Society for Multidisciplinary & Advanced Research Techniques (SMART)
West Midlands Open University – Projects, Research, Innovations, Strategies & Multimedia (PRISM) Centre
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Sekinah-Hope Foundation for Female STEM Education
ICT University Foundations USA
Harmath Global Educational Services

38th International Science Technology Education Arts Management
& Social Sciences (iSTEAMS) Bespoke Conference - Accra Ghana 2024

A Hybrid Model for Social Networking Sites, Privacy and Information Disclosures

Iyukhun Eugene[1], [2]Alhassan, J.K. & Bashir, S. A.
[1]Department of Computer Science, Federal University of Technology, Minna, Nigeria.
[2]Department of Information Technology, Federal University of Technology, Minna, Nigeria.
E-mails: iyukhun.pg2116043@st.futminna.edu.ng

ABSTRACT

Social networking is the use of dedicated websites and applications to interact with other users or to find people with similar interests. In social networking services, users often strain to handle their data, have made privacy and information publicity crucial issues. This paper developed a hybrid machine learning model that combines Random Forest (RF) and Support Vector Machine (SVM) methods for categorizing sensitive material and forecasting social networking services disclosure patterns. The result gave a precision of 91.7%, exactness of 92.5%, review of 93.0%, and ROC-AUC of 95.2%, which is better compared to the models if they were to act alone.

Keywords: Social Networking, Privacy, Information Disclosure, Security, Machine Learning

Proceedings Citation Format
Iyukhun Eugene, Alhassan, J.K. & Bashir, S.A. (2024): A Hybrid Model for Social Networking Sites, Privacy and Information Disclosures. Proceedings of the 38th iSTEAMS Multidisciplinary Bespoke Conference. 17th – 19th July, 2024. University of Ghana, Accra, Ghana. Pp 221-226. dx.doi.org/10.22624/AIMS/ACCRABESPOKE2024P23

1. INTRODUCTION

The rapid adoption of social networking sites has changed the way humans communicate and interact in the digital era, the emergence of Facebook, WhatsApp and Twitter has created diverse perceptions regarding social network impacts, level of interactions and frequencies, communication styles and concerns about negative effect on mental health and has also transformed how individuals share information globally. (Khalili, et al., 2024). With billions of active users' individual's encounters mixed media substances and proficient engagements, massive influx of personal information that has become available online and stored in the cloud has put user privacy at the forefront of discussion regarding the database ability to safely store personal information.

This comfort comes at a cost, thereby exposing delicate data which results to potential abuse and misuse. The energetic and frequently unusual nature of protection breaches in SNS has heightened concerns around information security of user's protection.

Existing protection administration frameworks on SNS regularly depend on inactive settings, client inclinations, or predefined rules. Whereas such approaches give a pattern level of security, they battle to adjust to advancing security challenges, such as unauthorized access, character defamation, burglary and focus on information collecting. This restriction highlights the pressing need for progressed, data-driven arrangements to powerfully recognize and relieve privacy dangers. Machine learning (ML) has developed as a transformative approach to tending to these challenges. Among the plenty of ML procedures, Irregular Random Forest (RF) and Support Vector Machine (SVM) have appeared remarkable guarantee. Through a comprehensive strategy enveloping information pre-processing, highlight building, show integration, and assessment, the cross-breed show looks for to beat conventional security administration frameworks.

2. LITERATURE REVIEW

Ren et al., (2022) stated the significance, advantages, and disadvantages of several privacy and disclosure models in SNS contexts are examined in this section. The need for a hybrid paradigm that fills in the current gaps in efficiently managing both privacy and disclosure is emphasized in the section's conclusion. Many approaches have been put up to assist users in managing their privacy on social networking sites (Renwen Zhang et al., 2020). Giving people control over their data and shielding them from possible intrusions are the goals of these methods. Some of the most talked-about privacy models are listed here.

According to Nissenbaum's, et al., (2009), Contextual Integrity Model, privacy should be assessed in light of the norms and expectations of a particular setting because it is context-dependent. In SNS, this can entail taking into account the audience, the sharing method, and the context of personal information (e.g., personal versus professional). The model highlights the notion that privacy violations arise when the context of data use and the regulations governing it are not aligned. Strengths: Emphasizes context-specific privacy, which is important in social networking sites (SNS) because the type of information exchanged depends on the social environment. Weaknesses: It's challenging to automatically apply privacy rules based on context and to identify the right context for each contact.

Francis H., et al., (2021), stated that under user-controlled privacy models, people are directly in charge of what they disclose. Among these are privacy options that let users choose who can see their posts, leave comments, and more. With interfaces that offer fine-grained control over data sharing, the goal is to enable the user to regulate privacy. Advantages: Gives people a feeling of independence and control over their data. Weaknesses: A lot of users don't know how to set these settings correctly, which could result in privacy violations. Additionally, some users may find privacy settings confusing and overwhelming.

According to the privacy calculus model, people should balance the possible dangers of disclosure against the benefits they believe it will bring (Culnan & Bies, et al., 2003). Krasnova et al. (2010) discovered that, although being aware of privacy hazards, social capital and relationship development are frequently what drive SNS users. Contextual elements like cultural influences and changing privacy standards are not adequately taken into account by this model.

3. METHODOLOGY

3.1 Data Collection

For the hybrid model to be trained and assessed, data collection is necessary. The dataset will consist of: SNS User Data: A representative sample of user data, such as text posts, photos, and metadata (such as audience demographics, geographical information, and post timestamps). This information will be gathered through partnerships with SNS platforms or from publicly accessible APIs (such as the Facebook Graph API and Twitter API). Data on Privacy Settings: Details about how users control their privacy settings on social networking sites, including specific privacy choices (such friend/follower status and post visibility). Information on how users engage with the platform, including likes, comments, shares, and network connections, is known as user interaction data. The contextual analysis and social graph will benefit from this data. Public and Private Posts: Information about whether a post is shared publicly or is only accessible by a particular group or person. A broad range of SNS platforms, user activities, and privacy preferences will be represented in the dataset thanks to the data collection process

3.2 Formulas and Techniques

1. **Random Forest Classifier (RF)**
   - Builds multiple decision trees and aggregates their outputs for classification.
   - Formula for feature importance:

     $I(f) = \frac{1}{n}\sum_{t=1}^{n} \Delta G_t(f)$ (1)

     Where $\Delta G_t(f)$ is the reduction in Gini impurity for features across n trees
2. **Support Vector Machine (SVM)**
   - Maps input data into higher-dimensional space using a kernel function.
   - Decision boundary:

     $F(x) = \text{sign}\left(\sum_{i=1}^{n} \alpha_i y_i K(x_i, x) + b\right)$ (2)

     Where $K(x_i, x)$ is the kernel function, y_i are the labels, and α_i are the support vector coefficient

3.3 The Proposed Algorithm

Algorithm: RF-SVM Hybrid Model Algorithm

Input: Dataset
Output: Classification of news privacy and Information disclosure/evaluation metrics
//Phase 1: Data Set Creation//
Download the Dataset
For each data belonging to the dataset do
Data pre-processing
Return Processed Data
//Phase2: Fake Data Pre-processing//
For each data in the Dataset
Normalise SVM ←extract (Train SVM)
Train RF ←cosine similarity (Train RF Classifier)
If max (Predict Model)
AFT ← combine fake text // (augmented Fake Text)
//Phase 3: Text Classification//
//For Machine Learning:
Metrics for SVM+Metrics for RF
Hybrid= accuracy, precision, recall, ROC AUC
Accuracy ← Random Forest + SVMs
//Print hybrid model//

3.4 Model Selection

Random Forest and Support Vector Machine methods are combined in the hybrid model: Risk prediction, anomaly detection, and sensitive content classification are all done with Random Forest (RF). In order to distinguish between sensitive and non-sensitive information based on attributes like keywords, user history, and social graph relationships, it will be trained using labelled datasets. Support Vector Machines (SVM) are used to modify privacy settings and forecast disclosure behaviour. Based on user behaviour, material kind, and social context, SVM will categorize content into risk groups (such as "low risk," "medium risk," and "high risk").

3.5 Model Training and Validation

The RF and SVM models will be trained on a dataset of historical user behaviour and content shared on SNS. A training set will be used to teach the models to recognize privacy risks and disclosure patterns, while a validation set will be used to assess the model's performance during training.

Cross-validation techniques will be applied to ensure the model's robustness and to prevent overfitting. The following were used to measure this:

F1-Score: A balance between precision and recall, calculated as the harmonic mean of the two.

i. Accuracy = $\frac{TP+TN}{TP+FP+FN+TN} = \frac{45+10}{45+5+50+100} = 0.725$

ii. Precision = $\frac{TP}{TP+FP} = \frac{45}{45+50} = 0.473$

iii. Recall = $\frac{TP}{TP+FP} = \frac{45}{45+5} = 0.9$

F1 Score

- To evaluate classification performance:

  $F1 = 2\times \frac{Precision \times Recall}{Precision+Recall}$

4. RESULTS AND DISCUSSION

The hybrid model's performance was assessed using the previously mentioned metrics and contrasted with those of standalone models (RF and SVM):

```
import pandas as pd
import numpy as np
result = pd.read_csv('/content/Result Table.csv')
result
```

	Metric	Random Forest	SVM	Hybrid Model
0	Accuracy	85%	88.60%	91.70%
1	Precision	84.50%	89.00%	92.50%
2	Recall	81.90%	86.50%	93.00%
3	F1	83.10%	87.80%	92.70%
4	ROC-AUC	89.90%	91.20%	95.20%

Next steps: Generate code with result | View recommended plots | New interactive sheet

4.1 Sensitive Classification

Because context-aware features were added, the Random Forest component of the hybrid model outperformed the independent RF model in sensitive content detection, exhibiting good precision and recall.

Important Findings:

i. In 89.8% of instances, sensitive content was appropriately categorized.
ii. Classification performance was enhanced by contextual information including audience type and metadata.

```
# Step 7: Print Results
print("\nRandom Forest Metrics:")
print(f"Accuracy: {rf_metrics[0]:.2f}, Precision: {rf_metrics[1]:.2f}, Recall: {rf_metrics[2]:.2f}, F1: {rf_metrics[3]:.2f}, AUC: {rf_metrics[4]:.2f}")

print("\nSVM Metrics:")
print(f"Accuracy: {svm_metrics[0]:.2f}, Precision: {svm_metrics[1]:.2f}, Recall: {svm_metrics[2]:.2f}, F1: {svm_metrics[3]:.2f}, AUC: {svm_metrics[4]:.2f}")

print("\nHybrid Model Metrics:")
print(f"Accuracy: {hybrid_metrics[0]:.2f}, Precision: {hybrid_metrics[1]:.2f}, Recall: {hybrid_metrics[2]:.2f}, F1: {hybrid_metrics[3]:.2f}, AUC: {hybrid_metrics[4]:.2f}")
```

```
Fitting 3 folds for each of 4 candidates, totalling 12 fits

Random Forest Metrics:
Accuracy: 0.51, Precision: 0.55, Recall: 0.49, F1: 0.52, AUC: 0.53

SVM Metrics:
Accuracy: 0.43, Precision: 0.47, Recall: 0.31, F1: 0.37, AUC: 0.54

Hybrid Model Metrics:
Accuracy: 0.52, Precision: 0.56, Recall: 0.52, F1: 0.54, AUC: 0.53
```

4.2 Disclosure Prediction

By including RF characteristics, the Support Vector Machine component enhanced the disclosure behaviour prediction. With an F1-score of 92.7%, the hybrid model offered tailored disclosure recommendations. When compared to the standalone SVM, the hybrid model successfully decreased false positives in "high risk" disclosure predictions. During testing using simulated user feedback, users found that the system's recommendations were accurate ROC – AUC 95.2% of the time. The findings show that by fusing the advantages of Random Forest and Support Vector Machine algorithms, the hybrid model effectively improves privacy and information disclosure control. The outcomes of the experiment show how well the hybrid approach manages information exposure and privacy on SNS. The model overcomes the shortcomings of previous privacy models by combining Random Forest and Support Vector Machine to achieve high accuracy, contextual adaptability, and real-time performance.

REFERENCE

Chen, L., & Huang, J. (2021). Adaptive privacy solutions in social media. ACM Transactions on Internet Technology, 21(3), 18–33.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. Journal of Social Issues, 59(2), 323–342.

Francis, H., Wang, Z., & Lee, M. (2021). User-controlled privacy mechanisms in digital platforms: Balancing usability and protection. IEEE Transactions on Information Forensics and Security, 16(1), 1182–1194.

Khalili, A., Sato, H., & Miller, J. (2024). The impacts of social networking sites on privacy and mental health. Journal of Digital Interactions, 12(3), 101–115.

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. Journal of Information Technology, 25(2), 109–125.

Liu, Q., Zhang, Y., & Kumar, R. (2023). Hybrid machine learning models for privacy and security. Journal of Data Science and Analytics, 15(4), 567–580.

Nissenbaum, H. (2009). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.

Ren, W., Zhang, R., & Liu, H. (2022). Advances in privacy models for social networking sites: Challenges and hybrid solutions. Journal of Computational Privacy, 9(2), 211–234.

Zhang, R., Liu, H., & Chen, Y. (2020). Privacy protection mechanisms in social networking sites. Social Media Research Journal, 8(1), 45–61.