control authentication mechanism	None, open authentication, shared key	802.1x PSK	802.1x	802.1x and AP nonce

For the purpose of evaluating the impact of the simulation model use of APN authentication and the use of frame validation on the bandwidth of the access point, we ran iperf so that we can be able to generate the various traffic loads ranging from 2 megabytes per second(mbps) to 54megabytes to a receiving station all the way through to an AP when an APN authentication and frame validation is enabled and when it is not enabled but instead using open system authentication, from the results as illustrated in the graph below fig. 6, indicates that it is possible for the bandwidth of the access point in the test bed can clock up to 18 megabytes per second; when the APN authentication is used and there is no effect on the bandwidth performance and therefore right to say that the performance of the AP is not degraded and also no effect on the maximum bandwidth.

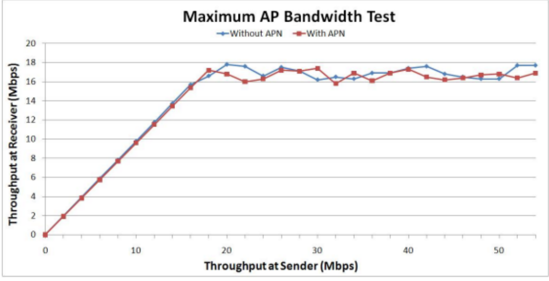


Fig 6 AP bandwidth with and without APN authentication**.**

For the purpose of further evaluating the whether the APN scheme is effective and can offer protection to the WLAN against the many different DoS attacks that are passively targeting the Stations and the access points, at the various stages during the RSNA attempt to establish a connection and using the various tools of attack as earlier mentioned to launch the attacks below.

Attacks carried out before authentication and association

1. Authentication flooding
2. Association flooding

Attacks carried out after securing the communication link

1. De-authentication frame flooding
2. Disassociation fame flooding

Attacks carried the process of authenticating and establishing key

1. Extensible authentication protocol over LAN (EAPOL) –begin flooding
2. Extensible authentication protocol over LAN (EAPOL) –logoff flooding
3. Extensible authentication protocol over LAN (EAPOL) - Failure flooding

The results from experiments that are shown by the table below show that APN can be effective in mitigating from DoS attacks

DoS Attack Type	Without APN Scheme	With APN Scheme
Authentication frame flooding	AP resource depletion	Successful mitigation
Association frame flooding	AP resource depletion	Successful mitigation
Deauthentication frame flooding	STA connectivity loss	Successful mitigation
Disassociation frame flooding	STA connectivity loss	Successful mitigation
EAPOL-Start flooding	AP resource depletion	Successful mitigation
EAPOL-Logoff flooding	STA connectivity loss	Successful mitigation
EAP-Failure flooding	STA connectivity loss	Successful mitigation

To examine how the access points, utilize resources when handling the flooding attacks at high rate, a series of high flooding authentication attack were carried out a rate of 18Mbps and this pushed the AP to its maximum bandwidth capacity. AP central processing unit and the effects on the utilization of the main memory were monitored when DoS flooding is introduced for a period of 10 minutes.

FIG 8 shows how the Access point and the CPU is utilized under the attack of DoS flooding, when the APN authentication is not being used, and the result is that when there is flooding, the load on the CPU is shoots up to almost 80%. This is as a result of the AP is responding to spoofed requests and allocating most of its resources for this purpose. However, when APN authentication scheme is enabled, CPU utilization drops to less than 40% under the same condition. This improved performance and drop in CPU utilization is as a result of the ability that the access point nonce scheme has to identify the attacking spoofed frames, and get rid of them without finding it necessary to store any state information of them. When other flooding schemes are introduced under the same conditions, the same level of load reduction on the CPU was observed.

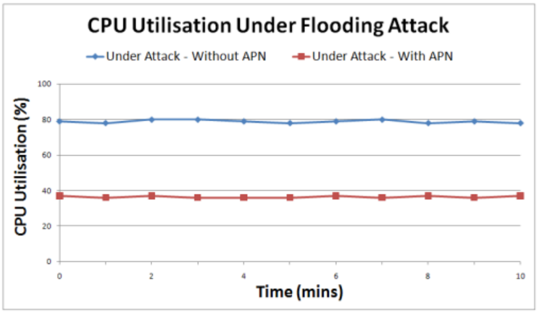


FIG 8. This figure shows the utilization of AP CPU when under a flooding attack

When the AP is not using APN authentication scheme, it is not equipped with the capability of

Identifying spoofed request and it will respond to them and this causes the usage of memory when the WLAN is under authentication flooding attack to continually rise as depicted in the figure 22. On the other hand, when APN authentication is being used, the utilization of the memory of the AP becomes steady

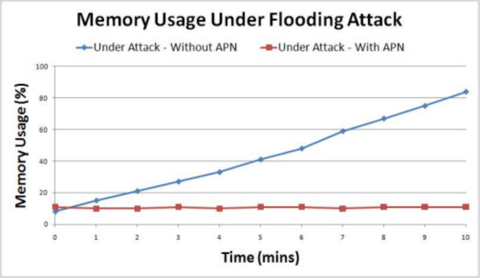


FIG 7. Aps Memory utilization under flooding condition

A de-authentication flooding attack was carried out on the client stations to do an evaluation of effect when stations are under DoS protection. These attacks were launched when stations are configured with APN authentication, and when this scheme is enabled on the AP. The WLAN was attacked with flooding attacks for a period of 15 seconds and as shown in the fig 9 below, when the AP is not configured with APN authentication, and the scheme is not in use, the station gets disconnected immediately on the start of the attack and during this period the AP throughput remains at zero for the entire attack period. On the Introduction of the APN authentication the stations throughput is no longer affected and this is because all the frames that are spoofed are dropped without having an effect on the other legitimate frames

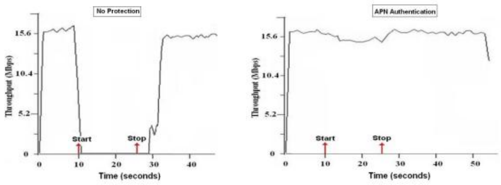


FIG 8 through put under DoS flooding attacks when protected with APN & when WLAN is under no Protection.

6. CONCLUSION AND FUTURE WORK

In this research the security of IEE802.11x was studied and it was found out that there exists a lot of vulnerabilities on the link-layer for DoS attacks that are specific to this standard. Experiments were carried out on the standard to determine and quantify and measure the impact of the DoS attacks that exploit these vulnerabilities. The research further analyzed the mitigation requirements and a number of potential techniques that could prevent network from spoofing and flooding activities. From the results obtained in the experiments carried out in this research, it can be concluded that to address the issue of DoS vulnerabilities, a frame authentication scheme that is lightweight and stateless and that introduces a nonce to the access point, APN authentication is introduced. s. The research recommended that a RSNA be established by the use of an introduction of an APN authentication scheme in preference to the open system authentication. In future since the APN method recommended in this research did not use an intra-domain handoff, that can support APN across multiple domains, we plan to look at this area.

7. REFERENCES

1. Imai, Shin SeongHan and K. Kobara, "Authenticated key exchange for wireless security", *Wireless Communications and Networking Conference 2005 IEEE*, vol. 2, pp. 1180-1186, 13-17 March 2015
2. **.**J.W. Branch, N.L. Petroni, L. Van Doorn and D. Safford, "Autonomic 802.11 wireless LAN security auditing", *Security & Privacy Magazine IEEE Volume 02*, no. 3, pp. 56-65, May-June 2004
3. **.**S.-H. Fang and T. Lin, "Principal component localization in indoor WLAN environments, " IEEE Transactions on Mobile Computing, vol. 11, no. 1, pp. 100-110, 2012
4. S.-H. Fang and T.-N. Lin, "Accurate WLAN indoor localization based on RSS fluctuations modeling, " in Intelligent Signal Processing, pp. 27-30, 26-28 2009.
5. S.-H. Fang, W.-J. Lai, and Y.-C. Liang, "N encryption-based approach for protecting privacy in network-based location systems, " International Conference on Machine Learning and Cybernetics, vol. 1, pp. 377-380, 2017
6. S.-H. Fang, C.-C. Chuang, and C. Wang, "Attack-resistant wireless localization using an inclusive disjunction model, " IEEE Transactions on Communications, vol. 60, no. 5, 2012
7. **1.**L. Eschenauer and V. Gligor, "A key-management scheme for distributed sensor networks", *Proceedings of the 9th ACM conference on Computer and Communication Security*, 2015
8. **.**J. Undercoffer, S. Avancha, A. Joshi and J. Pinkston, "Security for sensor networks", *CADIP Research Symposium*, 2016
9. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and Countermeasures", *Elsevier's Ad Hoc Networks Journal*, vol. 1, no. 2–3, pp. 293-315, 2014
10. H. Chan and A. Perrig, "Security and privacy in sensor networks", *IEEE Journal of Computing*, vol. 36, no. 10, pp. 103-105, Oct. 2003
11. R. Anderson, H. Chan and A. Perrig, "Key infection: smart trust for smart dust", *12th IEEE International Conference on Network Protocols*, Oct 5–8 2004
12. C. Perkins and E. Royer, "Ad hoc on-demand distance vector routing", *Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90-100, 1999.

International Journal of Computer Applications Technology and Research
Volume 13–Issue 02, 17 - 23, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1302.1003

Automation and Robotics in Apparel Industry

Navanendra Singh
National Institute of Fashion Technology, Patna, India

Omkar Singh*
National Institute of Fashion Technology, Patna, India

Vinoth R
National Institute of Fashion Technology, Patna, India

Abhilasha Singh
National Institute of Fashion Technology
Patna, India

Abstract: In a fiercely competitive and rapidly evolving industry such as apparel, effective supply chain management plays a pivotal role. Given the constant fluctuations in customer preferences, the optimization of supply chain processes requires the integration of cutting-edge technologies to achieve maximum efficiency across various activities. This study draws upon data obtained from secondary sources and a comprehensive review of existing literature to delve into the recent developments in supply chain management and technological advancements within the apparel industry. The paper aims to provide a succinct overview of contemporary literature, highlighting the intersection of supply chain dynamics and technological progress, while also identifying new directions in this emerging field. The review emphasizes technologies utilized in supply chain management across both developed and developing countries, encompassing relevant research on automation in the supply chain. Anticipated outcomes include insights that contribute to the understanding of advancements in supply chain practices, serving as a valuable resource for academic researchers in the field.

Keywords: Supply Chain Management, Literature, Research, Optimization, Automation

1. INTRODUCTION

The fashion sector is undergoing a significant transformation due to the impact of the fourth industrial revolution and manufacturing breakthroughs pioneered in Germany. Automation, characterized by the utilization of control systems like computers, is replacing human operators in the execution of industrial machinery and processes. In contrast to mechanization, which involves machines assisting human operators in their physical tasks, automation goes a step further by substantially reducing the reliance on human sensory and mental capabilities. In the contemporary world, a significant portion of manual labor is being replaced by automated and semi-automatic machines. These advanced equipment have not only improved the quality of products and the efficiency of manufacturing plants but have also contributed to reducing lead times, enabling swift operations in today's fast-paced environment.

The term "supply chain management" lacks a universally agreed-upon definition, as indicated by varying interpretations in the literature (New, 1997; Lummus et al., 2001; Mentzer et al., 2001; Kauffman, 2002). Kathawala and Abdou (2003, p. 141) note that SCM "has been poorly defined, and there is a high degree of variability in people's minds about what is meant." In an effort to address this ambiguity, Mentzer et al. (2001) proposed a broad definition that transcends specific disciplines and effectively encompasses the wide range of issues typically associated with the term. We have chosen to adopt this comprehensive definition as the guiding framework for our research, emphasizing its inclusivity and relevance to the diverse aspects covered under the umbrella of supply chain management.

Supply chain management is characterized as the systematic and strategic coordination of conventional business functions and strategies both within a particular company and across interconnected businesses within the supply chain. The primary objective is to enhance the long-term performance of individual companies as well as the overall efficiency of the supply chain. This comprehensive approach encompasses various stages, starting from the production of fibers, textiles, and finished garments, adding three crucial links to the chain before involving distributors and retailers. The supply chain initiation involves the conception of innovative designs, which are then manufactured, distributed, and ultimately sold. For the seamless progression of new products through the supply chain and effective control of inventory flow, the presence of an organized and competent logistics leader becomes imperative.

2. REALTED WORK

Garment manufacturing, recognized for its reliance on manual labor, has seen efforts to introduce automation over the past three decades. Despite the availability of robots for various tasks, many countries continue to rely on manual labor for these processes. Over the last 30 years, there has been a consistent push for companies to automate garment manufacturing operations. Substantial financial investments were made in developed countries, including Europe and the United States, during the 1980s to automate garment production processes. Despite these efforts, achieving widespread automation in the clothing industry proved challenging, although some individual processes were successfully automated.

Numerous research studies have been conducted since the 1980s to explore automation in clothing manufacturing. Currently, several companies are actively innovating new technologies to facilitate the automation process, incorporating robotic hands, automated spreading machines, and sewing robots. Robotic handling devices, employing reconfigurable automatic handling technology, are designed for the garment industry to handle cut fabrics. Each cut component is individually picked and delivered using a high-flow rate vacuum, with predetermined positions to minimize folds and wrinkles.

Automated spreading machines, utilizing robotic technology, are programmed to analyze nap, spreading mode, creases, and fabric conservation during the spreading process onto cutting tables. In the realm of sewing automation, there are two primary options. The first involves sewing machines equipped with multiple high-speed vision cameras that transmit input to actuators. The second option introduces a water-soluble stiffener, temporarily endowing the fabric with metal-like properties, allowing robots to cut, flip, sew, and move fabric pieces accurately.

Industry Size- The magnitude of the industry significantly influences the adoption of automated and advanced technologies. While smaller industries possess advantages such as operational agility, flexibility, and adaptability, they often shy away from automation due to their limited production volumes. In contrast, larger industries prioritize research and development efforts to explore and implement newer technologies.

Export Market- The industry's export potential influences its embrace of advanced technologies, providing a competitive edge, enabling cost-effective product pricing, and better navigating the challenges of a global market. In contrast, industries primarily catering to the domestic market may operate efficiently without relying extensively on advanced tools and automation.

Garment Styles- In various cases, the adoption and automation of advanced technologies are influenced by the styles and designs of clothing. For instance, a manufacturer specializing in men's clothing may opt for automatic attachment equipment for cuffs and collars, which is readily available at a competitive price.

Profitability- Increased profit levels directly impact the purchasing power of the industry.

Available Budget- The industry's ability to embrace new technologies is also shaped by the quality of its capital stock. The allocated budget for technology adoption significantly influences the extent of technological integration. Given the often high costs associated with advanced technologies, a constrained budget for adoption poses challenges in achieving technological competitiveness.

Management Policy- The external relationships of the industry and the policies for adopting advanced technologies are overseen by the top management. Top-level management is engaged in strategic decision-making, planning, implementation, research and development policies, as well as innovation and export policies. The extent of commitment from senior management to technology adoption plays a pivotal role in determining the adoption level of advanced technology within the plant. The commitment of top management to technology adoption is characterized by the alignment of their values and perceptions in favor of and openness to technology adoption. Consequently, an industry with a dedicated technology adoption team is indicative of this commitment.

Technical Skills-

The rising global demand for highly skilled operators has prompted an increased focus on the adoption of automated tools and equipment. Contemporary manufacturing industries are striving to equip operators with diverse skills; however, the availability of skilled operators is dwindling. Advanced technology-based manufacturing systems emerge as a viable solution to address the evolving skill requirements in this scenario.

Competitive Advantage- The globalization of clothing production has intensified competition among global partners, creating a highly competitive atmosphere. In such a context, the adoption of newer technologies and automation becomes crucial to secure a competitive advantage. Industries that gain a competitive edge through the implementation of new technologies are more inclined to embrace them.

2.1. Automation in Fabric Inspection

Fabric inspection, once a manual process, has undergone significant changes. Contemporary approaches include the adoption of techniques such as the Statistical Approach, Spectral Approach, and Model-based Approach for automated fabric inspection. In each of these methods, specialized software or modeling tools manipulate the fabric image to extract information regarding the severity of fabric defects. The defects are subsequently analyzed, and if the number surpasses the predetermined limit, the fabric is rejected.

2.2. Automation in Designing (CAD, CAM)

It represents a digital adaptation of the manual drafting process traditionally conducted on a drafting table with a pencil and ruler (Calasibetta and Tortora, 2005). The predominant manufacturing method in the majority of Ludhiana's apparel units (85%) remains the conventional approach, while 15% have adopted a blend of traditional garment production methods and CAD/CAM technology. Manual grading is still practiced in certain units, followed by digitization for computer integration. Notably, Nahar Fabrics and Sobhagia Sales Pvt Ltd utilize Gerber (AccuMark version-7.6) for digitization, grading, and marker layout. Sobhagia Sales Pvt Ltd and Astor Technologies at Bhandhari Hosiery Exports Limited also employ Indian-made M D CAD software. April Cornell, Superfine Knitters Ltd, and Cotton County Retail Ltd all leverage Modaris and Diamino Fashion Lectra software.

2.3. Automation in Fabric Spreading & Cutting

In mass garment manufacturing, multiple fabric plies are concurrently cut, and the skill of the spreader significantly influences the quality of the cut components, fabric consumption, and waste during the cutting operation. Traditionally, spreading is a manual process that involves several assistants and spreaders working together to handle tasks such as drawing the fabric, laying it out, and controlling the fabric edge on one side. Manual spreading is known for being time-consuming. To address this, automated spreading machines have been introduced for the spreading process, leading to more efficient fabric utilization. Automated spreading machines reduce the dependency on manual labor, resulting in improved efficiency and a reduction in fabric waste.

Automated spreading equipment is operated by one individual, while another person is positioned on the opposite side of the spreading table. The second person's responsibilities include inspecting the fabric edge, eliminating any excessive creases from the fabric layer, and gathering end parts. The implementation of automatic cutting machines has resulted in a notable reduction in both the workforce required and the time expended compared to manual or operator-controlled devices.

Fig. 1. A fully automatic fabric-spreading machine

2.4. Automation in Sewing: Sewbots

The sewing process is the most prevalent method for joining textiles, constituting 85 percent of all joining techniques. Despite being highly dependent on skilled manual labor, sewing contributes to 35 to 40% of overall costs. In a bid to reduce manufacturing expenses, many sewn goods producers have shifted their production facilities to low-wage developing countries in recent decades. Steve Dickerson, a professor at the Georgia Institute of Technology and the founder of Softwear Automation in Atlanta, delved into robotics technology for sewing. This exploration led to the creation of SEWBOT, an autonomous sewing system comprising an automatic sewing machine (ASM), a robotic arm for handling and moving textiles, and budgers facilitating multidirectional cloth movement to facilitate the sewing process.

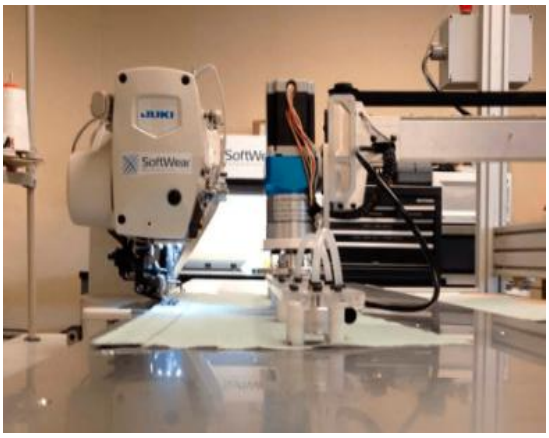


Fig. 2 (a): Automatic sewing machine (ASM)

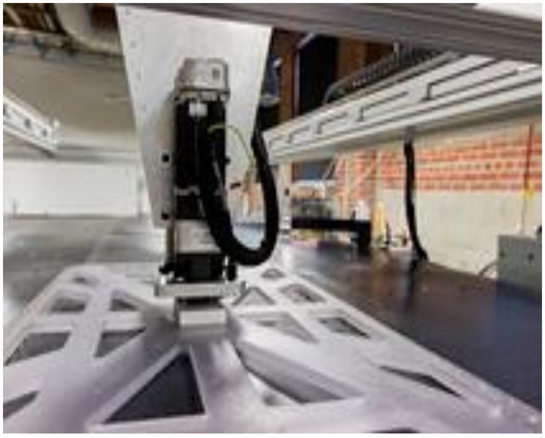


Fig. 2 (b): Robotic arm

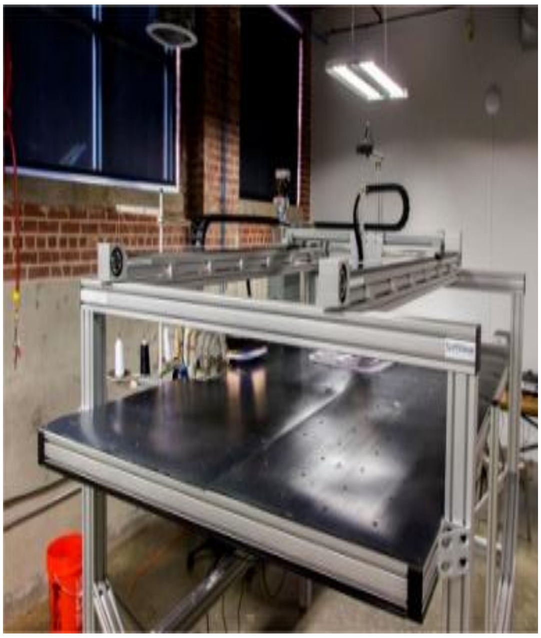


Fig. 2 (c): Budgers

Zornow's creation, the "Sewbo" robot, possesses the capability to autonomously handle fabric pieces during the stitching process. Designed in 2015, the "Sewbo" robot is adept at sewing an entire T-shirt from beginning to end. Another notable creation in this realm is the LOWRY SewBot, developed by the Atlanta-based company "Softwear Automation." Specifically designed for the textile industry, these SewBots incorporate cutting-edge technologies from the industrial 4.0 revolution, including computer vision and advanced robotics. These technologies enable them to analyze and manipulate fabric like human capabilities.

Table 1: Advantages and Disadvantages of implementing robotics in Garment Manufacturing.

Merits	**Demerits**
Increase in Productivity	High initial cost of installation
Increased Inventory Turnover	High cost of research and development
Improvement in quality	Security threats
Reduction in repetitive and monotonous work.	High cost of maintenance
Reduction of direct human labor cost	Unexpected product delays
Reduction of variability among the products and product batches.	Limited scope
Performing jobs beyond	Lack of

human capabilities	flexibility

3. Robotics and Automation in Apparel Supply Chain Management

The garment business, being vast, diverse, and global, has undergone significant revolutions in terms of shifting dynamics, evolving from the fundamental concept of "fashion" to the widely acknowledged notion of "fast fashion." The influence of globalization has extended competition in the garment industry beyond domestic borders, compelling it to maintain a youthful and agile character. This sector encompasses a diverse range of subsectors, including clothing, dyes, synthetic fibers, and performance fibers, catering to specific industries such as performance garments and healthcare garments, reflecting its multifaceted nature (Bruce et al., 2004).

The textile and garment industries play a pivotal role in a country's economic well-being, contributing significantly to employment through manufacturing, distribution, and retail activities. This holds true for both developed and developing nations, with a substantial portion of the workforce engaged in these sectors. The migration of garment manufacturing from wealthier nations to developing ones has been propelled by the allure of cheaper labor and reduced production costs in the latter.

Stengg (2001) observes the impact of globalization, particularly the localization of production in third-world countries, altering the competitive landscape for corporations and nations. This shift has led to a growing trend where certain nations find it challenging to compete with the cost advantages offered by countries engaged in lower-cost manufacturing (Nayak et al., 2015). As per en (2008), the clothing industries can be categorized into three groups based on their life cycle: "basic," "seasonal," and "fashion" items. Basic items typically have the longest life cycle compared to the other two, often remaining relevant throughout the entire year. Seasonal items, on the other hand, have a product life cycle of approximately 20 weeks, while fashion products exhibit the shortest life cycle of just 10 weeks. Abernathy et al. (1995) have modified this classification, asserting that "basic" and "seasonal" items primarily focus on men's and children's clothing, while women's wear falls into the "fashion" category, characterized by a greater emphasis on styles, variety, and possibilities.

As noted by Bhardwaj and Fairhurst (2010), "fashion" is a dynamic expression that evolves over time and is distinct for each individual. The emergence of international trade, intensified competition, concentrated production in developing nations, and the continually changing preferences of consumers gave rise to the concept of fast fashion (Djelic and Ainamo, 1999). Sparks and Fernie (2004) characterize fashion by attributes such as limited predictability, extensive diversity, fluctuating demand, a shorter life cycle, and impulsive buying tendencies. Several multinational corporations, including Zara, H&M, and Benetton, engage in competition to offer appealing items that capture a broader audience, expanding the market for their products (Christopher et al., 2004). Porter (1998) asserts that in a contemporary environment, it is not nations but supply networks that engage in competition, leading to significant transformations in supply chain dynamics. Mangan et al. (2008) describe the shift from a fragmented to a fully integrated supply chain. They highlight that in the 1960s, supply chain services, including transportation, storage, purchasing, and production, operated independently. Up until the late 1980s, fashion retailers traditionally relied on predicting trends and understanding customer preferences to place orders, operating on the concept of ready-to-wear clothing (Guercini, 2001). Doyle (Barnes et al., 2006a,b,c) illustrated the comprehensive integration of the modern fashion industry by shifting from the structural format of ready-to-wear clothing to bespoke items. This transformation compelled businesses to enhance flexibility, responsiveness, and offer a broader range of products to the market. Achieving this was made possible by integrating supply chain operations and sharing information across all stakeholders in the supply chain. Marketing and capital expenditure, along with factors like variety, speed, and flexibility, are crucial drivers of a company's competitiveness (Sinha et al., 2001).

As per Taplin (1997), contemporary retailers are increasingly adopting the concept of "rapid fashion," emphasizing speed to market and product customization to reduce the lead time between design inception and consumer consumption. Barnes et al. (2006a,b,c) observed that in the late 1980s, the fashion industry strategically embraced this approach and established an infrastructure that facilitated a rapid response by minimizing lead times, thus delivering clothing at the lowest feasible cost. Nowadays, the principles of low cost and short lead times are integral to the competition within the clothing industry. Consequently, the trend of relocating manufacturing processes to low-cost foreign locations, through outsourcing or offshoring, has become prominent in the garment business. According to Bruce et al. (2004), retailers prefer sourcing clothing from low-cost nations to save costs, as regularly adjusting infrastructure to accommodate evolving client demands would be impractical in industrialized countries. This strategy enables merchants and businesses not only to concentrate on their core competencies but also to allocate their resources and capital elsewhere for a higher return on investment.

Effectively managing supply chain operations and maintaining flexibility poses a substantial challenge in the realm of global outsourcing. Businesses may encounter difficulties restocking fast-selling items in the midst of the season if they run out or experience a surge in demand. Therefore, efficient logistics and supply chain management between suppliers and retailers, along with the exchange of real-time information and collaborative decision-making among all participants in a global supply chain, become crucial. Importantly, while this trend has generated a significant number of jobs in developed nations, it has also created additional opportunities in developing ones.

3.1 Activities in the garment supply chain

Since the late 1980s, the term "supply chain" has gained increasing popularity and usage. The heightened significance of the supply chain can be attributed to various factors, with global sourcing being a key driver. The forces of globalization have compelled businesses to establish online connections and explore innovative methods for enhanced productivity and efficient coordination of product and information flows. Tyndall et al. (1998) illustrated that the implementation of supply chain management varies in perspective, viewed by some as a management philosophy and by others as a management method, differing from operational viewpoints that focus on product and information flow. According to Jones (1995), the supply chain encompasses the movement of products and services from the provider to the end customer. Stevens (1989) defines supply chain management as the synchronization of operations to align with customer expectations, emphasizing high levels of customer service, inventory control, and logistics processes.

The initiation of the garment supply chain begins with the creation of a design. The first concrete phase involves the creation of fibers, which are then processed into yarn. Following various procedures, the yarn is woven or knitted into fabric, ultimately being transformed into a garment. While garment manufacturing processes are commonly perceived as labor-intensive, it's important to note that upstream processes like yarn and fabric manufacturing are capital-intensive.

3.2 Contemporary Trends in Apparel Supply Chain

In the 1990s, a significant transformation occurred for manufacturers and retailers, driven by the imperative of minimizing costs in the market. Despite significant market players achieving cost management through scale economies in production processes, bulk purchasing, ocean cargo transportation, and centralized distribution, they still struggled to match the cost efficiency of garments produced in the Far East and low-wage nations. Consequently, companies with extended process durations needed to enhance and make their supply chains more flexible and shorter (Fernie and Azuma, 2004). This led to the emergence of contemporary supply chain practices such as Just-In-Time (JIT), total quality management, and comprehensive functional support, helping manage complexities associated with substantial geographical distances (Bruce and Daly, 2006).

Supply chains are now more integrated than ever, primarily due to the utilization of Electronic Data Interchange (EDI). However, certain major players in the fashion industry, such as Zara and Benetton, prefer vertical integration, especially for capital and knowledge-intensive processes (Birtwistle et al., 2003; Bruce et al., 2004). The subsequent section discusses some prevailing trends widely accepted and utilized in the garment industry.

3.3 Electronic commerce and radio-frequency identification

The transformation spurred by advancements in information technologies and the Internet has impacted nearly every industry, and the clothing business is no exception. Online product sales have become the predominant market, superseding physical stores and experiencing rapid growth due to various cost-saving advantages. By showcasing products online, retailers can maintain a minimal level of inventory to serve customers from a centralized location, which can often be in a low-cost country.

RFID (Radio-Frequency Identification) stands out as the most promising upcoming technology employed for automatic product identification using radio waves (Dutta et al., 2007; Whitaker et al., 2007). RFID technology has superseded the barcode scanning system, as barcodes have a lower capacity to store data compared to RFID. Moreover, RFID provides the additional advantage of swiftly scanning items even without direct line of sight (Nath et al., 2006; Miles et al., 2008). While RFID can store up to 1000 bytes of data, the amount of information stored on a barcode is considerably less.

RFID technology is also employed in the clothing industry at various stages of the supply chain, marking one of the most significant technological advancements in modern times. In retail, distribution, and integrated operations, RFID is utilized to track and pair items, for theft control, inventory control and management, and more (Gimpel et al., 2004; Liu et al., 2010). Spinning, a capital-intensive process involving the creation of various sizes (counts) of yarn that are easily mixed, is critical. Even a single bobbin of incorrectly mixed yarn can have downstream effects when the fabric or garment is dyed due to different color pickup by different yarn counts. RFID can be used to prevent yarn mixing at the yarn stage. In fabric manufacturing and processing stages, RFID can be employed to segregate batches effectively.

A significant advantage arises at the garment stage, as retail stores and distribution centers can manage large numbers of stock-keeping units with garments easily tracked and traced in real-time. This stands in contrast to the barcode scanning system, which requires line of sight and is a time-consuming process. Retail chains house numerous products and brands under one roof, making it easy and feasible to monitor all items at an individual level using RFID (Loebbecke and Huyskens, 2008). Several retailers, including Walmart, Tesco, and Prada, have realized benefits from employing RFID, especially American clothing companies. This technology has saved many labor hours and reduced instances of unavailable products (Nayak et al., 2015a).

Sankei, a Japanese manufacturer, has implemented RFID at the clothing manufacturing stage for efficient inventory control and item tracking (Wu et al., 2009). Walmart emerged as an early adopter of this technology, urging its suppliers to incorporate RFID if they intended to continue doing business with Walmart. According to a report from the American Production and Inventory Control Society, Walmart persuaded its suppliers to adopt RFID by providing them regular access to point-of-sale (POS) data, ensuring they remained informed about their inventory levels to minimize overproduction costs (Weil, 2005). The successful implementation of this technology by Walmart aligned with its corporate strategy of being cost competitive and having a Quick Response (QR) (Vowels, 2006).

Fast fashion companies like Zara, H&M, and Benetton have captured a significant market share due to their agility, low cost, and high inventory turnover ratio. The realization of these advantages is made possible with the support of technology, and RFID emerges as a suitable choice (Nayak et al., 2015a). According to Loebbecke and Huyskens (2008), the renowned German brand Kaufhof utilized RFID technology to provide clothing and trend recommendations to men in the fitting room automatically, suggesting suitable suits or accessories through a "smart mirror." A RFID reader attached to the smart mirror scanned the items by reading the tag attached to the garment brought into the fitting room. Suggestions were made regarding matching accessories to facilitate upselling at a strategic point of interaction. Additionally, products attached to RFID tags helped prevent theft by sending signals and information to relevant departmental authorities if the item was removed from the store without authorization or without being scanned.

3.4 IoT

As the Internet of Things (IoT) continues to evolve daily, its further advancement is anticipated through related technologies that will propel it into powerful concepts such as Cloud computing, Big Data, robotics, Semantic technologies, and services. These technologies will contribute significantly to fostering the development of IoT and are, in a sense, interdependent. The primary goal of IoT is to enable various electronic devices to be connected anytime and anywhere in the world without constraints of a specific access point or service

The Internet of Things (IoT) is recognized as the new revolution in the realm of the Internet. Objects and devices are becoming more intelligent, manifesting their presence, and gaining knowledge by making various decisions based on their programmed interactions. This is primarily facilitated by their ability to communicate with each other using a common learning protocol. These products and devices can access information collected by physical objects, devices, and sensors, or they can be integral components of a complex network of services. This transformation is empowered by the advent of cloud computing capabilities and the progression of the Internet toward the IPv6 protocol, which offers nearly limitless addressing capacity, addressing a limitation in IPv4.

The Internet of Things provides solutions based on the integration of various information technologies, encompassing both hardware and software utilized for storing, retrieving, and processing information, and communications technology that includes electronic systems used for communication between individuals or groups of devices. The rapid development and convergence of information and communications technology are occurring at three layers of technological advancement: the cloud, data and communication pipelines/networks, and devices. Factors driving this convergence and contributing to the integration and transformation of the cloud.

3.5 Future Plant Idea with IoT

As development and industry transformation unfold, production will undergo a significant shift. Living beings and machines will be more interconnected and communicate with each other. In future factories, individuals will need to interact with a complex environment of processes, networks of processes, machines, sensors, robotics, and devices. This system will necessitate diverse operating concepts for improved human-machine interaction. In the future, the benchmarks for success and competitive advantage will revolve around fast, intelligent, and self-adaptive manufacturing processes.

Currently, the majority of manufacturing and production facilities are designing systems that will render devices and machines adaptable, fully integrated, intelligent, and more efficient, operating in a manner akin to living beings. These emerging manufacturing systems and devices will be the new industrial revolution, referred to as the factory of the future. This model heralds a new era of smart manufacturing based on full automation and increased utilization of technology in the manufacturing process. In the future, the factory model, integrating mechanical equipment and systems with the digital era, will be robust. Data accumulation will occur at a rapid pace, and a robust analytical system will be crucial for processing this data.

The concept of the future production line is primarily oriented towards ensuring and facilitating the availability of all relevant information for real-time processing. This will be achievable through the connectivity present among all components in the value chain. The interaction between people, objects, and various other system elements makes it possible for the value chain to evolve into a continuous process. Consequently, this can help achieve various business objectives, such as reducing costs, optimizing resource utilization, and ensuring high availability.

Manufacturers, factory workers, and customers need to comprehend and embrace the future supply chain as an increasingly complex system, involving various processes, equipment, and components that will operate in an integrated manner. This necessitates different operational concepts to enhance and foster collaboration between humans and machines, aiming to increase efficiency and reduce time-to-market. This approach ensures manufacturers can compete in a way that minimizes operational costs and maximizes resource utilization.

The global smart factory market is projected to reach nearly USD 87 billion by 2023, growing at a compounded annual growth rate of 6% from 2014 to 2020. Communication, automation, robotics, and programmatic intelligence will transform the product landscape as we know it today. Companies like SAP aim to accelerate growth in their IoT solution portfolio, enhance sales and marketing efforts, scale service, support and co-development, and expand their ecosystem of partners and startups in the estimated €350 billion IoT market by 2023.

3.6 Industry 4.0

In the context of Industry 4.0, the term represents the next industrial revolution, signifying a new level of control and coordination across various supply chain industries and their product life cycles, with a focus on individualized customer needs. The processes encompass the entire journey from idea generation, demand creation, development, and manufacturing of the product to its final delivery to the end consumer. Furthermore, it ensures recycling and all post-delivery services. The objective of the fourth industrial revolution is to ensure the availability of current information in real-time by integrating and connecting all parties involved in the value chain. In Industry 4.0, determining the optimal value-added flow is essential throughout the process. The interaction between people, things, and various systems creates a dynamic, interconnected, optimized, and value-adding flow across all organizations in the supply chain in real-time.

4. CONCLUSION

RFID and other technologies have been integral to supply chains since their inception, finding widespread adoption across various industries, especially in the fast fashion sector. The fashion industry has particularly embraced RFID technology for its potential to innovate numerous processes, including manufacturing, incoming and outbound logistics, transportation, distribution, inventory management, and after-sales services. While RFID benefits may vary across industries, its positive implications for the fashion sector are noteworthy.

This paper introduces and details a framework designed for the automation of multiple transactions within an ERP-enabled supply chain. Although RFID is predominantly utilized for item-level tagging and inventory management, the proposed framework goes beyond traditional applications. It leverages RFID data gathered at different points in the value chain to initiate various transactions and streamline processes within an ERP system, significantly enhancing operational efficiency. This becomes crucial in light of the ongoing industry transformation, requiring fashion companies to rapidly adapt their IT infrastructure to keep pace with global market changes.

The widespread adoption of RFID in supply chain manufacturing is now imperative, with a crucial need for the cost of RFID tags to decrease for item-level tagging to become more economically viable for fashion retailers. Companies must strategically restructure their IT landscapes to integrate the technologies discussed in this study. This transformation is necessary to compete with industry leaders, offer superior services to customers, enhance the overall shopping experience in the digital era, and sustain their business in the context of Industry 4.0.

5. REFERENCES

[1] Flechsig, C., Anslinger, F., & Lasch, R. (2021). Robotic Process Automation in purchasing and supply management: A multiple case study on potentials, barriers, and implementation. Journal of Purchasing and Supply Management, 1-21.

[2] Görçün, Ö. F. (2018). The Rise of Smart Factories in the Fourth Industrial Revolution and Its Impacts on the Textile Industry. International Journal of Materials, Mechanics and Manufacturing.

[3] JINDAL, H., & KAUR, S. (2021). Robotics and Automation in Textile. International Journal of Scientific Research in Science, Engineering and Technology, 40-45.

[4] Lee, S., Rho, S. H., Lee, S., Lee, J., Lee, S. W., Lim, D., & Jeong, W. (2021). Implementation of an Automated Manufacturing Process for Smart Clothing: The Case Study of a Smart Sports Bra. Processes 2021, 1-16.

[5] M, K., M, B., r, S., & A, C. A. (2011). Robotics: a hi-tech revolution in apparel manufacturing & technology. International Journal of Advanced Scientific Research and Review, 50-53.

[6] Ohmori, S. (2021). The impact of location of 3D printers and robots on the supply chain . Uncertain Supply Chain Management, 489–500.

[7] Saibani, N., Ghani, J. A., Akmar, M. S., Boon, W. K., Raj, R. M., Nawawi, M. M., & Asri, N. I. (2021). Latest Advancement of Technologies in Supply Chain Management: An Overview. Jurnal Kejuruteraan, 785-791.

International Journal of Computer Applications Technology and Research
Volume 13–Issue 02, 24 - 32, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1302.1004

Apparel Mass Customization and its Applicability

Vinoth R
National Institute of Fashion Technology, Patna, India

Abhilasha Singh
National Institute of Fashion Technology, Patna, India

Omkar Singh*
National Institute of Fashion Technology, Patna, India

Navanendra Singh
National Institute of Fashion Technology
Patna, India

Abstract: Apparel Mass Customization (AMC) has emerged as a transformative paradigm in the fashion industry, offering a departure from traditional mass production towards a more customer-centric and personalized approach. This paper provides a comprehensive review of AMC and explores its applicability in the dynamic landscape of contemporary fashion. The study delves into the key principles and technologies underpinning AMC, highlighting the integration of advanced manufacturing processes, digital design tools, and data-driven decision-making. By examining successful case studies and industry implementations, the paper underscores the potential benefits of AMC, including enhanced customer satisfaction, reduced inventory waste, and increased brand loyalty. Furthermore, the research investigates the challenges and barriers hindering the widespread adoption of AMC, such as cost implications, technological constraints, and the need for efficient supply chain management. It discusses strategies and solutions employed by leading fashion brands to overcome these challenges and leverage the full potential of customization. The applicability of AMC is then explored across various segments of the apparel industry, ranging from high-end luxury fashion to casual wear and sportswear. The paper analyzes consumer preferences and market trends, shedding light on the evolving demands that drive the need for personalized products. This review provides insights into the current state of AMC and its applicability, offering a roadmap for fashion industry stakeholders to navigate the complexities of customization. As consumers increasingly seek unique and tailored experiences, understanding the dynamics of AMC becomes imperative for fashion brands aiming to stay competitive and relevant in an era of individualized consumer preferences.

Keywords: AMC, Fashion Industry, Customization Techniques, Personalization.

1. INTRODUCTION

The intense global competition and the fragmented nature of markets have compelled numerous industries to undergo reorientation in order to sustain competitiveness and customer loyalty [1]. Across different segments of the global supply chain, there have been notable initiatives, encompassing organizational and technological transformations [2]. The swift adaptation of businesses to tailor their operational and marketing strategies to customization trends [3] [4] [5] has resulted in organizations specializing in customization competing with those that do not embrace such practices. Recognizing the diminishing lifespans of products, manufacturing companies have come to the realization that generating large quantities of a standard product for a broad market is causing them to lose market share and potential profits. Success in manufacturing is now determined by the efficiency of order fulfillment and customer acquisition processes that can swiftly and flexibly respond to changes. The solution encapsulating this approach is Mass Customization (MC). Mass customization is defined as "the mass production of individually customized goods and services" [6]. Pine asserts that leveraging advanced technologies, such as computer-integrated manufacturing, computer-aided design, flexible manufacturing systems, and advanced computer technology in the application of mass customization, will not only reduce product life cycles but also empower manufacturers to adeptly address evolving consumer preferences. Mass customization represents a technology-driven manufacturing process that empowers consumers to modify a company's product line according to their specific fit requirements and design preferences [7] [8].

The term "mass customization" was initially coined by Stanley Davis in 1987 in his book "Future Perfect." He stated, "the same large number of customers can be reached as in mass markets of the industrial economy, and simultaneously they can be treated individually as in the customized markets of pre-industrial economies" [9]. Subsequently, Joseph Pine further defined mass customization as "developing, producing, marketing, and delivering affordable goods and services with enough variety and customization that nearly everyone finds exactly what they want" [6]. Figure 1 illustrates the concept of mass customization as defined by Pine.

All the definitions converge at the intersection of three crucial factors – addressing individual consumer needs, ensuring profitable outcomes, and maintaining a flexible organizational structure. Over the past two decades, research on mass customization (MC) has witnessed significant advancements, with the emergence of more structured customer-interaction techniques and rapid developments in manufacturing technologies playing pivotal roles. In a 2012 study, Fogliatto et al. [10] concluded that MC is evolving into a contemporary business principle, driven by an increasing consumer demand for personalized products. The review provided a clear perspective on the MC strategy by elucidating the drivers for value and success, as well as the dynamics of customer-manufacturer interaction. The critical success factors encompassed customer demand, technology, markets, customizable offerings, knowledge, and the value chain. In terms of enabling factors, mass customization (MC) processes were categorized into four stages: 'order elicitation,' 'design,' 'manufacturing,' and 'supply chain coordination.' Beyond its advantages for customers, MC provides companies with substantial flexibility in both products and services [11]. Its implementation safeguards manufacturers from excessive inventories of finished products and the challenges associated with overly advanced forecasting.

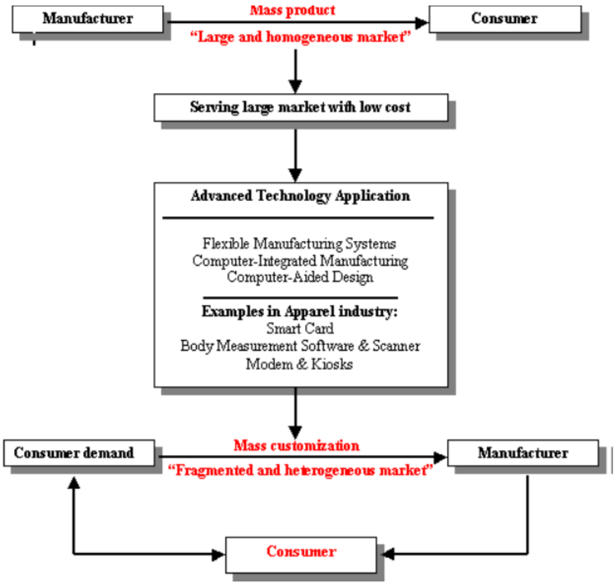

Manufacturer
Mass product
Consumer
"Large and homogeneous market"
Serving large market with low cost
Advanced Technology Application
Flexible Manufacturing Systems
Computer-Integrated Manufacturing
Computer-Aided Design
Examples in Apparel industry:
Smart Card
Body Measurement Software & Scanner
Modem & Kiosks
Consumer demand
Mass customization
Manufacturer
"Fragmented and heterogeneous market"
Consumer

Fig. 1. Mass Customization Concept

2. MASS COMMUNICATION IN THE APPAREL INDUSTRY

The strategy of mass customization (MC) has found application across a diverse array of product categories, including furniture, automobiles, computers, and apparel. A growing number of companies are embracing the concept of MC to meet the dynamic demands of their customers [12] [13]. In the apparel industry, numerous innovative technologies have played a crucial role in enhancing MC operations over the years. Beyond the realm of slow fashion, MC is a prominent theme driving product development through customer involvement among fashion manufacturing brands [14]. Design, fit, fabrication, and features are identified as pivotal aspects of apparel MC programs. Considerable research has delved into the intricacies surrounding mass customization in the past

Accurate customization of apparel products necessitates precise measurements of individual consumers. Typically, a trained salesperson follows the conventional practice of obtaining body measurements at specific points and inputting them into a system. This system then adjusts the size of corresponding points on the prototype pattern. However, the adoption of 3D body scanning, which streamlines and simplifies the process, is gaining popularity. Another method involves capturing a video image of the consumer and utilizing pattern generation software to convert the measurements extracted from the image into a distinct pattern [15]. Lee [16] highlighted the integration of digitized images and body scanning in mass customization (MC) practices. According to Lee, customers are measured three-dimensionally through a digitized image on a video screen or kiosk, enabling them to visually confirm whether the selected style aligns with their preferences. Anderson et al. [17] utilized consumer research to propose a model of MC for the apparel industry, demonstrating that new technology and digital information in the manufacturing process can facilitate customized apparel through four options: 'expanded selection/search,' 'design option,' 'co-design,' and 'total custom.' The 'expanded search' allows customers access to various manufacturers' product lines. In the 'design option,' computer-aided design and digital printing aid customers in selecting designs, style options, fabric, and color from the manufacturer or retailer. Lastly, in 'total custom,' customers can submit their own digital designs to manufacturers or retailers.

Mpampa et al. [18] developed a methodology for creating sizing systems in clothing mass customization (MC) systems. This approach aims to determine the optimal MC degree and the corresponding quantity of garment sizes while achieving a balance between the number of sizes and the satisfaction percentage of consumers. The methodology was successfully applied to the mass customization of male shirts, trousers, and coats in Greece. Notably, affluent retailers like Brooks Brothers and Land's End, who previously implemented MC for men's shirts, currently do not offer online MC services. This is likely due to men's shirts being considered a basic clothing item, with an extensive array of ready-to-wear options available in the market. Additionally, customers may not be willing to wait longer for a customized shirt. Another contributing factor, besides the higher cost of MC products, is that many companies implementing the program do not experience significant financial gains from it. However, despite these challenges, some firms such as Tailorism and Ownonly continue to provide mass customization services for gentleman shirts.

3. MASS CUSTOMIZATION, MASS PRODUCTION AND MASS-CUSTOMIZED PRODUCTION

'Mass Production' refers to the production of large quantities of standardized products using automated robotic machines, assembly lines, and human labor [19]. On the other hand, mass customization is defined as 'the technologies and systems to deliver goods that meet individual customers' needs with near mass production efficiency' [20]. Therefore, manufacturers or retailers implementing mass customization align themselves with flexible manufacturing to produce garments tailored to customer specifications. The Ford

Motor Company notably popularized mass production ahead of the Great War in 1913. Moving to the post-World War II era in 1948, businesses like McDonald's began applying the Ford model to the restaurant industry. Mass production evolved into a potent tool, expanding on a massive scale to enhance productivity, improve quality, and streamline prices. Businesses seized opportunities to capitalize on reduced energy costs, favorable tax rates, and lower labor expenses by relocating their mass production facilities to foreign territories. While the decline of the mass production model is underway, on the contrary, mass customization (MC) is still in its early stages. In MC, customers have the freedom to choose the product style, fabric, color, size, and trims from a set of options. They engage in an interactive setting to create the customized product and receive personalized apparel based on manually executed body size measurements or measurements obtained through body scanners [21]. The production process for a customized style order commences as soon as the customer places and pays for the order.

3.1 Examples of Application of Mass Customisation in the Apparel Industry

Presently, various brands like Custom Foot, Levi Strauss, and Second Skin Swimwear have embraced mass customization (MC). In 2000, Adidas initiated a shoe customization project called 'mi adidas,' leading to the establishment of the world's largest Adidas store, the futuristic 'Mi Innovation Center,' in 2006 [22]. This center showcases numerous technological innovations designed to efficiently capture customer preferences. The 'mi adidas' product line includes performance shoes tailored for soccer, running, and tennis. The Adidas store employs a three-step preference elicitation process encompassing fit, design, and performance. In the case of Custom Foot, consumers select their preferred style before a computer scanner takes precise measurements of their feet. A modem transmits the recorded measurements and details regarding the selected style, color, and material to Custom Foot's Florence office, with production and delivery typically taking approximately three to four weeks. Levi Strauss employs a similar approach. Initially, a trained salesperson records four measurements of the hip, waist, inseam, and rise, which are then input into the computer system. The customer wears the prototype-test garment recommended by the system and communicates any necessary adjustments in fit measurements for the hip, waist, inseam, or rise. Achieving the perfect fit usually requires no more than three prototypes. The finalized specifications are then forwarded to Levi Strauss in Mountain City, with production and delivery completed in about three weeks. Likewise, at Second Skin Swimwear, a trained salesperson guides the customer through the 'Digifit' process, which typically spans an hour. The process initiates with the customer trying on sample suits, encompassing 20 one-piece suit styles and around 20 top and bottom styles. Subsequently, all the recorded information is transmitted via a modem to the headquarters of Second Skin in Juno Beach, FL.

4. MASS CUSTOMIZATION STRATEGY FOR MANUFACTURING

This section delves into the settings and strategies necessary for the successful implementation of mass customization (MC).

4.1 Modularity

Modularity involves breaking down a product into modules and reassembling them to create the final product based on customers' personalized requirements. Many industries face challenges in determining the variety or modularity level of their products due to numerous variations. Modularity stands out as one of the most crucial factors in mass customization (MC) production [23], with significant impacts on both product and process management. Wang et al. conducted a study on Chinese manufacturers, illustrating that factors such as innovation, mass customization (MC) capability, standardization, and delivery speed exhibit strong relationships among them. Despite numerous studies on product modularity, it is observed that certain MC programs in the industry experience sudden discontinuation, often attributed to the overall complexity of the system escalating, particularly when suitable solutions for managing the increased production complexity are lacking [24].

4.2 Framework

In addition to the organizational integration of the design process, the realization of mass customization (MC) also necessitates the establishment of a system integration architecture and a relevant contextual framework for product development [25]. Feitzinger et al. [26] underscore the significance of research and development in redesigning products for efficient customization at the supply network's optimal end. Fang et al. [27] empirically investigate the impact of organizational learning on operations performance and process technology, demonstrating that process automation can be enhanced through team and systems orientation learning without affecting operations performance. Ellena et al. [28] introduced a design framework for custom-fit bicycle helmet models.

4.3 Technology for Mass Customisation

Technological advancements in communication, management systems, and production have sustained the feasibility of mass customization (MC) [29]. In the apparel industry, cutting-edge technologies that facilitate MC include Computer-aided Design (CAD) and Computer-aided Manufacturing (CAM) systems capable of transforming customer designs into cut garment pieces, 3D body scanners for collecting accurate body measurements, digital printing, the internet for seamless communication between manufacturers or retailers and customers, single-ply cutters, computerized processes to expedite error-free production and delivery, virtual try-on visualization techniques, and modular production systems.

4.3.1 CAD

CAD/CAM systems are becoming increasingly crucial as they enhance the efficiency of various processes associated with mass customization (MC) [9]. The realization of MC heavily relies on CAD systems, as they play a pivotal role in creating appropriate designs by incorporating changes in color, texture, and fabric, ultimately merging personalized measurements with virtual clothing. However, technological constraints, such as limited production speeds, make 3D production primarily suitable for customized products, small production volumes, or high-value items [30] [31]. In the past decade, there has been significant attention focused on integrating CAD systems with 3D laser scanning, particularly in the clothing and fashion industries, for virtual fit or design testing. Satam et al. [32] scrutinize the economic factors driving mass customization (MC) and suggest a Computer-Aided Design (CAD) system that incorporates both 2D and 3D intelligent design systems for clothing. This proposed system aims to facilitate design personalization throughout the apparel MC process, enhancing the overall efficiency of MC in the apparel industry. It provides a diverse array of fits and styles for garment production processes. Tao et al. [33] introduce a 3D garment collaborative design process that involves normalized sensory evaluation for garment fitting effects in a virtual environment. This approach combines interactions between specific customers and designers, with enhancements made to the involved actors.

4.3.2 3D Body Scanning

3D body scanners employ optical techniques or equivalent methods to capture images of the external surface of the human body [11]. They are built upon a diverse range of technologies, including LED, white light, laser-based systems, and similar devices. Their accuracy is noteworthy, capable of achieving measurements with an accuracy of an eighth of an inch. Moreover, measurements obtained through 3D body scanners have the potential to be even more precise and reproducible. The technology offers numerous advantages. With 3D body scanning, obtaining countless measurements of human bodies takes only seconds, and any alterations made are immediately reflected in the database, updating both garment size requirements and body dimensions. This results in a shortened time cycle, and data on customer preferences becomes readily available throughout the textile chain. Revamping body scanning is crucial to enhance its practicality in the application of apparel design and pattern [13]. Health considerations come into play, particularly regarding the safety of laser stripe projection or projection light for the eyes. Companies should also take into account parameters like the size of the scanner, the software used, and the size of the data when acquiring 3D body scanners. However, with advancing technology, these systems are becoming more affordable. Body scanning technology optimizes logistics and inventory management, freeing manufacturers from the need to employ skilled individuals for consistent body measurements. Despite these advantages, there are downsides to the technology. A significant portion of body scanners faces challenges in obtaining data from concealed areas of the body, such as the crotch, soles, armpits, under the bust, and chin, posing difficulties in determining sizes in these areas. Identifying body landmarks on the point cloud poses a challenging task, and various 3D scanning systems handle it differently. This highlights the necessity for a system that ensures stability and interchangeability between different scanners. Another challenge involves surface texture, where the quality of the scan can be compromised by factors such as hair and dark-textured clothing. These elements disperse light, hindering the cameras from capturing a complete set of data points.

4.3.3 Single Ply Cutting

In mass customization (MC), a garment is precisely cut according to consumer preferences. In each batch, a roll of fabric is placed on a laser-driven cutter, which then cuts each pattern individually using the entered digital pattern. However, this process is notably more expensive than conventional cutting systems and requires enhancements to enable automatic continuous cutting for MC [13]. In 2020, Xu et al. [34] conducted a case study on women's basic straight skirts, aiming to devise mass customization (MC) methods for cutting-related processes that effectively addressed the trade-off between cost acceptance and personalization levels when compared to existing MC methods. The primary focus of the study was on co-design customization and custom-fit, and the proposed methods assisted companies in identifying additional costs in intricate items. This allowed for the alignment of precise customization expectations with cost control, ultimately paving the way for the development of a production strategy to achieve garment mass customization. The study also suggested potential for the introduction of more advanced computer-aided technologies and the further development of performance evaluation criteria in the future.

4.3.4 3D Printing

Online mass customization (MC) programs often face challenges when customers are required to submit fit options for their MC orders. This is due to the fact that many individuals are not familiar with the precise measurements of the human body. Consequently, the data received may be imperfect, making physical fitting challenging and leading to dissatisfied customers. The use of 3D body scanning addresses this issue by creating precise body data, providing a mutually beneficial situation for both manufacturers and consumers. Numerous researchers have highlighted the extensive applications of 3D printing in the industry, with its advantages thoroughly examined in the literature. 3D printing enables the cost-effective manufacturing of small quantities of customized articles [35]. The technology has the potential to empower retailers to create and deliver goods in small quantities in real time [36]. This capability not only facilitates cost-effective mass customization but also reduces manufacturing lead time and personalization time [37]. However, when applied on a mass production scale, it faces challenges related to portability, increased costs, and the diminished experiential aspect for online customers. Recent research has been dedicated to the transformation of 2D-3D data, aiming to generate accurate measurements of the human body from a 2D photocopy of the customer. Additionally, several researchers have proposed reconstructive modeling methods that use limited information to generate more comprehensive data on the actual body shape.

4.3.5 Virtual try-on system

Virtual try-on represents one practical application of 3D body scan data, wherein customers are presented with a computer-generated visual display showcasing how a garment will appear on their body. This technique allows individuals to assess the garment's appearance before making a purchase, reducing the perceived risk associated with buying clothing. Virtual fitting provides more comprehensive information about a product compared to an e-catalogue, ultimately enhancing perceptual curiosity about the product and amplifying online purchase intention [38]. Zawadzki and Żywicki [39] conducted an examination into smart production control and product design for the effective implementation of mass customization (MC) in the context of Industry 4.0. They found that such a system must be proficient in processing and analyzing vast amounts of data, enabling it to make decisions related to material flow.

4.3.6 Flexible Manufacturing System

Mass customization (MC) involves producing a lower number of pieces compared to mass production. In the apparel industry, achieving reduced lead time and production costs poses a significant challenge for MC. The unpredictable nature of manufacturing requirements distinguishes MC, making it difficult to adapt to frequent changes in batch quantities and tight delivery schedules, even within a Lean Production setup. Therefore, the incorporation of a Flexible Manufacturing System (FMS) becomes crucial for cost-effective production. The traditional FMS is based on numerically controlled machines and features automated material handling facilities. In a mass customization (MC) environment, a wide array of part varieties is produced, with customer orders arriving randomly and having different delivery dates. Consequently, an MC system must possess sufficient flexibility and rapid response capabilities to manage complex manufacturing scenarios. The strategic placement of all manufacturing processes in well-organized locations, coupled with coordinated supply and material redesign, is essential for effective manufacturing and distribution functions [26]. An agile manufacturing system allows customization to occur without incurring additional costs, achieved through the efficient utilization of virtual alliances and a flexible workforce [40].

5. CONSUMER OUTLOOK ON MASS CUSTOMIZATION

Numerous companies initiate mass customization (MC) projects in online stores, empowering customers to design their own products according to individual requirements and submit them to the manufacturer for production. The implementation of MC captures customer attention, enhances satisfaction, and reinforces purchase intentions. A survey conducted in 2011, examining customers' perceptions of mass customization (MC) [41], concluded that customers are inclined towards owning personalized products. The primary factors influencing a consumer's decision regarding MC are identified as price, brand, and time. The survey revealed that at least half of brand loyalty among MC companies could be disrupted if there were no changes in price and quality. In the contemporary context, the application of MC is credited to two preference factors: minimizing design effort and maximizing achieved fit.

Tangchaiburana et al. [42] assessed the elements of mass customization (MC) websites that impact customer participation in the design process. The study showed that customization significantly influenced customers' desire for co-design tools and designing different types of clothing. A successful online consumer-customized experience not only enhances a consumer's preference fit but also enables them to imbue their sense of self into the products during customization [43]. Social technologies provide customers with a sense of confidence to showcase their creations with friends and strangers online. As mass customization (MC) programs gain popularity, especially among luxury brands like Burberry and Louis Vuitton, Yoo and Park [44] conducted a study to identify and explore the dimensions of consumers' perceived value in MC. The survey involved female online shoppers in South Korea. The findings revealed that both social value and utilitarian creative achievement influenced satisfaction with customization, subsequently impacting brand loyalty. Additionally, the relationships between satisfaction and consumer value varied based on the customer's desire for uniqueness and past loyalty.

6. MASS CUSTOMIZATION THROUGH SUPPLY CHAIN’s PERSPECTIVE

The relevant literature in the context of the supply chain encompasses both empirical and analytical perspectives. Lean practices, along with e-commerce and e-procurement, have been identified as factors that can reasonably predict mass customization (MC) performance in manufacturers [45]. Qualitative research examining the relationship between MC and sustainability concluded that MC can exhibit both sustainable and unsustainable aspects. Nevertheless, it has the potential to contribute to sustainability [46]. In the current landscape, companies require innovative supply chain management techniques to transform materials into distinct customized products. This necessitates further exploration into integration with mass production considerations such as cost, volume, and efficiency, encompassing aspects like 'shared custom-module,' 'design-to-order,' 'supplier,' and 'just-in-time.' Previous research has indicated that mass customization (MC) capability is positively associated with an organic organizational structure. Additionally, the development of MC is influenced by factors such as product modularity and supply chain coordination. Interestingly, it has been observed that MC can sometimes provide more advantages to a low-quality firm, despite the expectation that a high-quality firm is more likely to adopt it [47].

When companies strategically balance their production between standardized and custom-made products, the portion of sales from the latter tends to increase in response to heightened competition. In a study conducted in 2010, Chod et al. [48] investigated the value of flexibility in a mass customization (MC) system, encompassing assembly, procurement, and product pricing. The findings highlighted that the outcomes of correlation and demand variability are significantly dependent on the overall product line's commonality structure. Moreover, optimal prices are influenced by the degree of commonality between two products. Considerable literature has explored inventory management in a mass customization (MC) environment. Researchers propose that a firm can offer reduced prices to customers with extreme preferences, while charging a higher fixed price for those with more central preferences. The majority of MC programs do not provide a return policy since products personalized for individuals cannot be resold to others. However, some brands allow customers to return MC fashion products with a full refund and no service charge, aiming to attract potential customers and boost demand.

Piller and Blazek [49] emphasize the pivotal role of configuration systems in fulfilling the specific demands of each individual customer. They identify three vital strategic capabilities of mass customization (MC) as robust process design, solution space development, and choice navigation. The design of features, comfort, and fit, including the utilization of technologies like 3D body scanning, contributes to the value derived from MC. Additionally, value can be achieved through form and visual aspects such as color, flavors, style, and aesthetic designs. Functionality, associated with technical characteristics like power, speed, and memory, is another dimension contributing to the overall value of MC. Despite mass customization (MC) emerging as a prevalent trend in consumer goods markets, it remains unclear whether MC articles are environmentally positive, given the numerous influential factors compared to mass-produced articles. Sustainability enablers have been identified to impact MC, and the relationship between design for sustainability and customer involvement becomes more pronounced in the context of a sustainable mass-customized firm. In quick-response supply chains, consumer returns can enhance the supply value to the fashion supplier, leading to significant reductions in environmental costs as well [50].

7. REMODELING THE SUPPLY CHAIN

The current landscape, characterized by increased product variety and dynamic demands, is exerting pressure on the traditional supply chain channel – comprising a supplier, manufacturer, distributor, and retailer – to become more agile. This is especially evident in the apparel industry where demand levels are volatile and unpredictable, product preferences are diverse, style instincts vary, and there is a inclination towards acquiring differentiating factors in products, driving the inclination towards mass customization (MC).

Mass customization (MC) seeks to eliminate intermediaries in the value chain, specifically wholesalers and retailers, and establish direct channels from manufacturers to retailers. This gives rise to the concept of disintermediation in MC [51]. One crucial advantage of this concept is the transparency of raw material among suppliers. In an MC environment, retailers transmit accurate requirement information through web services to garment vendors. This eliminates information asymmetry among suppliers and saves the organization from excessive inventory investments.

The multitude of product variants resulting from customer design intensifies the challenges arising from supply chain constraints. An organization must determine the extent to which customization can be accommodated. Mass customization (MC) systems necessitate a foundational product on which further customization can be applied. This foundational product is known as the basic product architecture, while the components and accessories that constitute the family of the foundational product are collectively referred to as product family architecture. For instance, in the case of an apparel manufacturer engaged in MC, the basic product architecture would include base fabric, design library, standard pattern-making body blocks, sewing threads, and accessories. Inventory management becomes the foundation for determining delivery dates of customized products. Manufacturers must exercise extra caution with their inventories, particularly during peak seasons. As the industry progresses towards more fashionable products like designer clothing, a higher degree of mass customization (MC) will be evident, involving aspects such as button types, pocket styles, design parameters, and emerging fashion styles.

8. CHALLENGES OF MASS CUSTOMIZATION

Consumer behavior plays a significant role in the successful operation of mass customization (MC) [12]. Two key factors influencing MC are the uniqueness desired by the customer and the gap between available and desired products in the market. As this gap widens, more customers tend to prefer MC. However, the major drawback of offering a wide variety of products is that it can lead to confusion among consumers. Therefore, proper planning for an MC program is essential, taking into account all potential consequences. A broader array of products can overwhelm consumers during the selection process, potentially leading to erroneous decisions in product selection. Factors such as limited information processing capacity, insufficient customer knowledge about the product, and possible ignorance of consumers regarding their actual individual needs can impact the success of the mass customization (MC) process [52].

The fundamental requirement for achieving customized size and fit in mass customization (MC) is the implementation of Computer-Aided Design (CAD) and Computer-Aided Manufacturing (CAM) systems. In the apparel industry, 3D body scanning facilities and configuration systems are essential for MC [12]. The increasing prevalence of e-commerce has also played a significant role in driving MC. Information Technology (IT) enables the seamless transfer of information among buyers, sellers, and manufacturers. An efficient information transfer system allows manufacturers to respond to customers in minimal time. Therefore, IT serves as a powerful tool in effectively supporting MC by bridging the virtual distance between manufacturers and consumers.

Mass customization (MC) involves coordination among apparel retailers. Brands offering customized clothing typically outsource operations related to supply and production to various manufacturing companies or trading agents [25]. Lack of proper coordination between these entities poses risks, and as a result, MC may not function effectively. This implies that retail brands focus on their core competencies and avoid such challenges. MC requires the production of small batches, sometimes even a single item multipletimes. The manufacturing system for MC should possess sufficient flexibility to respond to the dynamic needs of consumers. Mass customization (MC) typically requires flexibility in operation, quantity, labor, and expansion, including the introduction of new products. Modularity is considered not only to enhance production flexibility in MC but also as an ideal approach. Those involved in manufacturing and the supply chain need to exhibit a high level of trust and coordination to collaboratively address problems in a mutually rewarding way [53]. Identifying trustworthy and potential suppliers is crucial as it impacts the network and ensures timely delivery [52].

9. CONCLUSION

Concerns about appearance and fit are enduring aspects of human nature. Once individuals discover the right outfit in a style and color that complements them, achieving the perfect fit becomes the ultimate enhancement. Mass customization (MC) in the apparel industry is not a distant vision but a forthcoming reality. Retail industries are just beginning to embrace the MC process to reduce the time spent searching for the right fit combined with customized style. While industries practicing MC are still working towards achieving optimal inventory management, ongoing technological innovations hold the promise of making MC a viable and beneficial option for both manufacturers and consumers. Trained salespersons play a crucial role in the practices of mass customization (MC) in the apparel industry, assisting customers in selecting specific styles at each step. It's noteworthy that the choices in style and size are often limited to keep overhead costs down. Limited research delves into the actual manufacturing processes within a factory that produce goods ordered by customers. As highlighted in Pine's study of the automobile industry [6], the future of MC in the apparel sector will require advanced, automated manufacturing systems along with dynamic, flexible organizational structures. The case study of Second Skin Swimwear suggests that the apparel industry may necessitate a distinctive assembly design, moving away from the traditional work-in-process approach. With the continuous development of the internet and high-speed computer technology, future innovations in 3D body measurements will empower consumers to store their body measurements digitally. This capability will enable them to electronically customize designer clothes using specialized software, all at a reasonable cost and from the convenience of their homes.

10. REFERENCES

[1] P. R. B. Holland, “A mass customised supply chain for the fashion system at the design-production customers,” Journal of Fashion Marketing and Management: An International Journal, vol. 10, no. 3, pp. 345 - 359, 2006.

[2] J. Winterton and R. Winterton, “De-regulation, division and decline: the UK clothing industry in transition,” in Rethinking Global Production, Abingdon, Ashgate Publishing, 1997, pp. 18 - 40.

[3] S. Kotha, “Mass Customization: Implementing the Emerging Paradigm for Competitive Advantage,” Strategic Management Journal, vol. 16, pp. 21 - 42, 1995.

[4] P. Zipkin, “The Limits of Mass Customization,” MIT Sloan Management Review, vol. 42, no. 3, pp. 81 - 89, 15 April 2001.

[5] J. Lampel and H. Mintzberg, “Customizing Customization,” MIT Sloan Management Review, vol. 38, no. 1, pp. 21 - 32, 15 October 1996.

[6] J. B. Pine II, “Mass-customization: the new frontier in business competition,” Harvard Business School Press, vol. 17, no. 2, p. 48, 1993.

[7] M. T. Fralix, “From mass production to mass customization,” Journal of Textile and Apparel, Technology and Management, vol. 1, no. 2, pp. 1 - 17, 2001.

[8] R. Westbrook and P. Williamson, “Mass customization: Japan’s new frontier,” European Management Journal, vol. 11, no. 1, pp. 38 - 45, 1993.

[9] S. Davis, Future Perfect, Addison-Wesley Publishing, 1987.

[10] F. S. Fogliattoa, G. J. Silveira and D. Borensteinc, “The mass customization decade: An updated review of the literature,” International Journal of Production Economics, vol. 138, no. 1, pp. 14 - 25, 2012.

[11] R. Nayak, R. Padhye, L. Wang, K. Chatterjee and S. Gupta, “The role of mass customisation in the apparel industry,” International Journal of Fashion Design, Technology and Education, vol. 8, no. 2, pp. 162 - 172, 2015.

[12] Anderson-Connell, L. Jo, U. P. V, B. and E. L, “A consumer-driven model for mass customization in the apparel market,” Journal of Fashion Marketing and Management, vol. 6, no. 3, pp. 240 - 258, 2002.

[13] S.-E. Lee and J. C. Chen, “Mass-customization Methodology for an Apparel Industry with a Future,” Journal of Industrial Technology, vol. 16, no. 1, pp. 2 - 8, 1999.

[14] D. C. L. Kuo, C. C. Lin and Y. K. Wu, “The connection between customer value creation and innovation strategy: A proposed framework and its implication in fashion products,” IEEE International Conference on Industrial Engineering and Engineering Management, pp. 1175 - 1179, 2011.

[15] R. W. Chase, CAD for Fashion Design, Pearson Education, 1997.

[16] L. Lee, “Garment scanner could be a perfect fit,” Wall Street Journal, pp. B1, B6, 20 September 1994.

[17] L. Anderson, E. Brannon, P. Ulrich, N. Staples, M. Grasso, P. Butenhoff and M. Beninati, “Discovering the Process of Mass Customization: A Paradigm Shift for Competitive Manufacturing,” National Textile Center Annual Report, pp. 57 - 61, August 1997.

[18] M. L. Mpampa, P. N. Azariadis and N. S. Sapidis, “A new methodology for the development of sizing systems for the mass customization of garments,” International Journal of Clothing Science & Technology, vol. 22, no. 1, pp. 49 - 68, 2010.

[19] ALutowicz, “Mass Production vs. Mass Customization (Welcome to 2017),” Commercial Construction, Facility Construction, 22 January 2017. [Online]. Available: https://verto360.com/mass-production/#:~:text=%E2%80%9CMass%20Production%E2%80%9D%20means%20large%20amounts,robotic%20machines%20and%20human%20labour..

[20] Tseng, M. and J. J, “Mass Customization,” Handbook of Industrial Engineering, vol. 3, pp. 684 - 709, 2001.

[21] J. Fan, W. Yu and L. Hunter, Clothing Appearance and Fit: Science and Technology, Cambridge, UK: Woodhead Publishing Series in Textiles, 2004.

[22] M. Kamanev, “Adidas’ high tech footwear,” Business Week, 3 November 2006. [Online]. Available: http://www.businessweek.com/innovate/content/nov2006/id20061103_196323.htm..

[23] V. Modrak, D. Marton and S. Bednar, “Modeling and Determining Product Variety for Mass-customized Manufacturing,” 5th CATS 2014 - CIRP Conference on Assembly Technologies and Systems, vol. 23, pp. 258 - 263, 2014.

[24] S. Bednar and V. Modrak, “Mass customization and its impact on assembly process’ complexity,” International Journal for Quality Research, vol. 8, no. 3, pp. 417 - 430, 2014.

[25] M. M. Tseng, J. Jiao and M. E. Merchant, “Design for mass customization,” CIRP Annals, vol. 45, no. 1, pp. 153 - 156, 1996.

[26] E. Feitzinger, and H. L. Lee, “Mass customization at Hewlett-Packard: The power of postponement,” Harvard Business Review, vol. 75, pp. 116 - 123, 1997.

[27] E. A. Fang, X. Li and J. Lu, “Effects of organizational learning on process technology and operations performance in mass customizers,” International Journal of Production Economics, vol. 174, pp. 68 - 75, 2016.

[28] T. Ellena, H. Mustafa, A. Subic and T. Y. Pang, “A design framework for the mass customisation of custom-fit bicycle helmet models,” International Journal of Industrial Ergonomics, vol. 64, pp. 122 - 133, 2018.

[29] G. S. Day and D. B. Montgomery, “Charting New Directions for Marketing,” The Journal of Marketing, vol. 63, pp. 3 - 13, 1999.

[30] B. Berman, “The new industrial revolution,” Business Horizons, vol. 55, pp. 155 - 162, 2012.

[31] N. Hopkinson, R. J. M. Hague and P. M. Dickens, Rapid manufacturing. An industrial revolution for the digital age, Chichester, 2006.

[32] D. Satam, Y. Liu and H. J. Lee, “Intelligent design systems for apparel mass customization,” Journal of the Textile Institute Proceedings & Abstracts, vol. 102, no. 4, pp. 353 - 365, 2011.

[33] X. Tao, X. Chen, X. Zeng and L. Koehl, “A customized garment collaborative design process by using virtual reality and sensory evaluation on garment fit,” Computers & Industrial Engineering, vol. 115, pp. 683 - 695, 2018.

[34] Y. Xu, S. Thomassey and X. Zeng, “Garment mass customization methods for the cutting-related processes,”

Textile Research Journal, vol. 91, no. 7 - 8, 9 September 2020.

[35] A. Gandhi, C. Magar and R. Roberts, “How technology can drive the next wave of mass customization,” Business Technology Office McKinsey & Company, vol. 2014, no. 2, pp. 1 - 8, 2014.

[36] C. J. Parker, “Is mass customization a bridge too far?,” WIT Transactions on Engineering Sciences, vol. 113, pp. 373 - 380, 2016.

[37] M. Attaran, “The advantages of additive manufacturing over traditional manufacturing,” Business Horizons, vol. 60, pp. 677 - 688, 2017.

[38] M. Beck and D. Crié, “I virtually try it … I want it ! Virtual Fitting Room: A tool to increase on-line and off-line exploratory behavior, patronage and purchase intentions,” Journal of Retailing and Consumer Services, vol. 40, pp. 279 - 286, 2018.

[39] P. Zawadzki and K. Żywicki, “Smart product design and production control for effective mass customization in the industry 4.0 concept,” Management and Production Engineering Review, vol. 7, no. 3, pp. 105 - 112, 2016.

[40] A. M. Hormozi,, “Agile manufacturing: The next logical step,” Benchmarking: An International Journal, vol. 8, no. 2, pp. 132 - 143, 2001.

[41] P. Coletti and T. Aichner, Mass customization: An exploration of european characteristics, Springer, 2011.

[42] S. Tangchaiburana and K. W. Techametheekul, “Development model of web design element for clothing e-commerce based on the concept of mass customization,” Kasetsart Journal of Social Sciences, vol. 38, pp. 242 - 250, 2017.

[43] S. Kwon, S. Ha and C. Kowal, “How online self-customization creates identification: Antecedents and consequences of consumer-customized product identification and the role of product involvement,” Computers in Human Behavior, vol. 75, pp. 1 - 13, 2017.

[44] J. Yoo and M. Park, “The effects of e-mass customization on consumer perceived value, satisfaction, and loyalty toward luxury brands,” Journal of Business Research, vol. 69, no. 12, pp. 5775 - 5784, 2016.

[45] P. Hong, D. D. Dobrzykowski and M. A. Vonderembse, “Integration of supply chain it and lean practices for mass customization: Benchmarking of product and service focused manufacturers.,” Benchmarking, vol. 17, no. 4, pp. 561 - 592, 2010.

[46] T. D. Brunø, K. Nielsen, S. B. Taps and K. A. Jørgense, Sustainability evaluation of mass customization. Advances in production management systems. sustainable production and service supply chains, Berlin: Springer, 2013.

[47] O. Loginova and X. H. Wang, “Mass customization in an endogenous-timing game with vertical differntiation,” Economic Modelling, vol. 33, pp. 164 - 173, 2013.

[48] J. Chod, D. Payke and N. Rudi, “he value of fexibility in make-to-order systems: The efect of demand correlation,” Operations Research, vol. 58, no. 4, pp. 834 - 848, 2010.

[49] F. T. Pillar and P. Blazek, “Core capabilities of sustainable mass customization,” Knowledge-based confguration from research to business cases, pp. 107 - 120, 2014.

[50] T. M. Choi and S. Guo, “Responsive supply in fashion mass customisation systems with consumer returns,” International Journal of Production Research, vol. 56, no. 10, pp. 3409 - 3422, 2018.

[51] A. Bhatia and R. G. Desai, “Mass Customization in Apparel & Footwear Industry– Today’s Strategy, Future’s Necessity,” WIPRO.

[52] T. Blecker and N. Abdelkafi, “Mass customization: State-of-the-art and challenges,” in Mass customization: Challenges and solutions, New York, Springer, 2006, pp. 1 - 25.

[53] A. Gunasekaran and E. W. Ngai, “Build-to-order supply chain management: A literature review and framework for development,” Journal of Operations Management, vol. 23, pp. 423 - 451, 2005.

International Journal of Computer Applications Technology and Research
Volume 13–Issue 02, 33 – 37, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1302.1005

Evaluation of Brushless Motors Parameters Used in Aeromodeling

E. F. Herinantenaina
Department of Electronic Engineering
Polytechnic Graduate School of Antananarivo
University of Antananarivo, Madagascar

E. Rastefano
Department of Electronic Engineering
Polytechnic Graduate School of Antananarivo
University of Antananarivo, Madagascar

Abstract: This article proposes a technique for evaluating the brushless motors parameters used in the domain of aeromodeling. Given the interest by this type of motor, in-depth analyzes have been made to determine its power consumption. For the simulations, an 11”×4.5” propeller was used. The brushless motor chosen is from the category of permanent magnet synchronous machines.

Keywords: aeromodeling, energy requirement, brushless motor, power consumption, permanent magnet synchronous machines

1. INTRODUCTION

At present time, more and more research work are devoted in design of prototypes in the field of aeromodeling. Many models are designed to meet different needs. To obtain an operational model, the study of the propulsion system is essential. The use of motors, especially brushless motors, is very common. The torque and thrust produced by the motor-propeller coupling are exploited to make the drone fly.

2. TORQUE AND THRUST PRODUCED BY A PROPRLLER

The torque and the thrust produced by a propeller depend on many parameters: physical parameters related to the environment status, parameters related to the propeller, and the speed of rotation of the motor that is used. These elements are essential in determining the power consumption.

2.1 Parameters

Civilian drones must meet certain conditions for their operations to be authorized. In this research work, attention is focused on altitude.

2.1.1 *Air density and athmospheric pressure*

The variation of air density as a function of atmospheric pressure is given by :

$$\rho = \frac{273.P_a}{101325(273+T_t)}\rho_0 \qquad (1)$$

where:

ρ_0 is the air density at sea level such that ρ_0 = 1,293 kg.m^{-3}, T_e the temperature in °C, at an altitude h, and P_a the atmospheric pressure at a given altitude.

The atmospheric pressure P_a varies according to the altitude h and the temperature T_t, and we have [1]:

$$P_a = 101325\left(1-0.0065\frac{h}{273+T_t}\right)^{5,2561} \qquad (2)$$

2.1.2 *Propeller parameters*

The diameter D_p, the pitch H_p, and other parameters shown in Table 1 are used to design a propeller.

Table 1. Parameters of a propeller [1]

Setting	Value	Setting	Value
A	5	**e**	0,83
E	0,85	**C_{fd}**	0,015
λ	0,75	**K_0**	6,11
ζ_p	0,5	-	-

2.2 Theoretical calculations

Two intermediate parameters, denoted C_M and C_T, are used to determine torque and thrust, such as [1]:

$$C_M = \frac{1}{8A}\pi^2 C_d \zeta^2 \lambda B_p^2 \qquad (3)$$

$$C_T = 0{,}25.\pi^3\lambda\zeta^2 B_p K_0\frac{\varepsilon.arctan\left(\frac{H_p}{\pi D_p}\right)}{\pi A+K_0} \qquad (4)$$

with

$$C_d = C_{fd} + \frac{\pi A K_0^2}{e}\frac{\left(\varepsilon.arctan\left(\frac{H_p}{\pi D_p}\right)\right)^2}{(\pi A+K_0)^2} \qquad (5)$$

If ω_m is the rotational speed of the motor expressed in rotations per minute (RPM), k the value of the drag coefficient and b the value of the thrust coefficient, the torque and the thrust produced by a propeller are given by the relations:

$$\mathrm{M} = k.\omega_m^2 \qquad (6)$$

$$\mathrm{T} = b.\omega_m^2 \qquad (7)$$

with

$$k = \rho.C_M.D_p^5 \qquad (8)$$

$$b = \rho.C_T.D_p^4 \qquad (9)$$

The coefficient k is expressed in N.m.s^2, while the coefficient b is expressed in N.s^2

2.3 Simulation results

Table 2 shows the values of the coefficients k and b, for different types of propellers, of dimension Dp×Hp.

Table 2. Coefficients k and b

Propeller	10×5	10×7	11×4,5	11×7
k	9.10^{-6}	15.10^{-6}	12.10^{-6}	22.10^{-6}
b	5.10^{-4}	7.10^{-4}	6.10^{-4}	10.10^{-4}

For the simulations, an 11”×4.5” propeller was used.

Figure 1 shows the variation of the torque as a function of altitude and rotor speed on which, the propeller is fixed.

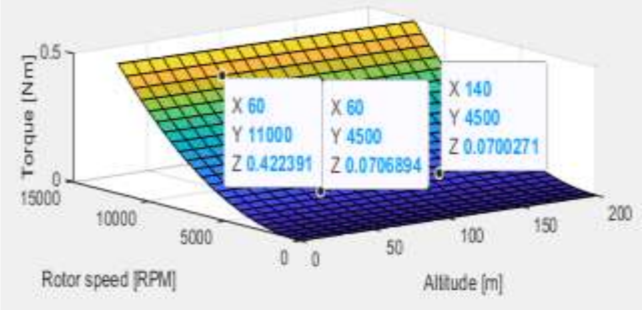


Figure. 1 Torque as a function of altitude and rotor speed

Figure 2 shows the variation of the thrust as a function of altitude and rotor speed on which, the propeller is fixed.

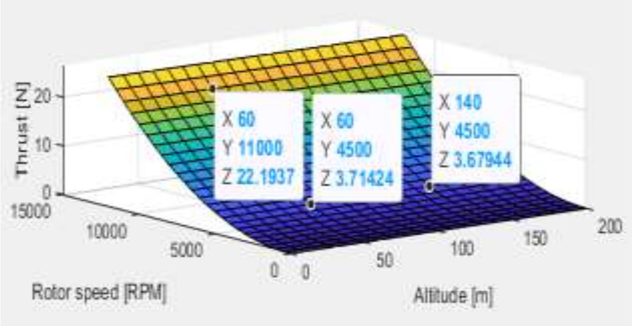


Figure. 2 Thrust as a function of altitude and rotor speed

It can be seen from these figures that the influence of altitude (X) on the torque and thrust (Z) produced by a propeller is insignificant, compared to the influence of speed rotor (Y).

3. BRUSHLESS MOTOR MODELING

In most of research on aeromodeling, brushless motor is used. It is an electric machine, of the category of synchronous machines. In this article, a three- phase brushless motor having a star connection is considered. Figure 3 shows the equivalent circuit of this type of motor.

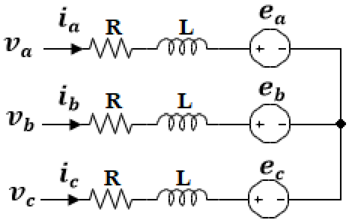


Figure. 3 Equivalent circuit of a three-phase brushless motor with star connection

3.1 Equations of the model

3.1.1 Electrical equations

The electrical equations that govern the operation of a brushless motor are given by:

$$v_a = Ri_a + L\frac{di_a}{dt} + e_a \quad (10)$$

$$v_b = Ri_b + L\frac{di_b}{dt} + e_b \quad (11)$$

$$v_c = Ri_c + L\frac{di_c}{dt} + e_c \quad (12)$$

with:

- $v_{a,b,c}$: voltages of the different phases a, b, and c
- $i_{a,b,c}$: currents in phases a, b, and c
- $e_{a,b,c}$: back electromotive forces or back emf
- R: armature resistance
- L: armature inductance

To operate at variable speed, the brushless motor must be able to be supplied at variable frequency by a three-phase voltage inverter. Figure 4 shows a simplified diagram of a brushless motor control.

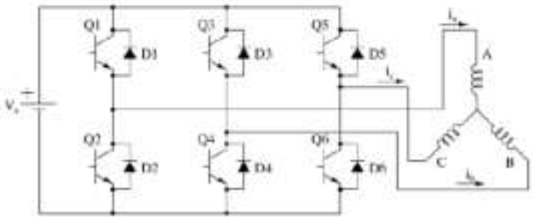


Figure. 4 Simplified diagram of the control of a brushless motor [2]

Switching control always makes it possible to have only one phase connected to the supply voltage, another phase connected to ground and another unconnected [3]. Also, the sum of the currents in each phase is always zero, i.e.:

$$i_a + i_b + i_c = 0 \quad (13)$$

Using this property and considering the voltages between the phases, the three electrical equations that govern the operation of a brushless motor can be reduced to two equations. Thus, we have:

$$v_{ab} = R(i_a - i_b) + L\frac{d(i_a - i_b)}{dt} + e_{ab} \quad (14)$$

$$v_{bc} = R(i_a + 2i_b) + L\frac{d(i_a + 2i_b)}{dt} + e_{bc} \quad (15)$$

3.1.2 Electromechanical equations

The electromagnetic torque generated by a brushless motor is given by equation 16:

$$T_e = \frac{e_a i_a + e_b i_b + e_c i_c}{\omega_m} \quad (16)$$

Using the trapezoidal drive for the motor, the expressions for the back emf are defined by the following equations:

$$e_a = \frac{1}{2}k_e\omega_m Tra(\theta_e) \quad (17)$$

$$e_a = \frac{1}{2}k_e\omega_m Tra\left(\theta_e - \frac{2\pi}{3}\right) \quad (18)$$

$$e_a = \frac{1}{2}k_e\omega_m Tra\left(\theta_e - \frac{4\pi}{3}\right) \quad (19)$$

k_e is the electrical constant of the motor and Tra(θ_e) is a trapezoidal function defined by equation 20.

$$Tra(\theta_e) = \begin{cases} 1 \;\; si\; 0 \le \theta_e < \frac{2\pi}{3} \\ 1 - \frac{6}{\pi}\left(\theta_e - \frac{2\pi}{3}\right) \; si \; \frac{2\pi}{3} \le \theta_e < \pi \\ -1 \;\; si\; \pi \le \theta_e < \frac{5\pi}{3} \\ -1 + \frac{6}{\pi}\left(\theta_e - \frac{2\pi}{3}\right) \; si \; \frac{5\pi}{3} \le \theta_e < 2\pi \end{cases} \quad (20)$$

The relationship between the rotational speed of the motor and the electromagnetic torque can be written as:

$$T_e = k_f\omega_m + J\frac{d\omega_m}{dt} + T_L \quad (21)$$

k_f : coefficient of friction
J: moment of inertia of the motor
T_L: torque load

By using equations (14), (15) and (21), we obtain the state space representation of a brushless motor. This representation is given in equation 22:

$$\begin{bmatrix} \frac{di_a}{dt} \\ \frac{di_b}{dt} \\ \frac{d\omega_m}{dt} \end{bmatrix} = \begin{bmatrix} -\frac{R}{L} & 0 & 0 \\ 0 & -\frac{R}{L} & 0 \\ 0 & 0 & -\frac{k_f}{J} \end{bmatrix} \begin{bmatrix} i_a \\ i_b \\ \omega_m \end{bmatrix} + \begin{bmatrix} \frac{2}{3L} & \frac{1}{3L} & 0 \\ -\frac{1}{3L} & \frac{1}{3L} & 0 \\ 0 & 0 & \frac{1}{J} \end{bmatrix} \begin{bmatrix} v_{ab} - e_{ab} \\ v_{bc} - e_{bc} \\ T_e - T_L \end{bmatrix}$$

3.1.3 Switching sequences

The switching device needs information on the position of the rotor, measured by three Hall Effect sensors (Table 3). This is the angle θ_e mentioned in equation 20. The device must also supply the three phases of the motor, by three half-bridges making it possible to connect each phase either to the DC supply voltage, or to ground [3].

Table 3. Switching sequences

Switching interval	Position sensor			Switch closed		Phase current		
0 – π/3	1	0	0	Q_1	Q_4	+	-	off
π/3 – 2π/3	1	1	0	Q_1	Q_6	+	off	-
2π/3 – π	0	1	0	Q_3	Q_6	off	+	-
π – 4π/3	0	1	1	Q_3	Q_2	-	+	off
4π/3 – 5π/3	0	0	1	Q_5	Q_2	-	off	+
5π/3 – 2π	1	0	1	Q_5	Q_4	off	-	+

On Table 3:

- "+" means that the phase is connected to the power supply,
- "–" means that the phase is connected to ground,
- "off" means that the phase is not connected.

3.2 Simulations

3.2.1 Brushless motor parameters

The brushless motor parameters used for the simulations are shown in Table 4.

Table 4. Brushless motor parameters used in simulations [4]

Setting	Value	Unit
k_f	$7{,}93.10^{-6}$	N.m.s
J	$9{,}26.10^{-6}$	$kg.m^2$
n_p	8	-
R	0,6	Ω
L	0,28	mH
k_e	0,001	$V/rad.s^{-1}$

3.2.2 Presentation of the model

The brushless motor chosen is from the category of permanent magnet synchronous machines. We therefore used the Permanent Magnet Synchronous Machine or PMSM model from SimScape. The six switches of the inverter are made up of MOSFET transistors associated with diodes mounted in antiparallel so that current reversibility is possible.

Figure 05 shows the model adopted to control and/or measure:

- the torque created by the propeller,
- motor speed,
- the currents for each phase,
- the back emf. in each phase,
- and the power consumed by the motor.

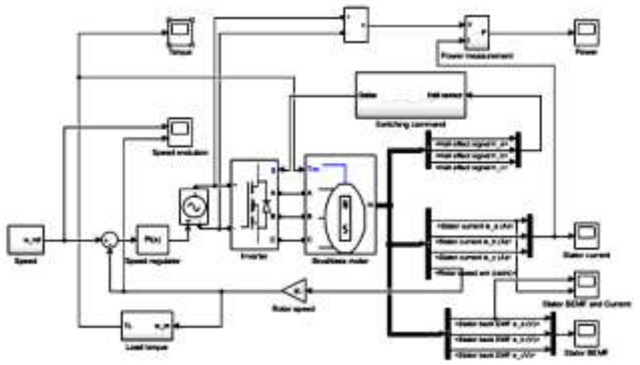


Figure. 5 Closed loop brushless motor speed control

3.2.3 Simulations results

In this section, X-axis represents time expressed in minutes. Figure 6 shows the reference speed, applied to the motor.

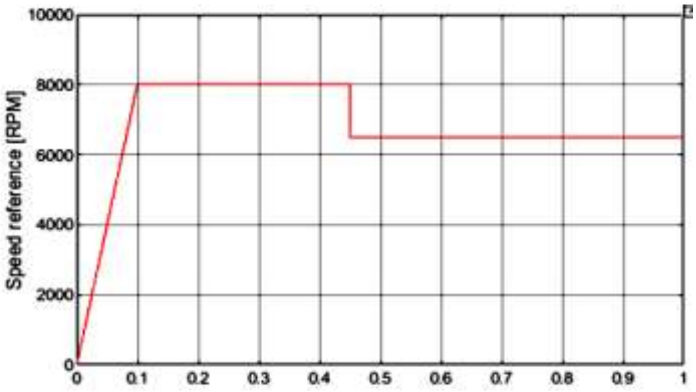


Figure. 6 Reference speed applied to the brushless motor

Figure 7 shows the variation of the torque created by the propeller, as a function of the engine speed (Equation 6).

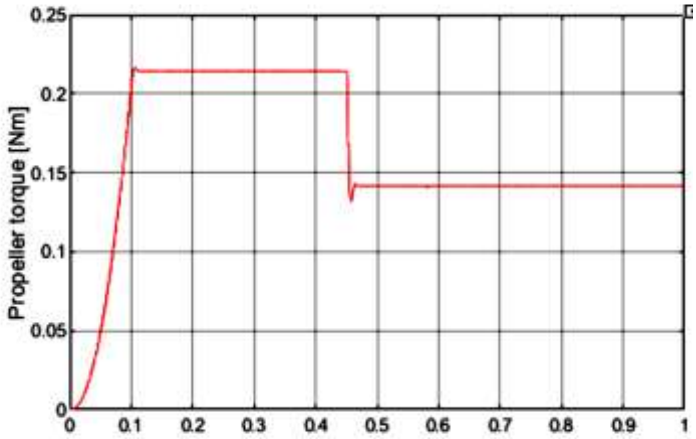


Figure. 7 Evolution of the torque created by the propeller

The torque created by the propeller is 0,2142 Nm when the motor reaches the speed of 8000 RPM. When the speed drops to 6500 RPM, its value is 0,1415 Nm.

Figure 08 represents the measured rotor speed.

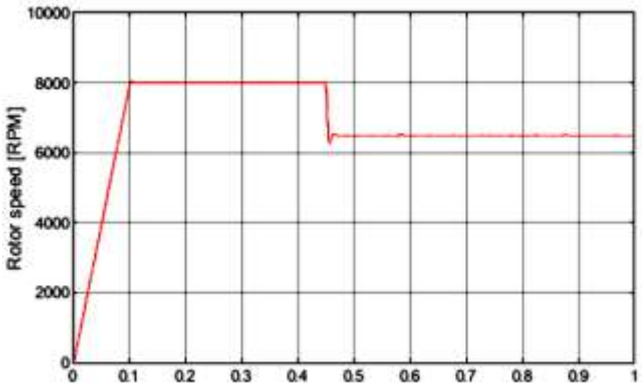


Figure. 8 Measured rotor speed

By comparing Fig. 6 and Fig. 8, it can be seen that the measured speed follows the reference speed.

The current variation in each phase of the motor is shown in Fig. 9.

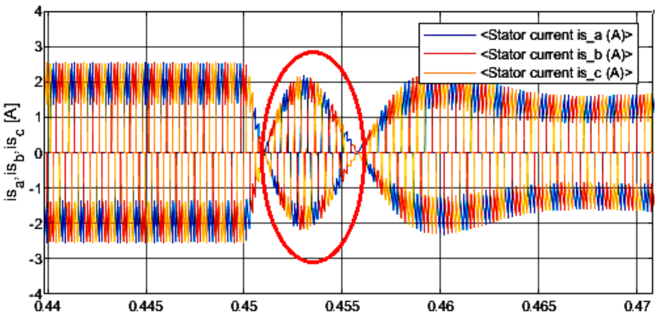


Figure. 9 Variation of phase currents

When the motor is running at 8000 RPM, the current in each phase reaches a peak of ±2.53 A. As the speed decreases, during the transition, this value decreases to ±2.18 A (circled in red). At the new speed of 6500 RPM, we have a peak of ±1.69 A.

Whatever the speed of the motor and taking into account the switching sequences of Table 3, if θ_e ϵ [0, π/3[, phase A is connected to the power supply and phase B, it will be connected to ground.

The variation of the back emf in each phase is given in Fig. 10.

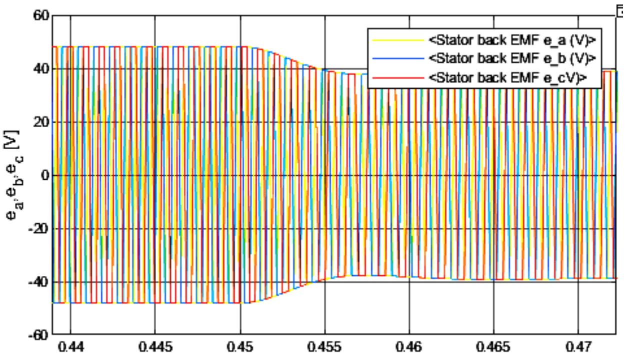


Figure. 10 Variation of the back emf

When the motor is running at 8000 RPM, the back emf in each phase reaches a peak of ±48 V. This value decreases, during the transition. At a speed of 6500 RPM, we have a peak of ±39 V.

Figure 11 shows the variations of the back emf and current in the same phase.

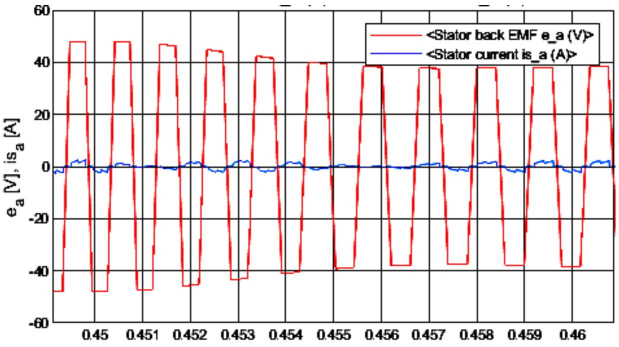


Figure. 11 Variation of the back emf and current in phase A

Figure 12 shows the evolution of the power consumption by the brushless motor.

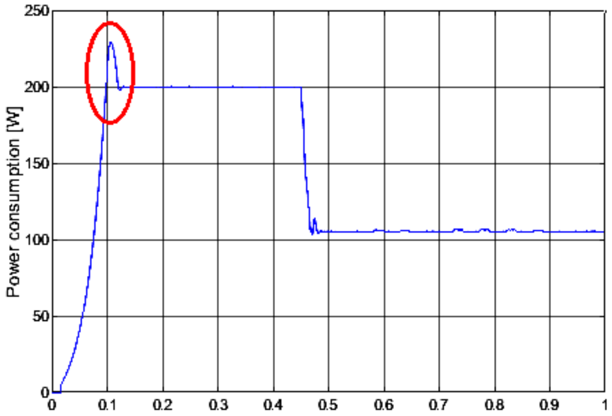


Figure. 12 Evolution of the power consumption by the motor

It can be seen that during starting, the power consumed by the motor reaches a peak of 229 W (circled in red). Afterwards, consumption stabilizes. At 8000 RPM, the motor consumes 200 W. When the speed decreases, the consumed power also decreases. In the simulation, it reaches 105 W for a speed of 6500 RPM.

4. CONCLUSION

Brushless motors have a considerable advantage in the aeromodeling domain. In this papers, the torque and the thrust that a propeller can produce are evaluated. The different parameters that are useful for the design of a propeller have been mentioned. It has been found that rotor speed has the greatest influence on the torque and thrust produced by a propeller.

Considering the interest that presents a brushless motor, its modeling is carried out in order to control the speed and to evaluate at the same time the power consumption. The SimScape tool from MATLAB-SIMULINK is used for the simulations.

5. REFERENCES

[1] Quan, Q. 2017. Introduction to Multicopter Design and Control. Springer Publication

[2] Baldursson, S. 2005. BLDC motor modelling and control. Master thesis. University of Chalmers.

[3] Derumaux, M. 2005. Modélisation des moteurs brushless

[4] Li, X. 2015. Model-based design of brushless dc motor control and motion control modelling for robocup ssl robots.

International Journal of Computer Applications Technology and Research
Volume 13–Issue 02, 38 - 57, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1302.1006

An Improved Security Architecture for Point-Of-Sale System

Terwase, Victor Sesugh
Department of Mathematics and Computer Science
Benue State University
Makurdi, Benue State, Nigeria

Aamo, Iorliam
Department of Mathematics and Computer Science
Benue State University
Makurdi, Benue State, Nigeria

Terwase, Aondona Isaac
Department of Mechanical Engineering
Heriot-Watt University
Edinburgh, United Kingdom

Abstract: Point-Of-Sale (POS) system has become ubiquitous and popular among micro and small-scale businesses such as retail stores, supermarkets, and other businesses for daily transactions especially in Nigeria. Among its numerous advantages such as better inventory management, simple invoicing, quick payment and others, it is fraught with a lot of security challenges or attacks some of which include: malware attacks, key logger attacks, and user identity attacks. The future of this promising technology looks bleak if these breaches or attacks are not identified and checked. This research proposes a detailed novel security architectural design identifying areas of possible breaches and possible solutions. It utilized KMeans clustering and KNearest Neighbour (KNN) algorithms on data collected from POS to classify the data generated and achieved an impressive result of 58.17% clustering separation and 99.51% accuracy classification of data points respectively.

Keywords: Point-of-Sale, Unsupervised Learning, Clustering, Attacks, Malware, Architecture, KMeans Clustering.

1. INTRODUCTION

The term Point of Sale (POS) is used to describe the technology used by a consumer to provide their payment information in exchange for a good or service[27]. POS technology has actually been around for many years with the first cash register dating back to 1879 [1]. However, it wasn’t until the mid-70s that this technology was converted from mechanical to electrical form. Today’s POS systems consist of many of the same components that are found in traditional information systems. One of the key differences between POS systems and other information systems is its key actors or stakeholders [4]. The primary key actors for today’s POS systems are as follows: consumers, merchants, acquirer, issuers, card brand companies, payment processors, payment gateways, software vendors, and hardware vendors. Consumers are those people that use payment cards for the purchase of goods (mostly humans). Merchants are businesses that accept payment cards as a form of payment for goods and services. Merchants are also the implementers of the POS systems [14]. An acquirer, also referred to as an acquiring bank, handles authorization requests from payment processors and settles the transaction with the card issuer. Issuers provide the cards to consumers and maintain the payment card accounts. Card Brands also referred to as card networks (e.g. MasterCard, VisaNet), manage the overall process of authorization and settlement [3]. In the 21st century, the use of electronic payment (e-payment) systems to carryout financial transactions by micro, small and medium scale enterprises have taken center stage in developing and developed economies [5]. Since 2012, the use of point-of-sale terminal popularly called POS terminals to make financial payment and other bank transactions in Nigeria was introduced by the Central Bank of Nigeria (CBN) to promote its cashless policy with the aim of improving payment system. Statistical figures from the Nigerian Inter-Bank Settlement System [22] shows that as of 2018, the number of active POS across Nigeria was 164, 607. This has risen to about 686,577 with over 3 trillion worth of transactions as of March 2021 [22]. The attribution to this growth can be the growing acceptance of POS terminal for making payments and increase in network penetration in Nigerian [5]. Furthermore, the growth of cashless transactions and the impact of the Covid-19 pandemic is expected to drive the global electronic Point-of-Sale (POS) market to reach 2 million units by 2027. POS technology can be found in various businesses such as cafes, bars, hotels, hospitals, gas stations, retail stores, and saloons. Some POS systems are cloud-based, allowing for payments through mobile devices, while others come with added features such as appointment scheduling for saloons[2]. Additionally, many merchants offer POS financing options, allowing customers to make large purchases and pay in installments through companies such as Affirm, Afterpay, and Klarna. Popular POS systems include. Square, TouchBistro, Poster POS, Vend with Vend being a combination of web and mobile.

According to the research conducted by[19], there are a number of POS system categories. A typical POS system is made up of several client computers connected through privately owned connection lines, such as the electronic data exchange (EDI), with local servers at one or more stores (Figure 1). The servers run all data processes for these on-line POS systems, while the client computers provide the user interface operations. Stemming from this strong, server-dependent design is the need to maintain the connection between the server and the clients throughout the processing of a sales transaction as disconnection will result in data loss and force the client(s) to suspend all transactions (sales/entries) until the link is re-established [8]. Subsequently, in this type of POS system, disconnection from the server can be a major hazard, and small business owners, who are vulnerable to the frustrations of their customers, may have to bear the expense of having an in-house server at each store location [19].

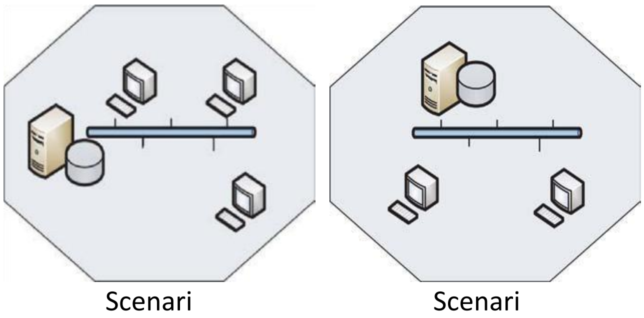


Figure 1   Local Client Server Model for POS system [19].

Moreso, another type of POS system is an off-line, batch-based POS system. In this system, all clients are capable of processing all transactions with their local data cache, and the processed transactions can be transmitted to the server periodically or on demand. For example, salespersons would upload the records of transactions in their handheld POS terminals (clients) when they go off duty. Since this type of off-line POS system is naturally immune to the hazard of being disconnected from the server and does not collect real-time information from its clients, the system will be adequate for certain business environments in which there is weak or limited network connectivity. It is important to note here that, the Electronic Payment System (EPS) functionality of the POS was added to enhance the robustness and easier business transactions to clients.

In a recent article published by the Information Technology Magazine[24], payment terminal malware has stolen $3.3m of worth credit card numbers in the United States alone. In developing countries, there are no concrete data to illustrate the quantum loss in monetary terms or otherwise as a result of malware at the terminals of the POS. The article further pointed out that cybercriminals have used two strains of point-of-sale (POS) malware to steal the details of more than 167,000.00 credit cards from payment terminals which when sold at the underground market is worth $3.3m[18].

Due to advancements in technology, cost reduction efforts, the desire to improve customer satisfaction, and keeping up with global banking trends, the use of electronic devices such as ATMs, POS terminals, and mobile phones for electronic transactions has become widespread in the Nigerian banking industry[6]. These transactions can now be conducted through online platforms, ATMs, POS systems, and mobile phones, among others. This new method of conducting banking business is referred to as Alternative Banking Channels (ABCs) [3]. The ABCs provide a variety of financial services, including cash withdrawals, fund transfers, cash deposits, payment of utility and credit card bills, request for checkbooks, and other financial inquiries. Most transactions on these ABCs are performed with a card, while some require card information.

Table 1 Types of Fraud with Frequencies [23, 22]**.**

YEAR	**CardPresent Fraud (ATM and PoS)**	**Card Not Present Fraud (online and Web)**
2012	1539	314
2013	1739	316
2014	7181	1271
2015	8039	1471
2016	11180	3374

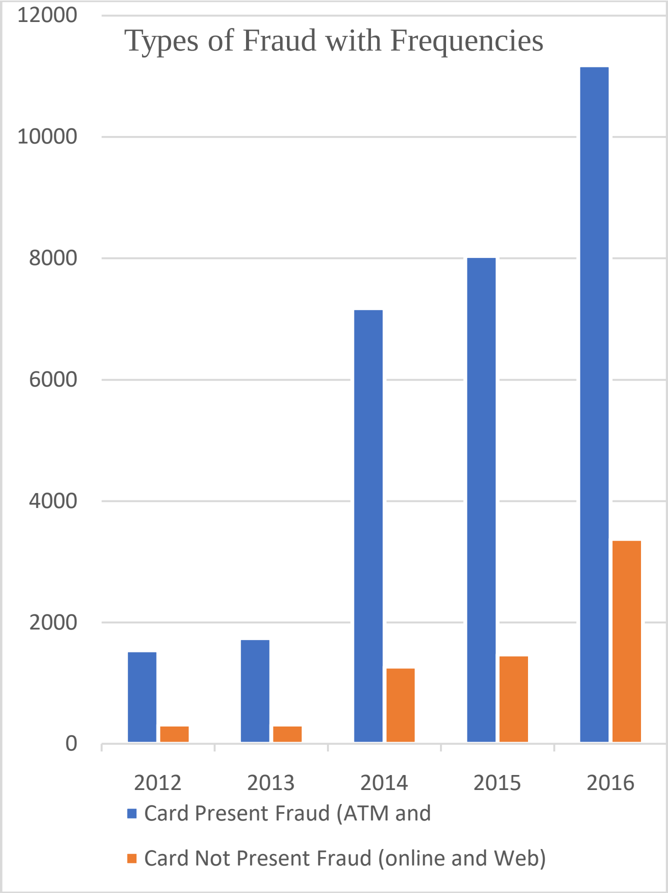


Figure 2 Types of Fraud with Frequencies (card present and card not present).

The number of reported fraud cases on Alternative Banking Channels (ABCs) has been steadily increasing. As shown in Table 1, the number of reported frauds on ATMs and POS terminals rose from 1539 in 2012 to 11,180 in 2016, representing a growth of 626% in just five years. Similarly, the number of reported frauds on online and web platforms increased from 314 in 2012 to 3,374 in 2016, reflecting a growth of 974% in just five years. According to [2], the losses due to fraud through POS terminals increased from N5.8 million in 2013 to N157.6 million in 2014, while mobile banking fraud losses rose from N6.8 million in 2013 to N13.3 million. Meanwhile, the losses due to fraud through ATMs and online banking declined from N1.242 billion to N0.5 billion and from N3.196 billion to N0.875 billion, respectively, over the same period. [23] Annual Report indicates that the actual fraud losses on ATMs, internet banking, POS, and web platforms were N464.5 million, N320.7 million, N243.3 million, and N83.8 million, respectively. The increasing number of fraud incidents on these ABCs may lead to a further loss of public confidence in these technologies, which were intended to provide convenience and comfort in banking and business transactions. Customers are losing trust and confidence in the banking system due to rampant frauds.

This calls for great concern considering the huge amount of monies loss due to security breaches at the POS terminals. Point of sale security is the prevention of unauthorized access to electronic payment systems by individuals who are typically looking to steal customers' personal details such as credit card information [20].Point-of-sale security (POS security) is also the study of vulnerabilities in retail checkout points and prevention of access by unauthorized parties looking to steal customer and payment card details from them. The purpose of POS security is creating a safe environment for customer transactions [11].

POS security aim to create a safe environment for customers to complete their purchases and transactions, and it is an important measure for fostering trust with today's business client or consumers. Understanding the areas where card data is vulnerable provides the area to look at some of the attack methods that have been used by hackers for intercepting payment card data within the POS system [25][10].

By integrating machine learning models into real-time monitoring systems, companies can identify fraudulent transactions as soon as they happen and take prompt action to stop additional losses [4].

Through the use of machine learning techniques and ongoing adaptation to changing fraud tendencies, firms may proficiently identify and avert point-of-sale fraud, safeguarding their funds and reputation.

2. RELATED WORKS AND BACKGROUND

To provide context for our review and analysis, it is important to understand that an Electronic Payment System (EPS) is a separate function from the typical POS function, although the EPS and POS system could be collocated on the same machine. In general, the EPS performs all the payment processing while the POS system is the tool used by the Cashier or Consumer (e.g self-checkout kiosk for the consumer) [14][7]. When looking at the payment systems, it is importantto follow the path the payment card data takes because the data is what is valuable to a hacker. The payment data enters the system via the POI device and then makes its way through processing – as seen in the diagram below. In a store EPS deployment model, the POS and EPS functions are located on separate Machines.

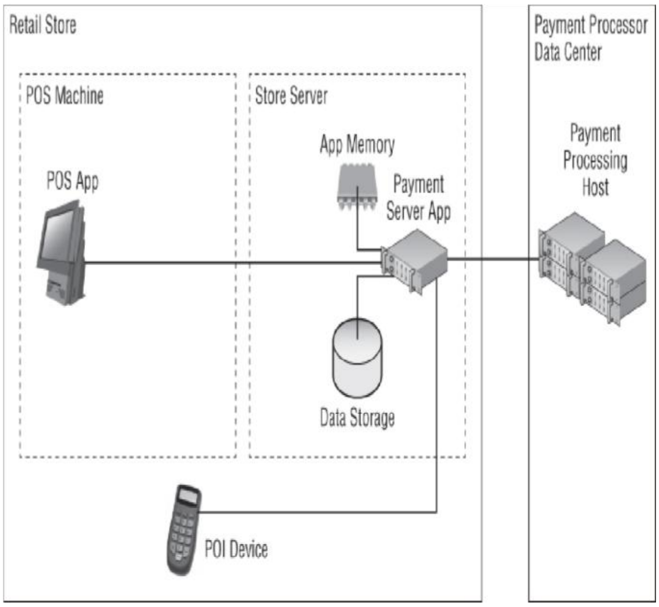


Figure 3 Point of Sale (POS) EPS Deployment Model [14].

Essentially, the EPS is serving as a "middle-man", which prevents any sensitive data from entering the actual POS system. As seen above Figure 3. The POI device connects directly to the EPS (i.e.Store Server) instead of the POS machine. In a POS/ EPS deployment model, the POI function and the EPS function are both are connected on the same system.

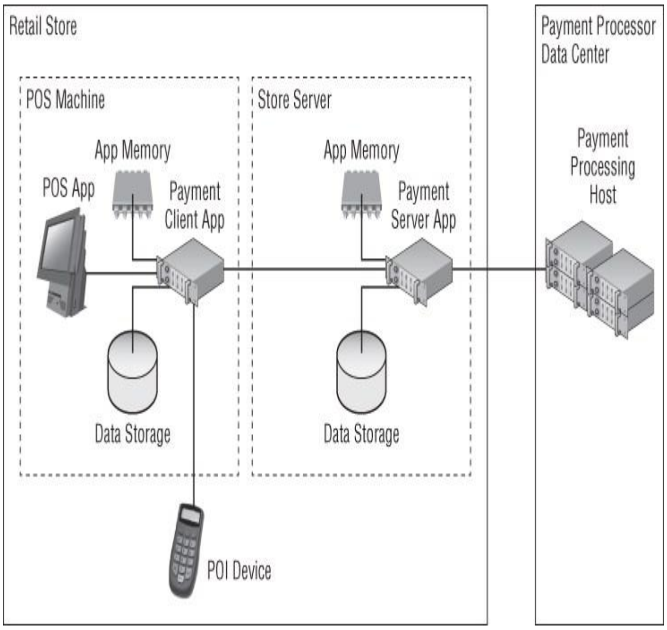


Figure 4Hybrid/POS Store Deployment Model [14].

This places the payment processing function on the actual POS machine. Thus, the POS machine is exposed to sensitive data in this model. In a hybrid/POS store deployment model (Figure 4), the EPS functions are broken up across multiple systems. In this model, multiple machines are exposed to sensitive data creating multiple targets of opportunity for the bad guys[14]. Furthermore, the internal network of these POS deployment models needs to be secured from the bad actors otherwise, this will make the model vulnerable[27].

The deployment models analyzed and depicted so far represent the POS systems seen in most retail stores. However, it's worth mentioning that other deployment models don't fit into the categories above such as gas station payment systems and mobile payments (e.g. NFC). The primary differences between these models and the ones mentioned are that there are a few different pieces of software (e.g. mobile apps) and hardware (e.g. mobile phone, fueling pump)[16].

POS breaches and occupational fraud (fraud committed by an insider) remains on the increase and a lucrative endeavor for fraudsters[21]. Unfortunately, the current retail point-of-sale payment system architecturesarchitecture are fraught with many security challenges and effectively detecting these security challengesis an issue that urgently need to be addressed in other to realize the full potential in the POS payment system. There are several POS systems in Nigeria, and it is reported that there exist several fraudulent activities being perpetrated by some fraudulent POS operators [5]. Some of these criminal activities include: keystroke logging, debiting a customer's account without his/her knowledge, password theft, malware attacks, physical tampering or skimming, identity theft from fraudsters or even dubious persons who use POS in retail supermarkets or businesses just to mention a few Several measures and other architectures have been developed to check some of these crimes/data breaches in POS systems but have not been enough. Most of these attacks or crimes go undetected, this research is motivated by identifying and using effective ways of detecting fraudulent transactions using data from point-of-sale system[13][15].

In [28], "A Novel Approach of Unprivileged Keylogger Detection" focuses on identifying unprivileged userspace keyloggers, which are software applications created to secretly record and capture user keystrokes. The authors stress the need to protect user input on computers and the risks that keyloggers may present, especially in systems like online banking where sensitive data is submitted.The authors draw attention to the fact that the majority of keyloggers used today run in userspace mode, which doesn't need special rights to run. They suggest a method based on detection techniques that compares the I/O activity of processes with simulated user activity in order to detect userspace keyloggers. Keyloggers are said to require a substantial amount of I/O activities in order to record keystrokes, and this pattern can be used for detection.n.

The paper conducts a thorough literature review, outlining the background of keyloggers, how to categorize them, and what research has already been done in the area. As instances of recorded incidents when keyloggers were used maliciously, it also discusses the potential risks and losses brought on by keyloggers[12].

The authors describe their research technique, which include examining different keyloggers' behaviour both with and without simulated user interaction. They offer C++ code samples to demonstrate their methodology and how they altered API calls to find keylogger activity.

The findings section displays their proposal's capacity for detection.

[17] in his research, gives an overview of the rapid developments in mobile telecommunication and handset technology, which have improved user experiences and led to the emergence of powerful smartphones that can mimic desktop computer features.Mobile payment (m-payment) systems have emerged as a result of the advent of products sales over the internet via mobile devices, which has increased the demand for secure payment methods[9]. The researchers emphasized the need for standalone mobile point of sale (POS) apps that cover safe financial transactions is highlighted in this study. Figure 5 shows the system architecture of the POS system we have in mind. In this architecture, the administrative user enters user data into the local database using a stationary computer. Employees use mobile devices to access the POS system, as do managers who use smartphones or tablets. Employees may have additional POS equipment in some circumstances to handle customer payments. Employee mobile devices must support NFC in order to accept mobile payments from customers using NFC-enabled devices. Certificates are issued to system entities by the Certificate Authority (CA) server. Because of the way our system is set up, users with SAFE accounts can pay invoices directly from their accounts. To manage customer payments, the system is additionally connected to the bank's IT server.

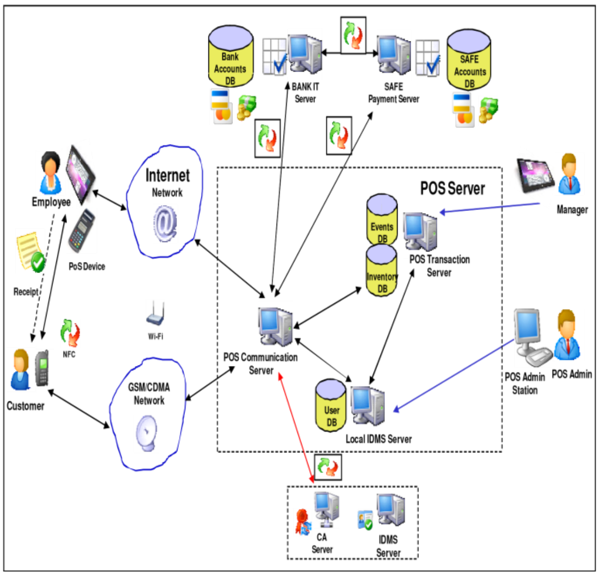


Figure 5System Architecture of the Mobile POS System[17]

Figure 5 shows the internal organization of the POS server that we created. The POS server includes a number of essential parts, such as:

Inventory IDMS (Identity Management System) database

Administration Service Security Manager Transaction Manager Communication Manager A programming language interface (API)

API Manager Service

API for Employee Service

Client/Customer Service API

The Manager application, Employee application, and Customer application are three mobile client applications that connect to the system via their respective APIs.

[16], provided an investigation into the use of various machine learning methods for the identification of "server rotating bill item" fraud in a dataset from a restaurant point-of-sale (POS) system. The effectiveness of several fraud detection algorithms is evaluated in the study, along with the effects of engineering features and artificial features on the models' performance. Here is a summary of the paper's main points:

The research highlighted the significance of feature engineering and model selection in generating accurate findings and shows the promise of machine learning techniques for detecting insider fraud in restaurant point-of-sale data. Decision trees (RandomForest), probabilistic classifiers (NaiveBayes), artificial neural networks (NeuralNet), k-nearest neighbour, linear/kernel-based classifiers (Support Vector Machine), and Adaboost are a few examples of machine learning techniques they employed on data from various restaurants.

3METHODOLOGY

3.1 Overview

This research employs qualitative and quantitative method in data analysis. Based on the literature reviews designed a conceptual architecture and proffer deep analysis on areas of likely breaches and possible solutions. The research assumes that the data contains transactions that are fraudulent and employs unsupervised and supervised machine learning to cluster and obtain insights into the datapoint which could help to detect fraudulent pattern. Unsupervised and supervised machine learning techniquessuch as kMeans clustering and KNearest Neighbour to get some insight and calculate the accuracy of the predictions. Some important metrics were used to evaluate our model.

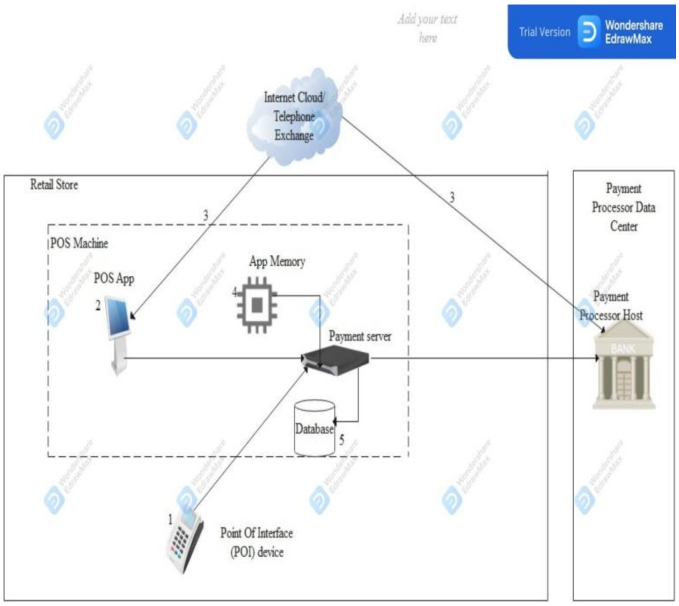


Figure 6Proposed Conceptual Security Architectural Design of POS System.

In our architecture in Figure 6, we try to ensure that we separate the POI terminal from the POS machine(computer) and separate the Point-of-Sale's internal network from the public network. To enhance further security of the model's network, we propose state of the art network security encryption techniques.

POS breach phases don't necessarily have to happen in any particular order but generally there is some consistency in the methodology.

Attacks on Terminals: attacks on the terminals can come from Id_theft, keystroke logger, Skimmers, Firmware, inserted hardware, malware assaults, physical tampering., Internal Network traffic sniffing.

1. Attacks on terminal (1): It has been observed based on experience that, about 3% of point-of-sale (POS) operators especially retail businesses devise devious ways to exploit systematic weaknesses to steal cash, credit card data and stock, either single-handedly or in collusion with other bad actors at the terminal. These fraud techniques hold until detected at a point of historical recovery. Before considering the layers of internal control and data analytics designed to prevent or detect retail POS fraud, here are some outlines of various schemes by which fraud can be perpetrated by POS operators and their collaborators, especially at the terminals.

(a) Manipulating Voids: An employee voids a valid transaction and keeps the money for themself in this type of POS theft. The staff at the grocery store or retail store gives the item to the consumer, but voids it off the bill and keeps the money.

(b) False Refunds: Employees steal real cash transactions in this particular blatant POS theft or attack, returning the money to their personal account after the consumer departs. It is possible for certain retail staff, such as cashiers, to reimburse credit card transactions to their personal credit card account.

1. Public networks are vulnerable if the device does not adhere to accepted modern security standards for credit card payments (PCI DSS) or if there are system vulnerabilities, such as the encryption key being exposed.
2. RAM scraping memory attacks: While a card is swiped or inserted, it details are transiently stored inside the terminal's memory while being transmitted to the payment processor. This presents a brief period for malware on terminals or charged processor reminiscence to copy vital card details.
3. SQL injection through public network to the database.

All the aforementioned attacks at the terminal by the POS employee can be classified under human behavior. Now we can now look at some solutions to these breaches:

1. i. A clear zero tolerance anti-fraud policy that spells out the repercussions for non-compliance, preventing any staff members who are subsequently discovered scamming the company from using ignorance as a defense.

ii. To guarantee individual accountability for every transaction, a mandatory POS login at the beginning of every shift and a mandatory logout at the conclusion are required. Operator logon code sharing should be strictly prohibited.

iii. Cash safes and point-of-sale systems should be placed so that operator activity is constantly visible and within the visual range of CCTV cameras. Printed dockets with the till operator’s ID routinely provided to
the customer so that individual transactions can be traced back to the operator.

iv. There should be Job separation between end-of-day totaling, banking, start-of-day float, refunds, and point-of-sale operations.

v. POS operator awareness that there is a shopper regime in place by which the above controls are randomly checked by anonymous members of management and audit.

A keystroke logger attack is the term for a malevolent computer program that surreptitiously logs the keystrokes that the point-of-sale (POS) user makes. In point of sale (POS) systems, keystroke tracking poses a unique problem to the security manager. Key loggers are devices—either hardware or software—that record characters from a keyboard and send them to a connected computer or point-of-sale system. Keystroke logging have both ethical and unethical application. Among some of the ethical application include. (1) Quality assurance testers analyzing sources of system error (2) System developers and analyst user interaction with systems (3) Employee monitoring (4) Law enforcement or investigators looking for evidence against a criminal suspect.

There are four sorts of key loggers: software, hardware, wireless, and acoustic. Their mode of operation differs on how they capture information. When using hardware or software keyboard loggers, the compromised system stores the log files. Keystroke data is recorded by software key loggers while it is transferred between the operating system and the computer interface. They can be developed as conventional apps or as kernel-based keystroke logging apps that use a hooking technique to record data from the keyboard. Keystroke loggers in both application and kernel software capture keyboard input, write an encrypted copy to a local log file, and then send the data to the operating system.

A hardware key logger is essentially a circuit that is positioned in the space between the computer and keyboard. Hardware key logger is connected directly to the POS keyboard or interface. Once, the key logger is connected, it immediately begins keystroke collection. Character and control code data are captured by the logger's CPU and written to the onboard memory.

Numerous methods have been put forth to identify and counteract this attack. One example of this is the usage of firewalls and anti-malware software on POS system terminals, which occasionally is insufficient to thwart system attacks. Following the criteria of the Multifactor Protection System, One example of this strategy in action is the use of firewalls and intrusion detection systems (IDS) to protect point-of-sale (POS) terminals against malware. Using the Host Based Intrusion Detection System (HIDS) is another method. An intrusion detection system, or HIDS, logs suspicious or malicious activity and analyses traffic on the computer it is installed on. (cybersecurity.att.com). HIDS resides in a single hosting system monitoring and reporting on the system’s configuration and activity. This added level of security protection ensures malware that passes the firewall does not leave the system vulnerable to attack. HIDS has many facets such as signature detection, anomaly detection and stateful protocol analysis detection to protect against malicious threats.

Secondly, another type of attack that might occur at the POS terminal is the skimming attack. Skimming is the illegal use of a rogue physical device, which frequently appears as a component of a POS terminal or other device, to transfer and acquire important data for the malevolent use of a skimmer. The POS system's integrity is compromised via skimming. Skimming devices can be rather complex, tiny, similar to a tiny chip and hard to spot because they frequently blend in with the POS system terminal. Skimmers are capable of recording the data embedded on the magnetic stripe of debit/credit card data as they are inserted into the payment terminals of the POS. The skimmer is installed as an overlay that blends in or is identical to a genuine terminal, or it is concealed inside the terminal's card reader.

2. Internal Network traffic sniffing: At this stage, sniffing may happen, particularly if the adversary (attacker) uses sniffing tools to penetrate the network. When it comes to retail point-of-sale systems, internal networks are used before they are connected to public networks.

The data on a credit or debit card is read and sent over several networks when a customer pays with a swipe at a point-of-sale system, ultimately arriving at the payment processor for the POS retailer. When data moves over these networks, it needs to be secured. Secure Socket Layer (SSL) or other network level encryption is required to secure data on public networks. Credit card numbers and other sensitive data are not needed to be encrypted within internal networks and systems unless they are being stored. Albert Gonzalez exploited this in 2005 by breaking into shop networks using network sniffing tools and collecting millions of credit card numbers as they travelled via internal networks. This type of challenge can be mitigated by the use of network level encryption within the POS retailer’s internal network. Also, the use of point-to-point encryption protects data while undergoing processing.

3. Public network attack: as previously mentioned, data from point-of-sale systems travels via multiple networks prior to reaching the payment processor (bank). If the network does not adhere to the accepted standard for safety procedure for card payment, such as PCI DSS, then critical data or credit/debit card credentials may be vulnerable to attack. Sniffing (using a packet analyzer) is one method of attack.

A denial of service (DoS) assault aims to overwhelm system resources so that no one else can use it, rendering the system unusable or severely slowing down the system or public network for authorized users. The goal of a denial-of-service (DoS) attack could be to stop a user in a point-of-sale system from connecting outside of the network. A DoS attack may also target an entire organization, to either prevent outgoing traffic or to prevent incoming traffic to certain network services, such as the organization’s webpage or data.

DoS attacks have become very common on the Internet. Deliberate or unintentional DoS attacks are both possible. When an unapproved user intentionally overloads a resource, it becomes a deliberate DOS. It is caused accidentally when an authorized user unintentionally does something that causes resources to become unavailable. Most DoS attacks rely upon weaknesses in the TCP/IP protocols. This research work looks at some of the DoS attacks that could occur in an electronic payment system network:

1. SYN Flood Attack

This kind of attack happens when a host receives so many Synchronization (SYN) packets requesting incomplete connections that it is unable to handle valid requests for connections.

A three-way handshake is the series of messages sent by the client and server during an effort to establish a TCP connection between the client and server. Actually, the client system starts by communicating with the server via a SYN (synchronization) message. Subsequently, the server sends the client a SYN-ACK (acknowledgment) message in response to the SYN message. The client then finishes establishing the connection by responding with an ACK message. Next, a connection is established between the client and the server so that the client and the server can exchange service-specific data.

The point at which the server system has acknowledged the client (SYNACK) but has not yet received the final ACK message is where abuse might occur. This is referred to as a half-opened connection. The server includes a built-in data structure that lists all pending connections in its system memory. This data structure is of a particular size, and it can be made to overflow by intentionally creating too many partially opened connections.

With IP spoofing, creating a partially opened connection is a simple task. The source address of the SYN packets that the attacker's system seems to be sending to the victim's server is really spoofing a system that is not currently connected to the network. This implies that the final ACK message is never sent to the victim server. Because the source address is spoofed, there is no way to determine the identity of the true attacker when the packet arrives at the victim’s system.

2. Teardrop Attack

The method used to reassemble fragmented IP packets is a vulnerability that teardrop attacks target. Fragmentation is required when IP datagrams are larger than the maximum transmission unit of a network segment that the datagrams must pass through. Each fractured packet's IP header contains an offset that indicates where the fragment fell within the original, unfragmented packet, allowing packets to be correctly reassembled at the receiving end. In a Teardrop attack, packet fragments are deliberately forged with overlapping offset fields, causing the host to hang or crash when it tries to reassemble them. Figure 7 shows that the second fragment packet purports to begin 20 bytes earlier (at 800) than the first fragment packet ends (at 820). The offset of fragment packet 2 is not in accord with the packet length of fragment packet 1. This discrepancy can cause some systems to crash during the reassembly attempt.

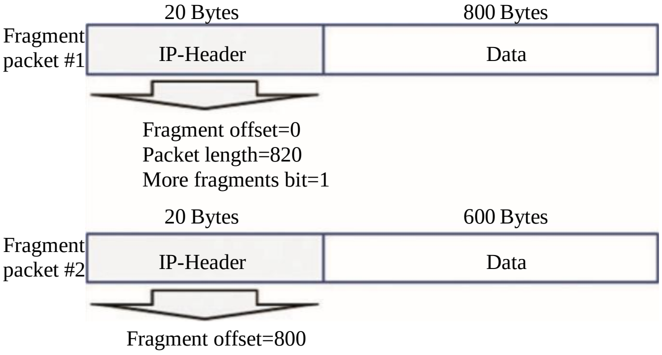


Figure 7**A** Tear Drop Attack.

3. UDP Flood Attack

Since UDP is a connectionless protocol, data transfer can occur without the need to establish a connection. When a hacker sends a UDP packet to any random port on the target system, it could result in a UDP flood attack. The victim system will identify the program that is waiting on the target UDP port upon receiving a UDP packet. Two scenarios could occur. The victim host will create an ICMP packet with a destination unreachable to the forged source address if there isn't an application listening on the port (closed UDP port). However, if there is an application running on the destination UDP port, then the application will handle the UDP packet. In both cases, if enough UDP packets are delivered to destination UDP ports, the victim host or application may slow down or go down.

We now analyze how the use of biometrics can mitigate against some of these public network attacks.

The term "biometric" comes from the Greek words "bio" (life) and "metric" (to measure). Biometrics refer to technologies used for measuring and analyzing a person's unique characteristics. In the security analysis research experiments results demonstrated clearly that tested biometric readers are very vulnerable to common Denial of Service (DoS) attacks, and their recognition performances significantly deteriorate just after launching the attacks.

Biometric devices can be easily crashed or disconnected from the network by common DoS attacks. The following lists some basic security considerations that should be taken into consideration when designing secure biometric readers to limit the effect of DoS attacks:

(a)The biometric reader's user interface should allow the filtering of network packets, such as blocking all incoming ping requests.

(b). Network traffic with high-speed rate targeting the biometric reader should be denied from reaching the kernel of the reader. This would allow protecting the reader from many common DoS flood attacks, such as SYN flood attack.

(c) The ARP cache of the biometric reader should be static, so that malicious ARP packets cannot update its contents with fake IP/MAC entries. This would allow protecting the reader from DoS attacks based on ARP cache poisoning attack.

One way to mitigate this type of attack is the use of double encryption data (Encryption data and use of SSL).

4. RAM scraping memory attack: This is the type of attack where the terminals of POS system is attacked with a malware to copy card data which is then transmitted to the attacker. When a card is swiped, it's details are briefly stored at the terminal's memory while being transmitted to the payment processor. This provides a brief window on the terminal to copy the card data which is then transmitted to the attacker. This technique is referred to as RAM-scraping. RAM-scraping malware is used to collect numbers as they are read into the POS terminal's memory. Any gathered data is locally stored in a file until it is transferred to the attacker's computer, hopping through internal networks until it reaches a system designated by the hacker that has access to external network. In this type of attack, the attacker may hijack an internal system to act as a staging server. The adversary (attacker) may attempt to identify a server that communicates with the POS system often and leverage on a normal communication to avoid detection. Any data collected by the RAM-scrapping malware will be sent to the staging server where it is collected over some time and transmitted to the attacker. The data is transferred through internal servers before finally arriving at a hacked external FTP server.

Credit cards also contain a three- to four-digit number printed or embossed on either the front or back side called the CVV, "Card Verification Number (CVN)," "Card Security Code (CSC)," "Card Validation Code (CVC2)," or some other similar term depending on the credit-card-issuing institutions. These institutions have different names for this number but it is a security verification feature used in "card-not-present" transactions (e.g., made via telephone, mail order, online, etc.). Merchants cannot physically verify if cards are present for transactions. It is important to note that by design, this number is not stored in Tracks 1 and 2 and without it, an exact counterfeit credit card cannot be created.

The Primary Account Number (PAN) format, defined in ISO/IEC 7812, is commonly 16 digits long but can reach up to 19 digits and has the following format: IIII-IIAA-AAAA-AAAC.

The first six digits are known as the "Issuer Identification Number (IIN)." In a credit card processing, the length of individual account can reach up to 12 digit the final digit is a check which is calculated using the Lunn Algorithm. It has been identified that POS RAM scrapers generally use regular expression (regex) matches to search for and harvest Tracks 1 and 2 credit card data from the process memory space in the RAM. The complexity of the regex determines how it can correctly/incorrectly capture non-essential data from the RAM in addition to valid card data. A well-defined regex will return clean results but may be computationally more expensive compared with a looser one. If the hacker's goal is to quickly capture data from the RAM, efficiency is more important than quality. To circumvent bad data problems, some PoS RAM scrapers implement Luhn validation to check the card data harvested prior to exfiltration.

Payment Card Industry (PCI) compliance for validating ex-filtrated data offline before selling it in underground forums.

The remedy from some of the loopholes exploited by POS Ram Scrappers can be remedied by applying the PCI Data Security (PCI DSS) framework in addition to other security measures.

PCI Data Security Standard (PCI DSS) refers to a set of requirements designed to ensure that all companies that process, store, or transmit credit card information maintain a secure environment.

PCI DSS does not offer new secure technologies to protect electronic payment systems but provides requirements to build up layers of security control around existing ones. PCI DSS v1.0 was published in December 2004, long after electronic payment systems were developed and deployed worldwide. At this point, defining, developing, and deploying a brand-new secure technology standard for payment cards would be extremely expensive.

PCI DSS has the following major requirements:

(1) Install and maintain a firewall configuration to protect cardholder data.

(2) Do not use vendor-supplied defaults for system passwords and other security parameters.

(3) Protect stored cardholder data.

(4) Encrypt cardholder data when transmitted across open, public networks.

(5) Protect all systems against malware and regularly update anti-malware solutions.

(6) Develop and maintain secure systems and applications.

(7) Restrict access to cardholder data on a need-to-know basis.

(8) Identify and authenticate access to system components.

5. SQL Injection through public network: As the adversary gain access to the public network server and traverse to the payment processor's network, the attacker may exploit vulnerabilities in the payment processor's network or exploit other techniques such as SQL Injection to gain access to the payment processor's database.

In recent times, the internet plays a very vital role in web applications, various Web application are signed up and make transaction through the retail point of sale terminal. Some of the POS terminals are used in sending mail, acknowledgement of goods purchase and other internet related activities thereby making the data stored on the internet to become huge in size and more valuable. Generally, some of these web applications that run on POS terminals consist of front-end, database back-end. Database is central to the web application, it stores those necessary data including users' names, passwords, various statistics, financial information and so on.

Structured Query Language (SQL) provide a way to manipulate data and change a database structure. SQL injection attacks allow hackers get access to vital information without authorization and authentication, thereby causing serious harm to the web application. SQL injection vulnerabilities provide an entrance for hacker to execute SQL statements on database. Therefore, the hacker can harvest any sensitive information and even can destroy the database. Different measures exist to mitigate against SQL injection but there are no standard one yet established. SQL injection attacks destroy the confidentiality, integrity and availability of the target system completely. The cost of SQL injection attacks varies with the value of information stored in the database. In 2009, Kaspersky was hacked through SQL injection and a lot of data was leaked including users, activation codes, lists of bugs, admins. This event not only caused economic loss owing to the stolen activation code but also affected its reputation as a security company seriously. In the case of electronic payment system like the POS, the monetary cost could be very huge and devastating to the victim.

In general, SQL injection attacks can cause the following effects:

- Data leakage
- Data modification
- Hacker getting full control of the database
- Hacker getting complete control of the host system

There are different attack methods against SQL injection vulnerabilities some of these attacks include:

1.Tautologies

This attack stems from the vulnerability which displays all query records on the web page of the front end in a web application. In this type of attack, all records of current table can be gotten through constructing query statements with where clause that always return true.

2. Union queries

Due to the fact that the union keyword requires two query statements having equal number of fields, the number of fields of the former query statements must be guessed by observing the error messages generated by

order by 'keyword. This attack is against the vulnerability which can display more than one query records and SQL error messages on the web page. This method can get additional information by concatenating the results of malicious query statements behind original query results, for instance, the name of the database and records of other tables and so on.

3. Boolean-based

A generic web page will be displayed instead of a database error message when there is an error in query statements. This page will also be shown when the query result is null. In this type of scenario, the error-base exploitation will not work in this situation. The Boolean-base exploitation technique which constructs a series of Boolean queries with some special built-in function (ex. Ascii(), length(), substring()) against the server can work perfectly because of the different responses to WHERE clause. When the where clause returns true the back-end will display some query result. In the event that the where clause return false, nothing will be displayed. By this method, the attacker can infer some useful information through the response.

4. RESEARCH METHODS AND MATERIALS

The dataset used is unlabeled and to achieve one of objectives in this research, we used an unsupervised machine learning called KMeans clustering. We employed KMeans clustering to find some shared features with collection of observations with similar characteristics. KMeans Clustering is comparatively fast, simple compared to other algorithms and preferable especially when dealing with very large dataset.

However, this algorithm employed is relatively sensitive to large outliers and the seed i.e the starting condition that is used to initialize the algorithm. Also, as the dimension increases, a distance-based similarity measure converges to a constant value between any given samples. We can overcome this by using principal component analysis (PCA) on the feature data to modify the clustering algorithm however, as observed in our dataset, the number of dimensions is relatively small. From our observation of the dataset, all our features are numeric and to achieve the objective of analyzing and discovering hidden pattern patterns from our point-of-sale data, we need to understand the main steps and logic in our program.

In other to analyze POS dataset to gain insight and detect fraudulent patterns, we employ the use of unsupervised machine learning models: KMeans Clustering, KNearest Neighbor (KNN). This is because our POS dataset is without label and we try to mine or extract patterns that would provide insight from the dataset which can aid segregate and classify fraudulent datapoints with greater degree of accuracy. Some of the research tools used includes:

Software:

Visual Studio Code or Google Collaboratory, Microsoft Excel.

Libraries:

Pandas, Numpy, Matplotlib, Seaborn, Sklearn, Keras, TensorFlow.

Hardware:

Configuration:

HP Pavilion DV 6, Intel Core I5, 600GB HDD, 2.3GHz Dual Core Processor, 8Gb RAM, Windows 10 Operating System.

Programming Language:

Python Programming

4.1 Dataset Collection and Description

This research was conducted using a combination of literature review. The literature review involved a comprehensive analysis of existing research on POS system security, including studies on security breaches, vulnerabilities, and countermeasures. This helped to identify the key security challenges faced by POS systems. The study also involved an in-depth analysis of the security practices and systems used by three large retailers. Data was collected through a supermarket data for a period of Four Months [26]. This helped to validate the findings of the literature review and to gather practical insights into the challenges faced by POS systems in real-world settings.

The data used was retrieved from retail supermarket checkout/POS system logs and cashier operations stored in XML files, which contained various low-level transactional data [26]. Once extracted, it was aggregated into six CSV files with the most important information about (i) transactions; and (ii) cashier operations, refer to Table 1, respectively. The data concerns retail operations in a grocery supermarket, equipped with manned (service) and self-service checkout.

Table 1 Transactions Data: Fields, Data types and Descriptions.

Field	Type	Description
WorkstationGroupID	Integer	Type of checkout: service, self-service
TranID	Numeric	Transaction ID (date, store ID, checkout ID, sequence no.)
BeginDateTime	Date/Time	Date and time of transaction start
EndDateTime	Date/Time	Date and time of transaction end
OperatorID	Integer	Unique cashier ID
TranTime	Integer	Transaction time in seconds
BreakTime	Integer	Break (including idle) time in seconds
ArtNum	Integer	Number of items, i.e., basket size
TNcash	True/False	Cash payment flag (true when transaction paid in cash)
TNcard	True/False	Card payment flag (true when transaction paid by a card)
Amount	Numeric	Transaction value
WorkstationGroupID	Integer	Type of checkout: service, self-service

WorkstationGroupID: This feature refers to the group or location of the workstation where the transaction was carried out. It is an integer value.

TranID: This feature refers to the unique identifier of the transaction. It is a float value.

BeginDateTime: This feature refers to the date and time when the transaction began. It is a string (object) value.

EndDateTime: This feature refers to the date and time when the transaction ended. It is also a string (object) value.

TranTime: This feature refers to the duration of the transaction in seconds. It is an integer value.

BreakTime: This feature refers to the duration of the break taken during the transaction, if any, in seconds. It is an integer value.

ArtNum: This feature refers to the article or product number associated with the transaction. It is an integer value.

TNcash: This feature is a boolean value that indicates whether the transaction was carried out using cash as the payment method (True) or not (False).

TNcard: This feature is a boolean value that indicates whether the transaction was carried out using a card as the payment method (True) or not (False).

Amount: This feature refers to the monetary value of the transaction in the local currency. It is a float value

OperatorId: This feature refers to the unique identifier of the operator who carried out the transaction. It is an integer value.

4.2 Feature Selection and Engineering

The features selected from the dataset in our experiment were: TranTime, BreakTime, ArtNum, Amount because the data points were clearly separable on the pairplot chart as shown in Figure 7.

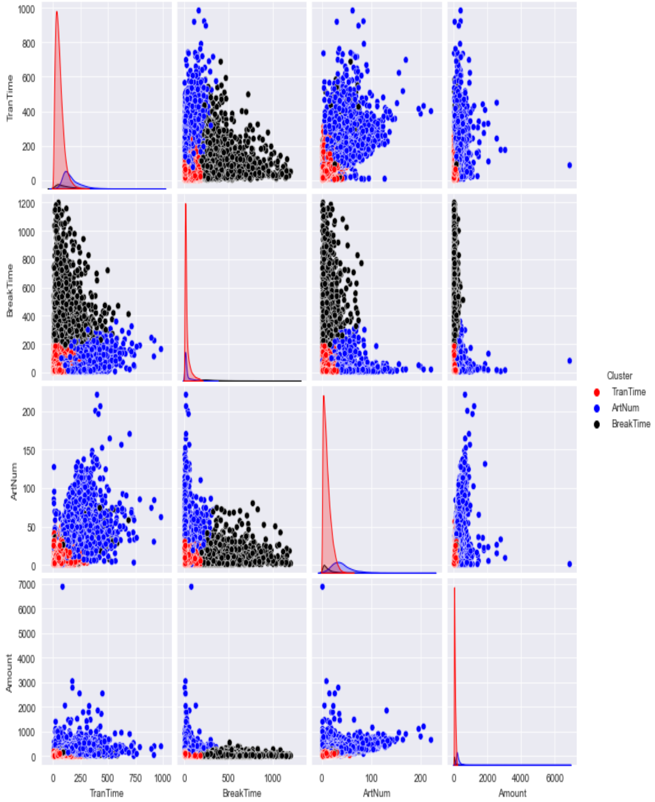


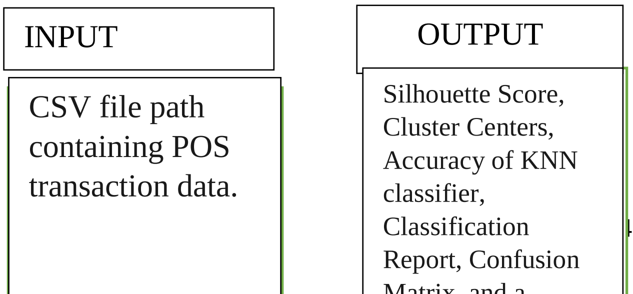
Figure 8 Pairplot Showing Separability of the Selected Features.

The pairplot in figure 8 also referred to as scatterplot matrix is used to understand and get insights into the best set of features to explain the relationship between two variables or to form the most separated clusters. It is particularly useful when there are multiple features and there is a need to understand how they relate with one another. It also aids in forming simple classification models by drawing some simple lines or make linear separation in the dataset. Diagonal Plots represent the distribution of a single variable uusually histograms or kernel density plots.Off-diagonal Plots are scatter plots showing the relationship between two variables. The colors represent different clusters. The diagonal plot indicates a Kernel Density Estimation (KDE) which is a way of looking at the distribution of the data. The pairplot creates a scatterplot which is colored according to its cluster assignment. This is used as a visualization tool for exploring how well-separated are the fratures, and based on the selected feature. If clusters are well-separated in some pairs of features but not in others, this can suggest that the well-separated features are more important for distinguishing between clusters. For example, if one variable tends to increase as the other increases, an upward-sloping trend in the scatter plot is visible.The pair plot also provides a comprehensive view of the pairwise relationships between all variables in the dataset, which can be particularly useful in multivariate analysis. In Figure 8, We have four features and are trying to create a pair of plots, we have four combination two ($4C_2 = 6$) which equates to 6 plots for visualization above and below the diagonal. The trantime (red color) feature in the x column and the breaktime (black color) feature are well separated in the second column of the grid implying that, this well separated features are important in our clusters. Also, the ArtNum(blue color) feature is well separated from the trantime feature in the third column and first row of the grid this further imply that a good model can be developed from these features. Likewise, the breaktime feature and artnum are well separated in the second column and third row of the grid which implies its suitability as a good feature to build a model. We can infer from the plot in Figure 8, in row 3 column 2 that as the ArtNum(the product number associated with the transaction) feature increases, the breaktime(idletime) feature increases forming a slightly gentle slope. This implies that there is a correlation between these two features.

In summary, the clusters are well separated especially between the red(trantime) and the blue (ArtNum). Additionally, there is a positive correlation trantime and breaktime.

4.3 Program Algorithm

The algorithm combines K-means clustering and K-nearest neighbors' classification to cluster the data and predict the cluster labels of new data points. The accuracy and other metrics help assess the performance of the clustering and classification tasks. Figure 8 shows the schematic representation of the program algorithm.


INPUT

CSV file path containing POS transaction data.

OUTPUT

Silhouette Score, Cluster Centers, Accuracy of KNN classifier, Classification Report, Confusion Matrix, and a

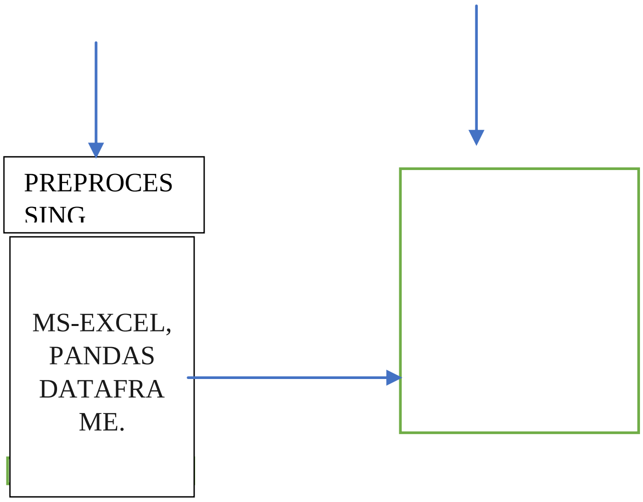


Figure 9 Schematic Diagram of the Program Algorithm

The following detailed processes were performed:

1. **Data Loading and Preprocessing:**
   - Import required libraries: pandas, numpy, KMeans from sklearn.cluster, train_test_split, silhouette_samples, silhouette_score, KNeighborsClassifier, accuracy_score, classification_report, confusion_matrix from sklearn.metrics, and matplotlib. pyplot and seaborn for data visualization.
   - Read the data from the CSV file 'dataset/POS_transactions_data.csv' into a pandas DataFrame named pos_df.
   - Select the numeric columns "TranTime", "BreakTime", "ArtNum", and "Amount" from the DataFrame and store them in X.
2. **Choose the Elbow Method for Optimal Cluster Choice:**
   i. Calculate KMeans clustering with different values of n_clusters (ranging from 2 to 10).
   ii. Compute the inertia (sum of squared distances from each data point to its assigned cluster center) for each n_clusters and store them in the list inertias.
   iii. Plot a graph to visualize the relationship between the number of clusters and the inertia to identify the optimal number of clusters (K) using the elbow method.
3. **Apply KMeans Clustering:**
   - Choose the number of clusters (K=3) based on the Elbow Method and create a KMeans model with n_clusters=3 and random_state=42.
   - Fit the model to the data points (X).
4. **Cluster Centers:**
   - Get the cluster centers' coordinates and create a DataFrame named cluster_centers_df with the columns "TranTime", "BreakTime", "ArtNum", and "Amount" to represent the centers of each cluster.
5. **Silhouette Score:**
   - Calculate the Silhouette clustering result with n_clusters=3 of the clusters.
6. **Assign Cluster Labels to Data Po**
   - Predict the cluster labels using the trained KMeans model.
   - Create a new DataFrame X_with_labels by concatenating the original X with an additional column "Cluster" containing the cluster labels.
   - Map the cluster labels to their corresponding feature names using the label_map dictionary.
7. **Data Visualization:**
   - Create a pairplot of the data points in X_with_labels, with points colored by their cluster assignment.
8. **Splitting Data into Train and Test Sets:**
   - Split the data into training and testing sets using train_test_split, with a test size of 20% and a random state of 42.
9. **Training KNN Classifier:**
   - Create a KNN classifier with n_neighbors=3 (3 nearest neighbors) and train it on the training data.
10. **Predicting Cluster Labels for the Test Set:**
    - Use the trained KNN model to predict the cluster labels for the test data.
11. **Evaluating KNN Model Accuracy:**
    - Compare the predicted cluster labels (y_pred_clusters) with the true cluster labels (y_test) and calculate the accuracy of the KNN model.
12. **Classification Report and Confusion Matrix:**
    - Generate a classification report to show precision, recall, F1-score, and support for each cluster label.

- Calculate the confusion matrix to evaluate the KNN model's performance.

13. **Visualization of Confusion Matrix:**
    - Create a heatmap of the confusion matrix using seaborn to visualize the KNN model's performance.

Below is the detailed Algorithm for our program:

1. **Input**: CSV file path containing POS transaction data.
2. **Output**: Silhouette Score, Cluster Centers, Accuracy of KNN classifier, Classification Report, Confusion Matrix, and a heatmap.

Algorithm Steps:

```
Begin.
Step 1: Import the required libraries: (Numpy, sklearn, seaborn, pandas, matplotlib).
Step 2: Read data from the dataframe.(pos_df).
Step 3: Select Numeric Columns.
        -TranTime, BreakTime, ArtNum
Step 4: Use the Elbow Method to determine the optimal number of clusters.
        - Set a range of cluster options from 2 to 10.
        -for each cluster option:
        a. Apply KMeans with the given number of clusters to 'X'.
        b. Calculate the inertia (within-cluster sum of squares) and store it in the 'inertias' list.
Step 5: Apply KMeans clustering with the selected number of clusters (3 in our case) to 'X'.
        - for n_clusters in Option:
            - Apply KMeans clustering with given number of Clustering.
            - Calculate the inertia (within-cluster sum of square) and store it in the inertia list.
            - Plot the number of clusters (K) against the inertia values to find the "elbow point," which indicates the optimal number of clusters.
Step 6: Compute and display the cluster centers for each cluster.
Step 7: Predict cluster labels for the data points in 'X' using the trained KMeans model.
Step 8: Compute the Silhouette Score to evaluate the clustering performance.
Step 10: Create a mapping from cluster labels to feature names (‘numeric_cols’).
Step 11. Add the predicted cluster labels to 'X' DataFrame and map
        the cluster labels to feature names.
Step12. Visualize the data using a pairplot colored by cluster assignment.
Step13. Split the data into train and test sets (80-20 split).
Step 14. Train a K-nearest neighbors (KNN) classifier with the
        number of neighbors set to 3 using the training data.
Step 15. Predict cluster labels for the test set using the KNN classifier.
Step 16. Evaluate the accuracy of the KNN classifier by comparing
        the predicted cluster labels with the true cluster labels from the test set.
Step 17. Print the accuracy of the KNN classifier.
Step 18: Print a classification report, which includes precision, recall,
        and F1-score for each cluster label.
Step 20: Create a confusion matrix to visualize the classification
        performance of the KNN classifier.
Step 21: Generate a heatmap of the confusion matrix, where the x-
        axis and y-axis are labeled with the predicted and true cluster labels, respectively.
End.
```

4.4 Evaluation Metrics

To evaluate our proposed model, we employed the use of the following metrics:

1. **Accuracy:** Refers to the ratio of correctly predicted observation to the total observation.

In machine learning, accuracy is one of the metrics used to evaluate the performance of a classification model. It measures the proportion of correctly classified instances out of the total instances in the dataset. In other words, it tells us how many predictions made by the model were correct compared to the actual labels.

To understand accuracy in the context of a confusion matrix, let's first define what a confusion matrix is:

A confusion matrix is a table that is used to evaluate the performance of a classification model. It presents a summary of the model's predictions on a classification problem where the true values of the target variable are known. The matrix consists of four components:

1. **True Positives (TP):** The number of instances that are correctly predicted as positive by the model.
2. **True Negatives (TN):** The number of instances that are correctly predicted as negative by the model.
3. **False Positives (FP):** The number of instances that are incorrectly predicted as positive by the model (i.e., the model predicted positive, but the true label was negative).
4. **False Negatives (FN):** The number of instances that are incorrectly predicted as negative by the model (i.e., the model predicted negative, but the true label was positive).

Using these components, we can define accuracy as follows:

Accuracy = (TP + TN) / (TP + TN + FP + FN)

Accuracy represents the overall correctness of the model's predictions. It measures the percentage of correct predictions out of all the predictions made by the model. It is a common metric, especially when the class distribution is relatively balanced, meaning the number of instances in each class is similar.

However, accuracy may not always be the best metric to evaluate the model's performance, especially in cases where the class distribution is highly imbalanced. For instance, if the positive class is rare, and the model predicts most instances as negative, the accuracy might be high even though the model is not performing well on the positive class.

In such cases, it is essential to consider other metrics like precision, recall, F1-score, or area under the ROC curve (AUC-ROC) to get a more comprehensive view of the model's performance and how well it is performing for each class.

1. **Precision**: Precision, also referred to as positive predictive value, measures the proportion of true positive predictions (correctly predicted positive instances) out of all positive predictions made by the model. It is a measure of how many of the predicted positive instances are actually positive.

Precision= TP / (TP + FP).

High precision indicates that the model has a low rate of false positives, meaning that when it predicts a positive class, it is likely to be correct.

2. **Recall**: Recall, also known as sensitivity or true positive rate, measures the proportion of true positive predictions (correctly predicted positive instances) out of all actual positive instances in the dataset. It is a measure of how many of the actual positive instances are correctly predicted by the model. Usually given as:

Recall= TP / (TP + FN).

High recall indicates that the model has a low rate of false negatives, meaning that it correctly identifies most of the positive instances.

3. **F1-score**: The F1-score is the harmonic mean of precision and recall. It is used to balance the trade-off between precision and recall. The F1-score provides a single metric that takes both precision and recall into account. It is expressed as:

F1-score = 2 * (Precision * Recall) / (Precision + Recall).

The F1-score ranges from 0 to 1, where 1 represents a perfect model, and 0 indicates poor performance.

The F1-score is particularly useful when we want to find a balance between precision and recall. It is commonly used when the class distribution is imbalanced, and the model needs to perform well for both positive and negative classes.

5. RESULTS ANALYSIS AND DISCUSSION

5.1 Overview

In this chapter, we present the methodology and results of our research on an improved security for point of sale (POS) systems. The study aimed to explore the current security challenges faced by POS systems and to propose a new architecture that analyzes and identify these challenges.

Based on the findings of the literature review and case studies, we propose a new security architecture design for POS systems that identify the following key elements as possible solutions to the various attacks already discussed:

1. End-to-end encryption: To protect sensitive data, such as credit card numbers and personal information, from being intercepted or stolen during transmission.

2. Tokenization: To replace sensitive data with unique, non-sensitive tokens, reducing the risk of data breaches.

3. Multi-factor authentication: To provide an additional layer of security by requiring multiple forms of identification, such as a password and a fingerprint, to access the POS system.

4. Regular security assessments: To identify and address vulnerabilities in the system on a regular basis.

5.Employee training: To ensure that all employees understand the importance of security and know how to follow best practices to protect sensitive data.

The proposed design architecture was however not tested through a pilot implementation. It is the researcher's conviction that the new architecture if implemented will be able to significantly improve the security of the retailer's POS system, reducing the risk of data breaches and other security incidents.

5.2 Exploratory Data Analysis

Table 2 An Overview Information of POS dataset using the Pandas Dataframe

```
<class 'pandas. core.frame.DataFrame'>
Range Index: 66863 entries, 0 to 66862
Data columns (total 11 columns):
 #  Column            Non-Null Count Dtype
--- ------            -------------- -----
 0  WorkstationGroupID     66863 non-null int64
 1  TranID                 66863 non-null float64
 2  BeginDateTime          66863 non-null object
 3  EndDateTime            66863 non-null object
 4  TranTime               66863 non-null int64
 5  BreakTime              66863 non-null int64
 6  ArtNum                 66863 non-null int64
 7  TNcash                 66863 non-null bool
 8  TNcard                 66863 non-null bool
 9  Amount                 66863 non-null float64
 10 OperatorId             66863 non-null int64
```

dtypes: bool (2), float64(2), int64(5), object(2)

Memory usage: 4.7+ MB

The dataset consists of 66863 entries and 11 columns.

5.3 Result Analysis and Discussion

We employed KMeans clustering algorithm from the Scikit-learn library to group similar POS data points into clusters based on their similarity. Our results show the relationship between the number of clusters and the inertia value of a KMeans Clustering Algorithm. The inertia value is a measure of how internally coherent the clusters are.

There is a point in the plot where the decrease in inertia value begins to slow down. This point is known as the elbow point.

The elbow method was used to determine the optimal number of clusters for the data. This is shown in Figure 9.

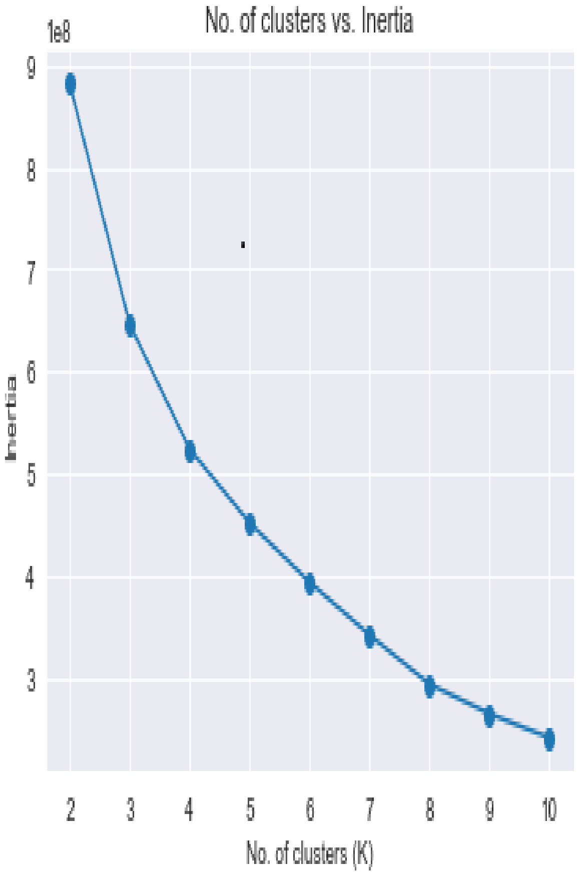


Figure 10The Elbow Method of Optimal Cluster Selection

The elbow represents a trade-off (balancing) between the number of clusters and the quality of the clustering. Choosing a larger number of clusters may result in better internal coherence within the clusters, but it may also lead to overfitting and reduced interpretability. On the other hand, choosing a smaller number of clusters may result in oversimplification and reduced accuracy.

By analyzing the elbow plot, we choose in our experiment three (3) as the optimal number of clusters for the dataset. Looking at Figure 10, at the third cluster, the line starts to deviate to the right forming the elbow. We choose the number of clusters at the elbow point, because it represents the best balance between the quality of the clustering and the complexity of the model.

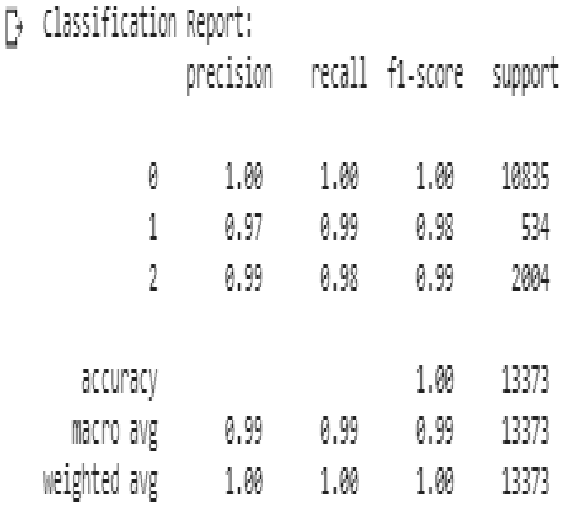
In our experiment, we chose a random state parameter of 42 to ensure reproducibility of the results. (That is the number to get the same results when the experiment is to be conducted).

After selecting the number of clusters, we use KMeans clustering algorithm to apply to the dataset and the cluster centers for each cluster is printed. The cluster centers provide insight into the characteristics of the data points in each cluster and can be used for interpretation and prediction. After, we provide a convenient way to summarize and interpret the characteristics of each cluster in terms of the mean value of each feature, and to associate each cluster label with its corresponding feature name. This is to help us predicts the cluster labels.

The silhouette score function from the Sklearn. metrics module is used to calculate the Silhouette score. It takes the data points X and the predicted cluster labels predictions as inputs and returns the Silhouette score as output. It shows how The Silhouette score is a measure of how well each data point fits into its assigned cluster compared to other clusters. Using the 3 as the number of clusters, the accuracy of Silhouette Score(n=3): was **0.581** percent.

The Neighbors Classifier is used to instantiate a KNN model with neighbors set to 3. This means that the model will consider the 3 nearest neighbors (clusters) of a data point when making a classification. The result bellow was obtained:

Table 3 Classification Report



```
Classification Report:
              precision    recall  f1-score   support

           0       1.00      1.00      1.00     10835
           1       0.97      0.99      0.98       534
           2       0.99      0.98      0.99      2004

    accuracy                           1.00     13373
   macro avg       0.99      0.99      0.99     13373
weighted avg       1.00      1.00      1.00     13373
```

The accuracy score represents the percentage of correctly classified instances in the test set, based on the KMeans cluster labels. In other words, it indicates how well the KNN model was able to classify new, unseen data points into the same clusters as the KMeans model. A higher accuracy score indicates better performance of the KNN model in classifying the test data. In our model, the accuracy score is used to calculate the accuracy of the predictions made by the KNN model on the test data (y_pred) compared to the actual labels of the test data (y_test).

This classification report provides an evaluation of the performance of a classifier for a multi-class classification problem with three classes, denoted by 0, 1, and 2. The report includes several metrics that measure the classifier's performance, such as precision, recall, and F1-score.

Precision: is the proportion of true positive predictions out of all the positive predictions made by the model. In other words, precision measures the accuracy of positive predictions. From Table 3, A precision of 1.0 means that all positive predictions made by the model are correct.

Recall: is the proportion of true positive predictions out of all the actual positive cases in the data. Recall measures how well the model identifies positive cases. A recall of 1.0 means that the model identifies all positive cases in the data.

F1-score: is the harmonic mean of precision and recall. It is a balanced measure that combines precision and recall into a single score. The F1-score is useful when the data is imbalanced, i.e., one class has many more samples than the other classes.

Support: is the number of samples in each class.

The report also includes an accuracy score, which measures the proportion of correctly classified samples out of all the samples in the dataset.

The macro-averaged metrics take the average of the metrics computed for each class, giving equal weight to each class. The weighted-average metrics, on the other hand, take the average of the metrics weighted by the number of samples in each class, giving more weight to classes with more samples.

In this particular report, the classifier achieved very high performance, with an accuracy of 1.0, indicating that all samples in the dataset were classified correctly. The precision for class 0 is also 1.0, indicating that all samples that were predicted as class 0 were correct. The precision for class 1 and class 2 are also high, at 0.97 and 0.99 respectively. The recall values are also high, with all classes having a recall of at least 0.98, indicating that the classifier identified almost all the positive cases in the dataset. The F1-scores are also high, indicating a good balance between precision and recall. In general, the classifier has performed very well on this particular dataset, with high precision, recall, and F1-scores across all classes. The result of KNN classifier can also be visualized in the confusion matrix as shown in Figure 11, The heatmap helps visualize the performance of the classifier by displaying the number of correctly and incorrectly classified instances in each class.

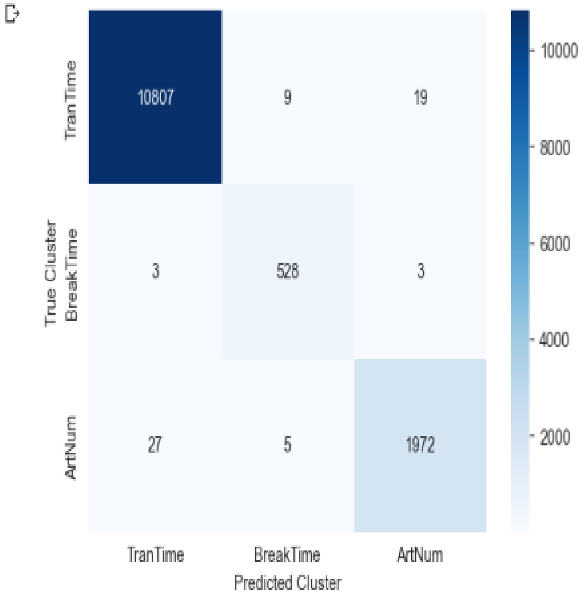


Figure 11 Confusion Matrix K-Means Clustering

The diagonal cells of the heatmap in Figure 11 represent the number of observations that were correctly classified. These cells show the number of test data points that were assigned to their true cluster label. The TranTime feature has 10807 data points that were correctly predicted. Also, from the confusion matrix, the BreakTime feature has 528 correctly predicted data points and the Artnum feature has 1972 correctly predicted points respectively. The non-diagonal cells represent the number of observations that were assigned to the wrong cluster or misclassified. The rows of the heatmap represent the true cluster labels, and the columns represent the predicted cluster labels. The numbers outside the diagonal of the confusion matrix represent the misclassifications, i.e. the instances that were predicted to belong to a different cluster than their actual cluster. These values give us an idea of which clusters are being confused with which other clusters.

For example, if we look at the row for Cluster 0 in the confusion matrix and see that there are some non-zero values in the columns for Clusters 1 and 2, it means that some of the instances that actually belong to Cluster 0 were misclassified as belonging to Clusters 1 or 2. Similarly, if we look at the column for Cluster 1 and see that there are some non-zero values in the rows for Clusters 0 and 2, it means that some of the instances that were predicted to belong to Cluster 1 actually belong to Clusters 0 or 2.

Overall, the confusion matrix gives us a more detailed view of the performance of the KNN classifier using the KMeans cluster labels as compared to just looking at the accuracy score. It allows us to see which clusters are being confused with each other and can help us identify patterns in the misclassifications that might inform future improvements to the clustering or classification models.

6. CONCLUSION

This research was aimed at identifying the key security breaches faced by POS systems and proposed a new architecture that addresses these challenges and proposes the use of end-to-end encryption, tokenization, multi-factor authentication, regular security assessments, and employee training. This research also used three clusters to separate POS data in order to mine similar patterns in the dataset. From the result obtained in the experiment, we can conclude that using KMeans clustering and KNearest Neighbour (KNN) algorithm presents the best algorithms to detect intrinsic patterns and it can be used to detect fraudulent transaction patterns in POS transactions.

6.1 Limitation of the work

Our experiment assumes our dataset contains fraudulent transactions or datapoints. The proposed architecture has not been tested practically.

6.2Recommendation

The improved architecture developed to identify and mitigate against point-of-sale breaches if adopted can be addressed the problem of point-of-sale system breaches and improve fraud detection. However, further study should be carried out in the combination of other clustering techniques (DBScan or LSTM) to identify and detect intrinsic patterns in POS dataset and the use of machine learning techniques to identify and detect fraud in keystroke dynamics of point-of-sale interface.

6.3 Contribution to knowledge

This research provides a novel architectural design that identifies areas or points of likely breach or attack in a point-of-sale system. Again, it performs a classification task based on the POS features and achieved a high accuracy of 99.51% which is very important to fraud detection in point-of-sale systems.

7. ACKWOLEDGEMENTS

My Sincere gratitude goes to Almighty God for the gift of knowledge and wisdom and for making this research possible.

To Dr. Aamo Iorliam, thank you so much for your guidance and direction all through this research.

I will also want to appreciate, Dr. Otache Innocent Ogwuche, Dr. Patrick Obilikwu, Dr. Adeyelu, A. A, Mr. Tivlumun Ge for their contributions. My appreciation also goes to my parents Capt. M. T. Anji (Rtd) and Mrs. Elizabeth M. Terwase for their love and support. My profound gratitude goes to my wife, Mrs. Terwase Agnes Edugwu, my children: Sophia, Fortune, Michael (Jnr), my siblings,

course mates and friends. Thank you for all your support, May God bless you all.

8. REFERENCES

[1] Abell, J. C. (2009, November 4). Nov. 4, 1879: Ka-Ching! The World's First Cash Register. Retrieved from Nov. 4, 1879: Ka-Ching! The World's First Cash Register | WIRED.

[2]Akinyele, A. I., Muturi, W., & Ngumi, P. (2017). Financial innovation and fraud risks in deposit money banks of Nigeria. EPRA *International Journal of Economic and Business Review*, 3(12), 56-66.

[3] Adegboyega, J. E., & Tomola, M. O. (2018). Card Frauds and Customers' Confidence in Alternative Banking Channels in Nigeria.DOI:10.19044/esj.2018.v14n16p40. URL:http://dx.doi.org/10.19044/esj.2018.v14n16p40.

[4] Alabi, O. F., & David, A. (2022). Framework For Detection Of Fraud At Point Of Sale On Electronic Commerce Sites Using Logistic Regression. https://doi.org/10.21203/rs.3.rs-1699624/v1

[5] Amaefule, I. A., & Njoku, D. O. (2019). The Prospect and Challenges of POS as Electronic Payment System in Nigeria. International Journal of Scientific Research and Management.

[6] Bandhakavi, S., Bisht, P., Parthasarathy, M., & Venkatakrishnan, V. (2007). CANDID: Preventing SQL injection attacks using dynamic candidate evaluations. *Journal Name, Volume Number(Issue Number)*, 12-24.https://doi.org/10.1145/1315245.1315249

[7] Bernardi, M. L., Cimitile, M., Di Francescomarino, C., & Maggi, F. M. (2014). Using discriminative rule mining to discover declarative process models with non-atomic activities.

[8] Coates, A., & Ng, A. Y. (2012). Learning Feature Representations with k-means. In *Advances in Neural Information Processing Systems* (pp. 561–580).

[9] Davis, W. C., & Wang, Z. J. (2015). A mobile retail POS: Design and implementation. In *Proceedings of the 13th International Conference on Advances in Mobile Computing and Multimedia* (pp. 426-432). ACM. http://dx.doi.org/10.1145/2757384.2757391.

[10] Dey, A., Jain, S., & Nandi, S. (2019). New method of pos based on artificial intelligence and cloud computing (pp. 1-6). https://doi.org/10.1109/ICRAECC43874.2019.8995078.

[11] Drimer, S., Murdoch, S. J., & Anderson, R. (2014). Security failures in smart card systems: tampering the tamper-proof. http://www.cl.cam.ac.uk/users/{sd410, sjm217, rja14} a. EE/library/WP_M-Trends2014_140409.pdf.

[12] Feit, A. M., Weir, D., & Oulasvirta, A. (2016). How we type: movement strategies and performance in everyday typing. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 4262-4273). ACM. https://doi.org/10.1145/2858036.2858233

[13] Goldman, J. (2021). Point of sale security measures for 2022.

[14]Gomzin, S. (2014). Hacking Point of Sale: Payment Application Secrets and Threats.

[15] Gundert, L. (2014). Detecting payment card data breaches today to avoid becoming tomorrow's headline. Retrieved from http://blogs.cisco.com/security/

[16] Hines, C., & Youssef, A. (2018). Machine Learning Applied to Point-of-Sale Fraud Detection. In *Information Security and Privacy* (pp. 201–210). Springer. https://doi.org/10.1007/978-3-319-96136-1_23

[17] Kazi, M. S. (2013). Secure Mobile POS System (Master's Thesis). KTH Royal Institute of Technology, Stockholm, Sweden.

[18] Kaspersky Lab. (2017). Type of malware. Retrieved from http://usa.kaspersky.com/internet security-center/threats/malware-classifications#.U755xLEe8SR

[19] Kundai, S. (2017). An analysis of point of sale systems physical configurations and security measures in Zimbabwean SMEs. *IRA International Journal of Education and Multidisciplinary Studies*, *6*(2), 5.

[20] Lord, N. (2021). Data protection 101. What is POS. Protecting Data in POS Environment.

[21] Mandiant, R. (2014). M-Trends: Beyond the breach. Retrieved from https://dl.mandiant.com.

[22] Nigerian Inter-bank Settlement System.

[23] Nigeria Electronic Fraud Forum Annual Report 2016).

[24] The Register@-Biting the hands that feeds IT. Mon, 24 Oct; 2022 //22:11 UTC.
The Unicode Consortium. (2011). The Unicode Standard. Available at https://unicode.org/standard/standard.html.

[25] Trend Micro Inc. (2014). Point-of-sale system breaches: Threats to the retail and hospitality industries.Retrievedfromhttp://www.trendmicro.com/cloud content/us/pdfs/securityintelligence/white-papers/wp-pos-system-breaches.pdf.

[26] Thomas, A., & Rafal, W. (2019). Point of sale (POS) data from a supermarket: Transactions and cashier operations.

[27] Whitteker, W. (2014). Point of sale system and security. *GIAC Gold Certification*. Wired. Retrieved from http://www.wired.com/2009/11/1104ritty-cash-register.

[28] Zhao, X., Chen, S., Zhou, L. and Chen, Y. (2020). Sound source localization based on SRP-PHAT spatial spectrum and deep neural network. *Computers, Materials & Continua64*(1), 253–271 DOI 10.32604/cmc.2020.09848.