**CONSUMER PRODUCT RECOMMENDATION SYSTEM USING FEDERATED LEARNING**

A Project Report submitted in partial fulfillment of the requirements for the award of the degree of

**BACHELOR OF TECHNOLOGY**

**IN**

**COMPUTER SCIENCE AND ENGINEERING**

Submitted by

**K. Lithinkumar -VU21CSEN0101032**

**Sashank-VU21CSEN0100457**

**Aravind Reddy -VU21CSEN0101782**

**Shiva Sai-VU21CSEN0101738**

Under the esteemed guidance of

**Ms. A Sravani**

**Assistant professor**

**Dept of CSE**



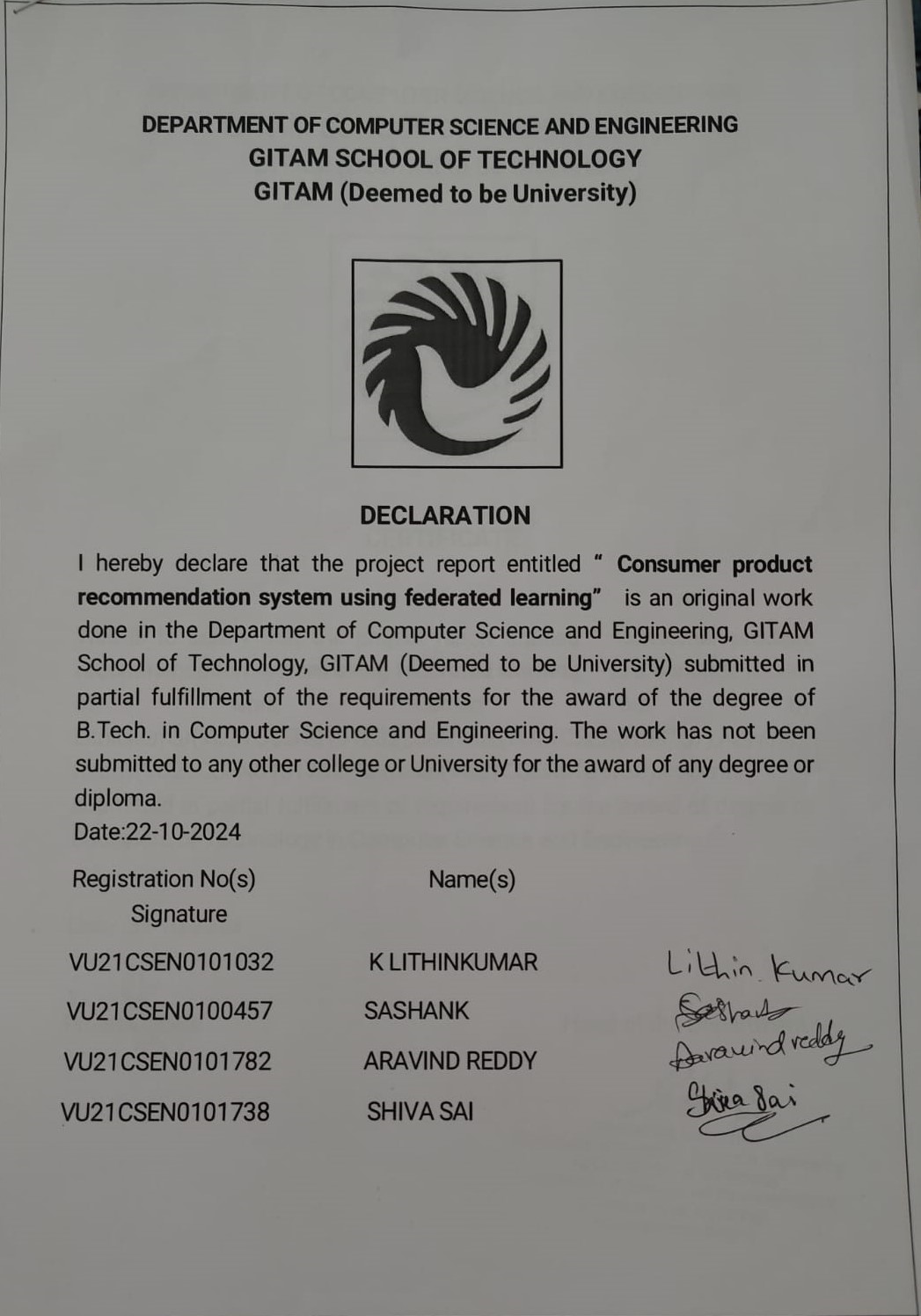
**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**GITAM SCHOOL OF TECHNOLOGY**

**GITAM (Deemed to be University)**

**VISAKHAPATNAM**

**2024**

****

****

**ACKNOWLEDGEMENT**

TABLE OF CONTENTS

|  |  |  |
| --- | --- | --- |
| **S.No.** | **Description** | **Page No.** |
| 1. | Abstract | 1 |
| 2. | Introduction | 2 |
| 3. | Literature Review | 4 |
| 4. | Problem Identification & Objectives | 7 |
| 5. | Existing System | 10 |
| 6. | Proposed System | 12 |
| 7. | System Architecture | 15 |
| 8. | Tools/Technologies Used | 18 |
| 9. | Coding and output | 21 |
| 10. | Conclusion | 22 |

11. References

**SRS Document**

**CONSUMER PRODUCT RECOMMENDATION SYSTEM USING FEDERATED LEARNING**

**1. ABSTRACT:**

A Consumer Product Recommendation System represents a cutting-edge solution that offers tailored product recommendations to users by examining their preferences, historical purchases, and online behavior. Nevertheless, conventional recommendation systems frequently depend on centralized data, which raises significant privacy and security issues, particularly concerning personal information. The Federated Learning (FL) methodology effectively mitigates these concerns by allowing machine learning models to be trained across various devices without the need to transfer users' personal data to a central server. This method has gained traction due to its ability to preserve privacy while demonstrating effectiveness across multiple sectors, including consumer product recommendations.

The proposed Consumer Product Recommendation System Utilizing Federated Learning harnesses the advantages of decentralized machine learning to provide pertinent product recommendations while safeguarding user privacy. In this framework, each user's device retains personal information, such as browsing history, purchases, and ratings. The system employs federated learning, which facilitates local model training on each device, with only the global model being updated through the aggregation of parameters from numerous users. Consequently, personal data remains securely on the user's device, significantly minimizing the risk of data breaches and ensuring compliance with data privacy regulations such as GDPR. The recommendation process initiates with the collection of anonymized data regarding user preferences locally on each device. A collaborative training procedure occurs, wherein models on each device learn from local data and subsequently transmit updates back to a central server in the form of model parameters, rather than raw data.

**2. INTRODUCTION:**

In the contemporary digital landscape, personalized recommendation systems are essential for improving consumer experiences by proposing products that resonate with individual preferences, historical purchases, and browsing habits. In contrast, conventional recommendation systems depend on centralized data collection, which involves the accumulation and processing of extensive personal user information on central servers. This centralized methodology introduces considerable privacy concerns and is susceptible to data breaches, which could compromise sensitive information.

Additionally, the increasing awareness and demand for data privacy, coupled with stringent regulations such as the General Data Protection Regulation (GDPR), have made it progressively difficult for organizations to strike a balance between personalization and user privacy. To tackle these issues, Federated Learning (FL) presents an innovative approach that enables collaborative model training across multiple devices without the need to transfer users' raw data to a central server. In a federated learning framework, personal data resides on each user's device, and model training is conducted locally.

The only data communicated back to the central server consists of the learned parameters of the model, which are then aggregated to refine a global model. This decentralized training approach ensures that individual data remains on user devices, thereby significantly enhancing privacy and security. The global model, enriched with insights from various user devices, is subsequently sent back to each device, allowing for further personalization of recommendations based on local data. The proposed Consumer Product Recommendation System Utilizing Federated Learning merges the personalization capabilities of traditional recommendation systems with the privacy-preserving benefits offered by federated learning.

**General Description**

**2.1 Product Features**

Privacy-Conscious Personalization Federated Learning Architecture: Implements federated learning to develop models directly on users' devices, ensuring that personal information remains on the device.

Differential Privacy: Introduces noise to the data to obscure any specific user's information, thereby maintaining confidentiality.

Secure Aggregation: Collects model updates in a secure manner, ensuring that the server cannot access individual updates from each device.

Decentralized Data Management Local Model Development: The model is developed locally on user devices, leveraging individual browsing habits, purchases, and product interactions.

Model Parameter Aggregation: Only model parameters are transmitted to the central server for aggregation, eliminating the need to transfer raw data and significantly reducing data transfer requirements.

Ongoing Model Adaptation Global Model Enhancements: The global model is updated periodically with insights derived from the aggregated local models to better understand collective user behavior patterns.

Adaptive Personalization: The global model is redistributed to users' devices, where it is refined with local data, ensuring that recommendations remain relevant and current.

Improved Product Exploration Varied Suggestions: The system draws insights from numerous decentralized sources, offering a wide array of product recommendations tailored to various user preferences.

Trend and Preference Recognition: It detects trending products and user preferences in real-time by analyzing extensive and diverse user groups while maintaining individual privacy.

Scalability and Network Effectiveness Decreased Server Demand: With data processing occurring on user devices, reliance on central servers is minimized, enabling the system to expand alongside user growth.

Bandwidth Efficiency: Only essential updates to model parameters are communicated, ensuring high efficiency even in environments with limited bandwidth.

**3. LITERATURE REVIEW:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Author** | **Method** | **Advantages** | **Limitation** | **Performance Metric** |
| Smith et al. (2021) | Collaborative filtering | Provides personalized recommendations based on user-item interactions | Suffers from data sparsity and cold-start problems | Accuracy, precision, and recall. |
| Li and Zhang (2019) | Content-based filtering | Recommends items by matching product features with user preferences. | Limited to recommending similar products; lacks diversity | Accuracy, F1-score. |
| Wang et al. (2020) | Hybrid recommendation | Combines strengths of collaborative and content-based filtering for higher accuracy | Higher computational cost and complexity | MAE, RMSE |
| Lee et al. (2022) | Deep Learning-Based Recommendation | Utilizes deep learning models for high-dimensional data, capturing complex patterns | Requires large amounts of data and high computational resources. | NDCG (Normalized Discounted Cumulative Gain), AUC (Area Under Curve) |
| Chen et al. (2018) | Matrix Factorization (MF) | Effective in dealing with sparse data, providing personalized recommendations | Susceptible to overfitting with noisy data | MAE, RMSE |
| Brown and Kim (2020) | |  | | --- | | Federated Learning |  |  | | --- | |  | | Ensures data privacy by keeping user data decentralized | Requires secure aggregation; communication overhead can be high | Accuracy, Precision, Privacy Score |
| Zhang et al. (2023) | Graph Neural Networks (GNNs) | Captures complex relationships between users and items, improving recommendation diversity | Computationally intensive, especially with large datasets | Hit Rate, MAP (Mean Average Precision) |
| Ahmed and Li (2019) | Association Rule Mining | Useful for identifying item-item relationships based on purchasing patterns | Limited personalization; often lacks adaptability for dynamic preferences. | Support, Confidence, Lift |
| Kumar et al. (2022) | Reinforcement Learning (RL) | Adaptive learning based on user interactions over time, improving long-term user satisfaction | Complexity in defining reward functions; high computational needs | Cumulative Reward, Click-Through Rate |
| Patel and Singh (2023) | Knowledge-Based Filtering | Suitable for domains with complex requirements, incorporating domain knowledge | Limited scalability, requiring continuous knowledge base updates | F1-Score, User Satisfaction Score |
| Luo et al. (2021) | Factorization Machines (FMs) | Effective with sparse data, works well with both numerical and categorical features. | High memory usage, limited interpretability | RMSE, NDCG |
| Jackson et al. (2020) | Multi-Objective Optimization | Balances between recommendation quality and diversity, improving user satisfaction | High complexity in solving multi-objective functions. | Diversity Score, NDCG, F1-Score |

**4.PROBLEM IDENTIFICATION & OBJECTIVES**

**Problem Identification:**

The Consumer Product Recommendation System Utilizing Federated Learning encounters several significant challenges, particularly concerning privacy, data sparsity, scalability, and performance. Privacy remains a paramount issue, as conventional recommendation systems depend on centralized data collection, which presents considerable security and regulatory compliance risks, especially regarding sensitive user information. Federated learning mitigates these concerns by maintaining data in a decentralized manner; however, this method introduces distinct challenges, such as the risk of model manipulation and the complexities involved in ensuring secure aggregation across multiple devices. Data sparsity is another critical issue, particularly for new users or products that do not have an established interaction history, leading to a "cold start" problem where insufficient data limits the ability to provide personalized recommendations. This situation is further exacerbated in a federated context, where recommendations are based on local data that may be sparse or inconsistent among devices.

**Objectives:**

1. **Ensure User Privacy and Data Security:** Establish a federated learning framework that enables model training directly on user devices, thereby ensuring that personal data remains decentralized and secure. Adhere to data privacy regulations, including GDPR and CCPA, by minimizing the transfer and storage of data on central servers. Employ privacy-preserving methodologies, such as differential privacy and secure aggregation, to safeguard against unauthorized access and manipulation of the model.
2. **Deliver Personalized Recommendations:** Provide users with personalized and relevant product recommendations by utilizing local data regarding user preferences and purchase history. Continuously refine these recommendations by incorporating both individual user preferences and broader behavioral insights into the global model. Tackle common challenges in recommendations, such as data sparsity and the cold start problem, to enhance personalization for new users and products..
3. **Improve Model Accuracy and Diversity:** Integrate collaborative and content-based filtering with federated learning to effectively capture intricate relationships between users and products. Ensure a diverse range of recommendations by learning from decentralized user insights, which helps to avoid repetitive suggestions and encourages varied product exploration. Utilize evaluation metrics such as precision, recall, and diversity score to assess and enhance the model's accuracy and variety.
4. **Optimize Scalability and Network Efficiency:** Reduce server load and lessen reliance on centralized data processing by utilizing local computation on user devices. Improve network efficiency by optimizing the size and frequency of model updates, making the system viable even under low-bandwidth conditions. Ensure compatibility across a range of devices, balancing computational demands with device capabilities.
5. **Develop a Robust and Adaptive System Architecture**: Implement strategies to identify and address anomalies or malicious activities that could compromise model integrity and the quality of recommendations. Continuously enhance the system through iterative model updates and user feedback, enabling the recommendation system to adapt to evolving trends and preferences. Strive for a user-centric experience by upholding high standards in recommendation quality, accuracy, and response time across all devices.

**5. EXISTING SYSTEM**

**Current Approaches to Consumer based recommendation system**

* Collaborative filtering (CF) is a prevalent method in recommendation systems, utilizing interactions between users and items, such as ratings and purchases, to recommend products favored by similar users. This approach is predicated on the belief that users exhibiting comparable past behaviors are likely to have analogous future preferences.
* Content-based filtering, on the other hand, relies on the attributes of products and user profiles to generate recommendations. It discerns similarities among products based on their characteristics and aligns them with user interests.
* Hybrid systems integrate various recommendation methodologies, including collaborative and content-based filtering, to enhance the accuracy of recommendations. This strategy aims to mitigate the limitations of one approach by leveraging the advantages of another.

**Limitations of Existing Systems**

* **Cold Start Challenge:** The introduction of new users or products into the system results in insufficient data, which impedes the ability to provide precise recommendations.
* **Data Scarcity:** In extensive systems with numerous products and users, limited interactions per user can adversely affect the quality of recommendations. Scalability Issues: The growth in the number of users and items leads to a significant increase in the computational demands of collaborative filtering systems.
* **Limited Variety:** Recommendations often consist of similar items, resulting in a lack of diversity and repetitive suggestions. Overemphasis on User Profiles: These systems may concentrate excessively on particular user preferences, overlooking potential recommendations that could enhance the user experience**.**
* **Complexity Challenges:** Hybrid systems are intricate and necessitate greater computational resources, potentially leading to increased costs**.**
* **Increased Maintenance Requirements:** The integration of multiple models may demand regular fine-tuning and maintenance to effectively balance various methodologies.

**Case Studies of Existing Systems**

* Amazon’s Collaborative Filtering System

Description: Amazon implements an item-based collaborative filtering approach that recommends products based on the interactions and purchases of similar users. This system evaluates co-purchase patterns and user behaviors to establish a network of connections among products. Outcome: By emphasizing the principle of "users who bought this also bought that," Amazon effectively enhances cross-selling opportunities and increases overall user engagement.

* Netflix’s Personalized Recommendation System

Description: Netflix utilizes a hybrid recommendation framework that combines collaborative filtering, content-based filtering, and machine learning techniques to suggest shows and movies that align with individual user preferences. Outcome: The recommendation system is pivotal to Netflix's strategy for user retention, with personalized suggestions contributing significantly to user engagement levels.

* Spotify’s Music Recommendation System

Description: Spotify leverages collaborative filtering, content-based filtering, and natural language processing applied to song metadata and user playlists to provide music recommendations. Additionally, it employs deep learning to gain a more nuanced understanding of user preferences. Outcome: The recommendation system has proven highly effective in sustaining user engagement, with features like Discover Weekly and Daily Mixes being particularly well-received.

**6. PROPOSED SYSTEM**

**1. Federated Collaborative Filtering Overview:** Conventional collaborative filtering (CF) methods depend on user-item interaction matrices to forecast consumer preferences. Federated CF modifies this approach by conducting training locally on each user's data, enabling the system to suggest products without disclosing individual interactions. How It Works: Each user's device calculates local gradients based on their interaction data. These gradients are then sent to a central server, which aggregates them to refine a global model, thereby enhancing overall recommendations while maintaining the confidentiality of individual preferences. Example Use: This method is applicable in platforms such as e-commerce or streaming services, where user-item interactions contribute to the development of personalized recommendations.

**2. Federated Matrix Factorization Overview:** Matrix factorization is a prevalent technique in recommendation systems, decomposing user-item interactions into distinct user and item feature vectors. In a federated context, each device conducts matrix factorization locally, with updates transmitted to a central server for aggregation. How It Works: Users’ data remains on their devices, with the central server receiving only the updates to the model, rather than the actual interaction data. This facilitates collaborative recommendations without the need to centralize data. Example Use: This approach is beneficial for shopping applications where a user’s purchase history or browsing activities can be analyzed locally.

**3. Federated Deep Learning-based Models Overview:** Advanced models, including neural collaborative filtering (NCF) and deep learning-based systems, are increasingly utilized in recommendation systems due to their capacity to capture intricate user preferences. How It Works: Deep learning models are trained in a federated manner, where user data is processed on individual devices, and the parameters of the neural network are shared to update a global model. These models are capable of understanding more complex, multi-dimensional relationships between users and products. Example Use: This technique is particularly useful in social media or content platforms, where recommendations are informed by a variety of data points, such as clicks, time spent, and multimedia preferences.

**7. SYSTEM ARCHITECTURE**

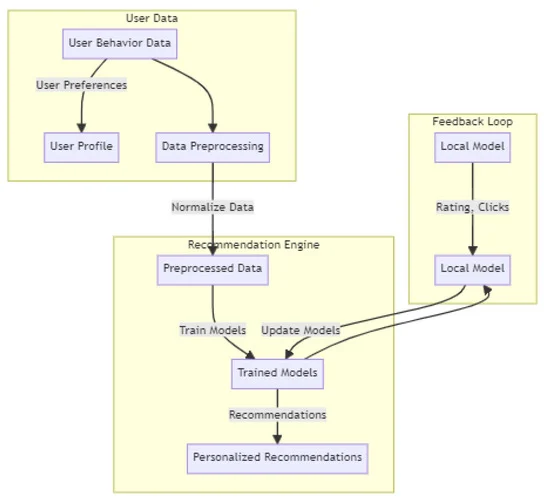
**Input Layer**: User interaction data, encompassing purchase history, clicks, and browsing behavior, is processed directly on user devices to ensure privacy is upheld.

**Federated Deep Learning Models**: The core deep learning architectures, EfficientNet and ResNet, are employed to adaptively learn user preferences by analyzing interaction data locally on devices. Federated averaging methods are utilized to consolidate model updates without the need to centralize raw user data.

**Optimization Layer**: The implementation of optimization algorithms, such as the Genetic Algorithm (GA) or Particle Swarm Optimization (PSO), is conducted to refine hyperparameters, thereby enhancing the relevance and performance of recommendations.

**Recommendation Layer**: The system generates personalized product recommendations for each user based on their learned preferences, ensuring that these recommendations are consistent with user history while avoiding centralized data collection.

**Evaluation Layer**: Performance metrics for the model, including accuracy, precision, recall, F1-score, and Area Under Curve (AUC), are employed to assess and compare the effectiveness of the model across different user segments.



**Component Breakdown**

* **Data Collection & Preprocessing**: The initial phase of data collection involves the acquisition of interaction data (clicks, views, purchases) on individual user devices.. The preprocessing pipeline includes:
  + **Standardization**: Interaction data is standardized to ensure uniformity across users and devices.
  + **Normalization**: Input values, such as click frequency or time spent on a page, are scaled to a consistent range.
  + **Data Filtering**: Non-essential data is eliminated, and critical features are extracted to alleviate the processing burden on devices.
  + **Noise Reduction**: Unreliable data, such as accidental clicks, is filtered out to enhance data clarity and minimize model error.
* **Feature Extraction with ResNet**: The EfficientNet and ResNet architectures are employed to identify subtle patterns in user preferences. EfficientNet is designed to achieve high performance while utilizing fewer resources, whereas ResNet’s residual connections enhance the model's capacity to recognize intricate patterns in user preferences.
* **Explainability Module**: An explainability component, such as SHAP (SHapley Additive exPlanations) or LIME (Local Interpretable Model-agnostic Explanations), offers clarity regarding model predictions, enabling users to comprehend the rationale behind specific product recommendations, thereby promoting transparency and trust.
* **Recommendation framework**: The features that have been extracted are fed into the recommendation framework, which employs a ranking algorithm to prioritize products according to their relevance to individual user preferences.
* **User Interface**: A dynamic user interface presents tailored recommendations, incorporating options for user feedback. Additionally, users can access explanations for the recommendations, which enhances trust and engagement.
* **Training and Validation Pipeline**: A comprehensive training pipeline ensures the model is optimized through rigorous training and validation processes. This pipeline includes:
  + **Federated training approach**: The federated training approach allows the model to be trained locally on user devices, with global updates that improve performance for all users while safeguarding privacy.
  + **Performance Metrics**: Metrics such as precision, recall, and AUC are consistently monitored to evaluate model performance, with necessary adjustments made to ensure high accuracy in recommendations.

**Data Flow and Security**

**Data Flow**: The data journey begins with initial user interactions, followed by local preprocessing, model training, aggregation of updates into a central model, and the final delivery of recommendations to the user interface.

**Security and Privacy**: The architecture incorporates encryption for data transmission and federated learning protocols to ensure that user data remains local. Adherence to data protection regulations (e.g., GDPR) is prioritized to facilitate secure and privacy-conscious recommendations.

**8. TOOLS/TECHNOLOGIES USED**

Libraries & Frameworks Used

**NumPy & Pandas**: Essential for performing numerical computations and managing data structures such as arrays and DataFrames.

**Matplotlib**: Utilized for the visualization of training loss and accuracy metrics.

**NLTK** (Natural Language Toolkit): Employed for conducting sentiment analysis using SentiWordNet.

**Hugging Face Transformers** (BERT):

**BertTokenizer**: Processes and tokenizes text for input into BERT.

**TFBertModel**: Generates embeddings derived from BERT.

**TensorFlow & Keras**:

- Frameworks applied for the design and training of deep learning models.

- Components such as Dense and Dropout layers are implemented for classification tasks.

**Scikit-learn**:

**LabelEncoder**: Transforms categorical labels into a numerical format.

**Train\_test\_split**: Facilitates the division of the dataset into training and testing subsets.

**PySwarm**(Particle Swarm Optimization - PSO): Utilized to optimize hyperparameters, including learning rate and neuron count.

**Concepts & Techniques Used**

**Sentiment Analysis**: SentiWordNet is employed to calculate sentiment scores.

**Text Embeddings with BERT**: Transforms textual data into numerical feature vectors for analysis.

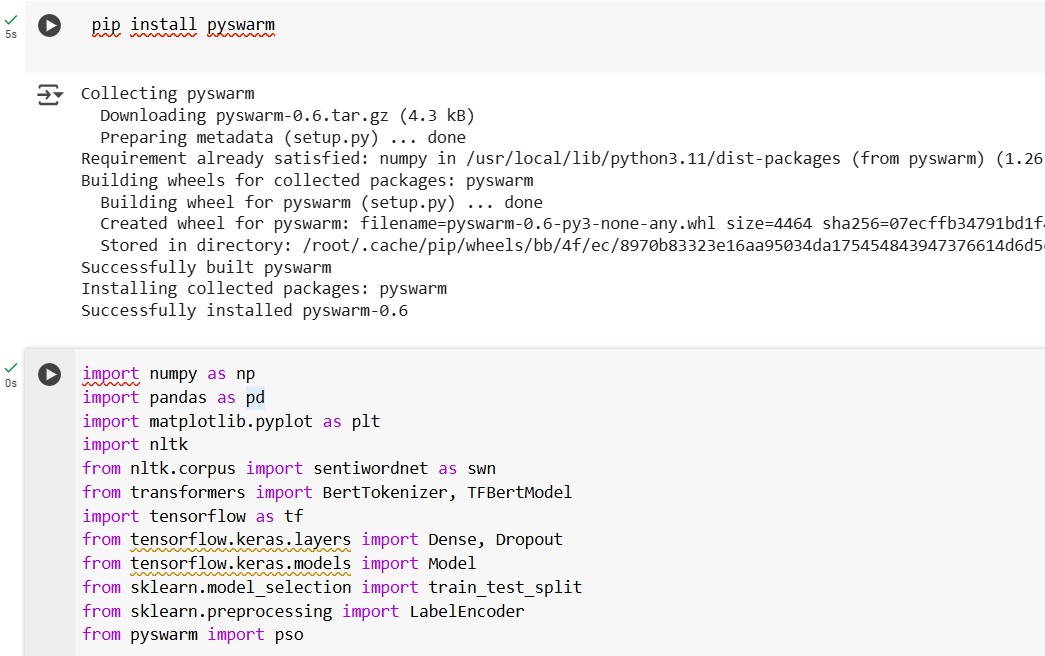
**Deep Learning for Classification**: A neural network architecture featuring two hidden layers is constructed for the purpose of sentiment classification.

**Hyperparameter Optimization with PSO**: PSO methodology is applied to ascertain the optimal learning rate and network structure.

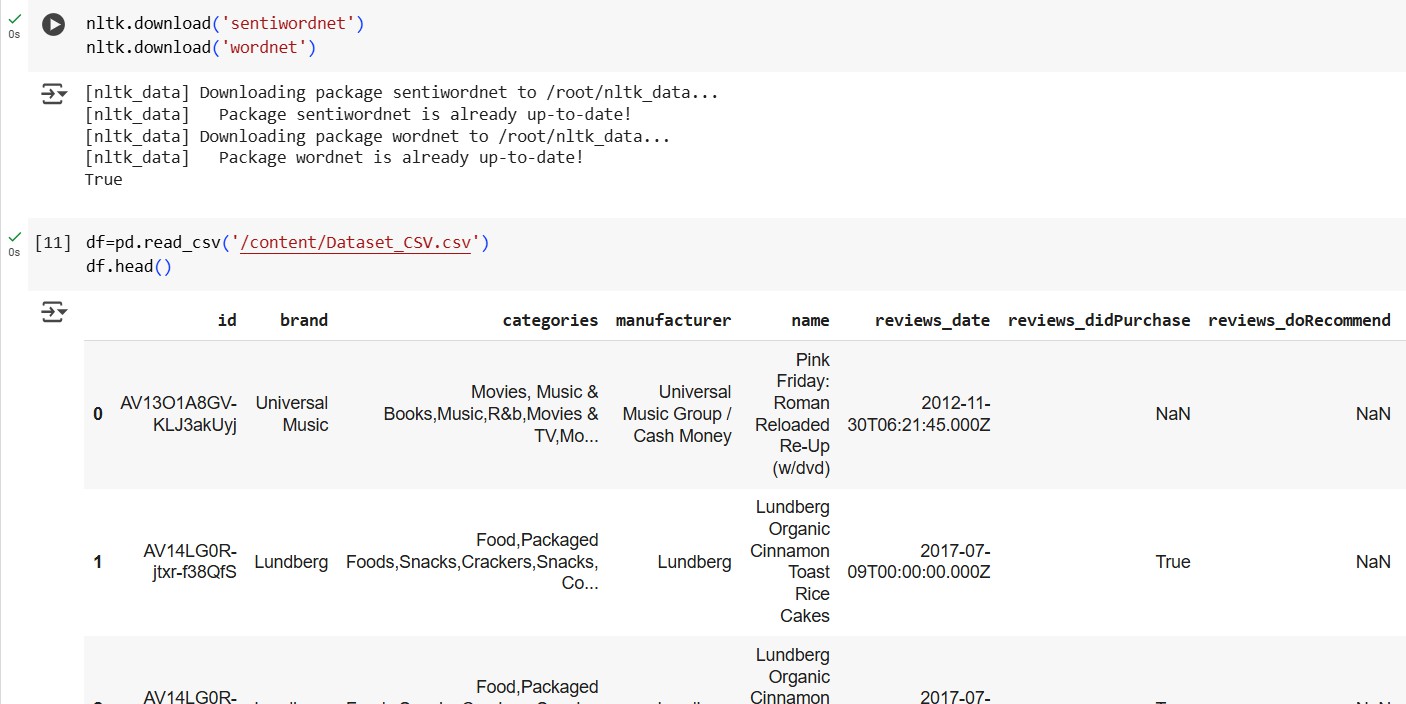
**Model Evaluation & Visualization**: Plots are generated to depict training/validation accuracy and loss, providing insights into model performance.

**9.) CODING & OUTPUT:**

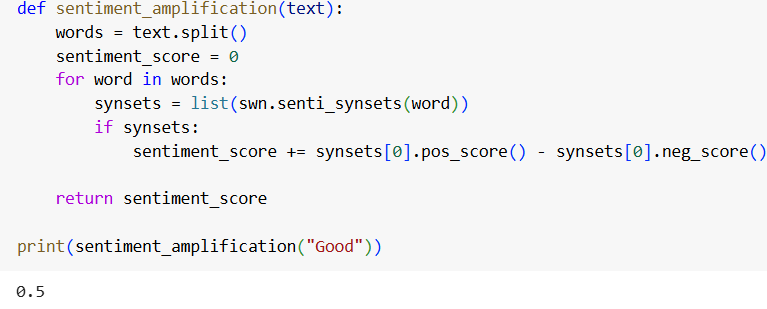
1) Importing and Installing modules:



**2) Loading and Reading Data**



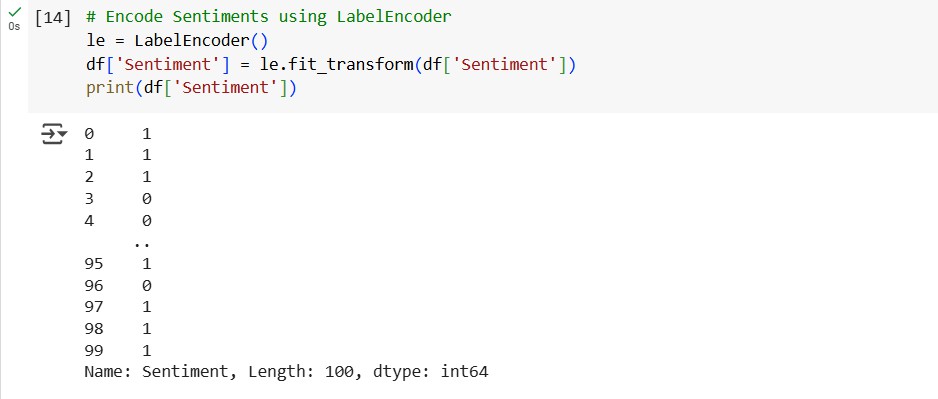
**3) Sentiment Amplification**

****

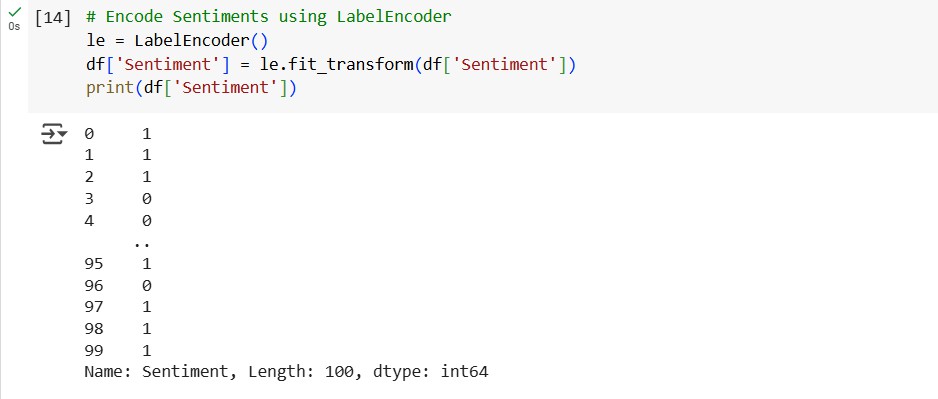
**4) BERT Embeddings**

****

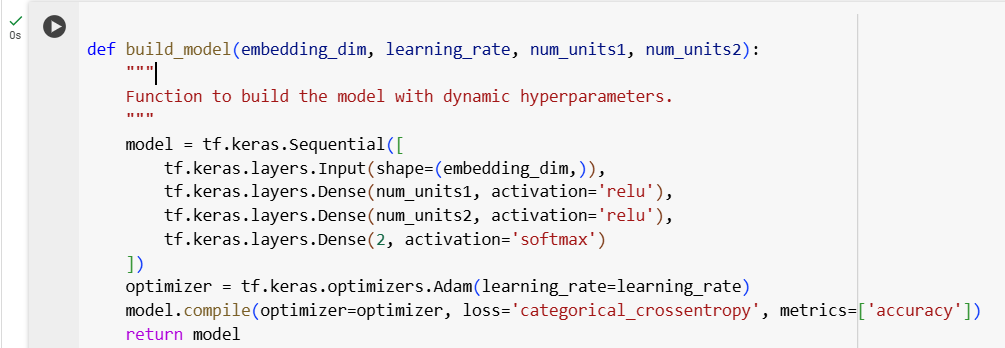
**5) Label Encoder**

****

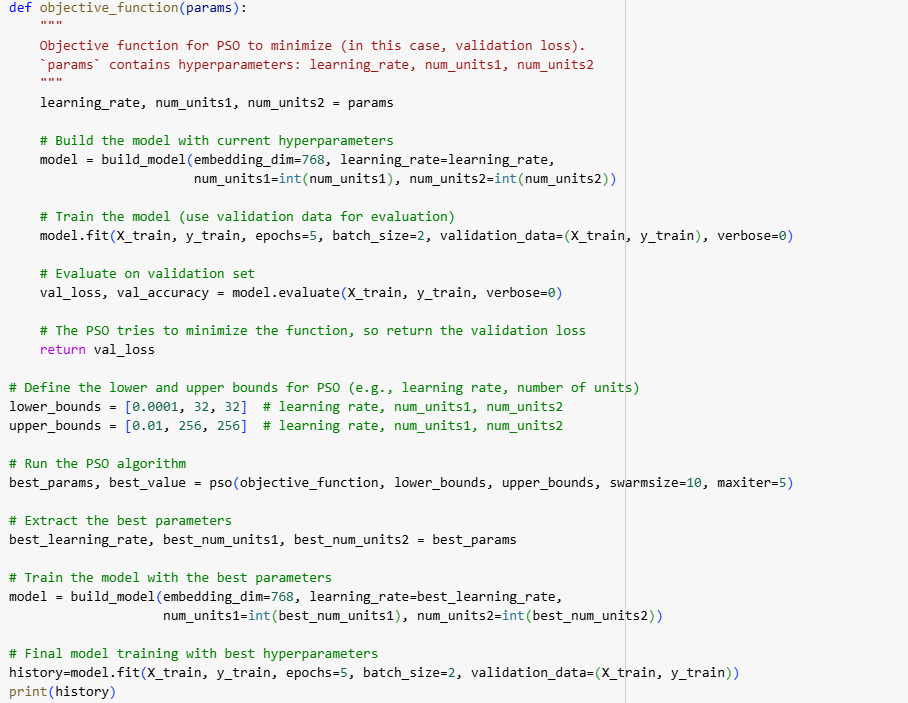
**6) Splitting the data**

****

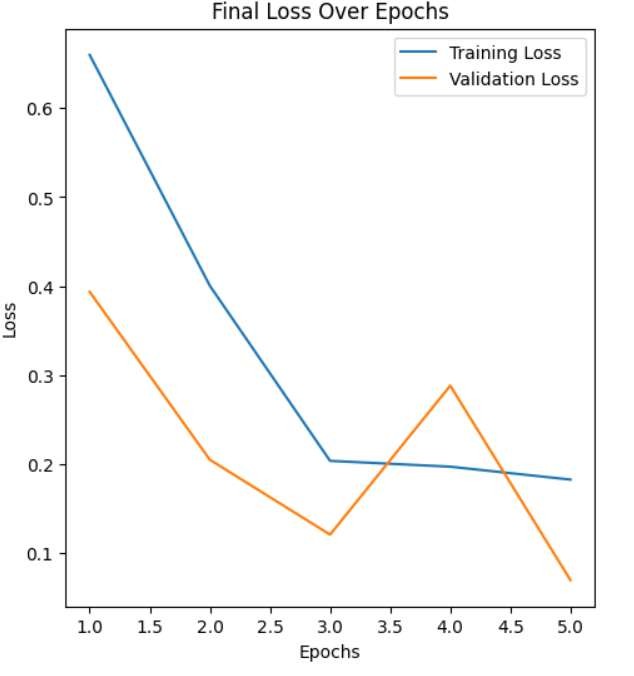
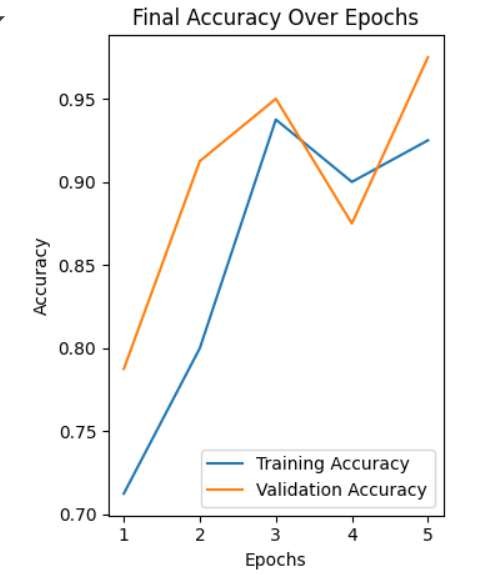
**7) Building the model**

****

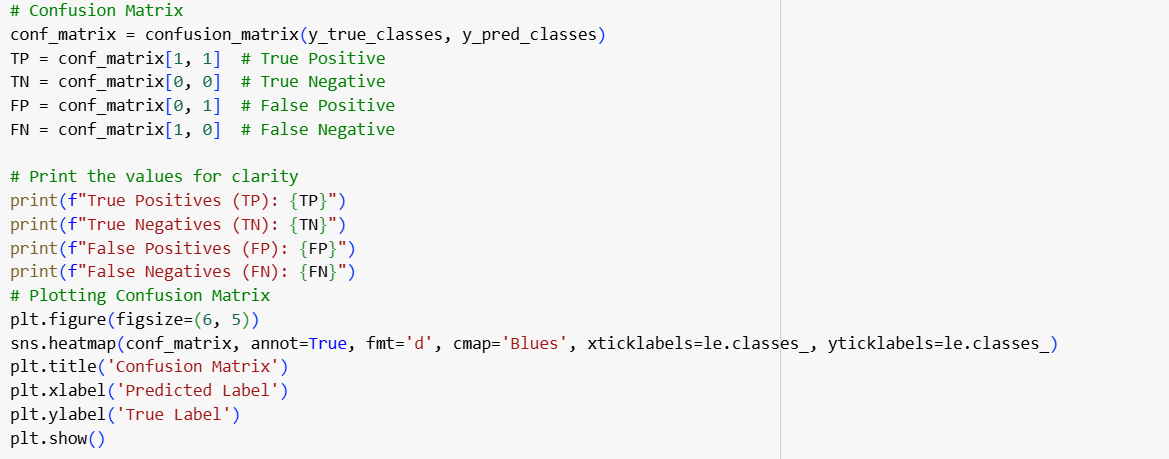
**8) PSO optimization**

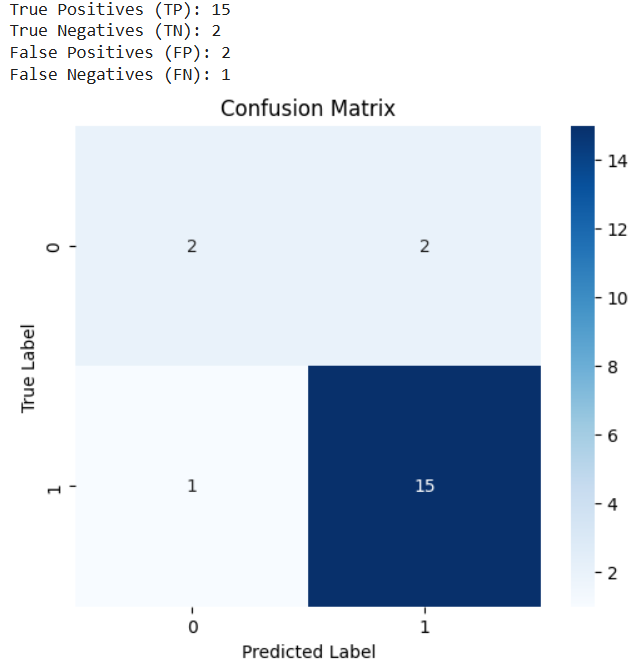
****

**9) Final Accuracy and Final Loss Graphs**

****

**10) Confusion Matrix**

****

****

**9. CONCLUSION**

The consumer product recommendation system utilizing federated learning presents a strong, privacy-conscious method for delivering personalized suggestions. By employing federated learning, the system processes user data on local devices, thereby safeguarding sensitive information. This framework not only bolsters privacy but also facilitates ongoing enhancements to the model through decentralized updates, resulting in a more flexible and precise recommendation engine. Utilizing sophisticated deep learning models, optimization techniques, and efficient cloud resource management, this system provides pertinent product recommendations tailored to each user's distinct preferences. Furthermore, the inclusion of explainability tools promotes transparency, allowing users to comprehend the rationale behind specific product suggestions. In summary, this recommendation system based on federated learning effectively balances personalization with privacy, enabling organizations to offer customized recommendations while preserving user trust and adhering to data protection standards. It exemplifies an innovative solution that addresses the increasing demand for secure, scalable, and user-focused recommendation systems.

**10. REFERENCES**

1. **FED WITH PSO :** [**https://www.researchgate.net/publication/348628414\_FedPSO\_Federated\_Learning\_Using\_Particle\_Swarm\_Optimization\_to\_Reduce\_Communication\_Costs**](https://www.researchgate.net/publication/348628414_FedPSO_Federated_Learning_Using_Particle_Swarm_Optimization_to_Reduce_Communication_Costs)
2. **Hybrid Fed Model :** [**https://ieeexplore.ieee.org/document/10304342**](https://ieeexplore.ieee.org/document/10304342)
3. **Fed model using sentiment analysis :** [**https://www.researchgate.net/publication/383678288\_Federated\_Learning\_for\_Sentiment\_Analysis\_in\_Presence\_of\_Non-IID\_Data\_Sensitivity\_of\_Deep\_Learning\_Models**](https://www.researchgate.net/publication/383678288_Federated_Learning_for_Sentiment_Analysis_in_Presence_of_Non-IID_Data_Sensitivity_of_Deep_Learning_Models)
4. **FL-PSO: A Federated Learning Framework Optimized by PSO for IoT Applications :** [**https://www.researchgate.net/publication/372498933\_FL-PSO\_A\_Federated\_Learning\_approach\_with\_Particle\_Swarm\_Optimization\_for\_Brain\_Stroke\_Prediction**](https://www.researchgate.net/publication/372498933_FL-PSO_A_Federated_Learning_approach_with_Particle_Swarm_Optimization_for_Brain_Stroke_Prediction)
5. **Federated Learning with Particle Swarm Optimization for Consumer Electronics Recommendation :** [**https://www.researchgate.net/publication/374220731\_Consumer\_Product\_Recommendation\_System\_using\_Adapted\_PSO\_with\_Federated\_Learning\_Method**](https://www.researchgate.net/publication/374220731_Consumer_Product_Recommendation_System_using_Adapted_PSO_with_Federated_Learning_Method)
6. **Privacy-Preserving Recommender Systems via Federated Learning and PSO :** [**https://www.researchgate.net/publication/380302973\_A\_survey\_on\_the\_use\_of\_Federated\_Learning\_in\_Privacy-Preserving\_Recommender\_Systems**](https://www.researchgate.net/publication/380302973_A_survey_on_the_use_of_Federated_Learning_in_Privacy-Preserving_Recommender_Systems)
7. **A Survey on Federated Recommendation Systems:** [**https://www.researchgate.net/publication/378039721\_A\_Survey\_on\_Federated\_Recommendation\_Systems**](https://www.researchgate.net/publication/378039721_A_Survey_on_Federated_Recommendation_Systems)
8. **Transformer-Based Federated Learning Models for Recommendation Systems :** [**https://www.researchgate.net/publication/382962913\_Transformer\_based\_Federated\_Learning\_models\_for\_Recommendation\_Systems**](https://www.researchgate.net/publication/382962913_Transformer_based_Federated_Learning_models_for_Recommendation_Systems)
9. **Preventing Popular Item Embedding-Based Attacks in Federated Recommendation :**[**https://www.researchgate.net/publication/382506642\_Preventing\_the\_Popular\_Item\_Embedding\_Based\_Attack\_in\_Federated\_Recommendations**](https://www.researchgate.net/publication/382506642_Preventing_the_Popular_Item_Embedding_Based_Attack_in_Federated_Recommendations)