JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

Volume 17, No. 3
December 2024
ISSN: 1946-1836

In this issue:

iscap
Information Systems
& Computing
Academic Professionals

The **Journal of Information Systems Applied Research** (JISAR) is a double-blind peer reviewed academic journal published by ISCAP, Information Systems and Computing Academic Professionals. Publishing frequency is three issues a year. The first date of publication was December 1, 2008.

JISAR is published online (https://jisar.org) in connection with the ISCAP (Information Systems and Computing Academic Professionals) Conference, where submissions are also double-blind peer reviewed. Our sister publication, the Proceedings of the ISCAP Conference, features all papers, teaching cases and abstracts from the conference. (https://iscap.us/proceedings)

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the conference. At that point papers are divided into award papers (top 15%) and other submitted works. The non-award winning papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in JISAR. Currently the acceptance rate for the journal is approximately 35%.

Questions should be addressed to the editor at editor@jisar.org or the publisher at publisher@jisar.org. Special thanks to members of ISCAP who perform the editorial and review processes for JISAR.

2024 ISCAP Board of Directors

JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

Network Intrusion Detection System with Machine Learning as a Service

Loma Kangethe
Lk07736@georgiasouthern.edu

Hayden Wimmer
hwimmer@georgiasouthern.edu

Department of Information Technology
Georgia Southern University
Statesboro, GA 30460, USA

Carl M Rebman, Jr.
carlr@sandiego.edu
Knauss School of Business
Department of Supply Chain, Operations, and Information Systems
University of San Diego
San Diego, CA 92110, USA

Abstract

Cloud Computing and Big Data continue to be disruptive forces in computing and has introduced new threats and vulnerabilities to our networks. The paper seeks to demonstrate how an end-to-end network intrusion detection system can be built, trained, and deployed using Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP). We determined the performance of these tools by building a network intrusion detection system (NIDS) and evaluating the performance of each based on precision, accuracy, F1 Score, recall, user experience, cost and computation time for training and predicting the model. Overall, all three platforms performed greater than 90% accuracy with Google Vertex AI having the highest accuracy using the decision tree and Microsoft Azure performing the best based on accuracy, precision, and computation time.

Keywords- Network Intrusion Detection, Machine Learning (ML), Microsoft Azure Machine Learning, Amazon Web Services (AWS), Sage Maker, Vertex AI

Recommended Citation: Kangethe, L., Wimmer, H., Rebman Jr., C.M., (2024). Network Intrusion Detection System with Machine Learning as a Service *Journal of Information Systems Applied Research.* 17(3), pp. 4-15, https://doi.org/10.62273/EWQL5023

Network Intrusion Detection System with Machine Learning as a Service

Koma Kangethe, Hayden Wimmer and Carl M. Rebman, Jr.

1. INTRODUCTION

Cloud computing is an on-demand access to computing resources such as servers (physical servers and virtual servers), data storage, applications, development tools, networking capabilities, analytics, intelligence and networking capabilities. This access is enabled via the internet by hosts as remote data centers that are managed by a cloud services provider (CSP) such as AWS, Microsoft Azure and Google. These CSP are able to offer faster innovation, flexible resources, and economies of scale. Some of the more specific services that CSP provides include r Software as a service (Saas), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Machine Learning as a Service (MLaaS). MLaaS is a range of services that offer machine-learning tools as part of Cloud Computing Services.

MLaaS is an automated and semi-automated cloud platform that is provided in a cloud marketplace that stores massive amounts of data, has low deployment costs, and has high computing performance. MLaaS providers use their own data center to handle calculations and prevent clients from running their own servers or installing their own software. This introduces cost savings and eliminates the risk associated with having the infrastructure on premises. The platform covers most infrastructure issues such as data pre-processing, model training, and evaluation. Predictions can easily be bridged through REST API to the respective applications. MLaaS services allow for fast model training and deployment with little to no data science expertise. MLaaS providers offer tools that include data visualization, APIs, face recognition, natural language processing, predictive analytics, deep learning and many more.

Figure 1 illustrates how these attacks occur in the network. There are mainly two types of intrusion detection systems (IDS): misuse (signature) based, and anomaly-based systems. A misuse-based system detects already known attacks by use of signature rules defined by network administrators or security specialists. Misuse detection requires frequent updates of signatures to ensure ample detection. If a new attack is reported the security specialists must update the signature database. The limitation with this system is that it cannot be helpful against unknown attacks such as zero-day attacks. An anomaly-based system checks the network behavior and classifies it as normal or abnormal. This system analyzes past data to detect both known and unknown attacks by using statistical based, machine learning based and knowledge-based techniques.

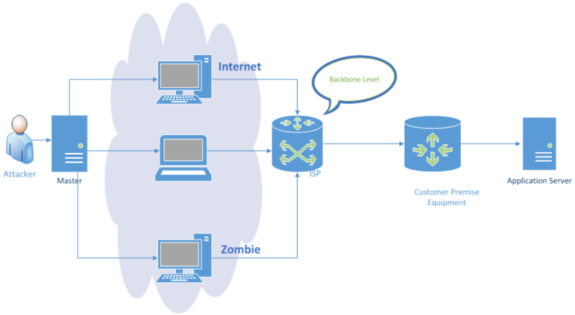


Figure 1: Malware Attack Architecture

The objective of the paper is to use and compare cloud-based machine learning tools for enhanced big data applications to provide data scientists with a set of tools and cloud services that cover the end-to-end machine learning development cycle: ranging from the models' creation, training, validation and testing to the models serving as a service, sharing and deployment. The cloud-based architecture will showcase how data scientists' researchers can develop complex models and train the models in a distributed manner hence automatically parallelizing models and datasets across multiple processors. This research will also compare with building the ML algorithm on-premises.

2. LITERATURE REVIEW

Mäkelä (2022) researched cloud machine learning service providers by comparing the end-to-end machine learning processes on both Amazon Web Services (AWS) and Google Cloud Platform (GCP). The objective was to build an end-to-end machine learning which included two main sections of data pre-processing, and model training and deployment. They then compared the features and performance between the two providers. Data was prepared by organizing and also removed unnecessary variables or information. Jobs were run to prepare the data, and once transformations were completed the dataset was exported back for model training. The GCP command line terminal was used to build the model using TensorFlow. Results show both platforms are equally capable of training an externally created model.

Berg (2022) studied image classification with Machine Learning as a Service seeks to compare Azure, AWS SageMaker, and Vertex AI. The study reviewed MLaaS needs and MLaaS providers and compared various characteristics of MLaaS providers. An image classification algorithm was built, trained, validated and deployed on all the management console on the three cloud platforms using three different datasets. The prediction accuracy, training time, and cost were measured with three different datasets and their features compared. Results indicated that Microsoft Azure ML performed best in terms of prediction accuracy, and training cost, across all datasets. Amazon Web Services SageMaker had the shortest time to train but performed the worst in terms of accuracy and had trouble with two of the three datasets. Google Cloud Platform Vertex AI did achieve the second-best prediction accuracy but was the most expensive platform as it had the largest time to train. It did, however, provide the smoothest user experience. Overall, Azure ML would be the platform of choice for image classification tasks after weighing together the results of the experiments as well as their subjective user experience.

Xhepa and Kanakala (2022) studied Machine Learning Model Computation in AWS and Azure. They examined the machine learning image classification service on cloud to determine the best cloud platform for machine learning projects. For AWS, Amazon SageMaker was used to build, train and deploy the model, S3 bucket for object storage, Amazon EC2 was used to configure instances and IAM for access management. For Microsoft Azure; AzureML was used for the development, training, and deployment of the model and Azure Blob Storage for object storage. Azure Machine Learning workspace was utilized for working with all of the artifacts generated by Azure Machine Learning. Results indicated an artificial intelligent system built on AWS and Azure cloud platforms has the capability to efficiently learn from increasingly complex images with a high degree of generalization using a relatively small repository of data. A highly accurate model was built using TensorFlow with an accuracy of 58%. AWS SageMaker appeared to be an excellent platform for developing simple models and deploying them in the cloud with minimal configuration. However, for predictive analytics, Azure ML may be a more versatile option and this study demonstrated how users can use Amazon Sage Maker and AzureML to easily build, train, and deploy machine learning models.

Opara, Wimmer, and Rebman (2022) studied building an Auto-ML model on the cloud environment. Their objective was to demonstrate the Auto ML functionalities against cyber security threat detection using three different cloud platforms Microsoft Azure, Google, and IBM. They then determined the performance of each platform by evaluating the optimization speed and accuracy results. The UNSW-NB15 dataset and Decision Tree Classifier, Random Forest Classifier and Gradient Boost Classifier algorithms were used and compared in terms of how they processed data and their accuracies. A comparison of the advantages of each of the results from the different platforms were presented and their results showed all three platforms performed greater than 70% accuracy with the IBM Cloud Platform having the strongest performance. They observed that the best machine learning algorithm utilized was the Gradient Boost Classifier algorithm with an accuracy score of 89.5%.

Liberty et al. (2020)’s work centered on scalable machine learning. They looked at the challenges of training ML models on large, continuously evolving datasets and included the following variables; support for incremental training and model freshness, predictability of training costs, elasticity and support for pausing and resuming training jobs for large-scale ML, and the ability to automate hyperparameter optimization and model tuning. Their study built, trained and deployed selected algorithms using Amazon SageMaker, which supports incremental, resumable and elastic learning, as well as automatic hyperparameter optimization. The platform was compared to JVM-based algorithm implementations with regard to computation time and cost. The algorithms selected were Linear Learner, Factorization Machines, K-Means Clustering, Principal Component Analysis (PCA), Neural Topic Model (NTM), Time Series Forecasting with DeepAR. Results indicated that SageMaker can train models both faster and more cost-effective in the majority JVM-based algorithm and is up to 8-times faster than MLlib, as they provided results two to three times cheaper when using the same amount of training time.

Lee (2018) focused on analyzing trends in machine learning as a service, the purpose of the study was to review MLaaS needs and MLaaS providers and compare various characteristics of MLaaS providers. Lee (2018) used four cloud platforms Microsoft Azure Machine Learning Studio, Amazon Machine Learning, Google Cloud Machine Learning Engine, BigML and IBM Watson Studio. Models were built, trained and deployed on the management console and are compared based on the features. Results showed that for AWS, data can be loaded from multiple sources including Amazon RDS, Amazon Redshift, and CSV file.

Kaymakci, et al. (2022) centered on the problems of digital transformation and a transition to cloud-based solutions to use AI/ML by small and medium-sized businesses (SMBs) in the industrial sector. The study presented a systematic selection process of ML cloud services for manufacturing SMB and posed a four-step process to select ML cloud services for SMBs based on an analytic hierarchy process. Their objective was to minimize the hurdles to ML cloud service adoption and to promote digital transformation in manufacturing SMBs. A decision matrix was used to identify the most-suited ML cloud service. The target was focused on IT Security, reliability, cloud management, flexibility, costs, performance, and normalized score. The normalized score showed that AWS SageMaker had a score of 0.3725, Azure ML had a score of 0.38334, and GVP AI platform had a score of 0.2441. Hence, Microsoft's Azure ML had the highest score of the three services and, therefore, is the most fitting for meeting the specific goals for SMB.

Developing classification algorithms using machine learning frameworks is time-consuming, costly, and requires a team with technical capabilities. Noshiri et al. (2021) focused on adopting Machine Learning-as-a-service (MLaaS) cloud delivery model. They used pre-built classification algorithms and evaluated the performance of BigML, Microsoft Azure ML Studio, IBM Watson ML Studio and Google AutoML platforms on the classification of multi-class datasets. They used the metrices of the average-micro-F-score, accuracy, training time, and cost. The purpose of the research was to assist small-to-medium companies in choosing the appropriate platform based on the trade-offs between the average-micro-F-score and training time. A 10 labeled dataset from the UC Irvine ML Repository was used. IBM SPSS Statistics 26, a statistical software was used to extract actionable insights from the data. random subsampling cross-validation procedure was performed on all datasets with different random seeds. Data was split in ratio of 85% to 15% for training and testing data, The data was then fed to the various cloud performs and evaluated. The study found that Google AutoML provided the user with the highest average micro-F score although it is costly and requires more training time.

Yao et al. (2017) focused on researching the complexity vs. performance of Machine Learning as a Service. They evaluated the effectiveness of MLaaS systems from customizable systems to fully automated ones to find out how control relates to risk. UCI machine learning repository was used to get the datasets. The datasets included both numeric and categorical features. Categorical features were converted to numerical values, missing fields with median values, and data samples were split into training and test set by a 70%–30% ratio. The models used were Logistic Regression, Support Vector Machine, Naïve Bayes, Multi-Layer Perceptron, Decision Tree, Bagging, and k-Nearest Neighbor. The platforms used were Amazon Google, Big ML, Prediction IO, Local and Microsoft. Results showed that platforms with higher complexity (more dimensions for user control) achieved better performance. Microsoft provided the highest performance across all platforms, and a highly tuned Microsoft model can produce performance identical to that of a highly tuned local scikit-learn instance. It was observed that server-side optimizations help fully automated systems outperform default settings on competitors, but still lag far behind well-tuned MLaaS systems which compare favorably to standalone ML libraries.

Zhao et al. (2020) used Machine-Learning Based TCP security action prediction in their study which focused on addressing the problems faced in network security. The use of TCP firewalls to either allow or deny traffic according to specific rules is a common exercise of network administrators. However, this is a daunting task due to the huge amount of data on the internet. Machine learning methods of computer security are used to ease this burden. The research sought to predict TCP security action based on TCP transmission characteristics using Machine

Learning techniques. Data Inspection was done and standardized. Importance of each feature analyzed by assessing their permutation importance and fed to the ML engine. Machine models used were AdaBoost, Logistic regression, Support Vector Machine (SVM) neural networks and other ensemble techniques. Results revealed ensemble methods that combine individually reasonable models to make an integrated classifier achieve the best accuracy. The predicted accuracy of TCP security action reached over 98%. Better accuracies can be attained by further preprocessing and fine tuning the algorithms (Zhao et al., 2020).

3. METHODOLOGY

In this section, we present the system setup architecture, the feature attributes of the dataset, the preprocessing techniques, the classification algorithms explored, and the test and evaluation methods used for each of the cloud platforms is described.

System Architecture

This section presents the design architecture of the system and explains the sequence of the process and procedure. This architecture was inspired by the architecture of the three renown cloud platforms to find a solution that is fit for use and purpose based on the use case.

Figure 2 is a system design architecture employed to the three-cloud platform namely AWS, Microsoft Azure, and Google cloud platform. It demonstrates the flow of the designed framework from when the data is loaded to the output of the network intrusion detection system.

The process can be summarized in the following steps:

1. **Data Extraction**: Fetch and Load the data – Data was generated within GSU Southern IT Lab in PCAP format and converted to CSV.
2. **Exploratory data analysis (EDA)**: Analysis was done on the dataset to help identify obvious errors, better understand patterns within the dataset, detect outliers, find relations among variables, and provide insight.
3. **Data Preprocessing**: Data was cleaned by dealing with missing values and the SMOTE technique used to deal with oversampling.
4. **Feature Importance:** This technique assigns a score to input features based on how useful they are at predicting a target variable. This is important for feature selection.

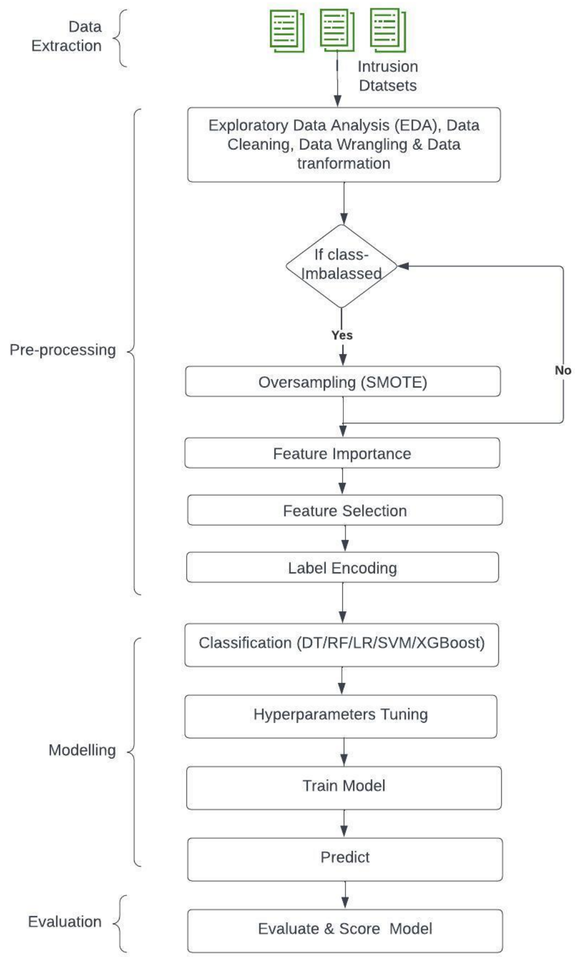


Figure 2: Cloud Machine Learning Flowchart

5. **Feature Selection**: This technique reduces the number of input variables when developing a predictive model. Hence redundant and irrelevant features in the data which may slow down the process of classification are handled. Tree based and Chi-Squared methods are used.
6. **Label Encoding:** converting the labels into a numeric form so as to convert them into the machine-readable form. This is to ensure the Label column is encoded without having any weights or has an ordinal nature.
7. **Train and Test Instance**: the data is split into training dataset and testing dataset randomly. The training dataset is set to 70% while the Test data is set

to 30%. The training data set is fed into different machine learning algorithms to build the model.

8. **Model Classifier**: Different classification models are built used to classify the network traffic in the test data set as normal or attack traffic. The five classification-based algorithms built are: Logistic Regression, Decision Tree, Random Forest, Gradient Boosting Tree (GBT) and Support vector machine (SVM).
9. **Model Evaluation**: This is the process where the models are evaluated based on Accuracy, Recall, Precision and F1 Score.
10. **Compute Time:** This is also evaluated based on the time taken to train the model and predict the model.

DATASET

The dataset was generated within the Georgia Southern University Lab environment. The dataset has real time activities and contemporary attack behavior. The purpose or goal of this research is to predict attacks in this dataset using the different cloud platforms discussed above. The implementation phase initially loads the extracted data into each of the cloud platforms. We shall cover the implementation in each of the cloud performance.

Machine Learning Process and Data Pre-processing

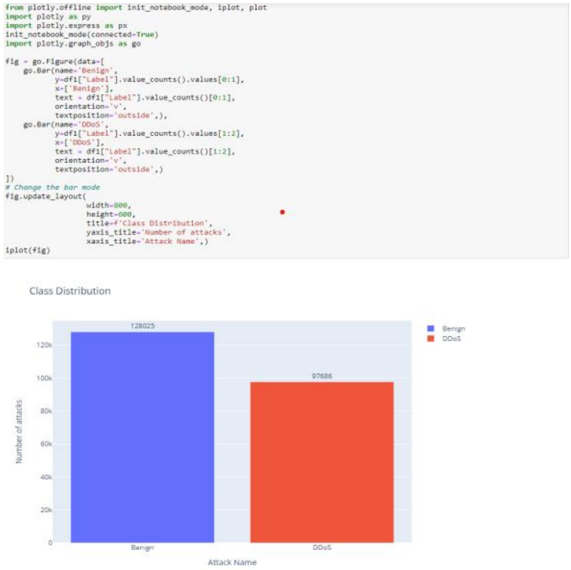
There are different preprocessing steps taken for the removal of unwanted data. The importance of this step is to have a high-quality dataset that will allow the process to be fast and the capture of malware efficient.

- **Missing values**: Features that had more than 70% of the data missing were dropped. The rest of the columns were imputed with the mode based on the descriptive statistics of the features; this ensured that the significance of the dataset was not impacted.
- **Single value columns**: The dataset contained columns with single constant values. The columns had zeros as the integer value. These columns were dropped as they added no value in the model.

Oversampling Technique

Anomaly Synthetic Minority Oversampling Technique (SMOTE) technique was used due to an imbalanced dataset resulting from the anomaly detection case not having a uniform distribution. Figure 3 visualizes the imbalance.

Smote is simply synthesizing duplicating examples from the minority class in the training dataset prior to fitting a model. This can balance the class distribution but does not provide any additional information to the model, hence can effectively learn the decision boundary during prediction.

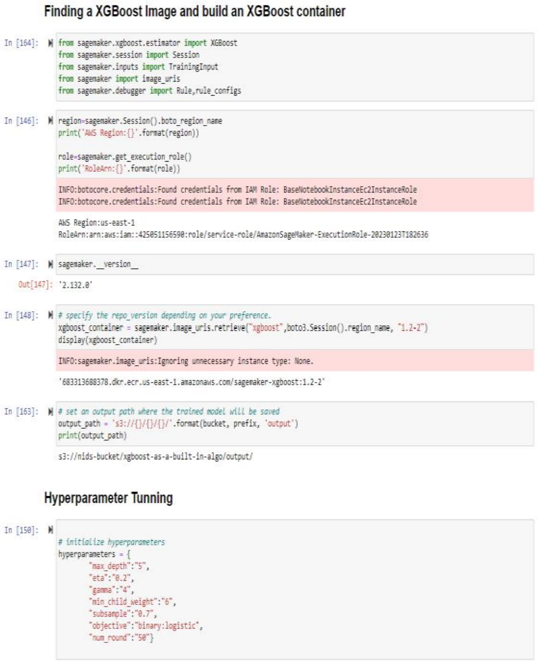


```
from plotly.offline import init_notebook_mode, iplot, plot
import plotly as py
import plotly.express as px
init_notebook_mode(connected=True)
import plotly.graph_objs as go

fig = go.Figure(data=[
    go.Bar(name='Benign',
           y=df1["Label"].value_counts().values[0:1],
           x=['Benign'],
           text = df1["Label"].value_counts()[0:1],
           orientation='v',
           textposition='outside',),
    go.Bar(name='DDoS',
           y=df1["Label"].value_counts().values[1:2],
           x=['DDoS'],
           text = df1["Label"].value_counts()[1:2],
           orientation='v',
           textposition='outside',)
])
# Change the bar mode
fig.update_layout(
                width=800,
                height=600,
                title=f'Class Distribution',
                yaxis_title='Number of attacks',
                xaxis_title='Attack Name',)
iplot(fig)
```

Figure 3: Class Distribution

Feature Importance & Feature Selection

The Random Forest Classifier (RFC) feature importance was used that was able to rank the features based on its relative importance to the predictor. The top 20 features were selected. Figures 4 and 5 show hyper-parameter tuning and XGB Model training respectively.



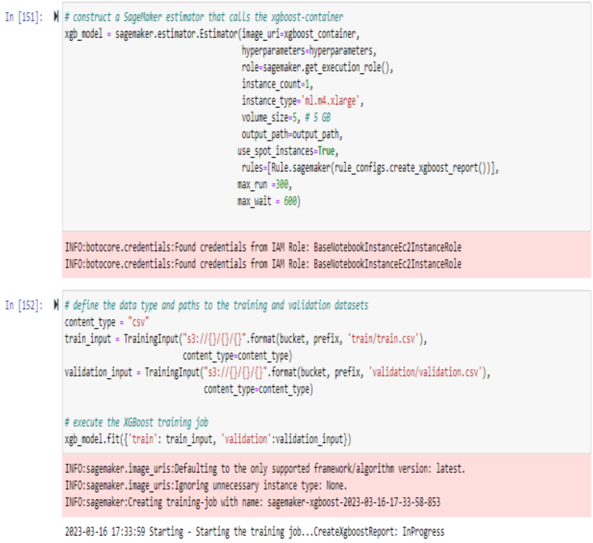
Finding a XGBoost Image and build an XGBoost container

```
In [164]:  from sagemaker.xgboost.estimator import XGBoost
           from sagemaker.session import Session
           from sagemaker.inputs import TrainingInput
           from sagemaker import image_uris
           from sagemaker.debugger import Rule,rule_configs

In [146]:  region=sagemaker.Session().boto_region_name
           print('AWS Region:{}'.format(region))

           role=sagemaker.get_execution_role()
           print('RoleArn:{}'.format(role))

           INFO:botocore.credentials:Found credentials from IAM Role: BaseNotebookInstanceEc2InstanceRole
           INFO:botocore.credentials:Found credentials from IAM Role: BaseNotebookInstanceEc2InstanceRole

           AWS Region:us-east-1
           RoleArn:arn:aws:iam::425051156590:role/service-role/AmazonSageMaker-ExecutionRole-20230123T182636

In [147]:  sagemaker.__version__

Out[147]:  '2.132.0'

In [148]:  # specify the repo_version depending on your preference.
           xgboost_container = sagemaker.image_uris.retrieve("xgboost",boto3.Session().region_name, "1.2-2")
           display(xgboost_container)

           INFO:sagemaker.image_uris:Ignoring unnecessary instance type: None.

           '683313688378.dkr.ecr.us-east-1.amazonaws.com/sagemaker-xgboost:1.2-2'

In [163]:  # set an output path where the trained model will be saved
           output_path = 's3://{}/{}/{}/'.format(bucket, prefix, 'output')
           print(output_path)

           s3://nids-bucket/xgboost-as-a-built-in-algo/output/
```

Hyperparameter Tunning

```
In [150]:
           # initialize hyperparameters
           hyperparameters = {
                   "max_depth":"5",
                   "eta":"0.2",
                   "gamma":"4",
                   "min_child_weight":"6",
                   "subsample":"0.7",
                   "objective":"binary:logistic",
                   "num_round":"50"}
```

Figure 4: AWS XGBoost Hyper-parameter-Tuning



```
In [151]:  # construct a SageMaker estimator that calls the xgboost-container
           xgb_model = sagemaker.estimator.Estimator(image_uri=xgboost_container,
                                                     hyperparameters=hyperparameters,
                                                     role=sagemaker.get_execution_role(),
                                                     instance_count=1,
                                                     instance_type='ml.m4.xlarge',
                                                     volume_size=5, # 5 GB
                                                     output_path=output_path,
                                                    use_spot_instances=True,
                                                     rules=[Rule.sagemaker(rule_configs.create_xgboost_report())],
                                                    max_run =300,
                                                    max_wait = 600)

           INFO:botocore.credentials:Found credentials from IAM Role: BaseNotebookInstanceEc2InstanceRole
           INFO:botocore.credentials:Found credentials from IAM Role: BaseNotebookInstanceEc2InstanceRole

In [152]:  # define the data type and paths to the training and validation datasets
           content_type = "csv"
           train_input = TrainingInput("s3://{}/{}/{}".format(bucket, prefix, 'train/train.csv'),
                                       content_type=content_type)
           validation_input = TrainingInput("s3://{}/{}/{}".format(bucket, prefix, 'validation/validation.csv'),
                                            content_type=content_type)

           # execute the XGBoost training job
           xgb_model.fit({'train': train_input, 'validation':validation_input})

           INFO:sagemaker.image_uris:Defaulting to the only supported framework/algorithm version: latest.
           INFO:sagemaker.image_uris:Ignoring unnecessary instance type: None.
           INFO:sagemaker:Creating training-job with name: sagemaker-xgboost-2023-03-16-17-33-58-853

           2023-03-16 17:33:59 Starting - Starting the training job...CreateXgboostReport: InProgress
```

Figure 5: XGB model train

Evaluation

The model is evaluated based on Accuracy, Precision, Recall F1Score, and Compute Time. The Classification Rate measures how accurate the IDS is in detecting normal or anomalous traffic behavior. It is the number of correct predictions made by the model over all kinds of predictions made. Equation 1 represents the formulae for accuracy.

$$\frac{TP + TN}{(TP + TN + FP + FN)}$$

Equation 1: Accuracy Calculation

Compute Time

There were two metrics measured. Time taken to train the model (i.e., the total time taken from starting the training until the training cycle is complete) and the time taken to make predictions.

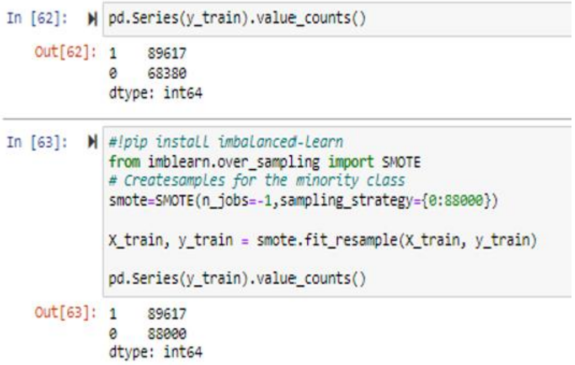
4. EXPERIMENTAL RESULTS

This section describes the results from data preprocessing, the evaluation performance of the network intrusion detection system built on Microsoft Azure, Amazon Web Services and Google Cloud platform. Machine learning models were built, trained, and deployed. The evaluation performance and features of the three platforms are compared amongst themselves and among an on-premise infrastructure.

Explanatory Data Analysis

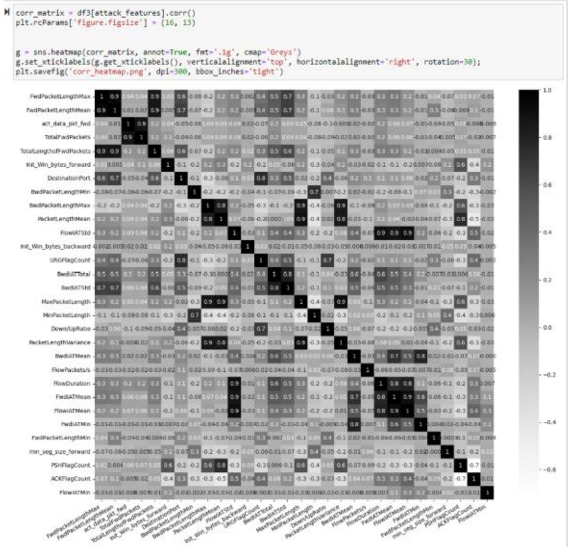
The nature of the dataset based on the class distribution of the target variable indicates an imbalanced dataset this was as the samples of benign outweigh the samples of attack. The dataset is considered not having a normal distribution. The SMOTE technique was applied to overcome this and is illustrated in Figure 6. is a snippet of the SMOTE technique applied.

The Pearson correlation was used to see the correlation between features and was used to reduce the features that were highly correlated. A correlation of greater than 0.95 was used that reduced the features to 30. Fig 7 represents the correlation matrix of features with less than 0.95 similarity. Figure 8 illustrates the importance of features assigned and ranked.



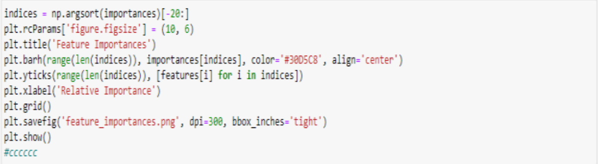
```
In [62]:  pd.Series(y_train).value_counts()

Out[62]:  1    89617
          0    68380
          dtype: int64

In [63]:  #!pip install imbalanced-learn
          from imblearn.over_sampling import SMOTE
          # Createsamples for the minority class
          smote=SMOTE(n_jobs=-1,sampling_strategy={0:88000})

          X_train, y_train = smote.fit_resample(X_train, y_train)

          pd.Series(y_train).value_counts()

Out[63]:  1    89617
          0    88000
          dtype: int64
```

Figure 6: SMOTE Technique



```
corr_matrix = df3[attack_features].corr()
plt.rcParams['figure.figsize'] = (16, 13)


g = sns.heatmap(corr_matrix, annot=True, fmt='.1g', cmap='Greys')
g.set_xticklabels(g.get_xticklabels(), verticalalignment='top', horizontalalignment='right', rotation=30);
plt.savefig('corr_heatmap.png', dpi=300, bbox_inches='tight')
```

Figure 7: Correlation Matrix



```
indices = np.argsort(importances)[-20:]
plt.rcParams['figure.figsize'] = (10, 6)
plt.title('Feature Importances')
plt.barh(range(len(indices)), importances[indices], color='#30D5C8', align='center')
plt.yticks(range(len(indices)), [features[i] for i in indices])
plt.xlabel('Relative Importance')
plt.grid()
plt.savefig('feature_importances.png', dpi=300, bbox_inches='tight')
plt.show()
#cccccc
```

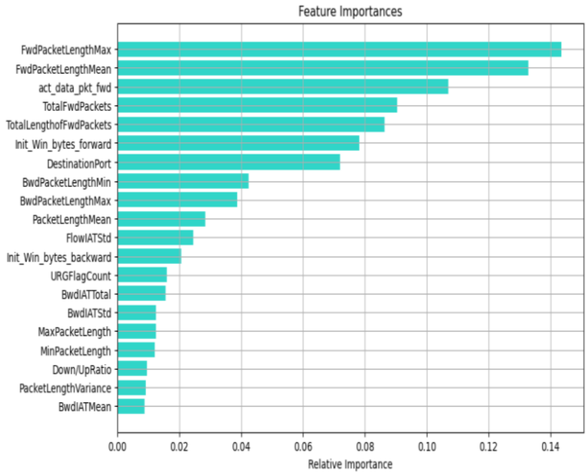


Figure 8: Feature Importance

Table 1 is a comparison of the three cloud platforms based on supported tools, Data types supported, cost etc.

Modeling Results

The models trained and deployed were Logistic Regression, SVM, Decision Tree, Random Forest, and Gradient Boost. Evaluations were compared against each of the three MlaaS and the on-premise set up. The evaluation matrix used was Accuracy, F1 score (overall performance), precision, recall and computation time which reflects on the cost and the time taken to get insights to act on.

	AWS Sage maker	GCP Vertex AI	Microsoft Azure ML
Programming Tools	Python, R studio License required.	REST API, Python, R	Python, R
ML Canvas	Drag and drop Sage maker canvas	Not available	Drag-and-drop UI Azure Ml Studio
ML Frame-works	TensorFlow, PyTorch, Keras ApacheMXNet, XGBoost, Gluon, Caffe2,Chainer, Torch	TensorFlow scikit-learn, XGBoost, Keras	TensorFlow scikit-learn, PyTorch, Microsoft Cognitive Toolkit, Spark ML
Data Types supported	Categorical Numerical Time-series Image Text	Categorical Numerical Time-series Image Text	Categorical Numerical Time-series Image Text
Feature Store	Yes	Yes	No
Built-in Algorithm	Yes	No	No
Schedule	Yes	Yes	Yes
Auto ML	Yes	Yes	Yes
Publish endpoint	Internal only	Yes	Yes
Ease of use	Score (1 -low, 5-high) Documentation – 5 Data Preparation -3 Steps in Training- 3	Score (1 -low, 5-high) Documentation-3 Data Preparation- 4 Steps in Training-4	Score (1 -low, 5-high) Documentation-4 Data Preparation- 5 Steps in Training -4
Cost Analysis	$1.125 per hour	$3.465 per hour	$0.9 per hour

Table 1: Comparison of Cloud Platforms

Results show that gradient boost gave the best parameters with an accuracy score of 93.7%, F1 score of 0.94, precision of 0.91, and recall of 0.92 followed by random forest and decision tree. Support Vector Machine and Logistic regression cave the lowest scores. In regards to computer time, Logistic Regression took the least amount of compute time across all platforms while SVM was noted to take the longest.

The average compute time on premises data warehouse is 77 sec of training and 0.26 sec for predicting time while on cloud is averagely 20 sec for training and 0.21 sec for predicting. Based on the dataset support vector machine took the longest time to train and predict.

Among the 3 MlaaS, Microsoft Azure ML takes the least amount to train and predict. This is followed by AWS. Vertex AI takes the most time to train and predict, however on premise took the longest across all models. Figures 9-14 illustrate the evaluation metrics results.

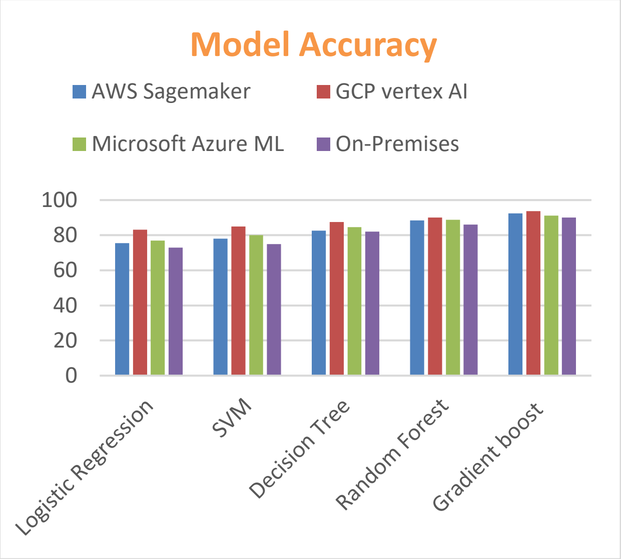


Figure 9: Model accuracy comparison

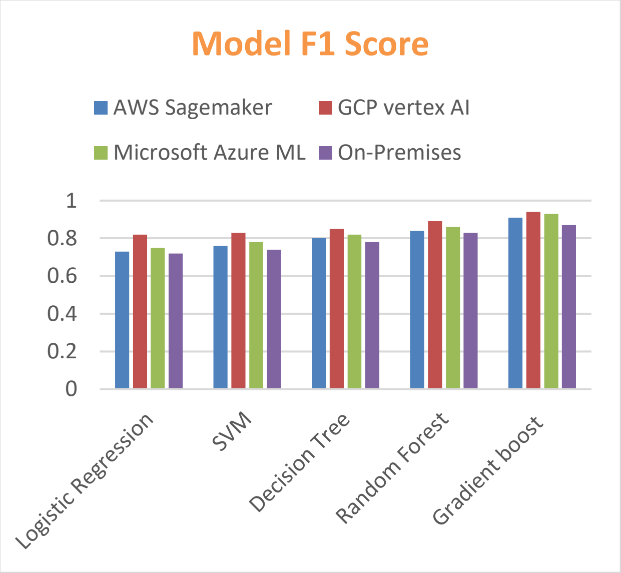


Figure 10: Model F1 score

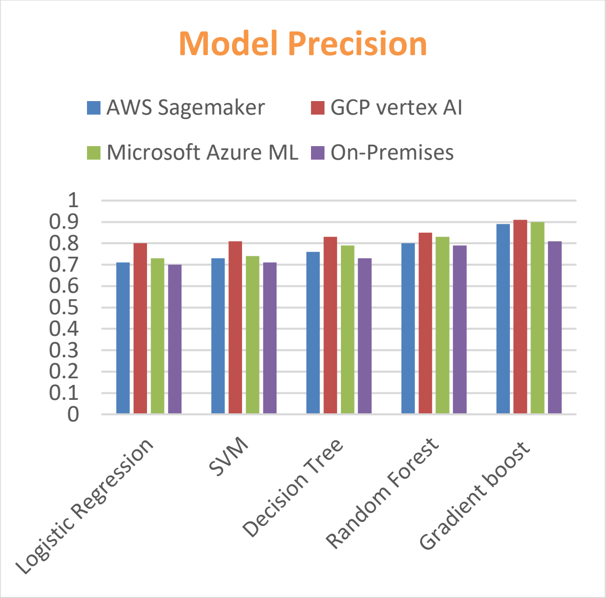


Figure 11: Model precision

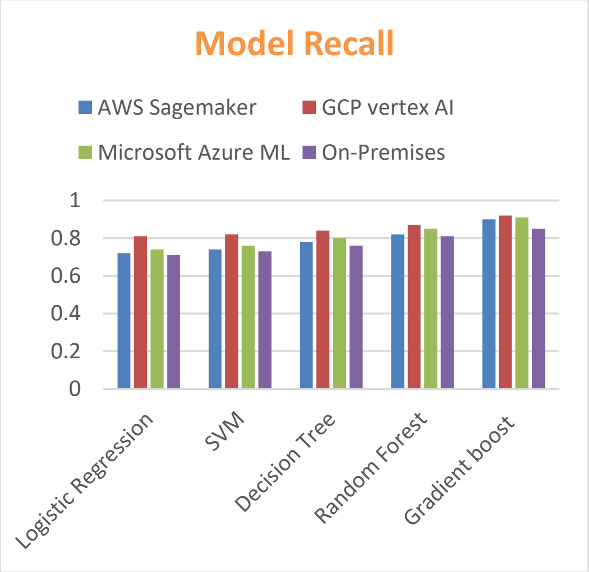


Figure 12: Model Recall

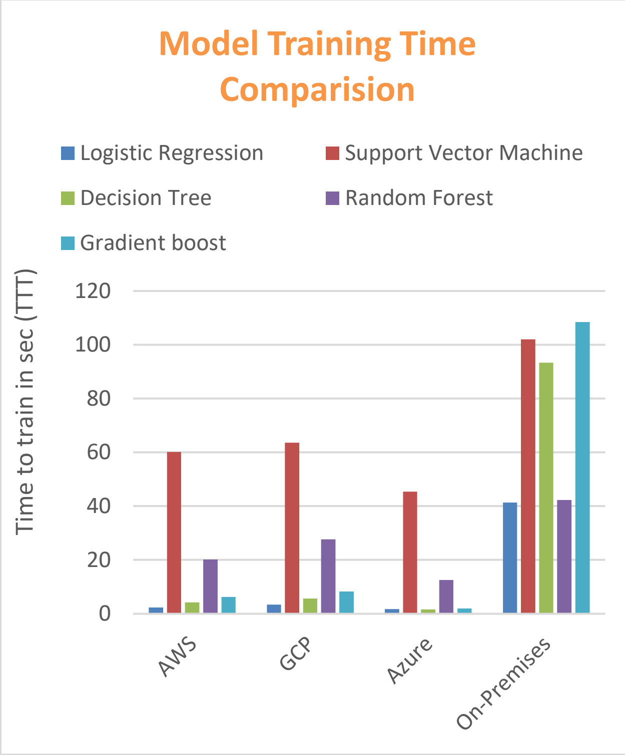


Figure 13: Model Training Time to Train in sec (TTT)

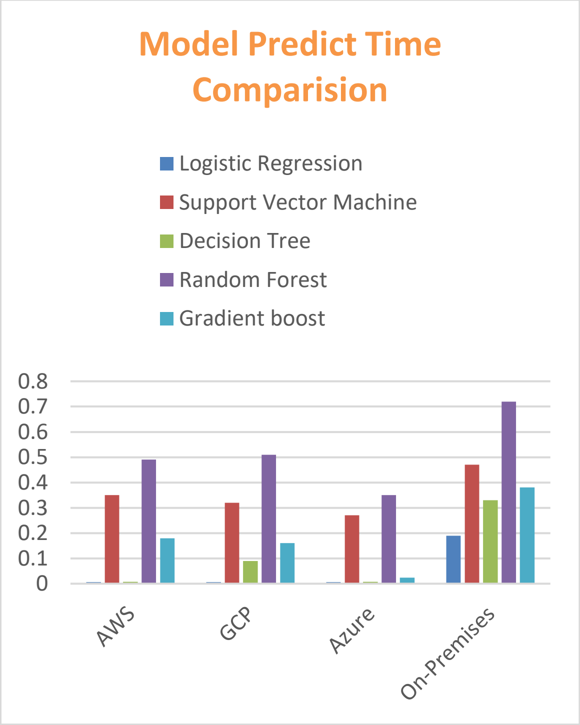


Figure 14: Model Prediction Time in seconds (TTP)

5. DISCUSSION

The MLaaS evaluation was categorized as below

Model Performance
Results show that all the models performed with an accuracy of above 75%. It is noted that ensemble methods namely Gradient Decision Tree, Random Forest and Gradient Boost gave a higher accuracy of greater than 80% with gradient boost giving the highest accuracy of 93.7%. It was observed that GCP Vertex AI gave the best performance with the least number of false positives and negatives.

Training Time and Prediction Time
Logistic regression had the least time to train and predict on all platforms between 3.4 sec-1.73 sec. This is attributed to the model complexity where logistic regression is not very complex, however it was seen to have the poorest performance. Models on cloud took less time to train which indicated that it's better to use MLaaS platforms when dealing with big data and resource intensive models.

User Experience
Microsoft Azure ML gave the best user experience as little coding is required on the canvas as well as it provides the option to code using the Azure terminal, VS code and Notebook hence gives several options to the user. Scheduling and model deployment was also noted to be a smooth and simple process. Azure was observed to provide a lot of flexibility compared to the rest of the platform.

Cost
Vertex AI was the most expensive training at $3.465 per hour, due to that it scales the training job amongst many instances at once. Azure was the cheapest followed by AWS. SageMaker and Azure, the cost is pretty much directly linked to the training time. The SageMaker instance that trained the models ran at a cost of $1.125 per hour and the Azure instance at $0.9 per hour.

Documentation
AWS SageMaker has the most documentation compared to Azure and Vertex AI hence makes it easier to implement AWS and get online solutions to problems frequently encountered.

Networks have been in existence for a long time however with the rapid growth in technology like the use of IoT devices and Edge computing Services, Network data is being produced in

great masses. The threat to networks is increasing and the need for an intelligent intrusion detection system is needed for the cyber security team and hence the framework is built to solve the problem by inspecting traffic traversing the network.
The proposed IDS can be:

- Placed at strategic points in the network as a NIDS (network-based intrusion detection)
- Installed on system computers connected to the network to examine inbound and outbound data on the network.
- Installed on each individual system as a HIDS (host-based intrusion detection)

The proposed framework will help Cyber Security Team to:

- Identify Security threats in the networks within a short period of time and hence reduce the delays and extent of damages that come from identifying malicious attacks late.
- The system provides comprehensive defense against identity theft, information mining, and network hacking. It monitors the network for malicious activity and protects it from unauthorized access with a detection accuracy of 99% and a false positive rate of 0.1%.
- Eliminate of on-premise data center associated risks as fire, faulty equipment etc., hence assurance of uptime and redundancy.
- Cost Savings : Since it is a pay as you go. This ensures you only pay for what you use.
- Faster Deployment : There is faster training and prediction time of the IDS model hence faster deployment.
- Increased Collaboration : Ease to synch files, workspaces in real time hence increase efficiency.

The above shows that our proposed framework can provide high scalability and performance in detecting malicious attacks in masses of network of data being generated in high velocity.

6. CONCLUSION

In this paper we propose the anomaly-based intrusion detection system on 3 different cloud platform (Vertex AI, Azure ML, AWS SageMaker) and compared the performance among them and with an on premise set up.

The system can manage large scale network packet analysis in a short period of time on different cloud platforms. Vertex AI provides the best accuracy and was the least costly. Azure ML performed the best in training and predicting time and offered the best user experience. AWS SageMaker was the fastest to set up due to availability of rich documentation. To test the system, we used the real IDS dataset provided by the Information Technology Department of Georgia Southern University. We built several classification models, and the decision tree performed the best based on accuracy and compute time.

We focused on designing the practical intelligent intrusion detection system with high accuracy of 93% and low false positive rate 7 %. In the future, we plan to use multimodal classifiers, introduce spark clusters and data balancing methods and extend to other cloud service providers, such as IBM.

7. REFERENCES

Berg, G. (2022). Image Classification with Machine Learning as a Service:-A comparison between Azure, SageMaker, and Vertex AI.

Kaymakci, C., Wenninger, S., Pelger, P., & Sauer, A. (2022). A systematic selection process of machine learning cloud services for manufacturing SMEs. Computers, 11(1), 14. https://doi.org/10.3390/computers11010014

Lee, Y.-S. (2018). Analysis on trends of machine learning-as-a-service. International Journal of Advanced Culture Technology, 6(4), 303-308. https://doi.org/10.17703//IJACT2018.6.4.303

Liberty, E., Karnin, Z., Xiang, B., Rouesnel, L., Coskun, B., Nallapati, R., . . . Das, P. (2020). Elastic machine learning algorithms in amazon sagemaker. Paper presented at the Proceedings of the 2020 ACM SIGMOD International Conference on Management of Data. https://doi.org/10.1145/3318464.3386126

Mäkelä, R. (2022). End-to-End Machine Learning Leveraging Cloud Service Providers: A Comparison of AWS and GCP (Bachelor's thesis).

Noshiri, N., Khorramfar, M., & Halabi, T. (2021). Machine Learning-as-a-Service Performance Evaluation on Multi-class Datasets. Paper presented at the 2021 IEEE International Conference on Smart Internet of Things (SmartIoT). DOI: 10.1109/SmartIoT52359.2021.00060

Opara, E., Wimmer, H., & Rebman, C. M. (2022). Auto-ML Cyber Security Data Analysis Using Google, Azure and IBM Cloud Platforms. Paper presented at the 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET). DOI: 10.1109/ICECET55527.2022.9872782

Xhepa, M., & Kanakala, N. S. (2022). Machine Learning Model Computation in AWS and Azure.

Yao, Y., Xiao, Z., Wang, B., Viswanath, B., Zheng, H., & Zhao, B. Y. (2017). Complexity vs. performance: empirical analysis of machine learning as a service. Paper presented at the Proceedings of the 2017 Internet Measurement Conference. https://doi.org/10.1145/3131365.3131372

Zhao, Q., Sun, J., Ren, H., & Sun, G. (2020). Machine-learning based TCP security action prediction. Paper presented at the 2020 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE). DOI: 10.1109/ICMCCE51767.2020.00291

U.S. Healthcare System's Electronic Health Records Security Threat Avoidance

Andualem Woldeyohannis
awoldeyohannis6256@ucumberlands.edu
University of the Cumberlands
School of Computer and Information Sciences
6178 College Station Drive, Williamsburg, KY 40769

Mary Lind
mary.lind@lsus.edu
Louisiana State University Shreveport
College of Business
1 University Drive
Shreveport, LA USA

Abstract

Security breaches of the U.S. healthcare system's electronic health records (EHRs) present a critical challenge in healthcare. Current literature indicates that healthcare professionals' poor cybersecurity behaviors are the leading cause of data breaches in the U.S. healthcare system. Using technology threat avoidance theory, this non-experimental quantitative correlational study aimed to determine to what extent U.S. healthcare professionals' perceived susceptibility, perceived severity, safeguard effectiveness, safeguard cost, self-efficacy, and threat perceptions of EHRs security breaches influenced their threat avoidance motivations and threat avoidance behaviors while using EHRs. The research findings indicated that perceived severity and perceived susceptibility significantly correlate with a user's threat perception. The cost of safeguarding measures and the user's self-efficacy were predictors of healthcare professionals' threat avoidance motivation. Perceived threat and safeguarding effectiveness were not proven to affect avoidance motivation significantly. Avoidance motivation strongly predicted healthcare professionals' EHRs security breach threat avoidance behavior.

Keywords: Electronic Health Records; Technology Threat Avoidance Theory; Data Breaches, Perceived Threat, Avoidance Motivation

Recommended Citation: Woldeyohannis, A., Lind, M., (2024). U.S. Healthcare System's Electronic Health Records Security Threat Avoidance U.S. *Journal of Information Systems Applied Research.* 17(3), pp. 16-28, https://doi.org/10.62273/HLGE2976

Healthcare System's Electronic Health Records Security Threat Avoidance

Andualem Woldeyohannis and Mary Lind

1. INTRODUCTION

This study focused on electronic health record (EHR) use in the U.S. healthcare system. Recent reports indicate that most EHR data breaches in the U.S. healthcare system are caused by human factors (Chua, 2021; Gioulekas et al., 2022; Yeng et al., 2022). As EHR adoption increases, the sector must adopt comprehensive cybersecurity practices to protect patients' data (Yeng et al., 2022). However, effective cybersecurity practices rely on understanding human factors (Gioulekas et al., 2022; Yeng et al., 2022).

Healthcare professionals' access to sensitive personal data when using EHRs highlights the need to account for the human element when developing healthcare IT cybersecurity infrastructure (Gioulekas et al., 2022). Yeng et al. (2022) argued that robust EHR cybersecurity requires a combination of technical safeguards and human behavioral interventions. Seminal threat avoidance scholars have suggested perceptions of threat susceptibility influence threat awareness, which, in turn, affects motivation and threat avoidance behaviors (Liang & Xue, 2010). As a critical component of designing comprehensive cybersecurity solutions for U.S. healthcare organizations, it is essential to understand healthcare professionals' threat awareness, motivation, and avoidance behaviors (Carpenter et al., 2019; Yeng et al., 2022).

The 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act spurred the adoption of EHR systems across the United States (Colicchio et al., 2019). The primary purpose of the HITECH Act was to encourage healthcare providers to use information technology in a meaningful and secure way (HHS Office for Civil Rights, 2017). One result of the HITECH Act was to increase healthcare providers' adoption of EHR (Colicchio et al., 2019).

As EHR adoption increased, cybersecurity became an even more significant concern for healthcare organizations (Colicchio et al., 2019). The healthcare system has become the top target of cybercriminals (Gioulekas et al., 2022), and cyber threats to the healthcare system have constantly increased (Colicchio et al., 2019). The susceptible nature of patient information, the development of highly interconnected medical and health information technologies, and the prevalence of large databases of diverse health data make cybersecurity a priority in the healthcare industry (Ronquillo et al., 2018). EHR security threats include healthcare provider carelessness/negligence, phishing/ransomware, malicious insiders, and hacking/unauthorized access to EHRs.

2. THEORETICAL FRAMEWORK

Liang and Xue's (2009) Technology Threat Avoidance Theory (TTAT) served as the study's theoretical framework. TTAT explains individual IT users' malicious information technology threat avoidance behavior (Liang & Xue, 2009, 2010). TTAT is one of the most integrated and well-developed theories used to explain information technology users' behavior regarding the avoidance of cybersecurity threats based on cybernetic and coping theory. TTAT defines avoidance behavior as the result of two cognitive processes: threat appraisal and coping appraisal (Liang & Xue, 2009). In the threat appraisal process, individuals perceive an information technology threat if they believe they are susceptible to a technology threat that poses a severe risk (Liang & Xue, 2009). Coping appraisal develops from threat perception, where individuals assess the degree to which individual information technology threats can be avoided (Liang & Xue, 2009).

TTAT also theorizes that individuals assess safeguarding measures based on their perceived effectiveness, cost, and the individuals' ability to take action (i.e., self-efficacy; Liang & Xue, 2009). TTAT postulates that when users perceive information technology threats and believe they are avoidable, they are motivated to take appropriate measures to avoid the threat (Liang & Xue, 2009). If users do not think they can prevent the threat with safeguarding measures, they will engage in emotion-based coping (Liang & Xue, 2009).

The original TTAT model included eight constructs: (a) perceived susceptibility, (b) perceived severity, (c) perceived threat, (d) safeguard effectiveness, (e) safeguard costs, (f) self-efficacy, (g) avoidance motivation, and (h) avoidance behavior. This study used all the core constructs of the TTAT model to understand the human behavior effect of U.S. healthcare system EHRs' security threats. Perceived threat refers to an individual's belief that malicious information technology is dangerous or harmful (Carpenter et al., 2019). Healthcare professionals develop EHR threat perceptions by detecting potential dangers and monitoring the computing environment.

TTAT indicates that two antecedents shape threat perception: perceived susceptibility and perceived severity (Carpenter et al., 2019; Liang & Xue, 2009, 2010). This study used TTAT to understand the influence of U.S. healthcare professionals' EHR security threat awareness on their threat avoidance motivations. As breaches caused by carelessness, negligence, phishing, ransomware, and malicious insiders are the leading cause of U.S. healthcare system data breaches, studying threat awareness was central to understanding how to improve EHR security.

The other TTAT construct, avoidance motivation, represents an individual's intent to avoid a security threat (Carpenter et al., 2019; Liang & Xue, 2009, 2010). In TTAT, threat perception, shaped by susceptibility and severity, is directly linked to threat avoidance motivation, a critical factor in effective cybersecurity solutions (Carpenter et al., 2019). Avoidance motivation was used in this study as a dependent variable affected by threat perception, but avoidance motivation also functioned as an independent variable influencing avoidance behavior.

Avoidance behavior was used in this research to study EHR security in the U.S. healthcare system. Avoidance behavior refers to actions taken to prevent a security breach (Carpenter et al., 2019; Liang & Xue, 2009, 2010). The present study examined the correlation between avoidance motivations and avoidance behavior, with avoidance motivation being the independent variable and avoidance behavior being the dependent variable. As any security measure's goal is actual threat avoidance, it was essential to focus on behavioral outcomes rather than just behavioral intentions. In this regard, understanding the effect of healthcare professionals' security threat awareness on their threat avoidance motivation and behavior is critical in designing adequate cybersecurity best practices for healthcare professionals and U.S. healthcare organizations (Carpenter et al., 2019).

Technology Threat Avoidance Theory (TTAT)

This study used the TTAT to analyze the correlation between U.S. healthcare professionals' EHR security threat awareness and their motivation to avoid security threats. Threat avoidance motivation was also correlated to threat avoidance behavior. The TTAT enabled the study to explain better U.S. healthcare professionals' behavior in avoiding EHR security threats (Liang & Xue, 2009).

TTAT is one of the most integrated theories developed to explain individual users' information technology behavior in avoiding malicious IT threats (Liang & Xue, 2009, 2010) based on cybernetic theory and coping theory. The TTAT defines avoidance behavior as a dynamic behavior, a positive feedback behavior loop, in which to decide how to cope with information technology threats, users go through two cognitive processes, threat appraisal and coping appraisal (Liang & Xue, 2009). In the threat appraisal mental process, individuals will perceive an IT threat if they believe they are susceptible to an IT threat that poses a severe threat. Coping appraisal develops from threat perception, where individuals assess the degree to which information technology threats can be avoided. The coping appraisal of the theory included components from Lazarus's (1966) coping orientations to problems experienced (COPE) framework. Individuals then asses the safeguarding measures based on their perceived effectiveness, cost of safeguarding measures, and self-efficacy in taking the actions. TTAT postulates that when users perceive information technology threats and believe that the IT threat is avoidable by taking appropriate safeguarding measures, they are motivated to avoid it. TTAT also postulates that if users think they cannot avoid the perceived threat with the safeguarding measures, they will engage in coping focused on emotion (Liang & Xue, 2009).

From a theoretical perspective, TTAT is based on two theories, the process, and the variance theory. Coping techniques are the primary tool for malicious technology threat avoidance in both process and variance theories (Liang & Xue, 2009). As per the theories, the TTAT model contextualization depends on the process and the variance theory models.

3. THEORETICAL MODEL

The original TTAT model included eight constructs. The original TTAT theory model had perceived susceptibility, severity, threat, safeguard effectiveness, safeguard costs, self-efficacy, avoidance motivation, and avoidance behavior as constructs to understand human behavior under information technology threats (Liang & Xue, 2009). Liang and Xue (2010) used the TTAT model (see Figure 1) in their study to understand the U.S. healthcare system professionals' EHR security threat awareness and the effect on their threat avoidance motivation and behavior. As human factor-related breaches caused by carelessness/negligence, phishing/ransomware, and malicious insider are the leading cause of U.S. healthcare system EHR data breaches, the theory constructs enabled the study to understand the relationship between the U.S. healthcare system professionals' EHR security threat awareness to their motivation to avoid them.

Figure 1
Technology Threat Avoidance Model (TTAT)

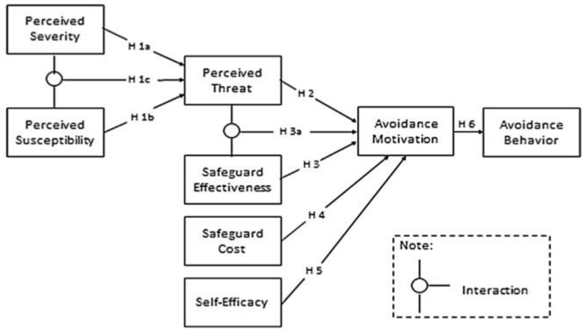


Figure 1 Note. Liang and Xue (2010). It is reprinted with permission.

Liang and Xue (2010) used TTAT to investigate personal computer users' information technology threat avoidance behavior by using safeguarding measures. The study tested a model developed from TTAT by using survey data. Consistent with the TTAT, they proposed that users' threat avoidance motivation is determined by their threat perception, which positively affects the user's threat avoidance behavior. The study also suggested that perceived severity, susceptibility, and interaction affect users' threat perception. In addition, the study hypothesized that avoidance motivation is directly determined by safeguard effectiveness, safeguard cost, and self-efficacy. The research results indicated that when individuals are threatened, they believe the safeguarding measures are effective (safeguarding effectiveness). They are confident in their self-efficacy with inexpensive safeguarding costs; they are more motivated to avoid the threat. The study also found negative interaction between avoidance motivation with perceived threat and safeguarding effectiveness, so when there is a higher perceived threat, there is a weaker relationship between safeguarding effectiveness and threat avoidance motivation, or on the other hand, when there is a high level of effective safeguarding measures, the weaker the relationship between perceived threat and the avoidance motivation. The study helped better understand the personal user's information technology threat avoidance behavior.

TTAT Constructs

Perceived severity is the first construct variable that predicts perceived threat and is the primary criterion variable of the avoidance behavior predictor variable. The perceived severity of a technology threat refers to an individual's subjective belief regarding the damage to their device and systems inflicted by malicious technology (Liang & Xue, 2009, 2010). Perceived severity measures to what extent an individual perceives the severity of the consequences of a malicious IT. The core of perceived severity correlation to a perceived threat is that users perceive that they are vulnerable to a threat and the threat consequence is severe (Liang & Xue, 2009). Falling to consider the vulnerability to a threat and its severity will lead to misunderstanding the threat perception. Alexandrou and Chen (2019) also described perceived severity as the degree to which an individual believes a compromised technology will have potential consequences. Young et al. (2016) and Carpenter et al. (2019) research results indicated that perceived severity is a strong indicator of perceived threat.

Perceived susceptibility is the second construct variable that predicts perceived threat and is the primary criterion variable of the avoidance behavior predictor variable. Perceived susceptibility to a technology threat refers to an individual's subjective belief that their device and system will likely be affected by a malicious technology (Liang & Xue, 2009). Alexandrou and Chen (2019) also define perceived susceptibility as an individual perception of how likely a threat to technology will occur. Liang and Xue (2009) indicated that research strongly supports perceived susceptibility to threat perception as positively correlated. Liang and Xue's (2010) study found a strong correlation between perceived susceptibility and threat. Alexandrou and Chen (2019) and Carpenter et al. (2019) also found that Perceived susceptibility positively impacts a perceived threat.

The interaction between perceived susceptibility and perceived security is a moderation phenomenon where perceived security positively moderates perceived susceptibility in the relationship between perceived susceptibility and perceived threat and vice versa (Liang & Xue, 2010). Both perceived susceptibility and perceived security, independently or together, influence an individual belief regarding the technology threat magnitude (Carpenter et al., 2019). As a function of perceived severity, the relationship between perceived severity and perceived threat can be seen as a positive relationship. The higher the perceived severity, the higher the relationship between perceived susceptibility and perceived threat (Alexandrou & Chen, 2019). The same logic works with the function of perceived susceptibility in the relationship between perceived severity and perceived threat. Liang and Xue's (2010) study found that although there is a positive effect of interaction between perceived susceptibility and perceived severity on the perceived threat, the correlation is not significant. Young et al. (2016) also found that the interaction effect of perceived susceptibility and perceived severity on a perceived threat is insignificant.

Perceived threat is the extent to which the individual understands malicious information technology as dangerous or harmful (Carpenter et al., 2019). Based on the cybernetic theory, a perceived threat indicates the users' current state's proximity to the undesired end state (Liang & Xue, 2009). Liang and Xue (2010) showed that threat perception is shaped by two antecedents: perceived susceptibility and perceived severity. According to Liang and Xue's TTAT model, threat perception outcome depends on the threat's perceived severity, perceived susceptibility, and the safeguarding measure effectiveness available to cope with the IT threat. The main idea behind perceived threat in technology threat avoidance is that when an individual feels that the perceived threat increases, they are more inclined to apply security measures, such as following security measures seriously if they think there is too much phishing activity (Liang & Xue, 2009).

Safeguard effectiveness of TTAT influences avoidance motivation directly and interacts with a perceived threat. Safeguard effectiveness indicates the individual subjective assessment of how safeguarding measures can effectively be applied in protecting from technology threats (Liang & Xue, 2010). It is akin to the perception of outcome expectancy, which reflects the individual user's notion of objective outcome produced by using the safeguard measure (Liang & Xue, 2010). Individuals start the coping appraisal process after a threat is perceived to evaluate potential safeguarding measures. According to Liang and Xue (2010), individuals use safeguard effectiveness, safeguard cost, and self-efficacy to assess IT threat's avoidability.

The self-efficacy construct (end-users self confidence in using computers), an essential variable in avoidance motivation, indicates the user's confidence in taking the safeguarding measure (Liang & Xue, 2010). Liang and Xue (2010) showed that as users' self-efficacy increases, they are motivated to perform IT security behavior. In explaining the reasoning behind the inclusion of self-efficacy in their TTAT model, Liang and Xue (2010) demonstrated that in any given instance, self-efficacy and outcome beliefs would best predict threat avoidance behavior, including applying safeguarding measures such as turning off cookies, editing the computer registry file, installing antivirus software, and updating antivirus software are safeguarding measures. Many studies examining the relationship between self-efficacy and IT threat avoidance motivation indicated that end users are more motivated to apply safeguarding measures as their self-efficacy increases (Liang & Xue, 2009, 2010

Avoidance motivation indicates the intent to avoid a security threat that an individual believes to be a threat (Carpenter et al., 2019; Liang & Xue, 2009, 2010). In plain words, avoidance motivation in IT is the degree to which individual IT users are motivated to take safeguarding measures to avoid IT threats (Liang & Xue, 2009, 2010). Individuals' perception of a technology threat susceptibility, severity, and threat perception coupled with the safeguarding effectiveness, safeguarding cost, and self-efficacy determine an individual's threat avoidance motivation (Liang & Xue, 2009, 2010). According to Liang and Xue (2009), Maslow's hierarchy of needs indicates that the safety of one's property and resources is an individual basic human need; as such, IT users are motivated to avoid threats when they feel the threat will cause privacy and financial losses. Individuals' understanding of susceptibility to a threat and its severity would lead to threat avoidance motivation and behavior, which is critical in designing effective cybersecurity solutions for both users and organizations (Carpenter et al., 2019). Individuals tend to increase their motivation to avoid a technology threat as the threat perception intensifies, and they believe the consequences of the threat outweigh the cost of the safeguarding measures. The study used the TTAT theory model to understand the correlation between perceived threat and avoidance motivation. The studies by Carpenter et al. (2019) and Liang and Xue (2010) showed a strong positive correlation between avoidance motivation and individuals' threat avoidance behavior.

Cybersecurity Threats in the Healthcare Systems

The healthcare industry is becoming more interconnected, making medical devices and clinical and business information electronically available 24/7 (Smith, 2018). EHRs are adopted across the United States healthcare system by the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act (Ronquillo et al., 2018). The act increased the vulnerability of health I.T. Security, making it a growing concern for healthcare organizations (Ronquillo et al., 2018). The sensitive nature of patient information, including the availability of *Protected Health Information (PHI)* and *Personally Identifiable Information (PII),* makes cybersecurity a significant concern. The availability of PHI and PII, the development of highly interconnected medical and health information technologies, and the prevalence of large databases of diverse health data make cybersecurity a priority in the healthcare industry (Ayyagari, 2012).

Data Breaches in the U.S. Healthcare System

A data breach is unauthorized access and illegal disclosing information (Seh et al., 2020). The U.S. health and human services define a health data breach as the illegal use or disclosure of confidential health information that compromises privacy or security under the privacy rule that poses a sufficient risk of financial, reputational, or other types of harm to the affected person (HHS, 2017). In addition to financial damage, data breaches cause tremendous reputation damage to healthcare organizations by lowering their trust level (Seh et al., 2020).

As EHR adoption increased, cybersecurity became an even more significant concern for healthcare organizations (Colicchio et al., 2019). The healthcare system has become the top target of cybercriminals (Gioulekas et al., 2022; Yeng et al., 2022), and cyber threats to the healthcare system have constantly increased (Colicchio et al., 2019). The susceptible nature of patient information, the development of highly interconnected medical and health information technologies, and the prevalence of large databases of diverse health data make cybersecurity a priority in the healthcare industry (Ronquillo et al., 2018). EHR security threats include healthcare provider carelessness/negligence, phishing/ransomware, malicious insiders, and hacking/unauthorized access to EHRs.

A variety of healthcare professionals handle EHRs. Human factors are the leading cause of data breaches in the U.S. healthcare system (Chua, 2021; Yeng et al., 2022). Thus, as doctors, nurses, administrative staff, and information technology workers access patient information, the potential security exposure of patients' health records increases. Poor human security practices cause most reported EHR breaches (Chua, 2021; Yeng et al., 2022). Yeng et al. (2022) indicated that unintentional insider threats cause more than twice the number of EHR breaches than external cyberattacks and theft with malicious intent. Yeng et al. cited phishing scams as the most common cause of breached patient records.

Enhancing Cybersecurity in the Healthcare

Maintaining the privacy, integrity, and accessibility of healthcare information and systems from internal and external threats should be the top priority of healthcare organizations. Several scholars have argued that the U.S. healthcare industry must develop a cybersecurity contingency plan that looks beyond the technical controls and includes human behavioral interventions to effectively protect sensitive patient data (Gioulekas et al., 2022; Yeo & Banfield, 2022). Healthcare organizations institute security policies to protect patient data. The Health Insurance Portability and Accountability Act (HIPPA) requires healthcare providers to use specified safeguards to protect the confidentiality, integrity, and availability of EHR that contain protected health information (CMS, 2021). Unfortunately, healthcare professionals fail to comply with EHRs' security policies for many reasons (Yeng et al., 2022). Yeng et al. (2022) suggested that healthcare professionals fail to comply with EHR security policies because they lack awareness of the severity of security threats.

4. RESEARCH FINDINGS

This nonexperimental, correlational, quantitative study aimed to determine the extent to which healthcare professionals' threat perceptions influenced their avoidance motivations and threat avoidance behaviors when using electronic health records (EHRs). The study filled a gap in the literature regarding U.S. healthcare professionals' perceptions of EHR security, threat avoidance motivations, and avoidance behaviors (Gioulekas et al., 2022; Yeng et al., 2022). The U.S. healthcare system faces significant EHR data security challenges due to healthcare professionals' poor understanding of security threats. Scholars have argued that improving healthcare professionals' understanding and awareness of security threats should be a core part of the U.S. healthcare systems' cybersecurity framework (Gioulekas et al., 2022; Yeng et al., 2022).

This study relied on the entire components of Liang and Xue's model constructs: perceived susceptibility, perceived severity, perceived threat, safeguard effectiveness, safeguard cost, self-efficacy, avoidance motivation, and avoidance behavior. The research examined nine research questions and corresponding sets of hypotheses to determine the extent of the relationships between healthcare professionals' perceptions of EHRs security threats, their motivations to avoid threats, and their threat avoidance behaviors when using EHRs. The hypotheses were as follows:

$H_0$1. Perceived susceptibility does not significantly influence a U.S. healthcare professional's perceived threat when using EHRs.

H_a1. Perceived susceptibility significantly influences a U.S. healthcare professional's perceived threat when using EHRs.
$H_0$2. Perceived severity does not significantly influence a U.S. healthcare professional's perceived threat when using EHRs.

H_a2. Perceived severity significantly influences a U.S. healthcare professional's perceived threat when using EHRs.

$H_0$3. The interaction of perceived severity and perceived susceptibility does not significantly influence a U.S. healthcare professional's perceived threat when using EHRs.

H_a3. The interaction of perceived severity and perceived susceptibility significantly influences a U.S. healthcare professional's perceived threat when using EHRs.

$H_0$4. Perceived threat does not significantly influence a U.S. healthcare professional's avoidance motivation when using EHRs.

H_a4. Perceived threat significantly influences a U.S. healthcare professional's avoidance motivation when using EHRs.

$H_0$5. Safeguard effectiveness does not significantly influence a U.S. healthcare professional's threat avoidance motivation when using EHRs.

H_a5. Safeguard effectiveness significantly influences a U.S. healthcare professional's threat avoidance motivation when using EHRs.

$H_0$6. The interaction of perceived threat and safeguard effectiveness does not significantly influence a U.S. healthcare professional's avoidance motivation when using EHRs.

H_a6. The interaction of perceived threat and safeguard effectiveness does not significantly influence a U.S. healthcare professional's avoidance motivation when using EHRs.

$H_0$7. Safeguard cost does not significantly influence a U.S. healthcare professional's threat avoidance motivation when using EHRs.

H_a7. Safeguard cost significantly influences a U.S. healthcare professional's threat avoidance motivation when using EHRs.

$H_0$8. Self-efficacy does not significantly influence a U.S. healthcare professional's threat avoidance motivation when using EHRs.

H_a8. Self-efficacy significantly influences a U.S. healthcare professional's threat avoidance motivation when using EHRs.

$H_0$9. Avoidance motivation does not significantly influence a U.S. healthcare professional's threat avoidance behavior when using EHRs.

H_a9. Avoidance motivation significantly influences a U.S. healthcare professional's threat avoidance behavior when using EHRs.

Participants and Research Setting
The study's target population comprises healthcare professionals currently employed in U.S. healthcare organizations. The target population is inclusive and does not exclude or focus on any type of healthcare professional. The study involved participants above 18 years of age, and there was no exclusion based on gender, ethnicity, or health status. A total of N = 168 participants completed the survey. An a priori sample size calculation determined that a minimum of N = 166 participants were required to maintain a 95% confidence level to test the significance between the study's nine predictor variables. Thus, the sample size was adequate to test the hypotheses.

The sample was predominantly female, with males accounting for 29.8% of the sample. The sample's gender distribution was not considered an issue because the study was not focused on the potential moderating effects of demographic characteristics. The sample was evenly distributed by age. The largest age cohort (i.e., participants aged 31-35) represented 21.4% of the sample. The smallest age cohort (i.e., participants aged 61-65) represented only 4.2% of the sample. Participants' work experience ranged between less than five years and 25+ years. Most of the sample (73.2%) had six or more years of work experience.

Regression Assumption Tests
The instrument's reliability was tested following the mean, standard error, and standard deviation calculations. While Liang and Xue (2010) validated the instrument, Cronbach's alpha reliability coefficients were calculated to determine the reliability of the survey when used to collect data from U.S. healthcare professionals. A standard threshold of 0.70 was used as a baseline for acceptable reliability. Reliability of the constructs were in the .801 to .943 range. The reliability coefficient values were all higher than the coefficients reported by Tu et al. (2015). After the assumptions were tested (linearity, independence of errors, homoscedasticity/homogeneity of variance, multicollinearity, and normality) and the data were determined to be suitable for multiple linear regression.

Based on the analysis, perceived susceptibility and perceived severity significantly influenced perceived threat. Safeguard cost and self-efficacy significantly influenced avoidance motivation, and avoidance motivation significantly influenced avoidance behavior.

Assessment of Hypotheses
The research questions' findings are discussed in this practical assessment of the research questions section. The results of each research question's alignment or difference from other scholarly published literature on the topic were discussed. In addition, unusual findings as well are discussed under each research question results discussion (Table 1).

Table 1

HQ	Variable Relationship	Null Result
1	Perceived susceptibility -> Perceived threat	Rejected
2	Perceived severity -> Perceived threat	Rejected
3	Perceived susceptibility/Perceived severity -> Perceived threat	Not Rejected
4	Perceived threat -> Avoidance motivation	Not Rejected
5	Safeguard effectiveness -> Avoidance motivation	Not Rejected
6	Perceived threat/Safeguard effectiveness -> Avoidance motivation	Not Rejected
7	Safeguard cost-> Avoidance motivation	Rejected
8	Self-efficacy -> Avoidance motivation	Rejected
9	Avoidance motivation -> Avoidance behavior	Rejected

Hypothesis one assessed perceived severity influence on U.S. healthcare professionals' perceived threat to security breaches while using EHRs. Based on the first regression model of the study, perceived susceptibility significantly influenced perceived threat. The model result indicated that as perceived susceptibility increased, perceived threat also increased (positive b value). The research finding supported Liang & Xue's (2010) finding that perceived susceptibility has a significant positive effect on perceived threat ($\beta = .41$, $p < .01$). The finding of the study also supported Carpenter et al. (2019) finding that showed both direct path from perceived susceptibility to a perceived threat ($\beta = .18$, $\rho < 0.001$), and indirect route from perceived susceptibility to perceived severity and then perceived threat, had a significant and positive effect on a perceived threat ($\beta = .37$, $\rho < 0.001$).

Hypothesis two, which investigated the relationship between perceived severity of security breaches and perceived threat, found perceived severity of security breaches while using EHRs positively affects perceived threat. The study finding supported Liang and Xue's (2010) finding of a strong positive relationship between perceived severity and perceived threat (β = .27, p < .01). On the other hand, the modified TTAT model by Carpenter et al. (2019), which correlated perceived susceptibility to perceived severity and then to a perceived threat, found perceived severity partially influences perceived threat.

Hypothesis three assessed the interaction effect of perceived severity and perceived susceptibility to U.S. healthcare professionals' perceived threat to security breaches while using EHRs. The study result did not find a significant relationship. The study results supported Liang and Xue's (2010) finding that correlation between perceived susceptibility and perceived severity of a security breach while using EHRs does not have a significant interaction effect on the perceived threat (β = .10, p > .05). Previous studies that tested the full TTAT model found differing outcomes on different hypotheses, including the interaction effect of perceived susceptibility and perceived severity on the perceived threat (Chen & Zahedi, 2016; Young et al., 2016).

Hypothesis four used the study model two to assess perceived threat influence on U.S. healthcare professionals' security breaches and threat avoidance motivation while using EHRs. The study did not find a significant relationship between perceived threat and avoidance motivation. The correlation between perceived threat and avoidance motivation was one of the hypothesis test results that a significant relationship was expected based on prior study results, but it was not found. Liang and Xue (2010) found that perceived threat significantly determines avoidance motivation. The Liang and Xue (2010) study results indicated that perceived threat positively affects avoidance motivation (β = .26, p < .01). Simple linear regression between perceived threat and avoidance motivation test showed a strong positive correlation between perceived threat and avoidance motivation. Carpenter et al. (2019) revised TTAT research model did not include the interaction effect of the perceived threat and safeguard effectiveness to avoidance motivation. They tested avoidance motivation with other independent variables, including perceived threat. However, without the inclusion of the interaction effect, Carpenter et al. (2019) found that perceived threat significantly determines perceived motivation (β = .12, ρ < 0.01). In the current research model two also, when the interaction between perceived threat and safeguard effectiveness was not included, the model result showed that all the independent variables, including perceived threat, have a significant positive relationship with avoidance motivation. Hence, the inclusion of the interaction effect in the model caused the model's results to be different from the expected. Chen and Zahedi (2016) study also supported the impact of perceived threat on avoidance motivation.

Hypothesis five of the study assessed safeguard effectiveness influence on U.S. healthcare professionals' threat avoidance motivation to security breaches while using EHRs. The current study results did not support this hypothesis. The correlation between safeguard effectiveness and avoidance motivation was another hypothesis question that the study was expecting a significant relationship based on previous studies but did not find. Liang and Xue (2010) study found avoidance motivation is significantly determined by safeguard effectiveness (β = .33, p < .01). Carpenter et al. (2019) also found safeguard effectiveness was significantly associated with avoidance motivation (β = .41, ρ < 0.001). However, Carpenter et al. (2019) revised TTAT model did not include the interaction effect of the perceived threat and safeguard effectiveness on avoidance motivation. To understand the cause of the unexpected result of model two, the Model 2 multi-regression test was done without including the interaction effect of the perceived threat and safeguard effectiveness. The regression model showed a strong positive correlation between avoidance motivation and safeguard effectiveness.

Hypothesis six was to what extent the interaction of perceived threat and safeguard effectiveness influences U.S. healthcare professionals' perceived threat avoidance motivation to security breaches while using EHRs. The perceived danger of EHRs security breaches interaction with safeguarding effectiveness of EHRs security has a negative interaction impact on avoidance motivation was the hypothesis of Liang and Xue (2009). The finding of Liang and Xue (2010) confirmed there is a significant negative (β = -.18, p < .05) interaction between perceived threat and safeguard effectiveness with avoidance motivation. The current study results also indicated a negative correlation between avoidance motivation and the interaction effect of the perceived threat and safeguard effectiveness. However, the interaction effect found was not significant. Carpenter et al. (2019) modified TTAT model did not include the interaction between perceived threat and safeguard effectiveness effect on avoidance motivation testing.

Hypothesis seven used Model 2 of the study to assess safeguard cost influences on U.S. healthcare professionals' threat avoidance motivation to security breaches while using EHRs. Safeguarding cost against EHRs security breaches negatively affects avoidance motivation, according to Liang and Xue's (2009) hypothesis. The current study results supported this hypothesis. Liang and Xue (2010) found out avoidance motivation is significantly determined by safeguard cost (β = -.14, p < .05), confirming their hypothesis. Carpenter et al. (2019) TTAT refined model also found safeguard cost significantly affects avoidance motivation cost (β = -.33, ρ < 0.001). The negative β values on both Liang and Xue (2010) and Carpenter et al. (2019) safeguard cost versus avoidance motivation shows that when the cost of safeguarding a threat increases, the avoidance motivation decreases, meaning people tend to accept the consequences of a threat to their security, rather than paying for the safeguarding measure. The study's results also confirmed a significant negative relationship between safeguarding cost and avoidance motivation. The significant correlation between safeguarding cost and avoidance motivation found in the current study makes safeguarding the cost of the TTAT model one of the constructs supported by all the prior TTAT-based research results reviewed by the researcher.

Hypothesis 8 analyzed by model two of the study was question eight, which assessed self-efficacy influences on U.S. healthcare professionals' threat avoidance motivation to security breaches while using EHRs. Self-efficacy in taking safeguard measures against EHRs security breaches positively affects avoidance motivation (Liang & Xue, 2010). The study results supported this hypothesis. Liang and Xue's (2010) study results showed avoidance motivation was significantly determined by self-efficacy (β = .19, p < .05). Carpenter et al. (2019) result, however, did not support the hypothesis. Carpenter et al. (2019) result indicated that self-efficacy was not significantly associated with avoidance motivation (β = .03, p < 0.28). The current study results are aligned with Liang and Xue's (2010) findings and do not support the findings of Carpenter et al. (2019).

Hypothesis 9 assessed avoidance motivation influence on U.S. healthcare professionals' threat avoidance behavior to security breaches while using EHRs. Avoidance motivation of EHRs security breaches threats positively affects healthcare professionals’ avoidance behavior while using safeguards (Liang & Xue, 2010). The study results supported the hypothesis. The independent variable of this hypothesis was avoidance motivation, and the dependent variable was avoidance behavior. The study by Liang and Xue (2010) found that avoidance motivation significantly influences avoidance behavior (β = .43, p < .01). In addition, Carpenter et al. (2019) and Arachchilage and Love's (2014) also found that avoidance motivation was highly positively associated with avoidance behavior (β = .82, p < 0.001), supporting the results of this study.

5. DISCUSSION AND IMPLICATIONS

Cybersecurity, by its nature, has a global effect and healthcare security breaches are not also different in their global nature. Considering such an effect, the current study has implications for future studies in expanding the scope of the target population globally instead of limiting it to the U.S. healthcare system. In line with the expansion of the target population sample, the study could also be used to expand the targeted healthcare professionals’ sample group to include doctors and all other healthcare professionals handling patient healthcare information.

The study used Liang and Xue's (2010) TTAT model and instrument to answer the research questions. The model hypothesized the interaction of perceived susceptibility and perceived severity to predict perceived threat and the interaction of perceived threat and safeguard effectiveness to predict avoidance motivation. The integration of the interaction effect on the models affected the significance of the relationship on their respective dependent variables and the significance of other variables' impact on their dependent variables. Case in point, when the survey data of model 2 of the current research was tested without considering the interaction effect of the perceived threat and safeguard effectiveness against avoidance motivation, the model result showed a significant impact of all four constructs on avoidance motivation; however, with the inclusion of the interaction effect (current model design), perceived threat and safeguard effectiveness variables were not significant in their effect against avoidance motivation. In their refining TTAT research, Carpenter et al. (2019) did not consider the interaction effect of the perceived threat and safeguard effectiveness on threat avoidance motivation. Future research on further refining Liang and Xue's (2010) TTAT model and instrument would possibly produce a better TTAT model design regarding the interaction of constructs. As Carpenter et al. (2019) added additional variables in their refining TTAT study, the current study would have future implications of expanding the present study using more variables and developed models that could potentially result in a comprehensive prediction of the technology threat avoidance behavior in U.S. healthcare system security breaches.

Implication for Practice

The study examined U.S. healthcare system healthcare professionals’ security breach threat avoidance behavior while using EHRs. As indicated earlier in the document, most security breaches in the U.S. healthcare system are related to or caused by human behavior mistakes. In this regard, U.S. healthcare organizations must incorporate human behavioral study considerations while implementing their security governance programs. The practical implication of the study will provide the necessary study output of healthcare professionals' security breach threat avoidance behavior while using EHRs.

U.S. healthcare organizations can use the study to understand the effect of human behavior on security breaches and make the necessary consideration while designing and implementing their centralized or decentralized IT security governance. Centralized security practices are implemented, controlled, and managed at the enterprise level, where healthcare professionals have no option of avoiding them. In centralized security systems, healthcare professionals’ awareness of security breach threats of EHRs is essential as they would be targeted by email phishing-related security breach threats, which are the leading causes of data breaches in the U.S. healthcare system. In a decentralized security system, healthcare professionals engage in voluntary security breach protective measures, such as updating their own antivirus/ antispyware software, enabling their firewall, and implementing HIPPA Security and Privacy measures while using electronic patient health records (ePHR). In decentralized IT security, healthcare professionals are more likely to engage in unsafe security behaviors and become a weak link for the healthcare organization's security system. For healthcare professionals in a decentralized security system, it is imperative to provide them with regular security awareness, education, and training to prepare them better to cope with security breach threats while using EHRs (Warkentin & Johnston, 2006).

The study's practical application in healthcare IT security programs extends in several ways. Most importantly, the study endorses the importance of healthcare professionals’ security awareness, education, and training. Healthcare professionals would be more motivated to avoid security breach threats and opt to use safeguarding measures if these programs help them develop threat perception, with effective safeguarding measures with low safeguarding cost and high self-efficacy.

Summary

This non-experimental quantitative correlational study determined to what extent U.S. healthcare professionals’ perceived susceptibility, perceived severity, safeguard effectiveness, safeguard cost, self-efficacy, and threat perceptions of EHRs security breaches influenced their threat avoidance motivations and threat avoidance behaviors while using EHRs. Technology threat avoidance theory served as the study’s theoretical framework. Liang and Xue's (2010) TTAT model and validated survey instrument were used to collect a total of 168 respondents' survey data for the study's simple and multiple regression analysis. The research findings indicated that perceived severity and perceived susceptibility significantly correlate with a user’s perception of threat. The cost of safeguarding measures and the user’s self-efficacy were predictors of healthcare professionals' threat avoidance motivation. Perceived threat and safeguarding effectiveness were not proven to affect avoidance motivation significantly. Avoidance motivation strongly predicted healthcare professionals’ EHRs security breach threat avoidance behavior. The study findings contribute significantly to understanding U.S. healthcare professionals' security breaches and threat avoidance behavior while using EHRs. The current study can be expanded and improved by testing TTAT more comprehensively, including other constructs like perceived avoidance, and developing and validating other TTAT models and instruments with the potential of better interaction among the constructs.

9. REFERENCES

Alexandrou, A., & Chen, L. C. (2019). A security risk perception model for the adoption of mobile devices in the healthcare industry. *Security Journal*, 32(4), 410-434. https://doi.org/10.1057/s41284-019-00170-0

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304-312.

Argaw, S. T., Bempong, N., Eshaya-Chauvin, B., & Flahault, A. (2019). The state of research on cyberattacks against hospitals and available best practice recommendations: A scoping review. *BMC Medical Informatics and Decision Making,* 19. http://dx.doi.org/10.1186/s129 11-018-0724-5

Ayyagari, R. (2012). An exploratory analysis of data breaches from 2005-2011: Trends and insights. *Journal of Information Privacy & Security*, 8(2), 33-56.

Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining technology threat avoidance theory. *Communications of the Association for Information Systems*, 44. doi: 10.17705/1CAIS.04422

Chamroonsawasdi, K., Chottanapund, S., Pamungkas, R. A., Tunyasitthisundhorn, P., Sornpaisarn, B., & Numpaisan, O. (2020). Protection motivation theory to predict the intention of healthy eating and sufficient physical activity to prevent diabetes mellitus in Thai population: A path analysis. *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, 15(1), 121-127.

Chen, Y., & Zahedi, F. M. (2016). Individuals' Internet security perceptions and behaviors: Poly-contextual contrasts between the United States and China. *MIS Quarterly*, *40*(1), 205-222.

Chua, J. A. (2021). Cybersecurity in the healthcare industry. *Physician Leadership Journal*, 8(1).

CMS (2021). HIPPA Basics for Providers: Privacy, Security, & Breach Notification Rules. *The Medicare Learning Network,* MLN909001.

Colicchio, T. K., Cimino, J. J., & Fiol, G. D. (2019). Unintended Consequences of Nationwide Electronic Health Record Adoption: Challenges and Opportunities in the Post-Meaningful Use Era. *Journal of Medical Internet Research,* 2(6). https://doi.org/10.2196/13313

Coventry, L. & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats, and ways forward. *Maturitas*, 113, 48-52. http://dx.doi.org/10.1016/j.maturitas.2018.04.008

Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Georgiadou, A., Michalitsi-Psarrou, A., Doukas, G., Kontoulis, M., Nikoloudakis, Y., & Marin, S. (2022). A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures. *Healthcare*, *10*, 327. https://doi.org/10.3390/healthcare10020327

HHS Office for Civil Rights (2017). HITECH Act Enforcement Interim Final Rule. *U.S. Health and Human Services* https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html

Lazarus, R. S. (1996). The role of coping in the emotions and how coping changes over the life course. In C. Magai & S. H. McFadden (Eds.), *Handbook of emotion, adult development, and aging* (pp. 289–306). Academic Press. https://doi.org/10.1016/B978-012464995-8/50017-0

Li, Q., Liu, Q., Chen, X., Tan, X., Zhang, M., Tuo, J,. & Zhu, Z. (2020). Protection motivation theory in predicting cervical cancer screening participation: A longitudinal study in rural Chinese women. Psycho-oncology, 29(3), 564-571.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, 33(1), 71-90.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective.

Journal of the Association for Information Systems, 11(7), 394-413.

Ronquillo, J. G., Winterholler, J. E., Cwikla, K., Szymanski, R., & Levy, C. (2018). Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information. Oxford University Press on behalf of the American Medical Informatics Association, *JAMIA Open*, 1(1), 15–19.

Rogers, R. W., & Prentice-Dunn, S. (1997). Protection motivation theory. In D. S. Gochman (Ed.), *Handbook of health behavior research 1: Personal and social determinants* (pp. 113–132). Plenum Press.

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R. & Khan, R. A. (2020). Healthcare Data Breaches: Insights and Implications. *Healthcare*, 8, 133. https://doi.org/10.3390/healthcare8020133

Smith, C. (2018). Cybersecurity implications in an interconnected healthcare system. *Frontiers of Health Services Management*, 35(1), 37-40. http://dx.doi.org/10.1097/HAP.0000000000000039

Steen, M., & Steen, M. (2019). Health Care industry increasingly faces cybersecurity breaches. In I. Gonzales, K. Joaquin Jay, & Roger L. (Eds.), Cybersecurity: current writings on threats and protection. *McFarland*. Credo Reference: https://go.openathens.net/redirector/ucumberlands.edu?url=https%3A%2F%2Fsearch.credoreference.com%2Fcontent%2Fentry%2Fmcfccwotap%2Fhealth_care_industry_increasingly_faces_cybersecurity_breaches%2F0%3FinstitutionId%3D4309

Truong, T. C., Zelinka, I., Plucar, J., Čandík, M., & Šulc, V. (2020). Artificial Intelligence and Cybersecurity: Past, Presence, and Future. *Artificial Intelligence and Evolutionary Computations in Engineering Systems*, 1056.

Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Information & Management*, 52, 506-517. doi:10.1016/j.im.2015.03.002

Warkentin, M. & Johnston, A. C. (2006). IT Security Governance and Centralized Security Controls, in Warkentin, M. and Vaughn, R. (Eds.) *Enterprise Information Assurance and System Security: Managerial and Technical Issues*, Hershey, PA: Idea Group Publishing, pp. 16-24.

Yeng, P. K., Fauzi, M. A. & Yang, B. A. (2022). Comprehensive Assessment of Human Factors in Cyber Security Compliance toward Enhancing the Security Practice of Healthcare Staff in Paperless Hospitals. *Information*, *13*, 335. https://doi.org/10.3390/info13070335

Yeo, L. H. & Banfield J. (2022). Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis. *Perspect Health Inf Manag*, 19(2).

Young, D. K., Carpenter, D., & McLeod, A. (2016). Malware avoidance motivations and behaviors: A technology threat avoidance replication. *AIS Transactions on Replication Research*, 2(6), 1-17.

Information Adoption of User-Generated Content: An Applied Model for COVID Pandemic Case

Wei Xie
Xiew1@appstate.edu
Computer Information Systems
Walker College of Business
Appalachian State University
Boone, NC 28608

Gurpreet Dhillon
Gurpreet.dhillon@unt.edu
Information Technology and Decision Sciences
University of North Texas
Denton, TX 76203

Abstract

This study proposes and empirically tests an alternative information adoption model to investigate how information quality and religiosity impact people's intake of user-generated COVID vaccination information posted on social media. Our results based on 359 survey responses suggest that the two constructs examined significantly impact the perceived usefulness of the user-generated vaccination information and the subsequent vaccination intention. Furthermore, our model shows that religiosity exerts a supplementary partial mediating impact through the information evaluation process, adding empirical evidence to clarify the inconsistency of direct and indirect effects from extant studies. This theory-guided applied study aims to decipher vaccination intention specifically and contributes to building knowledge about user-generated content and the online information adoption process in general.

Keywords: user-generated content, knowledge adoption, religiosity, vaccination hesitancy, elaboration likelihood

Recommended Citation: Xie, W., Dhillon, G., (2024). Information Adoption of User-Generated Content: An Applied Model for COVID Pandemic Case. *Journal of Information Systems Applied Research.* 17(3), pp.29-42, https://doi.org/10.62273/BJCO6308

Information Adoption of User-Generated Content: An Applied Model for COVID Pandemic Case

Wei Xie and Gurpreet Dhillon

1. INTRODUCTION

User-generated content (UGC) is a web- or mobile-based digital communication used for interactive dialogues, forming communities, and exchanging information (Mesko, 2013). UGC has emerged as a leading source of healthcare information since the mid-2000s (Reno et al., 2021). According to the first health information national trends survey (2013), up to 63% of internet users in the USA look for healthcare-related information online, and more than 48% follow online suggestions. In addition, 84% of people surveyed said they treat online reviews and content like personal recommendations (Bloem, 2017). Many people see UGC as the most authentic and trusted source of healthcare information (Ahmed et al., 2019). To this end, UGC results in a paradigm shift in how people share and access healthcare information.

However, because of the user-level participation, a lay user may be unable to critically comprehend online healthcare UGC, leading to a false sense of information usefulness and causing potential medical noncompliance (Tonsaker et al., 2014). For example, Wakefield (1998) published an article in Lancet with inaccurate information about the non-existent link between the MMR vaccine and autism (Godlee et al., 2011). Fear caused by this misleading information led to an increasingly featured search on Facebook and YouTube (Wong, 2019) and more than a half-million antivaccine posts on Twitter between 2009 and 2015 (Tomeny et al., 2017), even after the article was retracted and the key authors were discredited. The United Nations warned about the link between low MMR vaccination fueled by false information on social media and large outbreaks in several countries (UN.org, 2019). The COVID pandemic heightens this problem. During pandemic shutdowns, minimal knowledge, fear, and anxiety drive people to seek information from social networks and UGC to decide whether to take the COVID vaccination (Christensen, 2020). Compelling personal narratives on UGC, working together with people's beliefs, modify people's attitudes toward taking COVID vaccination, leading to vaccination hesitancy that directly threatens public health (Reno et al., 2021; Puri et al., 2020). The COVID vaccination hesitancy makes understanding the online UGC adoption process prominent and imperative.

To understand the information adoption process, Sussman and Siegal (2003) proposed a knowledge adoption model. This model focuses on aspects of information, namely quality and credibility. However, information adoption is a user-engaged and initiated process. Therefore, besides the factors of information and sources, users' characteristics also play essential roles in the UGC adoption process. The theory of planned behavior (TPB) suggests that human attitude as a motivational factor affects intention and behavior (Ajzen, 1991). Studies in the context of COVID vaccination show that personal narratives and postings on UGC can resonate with pre-existing attitudes and modify behavior (Christensen, 2020). For example, public health surveys show anecdotal evidence that religiosity predicts less compliance to protective behavior during the pandemic (Dein et al., 2020; Milligan et al., 2021). Other studies suggest that religiosity as a pre-existing attitudinal factor, coupled with the appropriate knowledge efficacy, can increase or decrease vaccination intention and impact vaccination inoculation (Garcia & Yap, 2021). What's more, disregarding the religious festivals of ethnic groups undermines trust, a common reason for vaccination hesitancy (Razai et al., 2021). Although extant empirical studies indicate that religion and spirituality are significant attitudinal factors associated with healthcare decision-making, few studies theoretically examine them in the UGC context (e.g., Thomas et al., 2015; Borges et al., 2021; Troiano & Nardi, 2021). Motivated to help decrease vaccination hesitancy and aiming to theorize and investigate the anecdotal and empirical evidence of religiosity in the UGC evaluation and adoption process, this study proposes and tests an attitude-oriented information adoption model. In particular, this model incorporates UGC information quality and religiosity into the knowledge adoption model, asking the following research questions: (1) How do UGC information quality and religiosity affect the perceived UGC usefulness and COVID vaccination intention? (2) How does religiosity exert its effect, direct or indirect?

The rest of the paper is organized as follows. In the next section, we review the literature regarding the supporting theory, build a conceptual research model, and propose hypotheses. Afterward, the methodology and results will be presented for this theory-guided empirical study. In the end, we discuss the study results, theoretical and practical implications, limitations, and future research.

2. THEORETICAL BACKGROUND AND HYPOTHESIS

Perceived Usefulness of COVID Vaccination UGC and Adoption Intention

The knowledge adoption model posits that argument quality and source credibility impact the perceived information usefulness, which further influences the information adoption intention (Sussman & Siegal, 2003). As a key construct, the perceived usefulness of using particular information to make decisions has been empirically supported. Studies show a significant positive relationship between perceived information usefulness and information adoption in different contexts (Sussman & Siegal, 2003; Venkatesh et al., 2003). For example, empirical research in consumer industries suggests that because of perceived usefulness, consumer-generated media and online reviews predict service acceptance and product purchase (e.g., Thao & Shurong, 2020; Filieri & McLeay, 2014). In addition, social media marketing influences online decision-making (Aggarwal et al., 2013). Electronic word of mouth (eWOM) affects travel planning (e.g., Muñoz-Leiva et al., 2012; Ayeh, 2015; Lee et al., 2012). Hence, this study proposes the following:

H1: The perceived usefulness of COVID vaccination UGC positively influences the UGC vaccination adoption intention.

Perceived UGC Information Quality on Perceived UGC Usefulness

The knowledge adoption model is inspired by the Elaboration Likelihood Model (ELM) (Petty & Cacioppo, 1986) and Technology Acceptance Model (TAM). The Elaboration Likelihood Model (ELM) suggests two cognitive ways to persuade people of something (Petty & Cacioppo, 1986). Sussman and Siegal (2003) thus propose that knowledge adoption results from two alternative elaborations on the information. First, when a person is motivated and able to critically and comprehensively analyze the information, he or she will elaborate on the argument (information) quality. The perceived argument quality is measured by the persuasive strength of completeness, consistency, and accuracy in the presented information (Sussman & Siegal, 2003). Second, without sufficient cognitive ability and motivation, a person is likely to rely on superficial cues to elaborate on the information. The original model proposes the perceived source credibility as the peripheral cue, measured by the information source's reliability, competency, knowledge, and trustworthiness. Extant research empirically applied and verified the effectiveness of the model on the information adoption in different information systems context such as websites (Tseng & Wang, 2016; Fillieri et al., 2015; Chung et al., 2015), online customers review, and online communities UGC (Cheung et al., 2008). A handful of studies also applied the model to assess the effect of the original constructs of source credibility and information quality on healthcare information adoption and healthcare-related behaviors (e.g., Ma & Atkin, 2017; Jin et al., 2016; Lagoe & Atkin, 2015).

However, questions remain about the factors, patterns, and outcomes of the UGC healthcare information adoption, especially in public health crises loaded with emotions. This study draws from the knowledge adoption model and the theory of planned behavior and proposes an attitude-oriented knowledge adoption model, shedding light on the importance of the information recipients in an extreme context.

Petty and Cacioppo (1986) posit that elaboration likelihood is a temporal state and that situational context will change the elaboration. Cyr et al. (2018) indicate that the level of elaboration in information depends on the information's relevancy to receivers. COVID-19 is a disease about life and death. COVID vaccination is highly relevant. The public has a strong motivation to understand what the disease is, what causes its spreading, and how COVID vaccination can mitigate the situation. Thus, this study argues that recipients will carefully evaluate and judge the quality of UGC vaccination information. The higher perceived information quality will positively influence the perceived information's usefulness. Following this argument, this study proposes the following:

H2: The perceived information quality of COVID vaccination UGC positively affects perceived COVID vaccination UGC usefulness.

Although people use social media for COVID vaccination information, the minimal knowledge about the disease and its vaccination makes it hard to tell the credibility of contributors in the study context (Puri et al., 2020; Liao & Mak, 2019). Studies indicated that people turn to friends, family, and people who suffer the same for anecdotal information. Facing crisis and the shutdowns, dealing with the deadly and lengthening pandemic around the globe, the public is overwhelmed by fear, anxiety, worries, and hopelessness. Studies demonstrated that users might be more vulnerable to narrative and emotional appeals of UGC and that users' baseline personal values and attitudes may affect responses to UGC (Puri et al., 2020). In this emotion-laden context, this study introduces an attitudinal construct, religiosity, as the independent construct, replacing source credibility.

Religiosity on Perceived UGC Information Quality and COVID Vaccination UGC Adoption Intention

Although individual attitude is a classic construct in information systems research, the effect of religiosity on behavioral intention has been largely overlooked (Ajzen, 1985; Kelecha & Belanger, 2013). Religiosity is how a person believes and follows a particular religion and practices the same (Panzini et al., 2017). The definition encompasses the importance of and belief in religious values and associated behavior (Wilkes et al., 1986). Studies have found that religion and spirituality strongly influence physical and mental health (Lucchetti & Lucchetti, 2014). For example, research suggests that religious individuals can better cope with adverse circumstances through social capital systems and mutual support (Abbott & Freeth, 2008; Abdulahad et al., 2014). In addition, individuals engage in religious practices to form optimistic attitudes (Rutter, 2012; Schwalm et al., 2022), and alter negative thoughts, increasing their resilience (Dolcos et al., 2021).

Interestingly, in COVID vaccination-related studies, the evidence of religiosity as a direct predictor of vaccination compliance and hesitancy is inconclusive. Some studies demonstrate the negative influence of religiosity on COVID vaccination intention (Murphy et al., 2021). Others show that the religiosity association of medical experts increases the intention of vaccination (Chu et al., 2021). An observational comparison study crossing 89 counties also shows mixed results to establish religiosity as a direct antecedent to predict a COVID vaccination (Omidvar & Perkins, 2022).

Careful examination of these studies indicates that the religiosity effect may be mediated through other factors, such as specific coping strategies and behaviors (Maltby & Day, 2003; Fabricatore et al., 2004). For example, in consumer behavioral studies, the effect of religiosity is activated through motivation and social utility (Junaidi et al., 2021). Orlandi et al. (2022) highlight the importance of perceived risk in the relationship between religiosity and COVID vaccination compliance. Mckinley and Lauby's (2021) study supports that the relationship between pre-existing vaccination beliefs and behavioral intention is mediated by information seeking on social media. Allport and Ross (1967) proposed differentiated intrinsic and extrinsic religiosity, stating that internalized (intrinsic) religiosity needs to be externalized (extrinsic) to realize its external effect. Hence, we argue that religiosity can directly influence the COVID vaccination intention while also mediated by the perceived COVID vaccination information quality to impact the COVID vaccination intention.

We also argue for an accentuation effect of religiosity (Wei & Zhu, 2023), meaning that religiosity can make good things better or bad things worse in mediated relationships. COVID vaccination decision concerns a life-threatening situation with uncertainties and emotional stress. Therefore, the vaccination decision can trigger an individual's mental coping mechanisms, such as religiosity, to regulate emotional stress and adjust behavioral responses, including comprehending and responding to vaccination UGC. We argue for the positive predictive power because of the emotional calming capacity provided by religiosity. We propose the following:

> **H3**: The perceived religiosity positively affects the perceived COVID vaccination UGC information quality.
> **H4**: The perceived religiosity positively affects the COVID vaccination UGC adoption intention.

Figure 1 shows our research model.

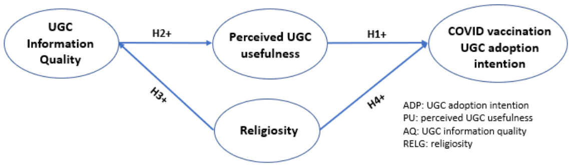

UGC Information Quality
H2+
Perceived UGC usefulness
H1+
COVID vaccination UGC adoption intention
H3+
Religiosity
H4+
ADP: UGC adoption intention
PU: perceived UGC usefulness
AQ: UGC information quality
RELG: religiosity

Figure 1 Research Model

3. METHODOLOGY

The primary objective of this applied study is to investigate how the COVID vaccination UGC on social media impacts the UGC adoption intention.

Data Collection Procedure

Our empirical data is collected between October 2021 and June 2022. Information or heated topics on social media usually take the form of hashtags for propagation. Extant studies utilized hashtags to study UGC's role in shaping vaccination discourse (Puri et al., 2020). Therefore, respondents were instructed to explore two hashtags for 5 mins each on Instagram or Facebook before taking the survey to ensure enough readings about the COVID vaccination UGC. First, we conducted a quick screening survey among college students about the popular social media used for COVID vaccination information. Instagram (26 votes), Twitter (22 votes), and FaceBook (11 votes) are the top three. Four graduate students then researched and identified the most popular hashtags for pros and cons opinions of COVID vaccination based on the total number of posts. Studies demonstrated that pros and cons content naturally cluster into distinct communities, possibly due to the self-selection of like minds (Gunaratne et al., 2019). Twitter is removed because it lacks the metrics of the total post count. Next, the ten most popular hashtags (five for each opinion) were cross-checked on Facebook and Instagram to ensure their popularity and content consistency. Afterward, two top hashtags, namely *#getvaccinated* (217k Instagram; 219k FaceBook) and *#protectyourfamily* (129k, Instagram; 200k, FaceBook), were selected to represent pros or cons attitudes accordingly. The four graduate students also suggested five minutes as a proper length for reviewing the content of each hashtag.

All survey responses were recorded on a 7-point Likert scale. After two Information Systems professors examined items, the first pilot survey collected 82 responses from college students. The items' wording was revised based on the results. The second pilot survey collected 116 data from the Amazon Mechanical Turk (MTurk) respondents with a 99% or higher HIT rate (Berinsky et al., 2012). At last, the primary survey collects an additional 311 data. The final admissible data of 359 was accumulated from the two MTurk data collections after deleting data that were (1) answered in less than 200 sec, using a suggested 7.5 sec each question as a guideline (qualtrics.com), and (2) answered the manipulation questions wrong. The consistent PLS algorithm in SmartPLS (version 4.0.9.3) is used to test our reflective research model. Partial least squares structural equation modeling (PLS-SEM) focuses on the variance captured in proposed constructs, which enables us to explore the hypothesized new predictive relationships between latent constructs (Hair et al., 2017, 2019). Table 1 below shows the basic demographics of respondents in the study. Figure 2 below gives us a snapshot of the data collection process.

	359	Count	%
GEN	Male	192	53%
	Female	167	47%
ETH	Native Indian	6	2%
	Asian	13	4%
	Black	38	11%
	Latino	17	5%
	Islander	1	0%
	White	284	79%
AGE	18-23 years	16	4%
	24-35 years	186	52%
	36-55 years	129	36%
	56-65 years	22	6%
	Over 65 years	6	2%

Table 1 Demographics

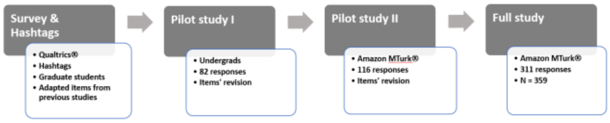


Figure 2 Data Collection Process

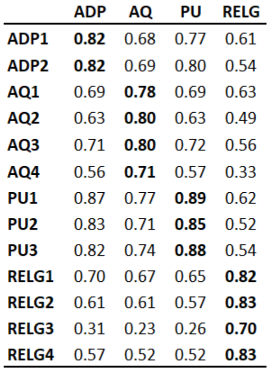
Survey Instruments

This study's constructs and measurement items were adapted from previously validated studies (Appendix A). For example, we adopt two items from Sussman and Siegal (2003) to gauge the UGC adoption intention. Respondents are asked to rate their intention for the COVID vaccination, such as "To what extent does the COVID vaccination UGC on social media motivate you to take COVID vaccination?" Wilkes et al. (2003) developed four short items to assess the consumers' religious values (importance and confidence), behavior (church attendance), and self-perceived religiousness, independent of any conditions. Three original items also measure respondents' perception of UGC usefulness (Sussman & Siegal, 2003). UGC information quality includes three original items plus one additional item to measure information relevancy in the study context (Filieri & McLeay, 2014). Three manipulation questions, such as speeder trap and attention filter, were used to eliminate common method bias (Oppenheimer et al., 2009; Meade & Craig, 2012; Berinsky et al., 2014).

4. FINDINGS

Measurement Model

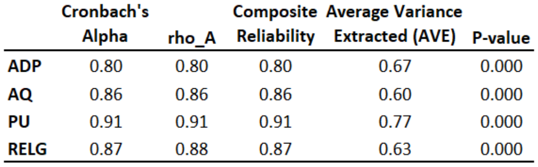
The measurement model estimates the accuracy of measurable items (variables), the relationships between the measured items, and the latent constructs these items represent. In addition, the measurement model estimates items' loadings, the construct's composite reliability, and convergent and discriminant validity. Table 2 below provides a snapshot of the final operationalized items' loadings and cross-loadings.



	ADP	AQ	PU	RELG
ADP1	**0.82**	0.68	0.77	0.61
ADP2	**0.82**	0.69	0.80	0.54
AQ1	0.69	**0.78**	0.69	0.63
AQ2	0.63	**0.80**	0.63	0.49
AQ3	0.71	**0.80**	0.72	0.56
AQ4	0.56	**0.71**	0.57	0.33
PU1	0.87	0.77	**0.89**	0.62
PU2	0.83	0.71	**0.85**	0.52
PU3	0.82	0.74	**0.88**	0.54
RELG1	0.70	0.67	0.65	**0.82**
RELG2	0.61	0.61	0.57	**0.83**
RELG3	0.31	0.23	0.26	**0.70**
RELG4	0.57	0.52	0.52	**0.83**

Table 2 Loadings & Cross Loadings

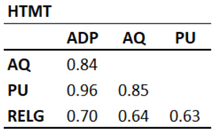
Item loading, Composite reliability, and rho_A should be 0.7 or higher to demonstrate adequate reliability for a construct in the study context (Nunnally, 1978). Convergent validity refers to the extent to which items for a construct measure the same construct, validated by a larger than 50% average variance extracted (AVE) of the construct (Hair et al., 2019). All metrics shown in Table 3 are at a 0.000 significant level, indicating that all reflective items are free from random measurement errors and consistent in measuring what they should measure. Items' loadings are all 0.7 and above.



	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)	P-value
ADP	0.80	0.80	0.80	0.67	0.000
AQ	0.86	0.86	0.86	0.60	0.000
PU	0.91	0.91	0.91	0.77	0.000
RELG	0.87	0.88	0.87	0.63	0.000

Table 3 Reliability & Validity

The discriminant validity ensures that each construct is empirically unique, and items only measure their associated constructs. It can be evaluated using a Fornell-Larcker criterion, cross-loading, and a heterotrait-monotrait ratio of correlations (HTMT). Henseler et al. (2015) criticize Fornell-Larcker's poor performance in PLS and propose a less-constrained HTMT based on observed correlations. Henseler et al. (2015) suggest a threshold value of 0.90 if the path model includes constructs that are conceptually very similar, or 0.85 if the constructs in the path model are conceptually more distinct (Franke & Sarstedt, 2019). Table 4 (below) is HTMT readings. All values of HTMT are smaller than 0.85 except for HTMT between UGC adoption intention and perceived UGC usefulness is 0.96. In addition, cross-loadings of UGC adoption intention and perceived UGC usefulness are also very close to the loadings of perceived UGC usefulness, suggesting a lack of discriminant validity of the two constructs. In other words, in the respondents' minds, the perceived UGC usefulness almost equals an intention to take the COVID vaccination in the study context. This is an interesting and significant finding.



HTMT

	ADP	AQ	PU
AQ	0.84		
PU	0.96	0.85	
RELG	0.70	0.64	0.63

Table 4 HTMT

Structural Model and Hypotheses Testing

The structural model estimation includes assessing construct relationships' multicollinearity, significance, relevance, and model fit in R², Q², and F². For the multicollinearity assessment, the variance inflation factor (VIF) ranges from 1.547 to 3.378 for all the variables (items) used in the model, smaller than the suggested cut-off value of 5, indicating admissible correlations among constructs (Ringle et al., 2015).

R² represents the variance explained in each endogenous construct, measuring the model's predictive accuracy. Our model significantly explains COVID vaccination UGC adoption intention (R² = 0.934, P = .000), UGC usefulness (R² = 0.714, P = .000), and information quality (R² = 0.423, P = .000) in the study (Hair et al., 2011; Chin, 1998). Q² is a latent construct score that measures the predictive relevance of the model and endogenous constructs. COVID vaccination UGC adoption intention (Q² = 0.334), UGC usefulness (Q² = 0.301), and information quality (Q² = 0.312) have values larger than 0, indicating the model is relevant and well-constructed (Fornell & Larcker, 1981). F² is also called the effect size. It is an important complement to null hypothesis significance testing (e.g., p-values), offering practical significance in the magnitude of the effect in endogenous constructs, and is independent of sample size (Kline, 2004). All paths' F² are significant (0.202 – 6.729). Figure

3 and Table 5 provide the psychometric structural model results, including the standardized path coefficients for each hypothesized relationship and associated p-values. As we can see from the results, all paths' coefficients significantly support our hypotheses in this model and context.

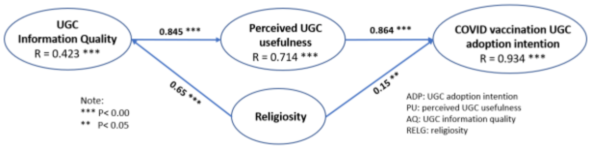
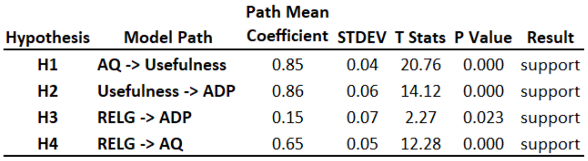


Figure 3 Research Model Results



Hypothesis	Model Path	Path Mean Coefficient	STDEV	T Stats	P Value	Result
H1	AQ -> Usefulness	0.85	0.04	20.76	0.000	support
H2	Usefulness -> ADP	0.86	0.06	14.12	0.000	support
H3	RELG -> ADP	0.15	0.07	2.27	0.023	support
H4	RELG -> AQ	0.65	0.05	12.28	0.000	support

Table 5 Research Hypotheses Results

The mediated effects of religiosity in the model were also tested using bootstrapping simulations (e.g., Hair et al., 2017). All indirect and direct effects of religiosity are significant (p=0.000). To analyze and decide on the mediating effect, Zhao et al. (2010) suggest a flow chart (Hair et al., 2017). Following the procedure in the flow chart, we conclude a complementary (partial) mediation of religiosity. The calculated Variance Account For (VAF) is 0.768, also suggesting a typical partial mediation (Hair et al., 2016; Nitzl et al., 2016). The result adds an empirical explanation to why the inconsistent effects of religiosity from extant studies.

5. IMPLICATIONS AND FUTURE RESEARCH

Millions of users go online daily to seek healthcare information for various reasons (Ma & Atkin, 2016). Therefore, understanding how people take on user-generated healthcare information is vital. This is especially critical if people follow the UGC content to make decisions about COVID vaccination. However, the emerging extant research on the effectiveness of UGC in vaccination shows inconclusive evidence, calling for better research designs (Giustini et al., 2018). This study, thus, is motivated to develop and test a theory-oriented model, proposing that the COVID vaccination intention is the function of the users' elaboration about the UGC quality and their religious attitude. Our major findings offer theoretical and practical implications and directions for future research.

Theoretical Implications and Limitations

The first theoretical implication of our study is the development of a theory-guided research model, which enables a more rigorous explanation of the effectiveness of UGC on COVID vaccination intention. Our study draws on the knowledge adoption model and planned behavior theory and introduces religiosity into the model. COVID is a novel disease with devastating death consequences. High uncertainty and unknown about the disease make people cognitively elaborate on UGC information quality more deeply and carefully. In the meantime, strong emotions such as fear and anxiety also drive people to rely on beliefs as coping mechanisms. The results demonstrate that UGC information quality and religiosity are significant exogenous constructs that greatly predict UGC usefulness and COVID vaccination adoption intention. As such, this study provides a successful empirical example to expand the knowledge adoption theory further to the context of social media UGC.

The multidimensional and abstract nature of religiosity often makes it challenging to establish direct relations with other psychological constructs and outcomes (Dolcos et al., 2021). This study proposes that the effects of religiosity can be realized and regulated through a mediator (Maltby & Day, 2003). The eventful coefficients add evidence to religiosity's direct and indirect effect, verifying its intrinsic and extrinsic influence routes (Allport & Ross, 1967). In addition, this study also proposes and proves an accentuated moderating effect of religiosity. Our mediated theorizing and convincing evidence contribute to the religiosity literature in healthcare and UGC contexts. Future research should continue to test medicated religiosity in different contexts to verify the differentiation between intrinsic and extrinsic religiosity effects (Omidvar & Perkins, 2022). In addition, future research should continue the investigation of the accentuated religiosity effect. Further, although the extreme COVID pandemic made information source credibility difficult to measure, future research should also add it back into the model to reflect the completeness of the knowledge adoption model.

Lastly, the discriminant criterion shows that respondents treat UGC information usefulness the same as the COVID vaccination intention. Given the extreme pandemic case, future studies should examine whether this holds in other less intense contexts. In addition, despite our efforts to conduct a theory-guided study and its robust empirical results, the data collected during the early COVID vaccination also limits our model's generalization power.

Practical Implications

This study has major practical implications. For public health regulators and organizations, vaccination reduces high infection, morbidity, and mortality rates, develops herd immunity, and alleviates overburdened healthcare systems and massive economic costs (Omidvar & Perkins, 2022). Our results tell that COVID UGC on social media significantly influences the perceived usefulness of the information and shapes the vaccination adoption intention. Given that social media plays a major role in disseminating healthcare information and influencing vaccine uptake (e.g., Stahl et al., 2016; Giustini et al., 2018), the UGC's strategic importance for public health has become self-evidenced. Therefore, healthcare regulators and organizations should be mindful of UGC's new opportunities and challenges to reducing vaccination hesitancy.

Research indicates the growing influence of social media as a source of information on the vaccination rate because of its "direct, unfiltered, and up-to-date" nature (Daley & Glanz, 2021). Our study proves that UGC on social media has become an essential form of public healthcare discourse. However, the UGC influence has dual effects. For example, a randomized experimental study shows that interactive social media components could increase the vaccine acceptance rate (Glanz et al., 2018). Yet another study shows that people's vaccine concerns might be magnified by the complex and fluid UGC ecosystems (Daley and Glanz, 2021). The outbreaks of infectious measles, which had been under control for years, showcased the negative impact of social media (CDC, 2021). Therefore, improving UGC's quality and credibility on social media is necessary to maximize the influential power of UGC while defending against the menace to people and public health systems. As such, regulation frameworks that oversee social media should be established and communicated to the public to improve awareness and ensure the positive effect of UGC.

Extant literature points out that vaccination attitudes result from various factors such as healthcare access, risk perception, social norms, trust, and beliefs (Ahmad et al., 2018). Religiosity is a belief that provides the cognitive base of attitude. Our evidence suggests that perceived intrinsic religiosity has significant attitudinal effects. Our evidence also suggests that intrinsic religiosity also plays out its effect through methods and channels that engage internal beliefs. Therefore, healthcare practitioners and organizations should design methods and utilize proper channels to operationalize the individual's perceived intrinsic religiosity to achieve the target results and promote vaccination.

6. CONCLUSIONS

User-generated content (UGC) and its effects on public health have been studied since the 2000s, but the evidence of its effectiveness is inconclusive (Giustini et al., 2018). The reasons could be attributed to the study designs and contexts. The vaccination against COVID zeroes in on the emergency of understanding UGC's effectiveness in the information adoption process. This study is thus motivated to apply theories to conduct more rigorous research in understanding UGC's effect on information adoption in a highly relevant practical context. The study demonstrates the opportunities for theory-guided applied research. Furthermore, the results of this study provide healthcare practitioners with insights to develop and implement UGC to increase vaccination rates and achieve public health interventions effectively.

7. REFERENCES

Ab Hamid MR, Sami W, Sidek MM. (2017). Discriminant validity assessment: Use of Fornell & Larcker criterion versus HTMT criterion. In Journal of Physics: Conference Series. 890(1), 012163.

Abbott S, Freeth D. (2008). Social capital and health: starting to make sense of the role of generalized trust and reciprocity. Journal Of Health Psychology. 13(7), 874-83.

Abdulahad R, Graham JR, Montelpare WJ, Brownlee K. (2014). Social capital: understanding acculturative stress in the Canadian Iraqi–Christian community. British Journal of Social Work. 44(3), 694-713.

Aggarwal R, Singh H. (2013). Differential influence of blogs across different stages of decision making: The case of venture capitalists. Mis Quarterly. 37(4), 1093-1112.

Ahmed N, Quinn SC, Hancock GR, Freimuth VS, Jamison A. (2018). Social media use and influenza vaccine uptake among White and African American adults. Vaccine. 36(49), 7556-7561.

Ajzen I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179-211.

Allport GW, Ross JM. (1967). Personal religious orientation and prejudice. Journal of personality and social psychology. 5(4), 432-443.

Ayeh JK. (2015). Travellers' acceptance of consumer-generated media: An integrated model of technology acceptance and source credibility theories. Computers in Human Behavior. 48, 173-180.

Berinsky AJ, Huber GA, Lenz GS. (2012). Evaluating online labor markets for experimental research: Amazon.com's Mechanical Turk. Political analysis. 20(3), 351-68.

Berinsky AJ, Margolis MF, Sances MW. (2014). Separating the shirkers from the workers? Making sure respondents pay attention on self-administered surveys. American Journal of Political Science. 58(3), 739-53.

Bhattacherjee A, Sanford C. (2006). Influence processes for information technology acceptance: An elaboration likelihood model. MIS Quarterly. 30(4), 805-25.

Bloem C. 84 percent of people trust online reviews as much as friends. Inc.com; 2017 Jul 31 [accessed 2022 Nov 20]. https://www.inc.com/craig-bloem/84-percent-of-people-trust-online-reviews-as-much-.html

Borges M, Lucchetti G, Leão FC, Vallada H, Peres MF. (2021). Religious affiliations influence health-related and general decision making: a Brazilian nationwide survey. International Journal of Environmental Research and Public Health.

Cheung CM, Lee MK, Rabjohn N. (2008). The impact of electronic word-of-mouth: The adoption of online opinions in online customer communities. Internet Research. 18(3), 229-247.

Chin WW. (1998). Commentary: Issues and opinion on structural equation modeling. MIS Quarterly. 1:vii-xvi.

Christensen, J. Social media rules. That's bad in a pandemic. CNN.com; 2020 May 15 [accessed Nov 2022]. https://www.cnn.com/2020/05/15/health/social-media-negative-impact-covid/index.html

Chu J, Pink SL, Willer R. (2021). Religious identity cues increase vaccination intentions and trust in medical experts among American Christians. Proc Natl Acad Sci U S A. 118(49), e2106481118.

Chung N, Han H, Koo C. (2015). Adoption of travel information in user-generated content on social media: the moderating effect of social presence. Behaviour & Information Technology. 34(9), 902-19.

Cyr D, Head M, Lim E, Stibe A. (2018). Using the elaboration likelihood model to examine online persuasion through website design. Information & Management. 55(7), 807-21.

Daley MF, Glanz JM. Using social media to increase vaccine acceptance. (2021). Academic Pediatrics. 21(4), S32-33.

Dein S, Loewenthal K, Lewis CA, Pargament KI. (2020). COVID-19, mental health and religion: An agenda for future research. Mental Health, Religion & Culture. 23(1):1–9.

Dilmaghani M. (2018). Religiosity and subjective wellbeing in Canada. Journal of Happiness Studies. 19(3), 629-647.

Dolcos F, Hohl K, Hu Y, Dolcos S. (2021). Religiosity and resilience: Cognitive reappraisal and coping self-efficacy mediate the link between religious coping and well-being. Journal of Religion and Health. 60(4), 2892-905.

Ekas NV, Tidman L, Timmons L. (2019). Religiosity/spirituality and mental health outcomes in mothers of children with autism spectrum disorder: the mediating role of positive thinking. Journal of Autism and Developmental Disorders. 49(11), 4547-58.

Fabricatore AN, Handal PJ, Rubio DM, Gilner FH. (2004). Stress, religion, and mental health: Religious coping in mediating and moderating roles. The International Journal for The Psychology of Religion. 14(2), 91-108.

Falk RF, Miller NB. (1992). A primer for soft modeling. University of Akron Press.

Filieri R, Alguezaui S, McLeay F. (2015). Why do travelers trust TripAdvisor? Antecedents of trust towards consumer-generated media and its influence on recommendation adoption and word of mouth. Tourism Management. 51, 174-85.

Filieri R, McLeay F. (2014). E-WOM and accommodation: An analysis of the factors that influence travelers' adoption of information from online reviews. Journal of travel research. 53(1), 44-57.

Fishbein M, Ajzen I. (1977). Belief, attitude, intention, and behavior: An introduction to theory and research. Philosophy and Rhetoric. 10(2).

Fornell C, Larcker DF. (1981). Structural equation models with unobservable variables and measurement error: Algebra and Statistics. 382-388.

Fox S. Duggan M. Information triage. Pew Research Center; 2013 Jan 15 [accessed Nov 2022].https://www.pewresearch.org/internet/2013/01/15/information-triage/

Franke, G. R., Sarstedt, M. (2019). Heuristics Versus Statistics in Discriminant Validity Testing: A Comparison of Four Procedures, Internet Research, 29(3), 430-447.

Garcia LL, Yap JF. (2021). The role of religiosity in COVID-19 vaccine hesitancy. Journal of Public Health. 43(3), e529-530.

Giustini DM, Ali SM, Fraser M, Boulos MN. (2018). Effective uses of social media in public health and medicine: a systematic review of systematic reviews. Online journal of public health informatics. 10(2).

Glanz JM, Wagner NM, Narwaney KJ, Kraus CR, Shoup JA, Xu S, O'Leary ST, Omer SB, Gleason KS, Daley MF. (2017). Web-based social media intervention to increase vaccine acceptance: a randomized controlled trial. Pediatrics. 140(6):e20171117.

Godlee F, Smith J, Marcovitch H. (2011). Wakefield's article linking MMR vaccine and autism was fraudulent. BMJ. 342.

Goh KY, Heng CS, Lin Z. (2013). Social media brand community and consumer behavior: Quantifying the relative impact of user-and marketer-generated content. Information Systems Research. 24(1), 88-107.

Gunaratne K, Coomes EA, Haghbayan H. (2019). Temporal trends in anti-vaccine discourse on twitter. Vaccine. 37(35), 4867–71.

Hair J, Hollingsworth CL, Randolph AB, Chong AY. (2017). An updated and expanded assessment of PLS-SEM in information systems research. Industrial Management & Data Systems. 117(3), 442-458.

Hair JF, Risher JJ, Sarstedt M, Ringle CM. (2019). When to use and how to report the results of PLS-SEM. European business review. 31(1), 2-4.

Hair Jr JF, Sarstedt M, Hopkins L, Kuppelwieser VG. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. European Business Review. 26(2), 106-121.

Hair Jr JF, Sarstedt M, Ringle CM, Gudergan SP. (2017). Advanced issues in partial least squares structural equation modeling. Sage publications.

Henseler J, Ringle CM, Sarstedt M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. Journal of the Academy Of Marketing Science. 43(1), 115-35.

Jin J, Yan X, Li Y, Li Y. (2016). How users adopt healthcare information: an empirical study of an online Q&A community. International Journal of Medical Informatics. 86, 91-103.

Junaidi J. (2021). The awareness and attitude of Muslim consumer preference: the role of religiosity. Journal of Islamic Accounting and Business Research. 12(6), 919-938.

Kelecha, Berhanu Borena and Belanger, France, "Religiosity and Information Security Policy Compliance" (2013). AMCIS 2013 Proceeding.

KFF.org dashboard. 2022 October 21 [accessed Nov 2022]. https://www.kff.org/coronavirus-covid-19/dashboard/kff-covid-19-vaccine-monitor-dashboard/#vaccines

Kline RB. (2004). Beyond significance testing: Reforming data analysis methods in behavioral research. APA.

Kline RB. (2011). Convergence of structural equation modeling and multilevel modeling.

Lagoe C, Atkin D. (2015). Health anxiety in the digital age: An exploration of psychological determinants of online health information seeking. Computers in Human Behavior. 52, 484-91.

Lee W, Xiong L, Hu C. (2012). The effect of Facebook users' arousal and valence on intention to go to the festival: Applying an extension of the technology acceptance model. International Journal of Hospitality Management. 31(3), 819-27

Liao M. Q., Mak A. K. Y. (2019). "Comments are disabled for this video": a technological affordances approach to understanding source credibility assessment of CSR information on YouTube. Public Relat. Rev. 45 1–12.

Lucchetti G, Lucchetti AL. (2014). Spirituality, religion, and health: Over the last 15 years of field research (1999–2013). The International Journal of Psychiatry in Medicine. 48(3), 199-215.

Ma TJ, Atkin D. (2017). User generated content and credibility evaluation of online health information: A meta-analytic study. Telematics and Informatics. 34(5), 472-86.

Maltby J, Day L. (2003). Religious orientation, religious coping and appraisals of stress: Assessing primary appraisal factors in the relationship between religiosity and psychological well-being. Personality and Individual Differences. 34(7), 1209-1224.

McKinley CJ, Lauby F. (2021). Anti-Vaccine Beliefs and COVID-19 Information Seeking on Social Media: Examining Processes Influencing COVID-19 Beliefs and Preventative Actions. International Journal of Communication. 15, 4252-4274.

Meade AW, Craig SB. (2012). Identifying careless responses in survey data. Psychological Methods. 17(3), 437.

Meskó B. (2013). Social media is transforming medicine and healthcare. In Social Media in Clinical Practice. 1-12.

Milligan MA, Hoyt DL, Gold AK, Hiserodt M, Otto MW. (2021). COVID-19 vaccine acceptance: Influential roles of political party and religiosity. Psychology, Health & Medicine.

Muñoz-Leiva F, Hernández-Méndez J, Sánchez-Fernández J. (2012). Generalising user behaviour in online travel sites through the Travel 2.0 website acceptance model. Online Information Review. 36(6), 879-902.

Murphy J, Vallières F, Bentall RP, Shevlin M, McBride O, Hartman TK, McKay R, Bennett K, Mason L, Gibson-Miller J, Levita L. (2021). Psychological characteristics associated with COVID-19 vaccine hesitancy and resistance in Ireland and the United Kingdom. Nature Communications. 12(1), 1-5.

Nitzl, C., Roldan, J. L., & Carrion, G. C. (2016). Mediation analysis in partial least squares path modelling: Helping researchers discuss more sophisticated models. Industrail Management & Data Systems, 116(9), 1849-1864

Nunnally JC. (1978). An overview of psychological measurement. Clinical Diagnosis of Mental Disorders. 97-146.

Olagoke AA, Olagoke OO, Hughes AM. (2021). Intention to vaccinate against the novel 2019 coronavirus disease: The role of health locus of control and religiosity. Journal of religion and health. 60(1), 65-80.

Omidvar Tehrani S, Perkins DD. (2022). Public Health Resources, Religion, and Freedom as Predictors of COVID-19 Vaccination Rates: A Global Study of 89 Countries. COVID. 2(6), 703-718.

Oppenheimer DM, Meyvis T, Davidenko N. (2009). Instructional manipulation checks: Detecting satisficing to increase statistical power. Journal of Experimental Social Psychology. 45(4), 867-72.

Orlandi LB, Febo V, Perdichizzi S. (2022). The role of religiosity in product and technology acceptance: Evidence from COVID-19 vaccines. Technol Forecast Soc Change. 122032.

Panzini RG, Mosqueiro BP, Zimpel RR, Bandeira DR, Rocha NS, Fleck MP. (2017). Quality-of-life and spirituality. International Review of Psychiatry. 29(3), 263-82.

Paolacci G, Chandler J, Ipeirotis PG. (2010). Running experiments on amazon mechanical turk. Judgment and Decision making. 5(5), 411-419.

Petty RE, Cacioppo JT. (1986). The elaboration likelihood model of persuasion. In Communication and Persuasion. Advances In Experimental Social Psychology. 19, 1-24.

Preacher KJ, Hayes AF. (2008). Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. Behavior Research Methods. 40(3), 879-91.

Puri, N., Coomes, E. A., Haghbayan, H., & Gunaratne, K. (2020). Social media and vaccine hesitancy: new updates for the era of COVID-19 and globalized infectious diseases. Human vaccines & immunotherapeutics, 16(11), 2586-2593.

Razai, M. S., Osama, T., McKechnie, D. G., & Majeed, A. (2021). Covid-19 vaccine hesitancy among ethnic minority groups. bmj, 372.

Reno C, Maietti E, Fantini MP, Savoia E, Manzoli L, Montalti M, Gori D. (2021). Enhancing COVID-19 vaccines acceptance: results from a survey on vaccine hesitancy in Northern Italy. Vaccines. 9(4), 378.

Ringle C, Da Silva D, Bido D. (2015). Structural equation modeling with the SmartPLS. Brazilian Journal of Marketing. 13(2).

Rutter M. (2012). Resilience as a dynamic concept. Development and psychopathology. 24(2), 335-344.

Schwalm FD, Zandavalli RB, de Castro Filho ED, Lucchetti G. (2022). Is there a relationship between spirituality/religiosity and resilience? A systematic review and meta-analysis of observational studies. Journal of Health Psychology. 27(5), 1218-32.

Shapiro DN, Chandler J, Mueller PA. (2013). Using Mechanical Turk to study clinical populations. Clinical Psychological Science. 1(2), 213-20.

Stahl JP, Cohen R, Denis F, Gaudelus J, Martinot A, Lery T, Lepetit H. (2016). The impact of the web and social networks on vaccination. New challenges and opportunities offered to fight against vaccine hesitancy. Medecine et Maladies. 46(3), 117-22.

Sussman SW, Siegal WS. (2003). Informational influence in organizations: An integrated approach to knowledge adoption. Information Systems Research. 14(1), 47-65.

Thao T, Shurong T. (2020). Is it possible for "electronic word-of-mouth" and "user-generated content" to be used interchangeably. Journal of Marketing and Consumer Research. 65, 41-48.

The United Nations. Measles' misinformation campaigns' through social media, fuel rising toll. 2019 December 5 [accessed 2022 Nov 20].https://news.un.org/en/story/2019/12/1052801

Thomas T, Blumling A, Delaney A. (2015). The influence of religiosity and spirituality on rural parents' health decision-making and human papillomavirus vaccine choices. Advances in Nursing Science. 38(4), E1.

Tomeny TS, Vargo CJ, El-Toukhy S. (2017). Geographic and demographic correlates of autism-related anti-vaccine beliefs on Twitter, 2009-15. Social Science & Medicine. 191, 168-175.

Tonsaker T, Bartlett G, Trpkov C. (2014). Health information on the Internet: gold mine or minefield?. Canadian Family Physician. 60(5), 407-408.

Troiano G, Nardi A. (2021). Vaccine hesitancy in the era of COVID-19. Public Health. 194, 245-51.

Tseng SY, Wang CN. (2016). Perceived risk influence on dual-route information adoption processes on travel websites. Journal of Business Research. 69(6), 2289-2296.

Venkatesh V, Morris MG, Davis GB, Davis FD. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly. 27(3), 425-478.

Voorhees CM, Brady MK, Calantone R, Ramirez E. (2016). Discriminant validity testing in marketing: an analysis, causes for concern, and proposed remedies. Journal of the Academy of Marketing Science. 44(1), 119-134.

Weber TJ, Muehling DD, Kareklas I. (2021). How unsponsored, online user-generated content impacts consumer attitudes and intentions toward vaccinations. Journal of Marketing Communications. 27(4), 389-414.

Wei, Z., Zhu, Y. (2023). Does religiosity improve analyst forecast accuracy?. Rev Quant Finan Acc 60, 915–948.

Wilkes RE, Burnett JJ, Howell RD. (1986). On the meaning and measurement of religiosity in consumer research. Journal of the Academy of Marketing Science. 14(1), 47-56.

Wong JC. How Facebook and YouTube help spread anti-vaxxer propaganda. TheGuardian.com; 2019 Feb 1 [accessed Nov 2022].https://www.theguardian.com/media/2019/feb/01/facebook-youtube-anti-vaccination-misinformation-social-

Zhao, X., Lynch, J. G., & Chen, Q. (2010). Reconsidering Baron and Kenny: Myths and Truths about Mediation Analysis. Journal of Consumer Research, 37(3), 197-206.

Zhou W, Duan W. (2016). Do professional reviews affect online user choices through user reviews? An empirical study. Journal of Management Information Systems. 33(1), 202-228.

Editor's Note:

This paper was selected for inclusion in the journal as the 2023 ISCAP Conference Information Systems Applied Research Best Paper The acceptance rate is typically 2% for this category of paper based on blind reviews from six or more peers including three or more former best papers authors who did not submit a paper in 2023.

APPENDIX A
Survey Items

Construct		ItemCode	Items	Source
Basic Demographics	Gender	GEN	With what gender do you identify? (Male, Female, Prefer not to answer)	
	Ethnicity	ETH	Your ethinicity? (American Indian or Alaska Native, Asian, Black or African American, Hispanic or Latino, Native Hawaiian orother Pacific Islander, White)	
	Age	AGE	What is your age? (18-23 years, 24-35 years, 36-55 years, 56-65 years, Over 65 years)	
UGC Information Quality			Not at All = 1, Very Little =2, Little = 3, Somewhat = 4, To Some Extent = 5, To a Moderate Extent = 6, To a Great Extent = 7	
	Complete	AQ1	The vaccination HUGC on the social network is complete	Sussman & Siegal, 2003
	Consitent	AQ2	The vaccination HUGC on the social network is consistent	Sussman & Siegal, 2003
	Accurate	AQ3	The vaccination HUGC on the social network is accurate	Sussman & Siegal, 2003
	Relevant	AQ4	The vaccination HUGC on the social network is relevant	Filieri & McLeay, 2014
Religiosity			Not at All = 1, Very Little =2, Little = 3, Somewhat = 4, To Some Extent = 5, To a Moderate Extent = 6, To a Great Extent = 7	
		RELG1	I go to church regularly.	Wilkes et al., 1986
		RELG2	If Americans were more religious, this would be a better country.	Wilkes et al., 1986
		RELG3	Spiritual values are more important than material things.	Wilkes et al., 1986
		RELG4	What is your self-perceived religiousness? (Anti-religious, not at all, slightly, moderately, Very religious)	Wilkes et al., 1986
UGC Information Usefulness			Not at All = 1, Very Little =2, Little = 3, Somewhat = 4, To Some Extent = 5, To a Moderate Extent = 6, To a Great Extent = 7	
	Valuable	PU1	The COVID vaccination HUGC on social media is valuable	Sussman & Siegal, 2003
	Informative	PU2	The COVID vaccination HUGC on social media is informative	Sussman & Siegal, 2003
	Helpful	PU3	The COVID vaccination HUGC on social media is helpful	Sussman & Siegal, 2003
	Useful	PU4	Overall, I find COVID vaccination HUGC on social media useful	Bhattacherjee & Sanford, 2006
UGC Information Adoption		ADP1	How closely did you follow the COVID vaccination HUGC on social media? Not at all (1) - To the letter (7)	Sussman & Siegal, 2003
		ADP2	To what extent does the COVID vaccination HUGC on social media motivate you to take COVID vaccination? Not motivated (1) - Highly motivated (7)	Sussman & Siegal, 2003
Attention Questions		SPEED	We want to test your attention, so please click on the answer '**Little**'. Not at all, Very little, Little, Somewhat, To Some Extent, To a great Extent	Meade, A. W., & Craig, S. B., 2012
		ATTN	When a big news story breaks people often go online to get up-to-the-minute details on what is going on. We want to know which websites people trust to get this information. We also want to know if people are paying attention to the question. To show that you've read this much, please ignore the question and select The Drudge Report as your answer. *New York Times *MSNBC *The drudge Report *Fox News *CNN *Huffington Post *Washington Post	Berinsky, A. J., Margolis, M. F., & Sances, M. W., 2014
		MANIP	The postings for hashtag #getvaccinated is dominated by Pro-vaccination voices. Yes / No (1)	Weber et al., 2019

Social Media Only Has Two Clusters: A United States Analysis

Alan Peslak
arp14@psu.edu
Information Sciences and Technology
Penn State University
Dunmore, PA 18512, USA

Pratibha Menon
menon@pennwest.edu

Lisa Kovalchick
kovalchick@pennwest.edu

Computing and Engineering Technology
Pennsylvania Western University
California, PA 15419, USA

Abstract

The expansion of social media and networking has been remarkable. Since its inception in 1995 with Classmates.com, the landscape evolved to include Friendster in 2002, LinkedIn and MySpace in 2003, and Facebook in 2004. Today, social networking is a global phenomenon, with Facebook boasting nearly 2.95 billion active users worldwide (Statista, 2023a). The number of significant social media platforms has also increased, with the top sites in the United States accounting for most of the activity. This study explores a 2021 Pew Internet dataset through Two-Step Cluster Analysis to identify Social Networking User Groups. By combining usage data from top social media websites with pertinent demographic and sociographic information, we establish two distinct user clusters for social media in the US as of 2021. The implications for marketers, researchers, and society at large are also considered.

Keywords: Social networking, social media, cluster analysis, Facebook, YouTube, TikTok

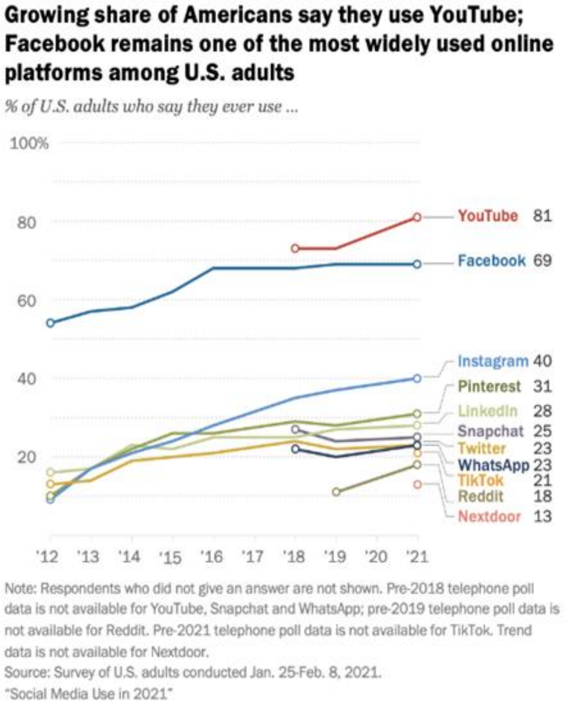
Recommended Citation: Peslak, A., Menon, P., Kovalchick, L., (2024). Social Media Only Has Two Clusters: A United States Analysis. *Journal of Information Systems Applied Research,* 17(3), pp. 43-55. https://doi.org/10.62273/MFUN2972

Social Media Only Has Two Clusters: A United States Analysis

Alan Peslak, Pratibha Menon and Lisa Kovalchick

1. INTRODUCTION

Social networking involves utilizing internet-based platforms to engage with other users and establish new connections with individuals who share similar interests. Since the mid-1990s, the number and popularity of social networking platforms have experienced significant growth. Figure 1 illustrates the increasing monthly usage of these applications. In the United States, at least 72% of adults utilize some of the social media platforms (Auxier & Anderson, 2021). Prominent social networking sites and applications include Facebook, Instagram, Twitter, Snapchat, TikTok, and YouTube.



Growing share of Americans say they use YouTube; Facebook remains one of the most widely used online platforms among U.S. adults

% of U.S. adults who say they ever use ...

Note: Respondents who did not give an answer are not shown. Pre-2018 telephone poll data is not available for YouTube, Snapchat and WhatsApp; pre-2019 telephone poll data is not available for Reddit. Pre-2021 telephone poll data is not available for TikTok. Trend data is not available for Nextdoor.
Source: Survey of U.S. adults conducted Jan. 25-Feb. 8, 2021.
"Social Media Use in 2021"

Figure 1: Increasing Monthly Use of Popular Social Networking Platforms

Users of these platforms may exhibit comparable traits. Identifying clusters of similar social networking users can benefit various audiences. To pinpoint social media networking groups, we initiate a literature review that explores social media usage in the US across multiple categories, such as age and gender, education level, and income level. We also offer a summary of cluster analysis, the technique employed to identify the groupings. Following this, we outline the methodology applied in our study and the predictor importance. We identify two distinct clusters of social media users in the US. In the discussion and conclusions section, we examine the implications of our discoveries and propose ideas for future research.

2. LITERATURE REVIEW

Many authors have studied social media usage and employed various techniques to categorize social media users. Java, Song, Finin, and Tseng (2007) analyzed Twitter users and their connections to understand the nature of microblogging communities and their communication patterns; they identified four types of user intentions in these communities: daily chatter, conversations, information sharing, and news reporting. In addition, they categorized Twitter users into three main categories: information sources, friends, and information seekers (Java et al., 2007). Gjoka, Kurant, Butts, and Markopoulou (2010) utilized sampling techniques to understand the structure and properties of online social networks, specifically using Facebook as a case study; they proposed a new sampling methodology that allowed them to identify and study unbiased samples of Facebook's user network. Riquelme and González-Cantergiani (2016) performed the first comprehensive study of measures used to identify the most influential Twitter users.

Researchers have utilized cluster analysis to develop new techniques, methods, and algorithms to study the vast number of social media users. Agarwal and Liu (2009) provide an overview of various research techniques for analyzing and mining the blogosphere; their book discusses topics such as blog data collection, preprocessing, analysis, and modeling, including social network analysis, to identify clusters and communities within the blogosphere. Catanese, Meo, Ferrara, Fiumara, and Provetti (2011) presented a methodology for crawling Facebook to perform social network analysis; they demonstrated how their methodology could be used to identify clusters and communities within Facebook, providing insights into the structure and dynamics of the network. McAuley and Leskovec (2012) developed a machine learning model to discover social circles in ego networks (i.e., networks centered around an individual user); their model was tested on various social media platforms, including Facebook, Google+, and Twitter, and demonstrated strong performance in identifying clusters of users with shared interests. Raghavan, Albert, and Kumara (2007) presented a near-linear time algorithm for detecting community structures in large-scale networks, including social media platforms; their proposed algorithm was tested on synthetic and real-world networks, showing its efficiency and scalability for analyzing social media clusters. Backstrom and Leskovec (2011) proposed a supervised random walk algorithm for predicting and recommending links in social networks; their algorithm was applied to various social media platforms, including Facebook, and showed strong performance in identifying potential connections between users based on their existing social media clusters. Zafarani and Liu (2009) utilized a user’s behavior patterns to identify users across various social media platforms. Their technique could improve user experience, including verifying user identity across multiple social media platforms; researchers could also use it when studying user behavior across platforms.

Others have used cluster analysis to study user behavior on social media. Xu, Zhang, Wu, and Yang (2012) analyzed user posting behavior on Twitter; their work assumes user behavior is usually influenced by the following three factors: breaking news, friends' posts, and the user's interests. They proposed a mixture latent topic model to predict a user’s motivation to create and share content on Twitter (Xu et al., 2012). Naveed, Gottron, Kunegis, and Alhadi (2011) studied tweets and retweets on Twitter and trained a prediction model to forecast the likelihood of a Tweet being retweeted; they discovered that Tweets on general topics are more likely to be retweeted than Tweets concerning very specific interests and content. Rizoiu, Xie, Sanner, Cebrian, Yu, and Van Hentenryck (2017, p. 735) studied videos on Twitter and developed a mathematical model using the Hawkes intensity process to “explain the complex popularity history of each video according to its type, content, network of diffusion, and sensitivity to promotion.” The authors used this model to predict the likelihood of a video going viral and those with little likelihood of going viral, regardless of promotion.

3. METHODOLOGY

Data

Our analysis used data from Pew Research and was obtained from phone interviews conducted from January 25 to February 8, 2021, with a nationwide sample of 1,502 adults aged 18 or older residing in all 50 U.S. states and the District of Columbia. Abt Associates directed the interviewers who conducted the interviews with 300 respondents on landline phones and 1,202 on cellphones, including 845 without landlines. The survey employed a mix of landline and cellphone random-digit-dial samples provided by Dynata per Abt Associates' specifications. Interviews were in English and Spanish (Methodology, 2021). More details about the survey methodology can be found from the U. S. Survey published by Pew Research Center (U.S. Surveys, 2021).

For the landline sample, the youngest adult male or female present at home was randomly selected. In the cell sample, interviews were conducted with the adult (18 years or older) who answered the phone. The combined landline and cellphone samples were weighted using an iterative method, aligning gender, age, education, race, Hispanic origin, nativity, region, and population density with parameters from the U.S. Census Bureau’s 2019 American Community Survey one-year estimates and the decennial census. The sample was also weighted to match current telephone usage patterns (landline only, cellphone only, or both) based on extrapolations from the 2019 National Health Interview Survey.

Cluster Analysis

Clustering refers to assembling similar data points into smaller subgroups within a broader dataset. Ideally, these clusters should consist of homogeneous elements that share more similarities with members within the same cluster than with those in different clusters. Clustering, or cluster analysis, is an unsupervised machine learning technique to detect inherent groupings in data (Wilson, 2020). It interprets the input data and identifies natural clusters or groups based on feature similarity.

In this study, we employed the silhouette method to create distinct clusters of social media users. The silhouette method, introduced by Kaufman and Rousseuw (1990), is a standard tool for validating data clusters and determining the optimal number of clusters. This method gauges a data point's similarity to its own cluster (cohesion) versus other clusters (separation), thereby assessing the quality of its placement within the cluster. Silhouette coefficients range between -1 and 1, with higher values denoting better clustering. A value close to 1 signifies that the data point is far from adjacent clusters, whereas a value near 0 means the data point is close to or between two clusters, without a clear preference for either. A negative silhouette value may suggest incorrect cluster assignment.

The number of clusters that yield the highest average silhouette value represents the optimal cluster number. To compute the silhouette score for each data point, i, the formula is $s(i) = (b(i)–- a(i)) / \max(b(i), a(i))$, where $a(i)$ represents the average distance between the data point and all other points in its cluster, and $b(i)$ represents the minimum average distance to points in any other cluster. A silhouette score of 1 implies highly dense and well-separated clusters. A score of 0 indicates an overlap between clusters, and a score below 0 suggests potential inaccuracies in data cluster assignment (Bhardwaj, 2020).

We aimed to obtain clusters with a minimum silhouette score of .3 or above. Cluster results are considered appropriate when the silhouette score is > 0.2. Though 0.2 is regarded as a fair score (Boos et al., 2021), we wished to provide a more robust clustering.

4. RESULTS

Social Media Use

We performed a two-step cluster analysis on the data provided by 1,502 users who responded to the survey on social media usage. Social media usage was measured using predictor variables representing the use and non-use of 11 social media platforms, as tabulated for the WEB1 set of questions in the dataset for the questionnaire that can be obtained from the Social Media Use in 2021 report published by Pew Research Center (Auxier & Anderson, 2021). The two-step cluster analysis of social media usage displayed two clusters that we will first call Clusters 1 and 2.

The silhouette score was above 0.3 and was considered fair and meaningful. Cluster 1 comprised 61% of users in the dataset, and Cluster 2 comprised the remaining 39%. The predictor importance chart in Table 1 indicates the relative importance of each of the predictor variables in defining the cluster model.

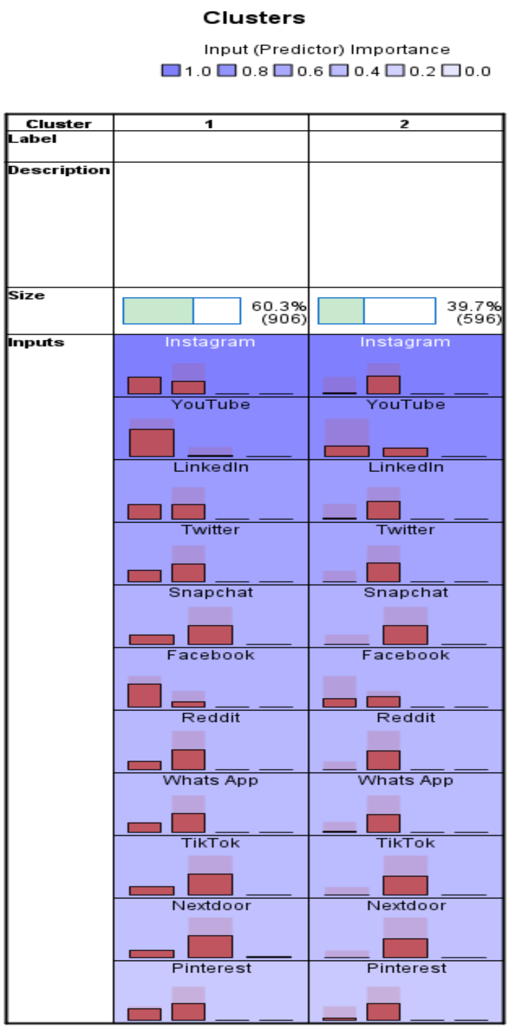
Question: "Please tell me if you ever use any of the following. Do you ever use…	Predictor Importance
Pinterest?	0.2835
Nextdoor?	0.3631
TikTok?	0.4167
WhatsApp?	0.4199
Reddit?	0.4483
Facebook?	0.4991
Snapchat?	0.5183
Twitter?	0.6373
LinkedIn?	0.7181
YouTube?	0.8911
Instagram?	1

Table 1: Social Media Use Predictor Importance from the WEB1 Questions.

Table 2 shows the two clusters and the predictor variables arranged in the order of predictor importance. This chart also visually depicts, in the form of distinct bars, the use (and non-use) of each social media platform for users from each cluster. Figure 2 presents another view of the predictor importance of the variables within each cluster.

Table A.1 in Appendix A shows an example of crosstabulation results for the two-step clusters and Instagram usage. Similarly, results obtained for the remaining predictors are summarized in Appendix B. A correlation matrix was developed for each predictor, which is displayed in Appendix C.

Upon inspecting the usage of each social media platform, for each cluster, we determined that there are two clear groups of users: Multi-Platform (MP) social media users and Limited-Platform (LP) social media users.



Clusters

Input (Predictor) Importance

▨ 1.0 ▨ 0.8 ▨ 0.6 ▨ 0.4 ▨ 0.2 □ 0.0

Cluster	1	2
Label		
Description		
Size	60.3% (906)	39.7% (596)
Inputs	Instagram	Instagram
	YouTube	YouTube
	LinkedIn	LinkedIn
	Twitter	Twitter
	Snapchat	Snapchat
	Facebook	Facebook
	Reddit	Reddit
	Whats App	Whats App
	TikTok	TikTok
	Nextdoor	Nextdoor
	Pinterest	Pinterest

Table 2: Clusters with Input Predictors

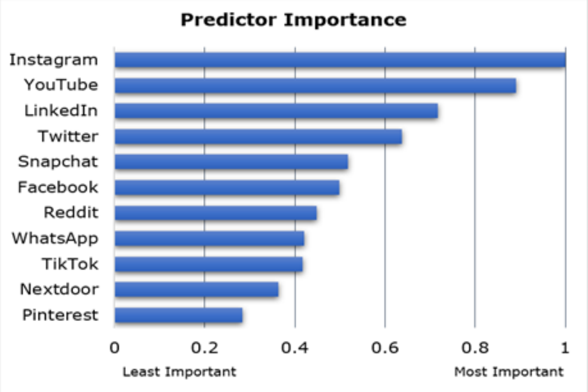


Figure 2: Predictor Importance of Cluster Variables

MP users are distinct from LP users. The MP users use all platforms surveyed and do so with a significant participation rate ranging from 24% to 97%, depending on the platform. The LP users primarily only use Facebook and YouTube, and even those platforms are 88% and 77%, respectively, more likely to be used by the MP user group. As shown in the last column in the table in Appendix B, we have calculated the percentage Cluster 1 is more likely to use each social media platform over Cluster 2 by diving the percentage of Cluster 1 users, who report using a specific platform, by the percentage of Cluster 2 users who report using that same platform, multiplying this result by 100 to obtain a percentage and subtracting 100. These results show that Twitter is 22324% more likely to be used by MP users than by LP users. Likewise, Reddit is 16812% more likely, and TikTok is 7894% more likely to be used by MP users than by LP users. The table shows a revealing picture of the current state of social media usage today. There are two distinct clusters of users, and though their participation rates vary by platform, there are significant differences in the usage of the platforms between the two groups. Some, such as Twitter, Instagram, Snapchat, Redditt, and TikTok, show tremendous differences; however, even Facebook and YouTube are nearly twice as likely to be used by MP than by LP users.

The values of the correlation coefficients (also known as the r values), tabulated in the correlation matrix in Appendix C, show many platform usages significantly correlated at $p < 0.001$. Only SnapChat and Nextdoor, YouTube and Nextdoor, and TikTok and Nextdoor are not correlated at $p < 0.05$. However, many correlations are not strong. Generally, an absolute r value less than or equal to 0.35 is viewed as showing a low or weak correlation. A value ranging from 0.36 to 0.67 represents a modest or moderate correlation, whereas a value from 0.68 to 1.0 indicates a strong or high correlation. An r coefficient equal to or greater than 0.90 symbolizes a remarkably high correlation (Taylor, 1990). Many of the significant correlations in Appendix C can be considered low or weak. The ones that show modest or moderate correlation include TikTok and Snapchat, Twitter and Instagram, Twitter and TikTok, Twitter and Snapchat, Instagram and Facebook, and Instagram and TikTok. In addition, Facebook and YouTube show a moderate correlation as well. Twitter and Instagram use were more correlated with the usage of other platforms. Snapchat and TikTok usage showed higher correlation coefficients with the use of other platforms.

Demographic Analyses
Demographic analyses of the two clusters are studied by considering predictors such as age, gender, educational attainment, and political affiliation that were obtained from social media users who responded to the survey.

Table 3 shows the mean age reported by users who are grouped under Clusters 1 (MP) and 2 (LP) by the two-step analysis. The active multi-platform users who characterize Cluster 1 are younger by almost two decades than the infrequent and limited platform users typical to Cluster 2.

Two-Step Cluster Number * AGE. What is your age?			
Cluster	Mean	N	Std. Dev
1	46.20	906	18.63
2	64.77	596	17.61
Total	53.57	1502	20.37

Table 3: Two-Step Cluster Number and Age

Two-Step Cluster Number * GENDER. Do you describe yourself as a man, a woman or in some other way?			
	Mean	N	Std. Dev
A man	1.40	854	.490
A woman	1.39	628	.489
In some other way	1.25	8	.463
Don't know	1.67	3	.577
Refused	1.78	9	.441
Total	1.40	1502	.489

Table 4: Two-Step Cluster Number and Gender

To analyze how gender responses from the social media users may be associated with the two clusters, we find the mean cluster number for each response value, as shown in Table 4. The mean cluster is the mean of the frequency of each of the responses for each cluster, weighted by the cluster number. Table A.2 in Appendix A shows the frequency of each of the gender related survey responses for each cluster number. As shown in Table 4, most of the respondents identified themselves along the traditional gender lines as a man, or a woman and the cluster numbers were somewhat the same for both of these responses. Table 4 indicates that although fewer in number, users who do not describe their gender as either male or female, and instead express their gender "in some other way" may have greater presence within Cluster 1 (MP). At the same time, users who refused to answer, or expressed that they "don't know" had higher mean values and therefore, could lean more towards the LP cluster (i.e., Cluster 2). While the survey did not ask the respondents to identify themselves as the LGBTQ+ group, prior studies have shown social media serves as informal learning environments for LGBTQ+ youth during their identity developmental processes (Fox & Ralston 2016; McInroy, Craig, & Leung, 2019). Therefore, there is a possibility that active use of social media may be prevalent with users who prefer to identify their gender "in some other way."

Two-Step Cluster Number * MARITAL. Are you currently married, living with a partner, divorced, separated, widowed, or have you never been married?			
	Mean	N	Std. Dev
Married	1.39	721	.488
Living with a partner	1.40	115	.492
Divorced	1.46	171	.500
Separated	1.36	36	.487
Widowed	1.71	107	.456
Never been married	1.26	325	.438
Don't know	1.67	3	.577
Refused	1.62	24	.495
Total	1.40	1502	.489

Table 5: Two-Step cluster number * marital status

Table 5 shows the mean cluster number for various survey responses concerning marital status. Those who responded as "never being married" had a lower mean cluster number and, therefore, were more likely to fall under Cluster 1. This could also be indicative of the fact that Cluster 1 social media users tend to be younger (as evident from Table 3).

Two-Step Cluster Number * PARTY. In politics TODAY, do you consider yourself a Republican, Democrat, or Independent?			
	Mean	N	Std. Deviation
Republican	1.48	359	.500
Democrat	1.33	482	.469
Independent	1.36	470	.480
No preference	1.47	78	.503
Other party	1.39	18	.502
Don't know	1.45	20	.510
Refused	1.59	75	.496
Total	1.40	1502	.489

Table 6: Two-Step cluster number * Party

Table 6 shows a smaller mean cluster number associated with Democrats and Independents than with Republicans. Younger social-media users, who are more present in Cluster 1 might tend to affiliate themselves with the Democratic party (Statista, 2023b).

Educational attainment of respondents, as listed in Table 7, shows that social-media users with a higher level of education tend to have lower cluster numbers and, therefore, lean towards Cluster 1 and may tend to be MP. However, people with a bachelor's degree showed a lower mean cluster number than people with post graduate schooling and those with a post grad degree.

Two-Step Cluster Number *EDUC			
Education	Mean	N	Std. Dev
1 – Less than High School	1.65	17	.493
2 – High school incomplete	1.59	44	.497
3 -High school graduate	1.49	313	.501
4 – Some college, no degree	1.42	244	.494
5 – 2 yr. associate degree	1.49	156	.501
6 – 4 yr. bachelor's degree	1.29	389	.455
7 – Some Postgrad or Professional schooling	1.36	42	.485
8 – Post grad/professional degree	1.31	274	.462
98 – don't know	1.67	3	.577
99 – refuse to answer	1.75	20	.444
Total	1.40	1502	.489

Table 7: Two-Step cluster number * Educational Attainment

Two-Step Cluster Number * INCOME			
INCOME. Last year, that is in 2020, what was your total family income from all sources, before taxes? Just stop me when I get to the right category.	Mean	N	Std. Dev
Less than $10,000	1.49	70	.503
10 to under $20,000	1.57	99	.498
20 to under $30,000	1.45	110	.500
30 to under $40,000	1.37	120	.484
40 to under $50,000	1.48	89	.503
50 to under $75,000	1.48	182	.501
75 to under $100,000	1.28	193	.453
100 to under $150,000	1.26	193	.439
$150,000 or more	1.27	217	.444
Don't know/Refused	1.52	229	.501
Total	1.40	1502	.489

Table 8: Two-Step cluster number * Income

Income appears to influence social-media use. Table 8 shows that the mean cluster number is lower for users who reported a higher income. Therefore, there is a likelihood that users who have a higher income tend display the MP characteristics associated with Cluster 1 and people with a lower income tend to be LP and reside in Cluster 2.

5. DISCUSSION AND CONCLUSION

The result of this study, which is based on the survey data collected from the Pew Research, indicate that social media users form two clusters based on the number of social media platforms they use.

Based on the data collected from a nationwide survey, social-media users could be classified as multi-platform (MP) or limited-platform (LP) users. Our paper is an update of a prior study on the cluster analysis of social media user groups (Peslak, Ceccucci, & Hunsinger, 2022). That study reviewed a 2019 Pew data survey but did not include many newer platforms including TikTok and Nextdoor; therefore, this study expands upon the prior study. Cluster analysis of the 2019 social media usage data revealed three clusters but since then, as evidenced by the current study, the distinction has narrowed to only these two clusters, despite an increase in the number of social media platforms.

Based on the survey results, demographic analyses of users who fall under the two clusters indicates that MP users have a higher chance of reporting themselves as younger, single, and democrat, or independent. MP users also tend to report their gender non-traditionally, have a higher chance of attaining higher levels of education, and tend to report higher income levels. On the other hand, there is a greater chance that LP users are older, report lower income levels and educational attainment lower than a bachelor's degree. LP users also tend to report their political stance as leaning toward Republican and have a higher chance of refusing to report their gender identities, or of choosing the gender identity option of 'do not know'. Survey responses also reveal that LP users have reported their marital status as widowed or as something that they 'do not know.'

The existence of two social media clusters that display divergent demographic characteristics may have several economic and social implications. One such implication may result from the spillover effects of incidental information exposure from one platform to another. Spillover effects have been observed in marketing of product brands that allocate their social media advertising across multiple platforms such as Facebook, Twitter, Instagram, and YouTube. Since consumers use multiple social media platforms, brand communications on one platform could potentially impact engagement with the brand on the other platforms; this phenomenon is known as spillover effect. By knowing the demographics that constitute multi-platform users, social media advertising could take advantage of the spillover of brand information from one platform into another. This spillover effect has been previously used to inform marketing resource allocation across platforms for a company's brand (Unnava & Aravindakshan, 2021).

Similar spillover effects could also influence the way social media users consume news. Multi-platform social media news consumption affords diversified information and exposure to pro- and counter-attitudinal viewpoints (Lee, Choi, Kim, & Kim, 2014). At the same time, studies have shown how incidental, counter-attitudinal exposure enabled by multiple-platform social media use leads to a greater tendency of in-group support consisting of users from the same demographic profile and criticism against out-groups possibly consisting of users with different demographic characteristics (Guo & Chen, 2022). Therefore, awareness of the fact that social media clusters could display polarized demographic characteristics makes it critical to ensure that social media news content equitably serves a larger population.

The two social media usage clusters identified in this study vary based on two main factors that impact economic equality among the US population – education and income levels. MP users tend to report higher education levels and higher income and more LP users have reported lower education and income levels. The social benefits and opportunities afforded by networking via multiple social media platforms could go unrealized by people with lower incomes, who also typically tend to have lower educational attainment.

This study does not address the factors that could have led to the formation of the two social media clusters. More research is needed to investigate how factors such as unequal access to digital media, lack of digital skills, or the inability to leverage the affordances of social media could be reasons for the formation of demographically distinct social media clusters that are identified in this study. Nevertheless, the findings of this study indicate a possible digital divide among social media users based on their use of multiple platforms that could potentially confer more economical and social advantages to one group of demographics over the other. Future studies could systematically investigate why and how social media clusters are formed due to the demographic characteristics of users.

6. ACKNOWLEDGEMENTS

The article includes contents edited by ChatGPT, a language model developed by OpenAI in San Francisco, CA, USA. Additionally, ChatGPT provided assistance in sentence editing.

Papers and publications using our data should reference Pew Research Center's Religion & Public life project as the source of the data and should acknowledge that the Center bears no responsibility for the interpretations presented or conclusions reached based on analysis of the data.

7. REFERENCES

Agarwal, N., & Liu, H. (2009). Modeling and Data Mining in Blogosphere. Morgan & Claypool Publishers.

Auxier, B., & Anderson, M. (2021, April 7). Social Media Use in 2021. Retrieved June 15, 2023. https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/

Backstrom, L., & Leskovec, J. (2011). Supervised random walks: Predicting and recommending links in social networks. Proceedings of the Fourth ACM International Conference on Web Search and Data Mining, Hong Kong, China, 635-644. https://doi.org/10.1145/1935826.1935914

Bhardwaj. A. (2020). Silhouette Coefficient. Retrieved June 15, 2023, from https://towardsdatascience.com/silhouette-coefficient-validating-clustering-techniques-e976bb81d10c

Boos, S. C., Wang, M., Karst, W. A., & Hymel, K. P. (2021). Traumatic Head Injury and the Diagnosis of Abuse: A Cluster Analysis. Pediatrics, 149(1). https://doi.org/10.1542/peds.2021-051742

Catanese, S., Meo, P.D., Ferrara, E., Fiumara, G., & Provetti, A. (2011). Crawling Facebook for social network analysis purposes. Web Intelligence, Mining, and Semantics. https://doi.org/10.1145/1988688.1988749

Fox J., & Ralston R. (2016). Queer identity online: Informal learning and teaching experiences of LGBTQ+ individuals on social media. Computers in Human Behavior, pp. 65, 635–642. https://doi.org/10.1016/j.chb.2016.06.009

Gjoka, M., Kurant, M., Butts, C. T., & Markopoulou, A. (2010). Walking in Facebook: A case study of unbiased sampling of OSNs. Proceedings of the 29th Conference on Information Communications, San Diego, CA,pp.1-9.1. https://doi.org/10.1109/INFCOM.2010.5462078

Guo, J., & Chen, H.-T. (2022). How Does Multi-Platform Social Media Use Lead to Biased News Engagement? Examining the Role of Counter-Attitudinal Incidental Exposure, Cognitive Elaboration, and Network Homogeneity. Social Media + Society, 8(4). https://doi.org/10.1177/20563051221129140

Java, A., Song, X., Finin, T., & Tseng, B. (2007). Why we Twitter: Understanding microblogging usage and communities. Proceedings of the 9th WebKDD and 1st SNA-KDD 2007 Workshop on Web Mining and Social Network Analysis, San Jose, CA, 56-65. https://doi.org/10.1145/1348549.1348556

Kaufman, L., & Rousseuw, P. J. (1990). Finding Groups in Data, New York: John Wiley and Sons.

Lee J. K., Choi J., Kim C., Kim Y. (2014). Social media, network heterogeneity, and opinion polarization. Journal of Communication, 64(4),702–722. https://doi.org/10.1111/jcom.12077

McAuley, J. J. & Leskovec, J. (2012). Learning to discover social circles in ego networks. Proceedings of the 25th International Conference on Neural Information Processing Systems, Lake Tahoe, NV, 1, 539-547. https://doi.org/10.1145/2556612

McInroy L. B., Craig S. L., Leung V. W. Y. (2019). Platforms and patterns for practice: LGBTQ+ youths' use of information and communication technologies. Child and Adolescent Social Work Journal, pp. 36, 507–520. https://doi.org/10.1007/s10560-018-0577-x

Naveed, N., Gottron, T., Kunegis, J., & Alhadi, A. C. (2011). Bad news travel fast: A content-based analysis of interestingness on Twitter. Proceedings of the 3rd International Web Science Conference, Koblenz, Germany, 1-7. Methodology.(2021).https://www.pewresearch.org. Retrieved June 18, 2023, from https://www.pewresearch.org/internet/2021/04/07/social-media-use-methodology/

Peslak, Alan, Ceccucci, Wendy and Hunsinger. Scott (2022). Using unsupervised machine learning to determine social networking user groups. Issues in Information Systems, 23(2), 215-230.

Raghavan, U. N., Albert, R., & Kumara, S. (2007). Near-linear time algorithm to detect community structures in large-scale networks. Physical Review E, 76(3), 036106. https://doi.org/10.1103/PhysRevE.76.036106

Riquelme, F., & González-Cantergiani, P. (2016). Measuring user influence on Twitter: A survey. Information Processing & Management,52(5),949-975. https://doi.org/10.1016/j.ipm.2016.04.003

Rizoiu, M. A., Xie, L., Sanner, S., Cebrian, M., Yu, H., & Van Hentenryck, P. (2017). Expecting to be HIP: Hawkes Intensity Processes for social media popularity. Proceedings of the 26th International Conference on World Wide Web, Republic and Canton of Geneva, Switzerland,735-744. https://doi.org/10.1145/3038912.3052650

Statista (2023a, February 14). https://www.statista.com. Most popular social networks worldwide as of January 2023, ranked by number of monthly active users. Retrieved June 15, 2023. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Statista. (2023b, April 6). https://www.statista.com. Party identification in the United States in 2022, by generation. Retrieved June 15, 2023. https://www.statista.com/statistics/319068/party-identification-in-the-united-states-by-generation/

Taylor, R. (1990). Interpretation of the correlation coefficient: a basic review. Journal of Diagnostic Medical Sonography, 6(1), 35–39. https://doi.org/10.1177/875647939000600106

Unnava, V., Aravindakshan, A. (2021). How does consumer engagement evolve when brands post across multiple social media? Journal of the Academy of Marketing Science, 49, 864–881.

https://doi.org/10.1007/s11747-021-00785-z

U.S. Surveys. (2021). https://www.pewresearch.org. Retrieved June 18, 2023, from https://www.pewresearch.org/our-methods/u-s-surveys/

Wilson, J. (2020). How are clustering algorithms different from supervised learning? Technical-QA.COM. Retrieved June 15, 2022, from https://it-qa.com/how-are-clustering-algorithms-different-from-supervised-learning

Xu, Z., Zhang, J., Wu, Y., & Yang, Q. (2012). Modeling user posting behavior on social media. Proceedings of the 35th International ACM SIGIR Conference on Research and Development in Information Retrieval, Portland, OR, 545-554. https://doi.org/10.1145/2348283.2348358

Zafarani, R., & Liu, H. (2009). Connecting users across social media sites: A behavioral-modeling approach. Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Chicago, IL, 41-49. https://doi.org/10.1145/2487575.2487648

Editor's Note:

This paper was selected for inclusion in the journal as a 2023 ISCAP Conference Meritorious Information Systems Applied Research Paper. The acceptance rate is typically 15% for this category of paper based on blind reviews from six or more peers including three or more former best papers authors who did not submit a paper in 2023.

Appendices and Annexures

APPENDIX A
Crosstabulation Results

Crosstabulation – Two-Step Cluster Number * WEB1B (Instagram use)

			WEB1B. Please tell me if you ever use any of the following. Do you ever use... **Instagram**?				Total
			Yes, do this	No, do not do this	Don't know	Refused	
Two-Step Cluster Number	1	Count	513	392	0	1	906
		% within Two-Step Cluster Number	56.6%	43.3%	0.0%	0.1%	100.0%
	2	Count	17	577	2	0	596
		% within Two-Step Cluster Number	2.9%	96.8%	0.3%	0.0%	100.0%
Total		Count	530	969	2	1	1502
		% within Two-Step Cluster Number	35.3%	64.5%	0.1%	0.1%	100.0%

Table A.1: Crosstabulation of Two-Step cluster number and Instagram use
Similar crosstabulations were generated for the Two-Step cluster number and the use of each of the social media types discussed in this paper. WEB1 is a question identifier that was used in the survey.

Two-Step Cluster Number * GENDER. Do you describe yourself as a man, a woman or in some other way? Crosstabulation

			A man	A woman	In some other way	Don't know	Refused	Total
Two-Step Cluster Number	1	Count	515	382	6	1	2	906
		% within Two-Step Cluster Number	56.8%	42.2%	0.7%	0.1%	0.2%	100.0%
	2	Count	339	246	2	2	7	596
		% within Two-Step Cluster Number	56.9%	41.3%	0.3%	0.3%	1.2%	100.0%
Total		Count	854	628	8	3	9	1502
		% within Two-Step Cluster Number	56.9%	41.8%	0.5%	0.2%	0.6%	100.0%

Table A.2: Crosstabulation of Two-Step cluster number and Gender responses
Similar crosstabulations were generated for the Two-Step cluster number and each of the demographic variables discussed in this paper.

APPENDIX B
Participation of users from each cluster for each social media platform

Cluster->	**1**	**1**	**2**	**2**	1 vs 2
User Participation Response ->	**Yes**	**No**	**Yes**	**No**	more likely
Twitter	38.12%	61.88%	0.17%	99.83%	22324%
Instagram	56.69%	43.31%	2.86%	97.14%	1882%
Facebook	80.97%	19.03%	43.03%	56.97%	88%
Snapchat	33.37%	66.63%	0.84%	99.16%	3873%
YouTube	96.91%	3.09%	54.70%	45.30%	77%
WhatsApp	33.81%	66.19%	3.38%	96.62%	900%
Pinterest	39.98%	60.02%	12.58%	87.42%	218%
LinkedIn	49.83%	50.17%	5.37%	94.63%	828%
Reddit	28.75%	71.25%	0.17%	99.83%	16812%
TikTok	27.18%	72.82%	0.34%	99.66%	7894%
Nextdoor	24.13%	75.87%	0.67%	99.33%	3501%

APPENDIX C
Social media usage survey responses correlation matrix. Sample size n = 1502. Moderate correlation coefficients (r value) are highlighted in gray.

	WEB1A **Twitter?**	WEB1B **Instagram?**	WEB1C **Facebook?**	WEB1D **Snapchat?**	WEB1E **YouTube?**	WEB1F **WhatsApp?**	WEB1G **Pinterest?**	WEB1H **LinkedIn?**	WEB1I **Reddit?**	WEB1J **TikTok?**	WEB1K **Nextdoor?**
Twitter	**1**	**.460**	**.289**	**.420**	**.351**	**.233**	**.238**	**.328**	**.350**	**.427**	**.099**
		<.001	*<.001*	*<.001*	*<.001*	*<.001*	*<.001*	*<.001*	*<.001*	*<.001*	*<.001*
Instagram	**.460**	**1**	**.325**	**.508**	**.392**	**.242**	**.310**	**.279**	**.296**	**.439**	**.102**
	<.001		*<.001*	*<.001*	*<.001*	*<.001*	*<.001*	*<.001*	*<.001*	*<.001*	*<.001*
Facebook	**.289**	**.325**	**1**	**.294**	**.387**	**.226**	**.318**	**.212**	**.165**	**.270**	**.066**
	<.001	*<.001*		*<.001*	*<.001*	*<.001*	*<.001*	*<.001*	*<.001*	*<.001*	*0.01*
Snapchat	**.420**	**.508**	**.294**	**1**	**.339**	**.192**	**.287**	**.196**	**.285**	**.545**	**0.041**
	<.001	*<.001*	*<.001*		*<.001*	*<.001*	*<.001*	*<.001*	*<.001*	*<.001*	*0.113*
YouTube	**.351**	**.392**	**.387**	**.339**	**1**	**.252**	**.305**	**.293**	**.265**	**.345**	**0.048**
	<.001	*<.001*	*<.001*	*<.001*		*<.001*	*<.001*	*<.001*	*<.001*	*<.001*	*0.063*
Whats App	**.233**	**.242**	**.226**	**.192**	**.252**	**1**	**.146**	**.303**	**.155**	**.169**	**.126**
	<.001	*<.001*	*<.001*	*<.001*	*<.001*		*<.001*	*<.001*	*<.001*	*<.001*	*<.001*
Pinterest	**.238**	**.310**	**.318**	**.287**	**.305**	**.146**	**1**	**.172**	**.155**	**.305**	**.070**
	<.001	*<.001*	*<.001*	*<.001*	*<.001*	*<.001*		*<.001*	*<.001*	*<.001*	*0.006*
Linked	**.328**	**.279**	**.212**	**.196**	**.293**	**.303**	**.172**	**1**	**.215**	**.162**	**.145**
	<.001	*<.001*	*<.001*	*<.001*	*<.001*	*<.001*	*<.001*		*<.001*	*<.001*	*<.001*
Redditt	**.350**	**.296**	**.165**	**.285**	**.265**	**.155**	**.155**	**.215**	**1**	**.272**	**.089**
	<.001	*<.001*	*<.001*	*<.001*	*<.001*	*<.001*	*<.001*	*<.001*		*<.001*	*<.001*
TikTok	**.427**	**.439**	**.270**	**.545**	**.345**	**.169**	**.305**	**.162**	**.272**	**1**	**0.041**
	<.001	*<.001*	*<.001*	*<.001*	*<.001*	*<.001*	*<.001*	*<.001*	*<.001*		*0.109*
Nextdoor	**.099**	**.102**	**.066**	**0.041**	**0.048**	**.126**	**.070**	**.145**	**.089**	**0.041**	**1**
	<.001	*<.001*	*0.01*	*0.113*	*0.063*	*<.001*	*0.006*	*<.001*	*<.001*	*0.109*	

Mobile Technology Has Changed Our Culture

Karen Paullet
paullet@rmu.edu

Jamie Pinchot
pinchot@rmu.edu

Computer Information Systems Department
Robert Morris University
Moon Township, PA 15108 USA

Abstract

Mobile technology usage has become a common part of everyday life. Smartphones have not only become a communication source for news, talking, texting, searching the web and more; but they have become a part of our culture. This study sought to determine how mobile phone acceptance and users' perceptions of socially acceptable styles of communication using mobile phones have changed. The researchers have conducted a study comparing results from 2010 to 2023. Results from 293 participants from the 2023 study were analyzed to show how mobile technology has changed our culture over time.

Keywords: mobile technology, smart phones, culture, communication

Recommended Citation: Paullet, K., Pinchot, J., (2024). Mobile Technology Has Changed Our Culture. *Journal of Information Systems Applied Research.* 17(3), pp. 56-65. https://doi.org/10.62273/IPBM8613

Mobile Technology Has Changed Our Culture

Karen Paullet and Jamie Pinchot

1. INTRODUCTION

Using mobile devices/smartphones has become an integral part of people's everyday lives. The way in which people communicate with the devices continues to change. In 2023 we are living in an "always-on" world where we are almost expected to be connected 24 hours per day, 7 days per week. Smartphones allow people to connect "anytime", "anywhere" to "anybody". It is hard to imagine living without them. Smartphones, along with keys and money are considered to be one of the three survival tools that most people always carry with them (Emanuel et al., 2015). The use of mobile devices has become part of our culture.

As smartphones are becoming a companion for most people in the United States, landlines are barely holding ground. Since 2004, 60% of people no longer have a landline and rely solely on using their mobile devices for communications (Centers for Disease Control and Prevention, 2022). According to a 2022 study of 1,591 respondents, 21% of smartphone users between the ages of 18-54 and 10% over the age of 55 spend on average 40 or more hours per week on their devices (Statista, 2022). The majority of all users surveyed spent approximately 19 hours per week on their phones.

In 2010, the researchers conducted a study to determine if mobile technology is changing the way people communicate (Pinchot, et.al, 2011). At that time, there were 81.6 million cell phone users in the United States. As of December 2022, approximately 12 years after the original study was conducted there are now over 302 million cell phone users in the United States which shows a continued acceptance of the technology over time (Statista, 2022).

The number of unique mobile Internet users stood at 5 billion in 2022, indicating that over 60 percent of the global Internet population uses mobile devices to go online. In 2022, mobile Internet traffic accounted for almost 60 percent of total web traffic. There are currently 6.8 billion users worldwide (Statista, 2022). According to a Pew study on mobile phones, over 97% of all Americans own a cellular phone of some kind as of 2022. There has been a 50% increase in smartphone ownership from 2011 until 2022. Additionally, 15% of American adults are smartphone-only Internet users – meaning they do not have broadband Internet in their homes (Pew Research Center, 2022).

This study seeks to determine how mobile phone acceptance and users' perceptions of socially acceptable styles of communication have changed from 2010 when the original study was conducted until 2023. In 2010, mobile phone use was in its infancy, only three years after the introduction of the iPhone as the first modern smartphone in 2007, followed by Android and App Stores for both platforms in 2008 (Eadicicco, 2017). Still, the results from that 2010 study showed that mobile technology was starting to change our culture. More than a decade has passed since the first study was conducted, and all indicators show that mobile phones have only become more ingrained in our daily lives, and integral to how we communicate both personally and professionally.

The researchers will compare results from the past study to the present study by exploring the following research question:

RQ1: In what ways has social acceptance of mobile phone use changed from 2010 to 2023?

2. RELATED LITERATURE AND HYPOTHESIS DEVELOPMENT

Smartphones are the most commonly used devices for communications and online activities. Smartphones are used for purposes such as email, texting, video calls and conferencing, banking, making travel arrangements, accessing educational content or social media, and surfing the Internet to name a few. In addition to the positive attributes of mobile devices, they have also been known to prevent individuals from engaging in their work or even to cause sleep deprivation due to the number of hours spent on the device. Additionally, mobile devices can lead to excessive dependence and use of the technology which is known as nomophobia (King et al., 2014; Yildirim & Coreia, 2015). Meluman and Pham (2020) note that, "no recent technological innovation has had a more transformative effect on consumers' lives than the virtually indispensable smartphone" (pp.231).

The remainder of this literature review focuses on mobile phone usage habits and cultural changes that have been noted in the literature in the past decade in regard to how people interact with their mobile devices.

The Adult "Pacifier"

Meluman and Pham (2020) describe smartphones as an "adult pacifier" because people have their phone with them at all times and tend to be less inhibited when they use it compared to a desktop or laptop. The devices are so important that employers supply employees with phones so that they can stay connected. This has blurred the lines as to when work starts and ends each day, creating challenges for a work-life balance. Consumers of smartphones also derive emotional benefits such as comfort and a way to relieve stress. This comfort arises due to the portability of the device, being able to touch and move things on the device, and a sense of privacy since each individual usually owns their own device. In moments of stress, consumers tend to seek out their smartphones to use as a stress reliever.

Work-Life Balance

Due to the COVID-19 pandemic starting in 2020, people were forced to work from home. In 2023, working in a hybrid format or working from home has become part of what is considered the "new normal". With this benefit comes the non-stop connectivity to work. Since the pandemic, 32% of workers have to be available to their employers in their free time as compared to 18% prior to the pandemic. Additionally, 28% of employees work outside their regular hours without pay as compared to 13% prior to the pandemic. Lastly, close to 50% of workers have shorter breaks while working from home as compared to 29% prior to the pandemic (Schmucker, 2022). In order to stay healthy, workers need to be able to detach from work matters in their personal time. However, almost half of all employees working from home cannot detach. They take calls at night, while on vacation, out to dinner with friends and during family time.

It has been noted that work-life balance has become a problem with the continued use of mobile devices. Employees often blur lines associated with work by using social media during work hours. When a person's social media use includes co-workers as well as friends and family, it can also become increasingly difficult to keep personal life separate from work life (Pinchot, et.al, 2011). There have been instances where employees were even fired for taking a sick day and then posting their activities for the day on social media or were fired for posting comments about the employer (Matyszczyk, 2009; Sondergaard, 2009).

Phone Numbers as Identity

It is important to note that phone numbers now refer to people instead of places. Meaning that just because your area code is from New York for example, does not mean that you actually live in New York. The phone number itself is almost a form of identity. In 2023, we are living in a time where area codes are irrelevant to a person's location. Our cell numbers follow us instead of us following a number (Pinchot, et.al, 2011).

High Usage Levels by Generation Z

The number of mobile phone users continues to grow exponentially across all economic and age sectors. However, university students have been identified as one of the largest and most important target markets and the most active users of smartphones (Al-Barashdi, et al. 2015). Generation Z, those born in the late 1990's and early 2000's, use their smartphones more than other generations (Ozkan & Solmaz, 2015).

A 2021 qualitative study on smartphone usage of 29 university students revealed that students on average use their smartphones for 317 minutes per day which is approximately 5-1/2 hours. Students spent an average of 1 hour and 20 minutes per day on messaging applications, 1 hour and 10 minutes on social networks and 1 hour and 7 minutes watching videos (Kaysi et al, 2021).

A 2021 study on smartphone usage among university students revealed that there are a number of factors that have been identified to be associated with students spending long hours on their smartphones. The findings show that 61% of students used their smartphones based on their mood followed by 58% who use their phones based on how much time they had available during the day. Additionally, almost 42% of students use their mobile devices whether they are alone or with others (Fook et al., 2021). Not surprisingly, the study also revealed that 98% of students use their smartphones to surf the Internet as their number one use. Over 92% of students use their smartphones to update information on social media and close to 91% are using apps. Students in this study on average spent 25% of their day on their mobile device (Fook et al., 2021).

Mobile Phone Addiction

The use of smart phones has led people to become addicted to the technology. A study conducted by Tosell et al. (2015) discussed that e-mail, text messaging, social media, and Internet use all assisted in addiction to smart phones. However, Beranuey et al. (2009) determined that the mobile phone is not the source of the addiction, but rather the content that is accessed through the device that causes addiction.

Literature continues to support the relationship that people seem to develop with their smartphone (Alter 2017; Fullwood et al., 2017; Melumad et al., 2019; Wilmer et al., 2017). The most common description of a person's relationship with their mobile phone found in the literature is that it resembles behavioral addiction leading to a desire to engage in risks of social, physical, or financial harm (Albrecht et al., 2007). Prior work shows that users report problematic behaviors such as a loss of productivity (e.g., using the phone during work), degradation of interpersonal interactions (e.g., using the phone while at dinner with friends or family) or being unsafe (e.g., texting while driving) (Bianchi & Phillips, 2005; Pinchot et al., 2011; Vahedi & Saiphoo, 2017; Yen et al., 2009).

Rozgonjuk et al. (2019) conducted research that shows that college students are addicted to their mobile devices because they have a fear of missing out. The findings revealed that daily life disruptions are led by students constantly checking their phones for updated content and actions that they believe require immediate responses. This frequency of checking the mobile device has correlated with detrimental effects on academic work.

The researchers note that there has been a major shift in literature from the original study in 2010 until today 2023. The literature in 2010 focused on the ways people were using their smartphones as compared to 2023 when a vast majority of the literature has shifted to dependency and addiction to the device. This change shows an acceptance of the technology but also a growing dependency on mobile devices to fulfill normal functions of our everyday lives.

3. METHODOLOGY

This study used an electronic survey (n=293) to survey smartphone users. The survey consisted of 30 quantitative questions: 20 that were taken from the authors' previous study (Pinchot, et.al, 2011) and 10 that were added for additional insight for this comparison study based on the review of the literature. Two of the 20 repeated questions were focused on demographics (age and gender), and 18 of the repeated questions were focused on understanding the mobile phone habits of participants.

These questions asked about scenarios such as whether the participant had ever answered a mobile phone at a funeral, in a place of worship, or while at lunch or dinner with friends. In addition, questions were asked about phone communication preferences, such as whether the participant preferred voice calls or text messages, and how the participant received the majority of their phone communications – landline, mobile phone via voice call, or text messaging. Further, they asked whether the participant found it rude if someone took a phone call while they were speaking or meeting with the participant.

The authors' original study was conducted in 2010 when mobile phone usage was still relatively new. (Pinchot, et.al, 2011). The iPhone was released in 2007, with Android following in 2008. App stores were only released for both platforms in 2008 as well, so mobile phone usage was still new in many ways. The 10 additional survey questions focused on updating the survey to include similar questions on phone communication preferences over a decade later, in 2023. For instance, a question in the original survey that asked whether the participant had ever used a phone while driving was revised into four questions that distinguished between using a phone in hand vs. hands-free while driving, or texting in hand vs. hands-free while driving. Other updated behavioral questions were also added including whether the participant ever talks on speakerphone while in public or finds it rude if others have the speaker on while talking on the phone in public. More direct questions were also asked such as whether the participant believes it is socially acceptable to use a mobile phone in public and if the participant could make it through the day without using or checking their phone.

The sample (n=293) for the study included adults aged 18 and older who have used a mobile phone. A total of 319 people started the survey, but 293 (92%) participants completed usable surveys.

The survey used in this study was created in Question Pro and posted on Amazon Mechanical Turk (MTurk) for data collection in July 2023, with approval from the university Institutional Review Board. MTurk is a crowdsourcing tool that has been widely used by academic researchers for survey research (Lovett, 2018; Redmiles et al., 2019).

4. RESULTS

Of the participants who completed the survey (n=293), 55% (160) identified their gender as male, 45% (131) female, and .3% (1) non-binary. Of the 293 participants, 161 were between the ages of 30-39, 53 were 18-29, 45 were 40-49, 20 were 50-59, and 14 were 60 or over. The age breakdown is illustrated in Table 1.

Age Range	No. of Participants	Percentage
18-29	53	18.1%
30-39	161	54.9%
40-49	45	15.4%
50-59	20	6.8%
60 +	14	4.8%

Table 1: Participants by age

The research question for this study was:

RQ1: In what ways has social acceptance of mobile phone use changed from 2010 to 2023?

The following results compare the findings from the 2010 study to the current study. The first set of questions asked participants whether they had answered their mobile phone in several different social situations. The results from this set of questions are shown in Table 2.

The authors chose these questions to represent social situations where it would be questionable as to whether it is socially acceptable to answer a mobile phone. Several social situations decreased, including in a store, sporting event, and having a meal with friends. But the majority of categories saw an increase in usage of mobile phones in these social situations, including in a meeting and in a classroom. Major increases in percentage were seen for some of the most controversial social situations, including in a movie theatre, in a place of worship, and at a funeral.

Have you answered your mobile phone:	2010	2023	% Change
In a store	99%	94%	-%5
In a meeting	42%	56%	+14%
In a classroom	33%	48%	+15%
At a sporting event	86%	67%	-19%
At a meal with friends	91%	86%	-5%
In a movie theatre	18%	72%	+54%
In a place of worship	11%	46%	+35%
At a funeral	11%	60%	+49%

Table 2: Comparison of participants' use of mobile phones in various social situations

Behaviors and Opinions	2010	2023	% Change
Talk on mobile phone regularly in public places	73%	95%	+22%
Believe it is socially acceptable to talk on your mobile phone in public	-	87%	-
Taken a work call while on vacation	73%	89%	+16%
Use texting as a form of communication	93%	88%	-5%
Prefer texting to making a phone call	53%	92%	+39%

Table 3: Comparison of participants' mobile phone behaviors or opinions

The next set of questions asked about behaviors when using mobile phones, and the results are shown in Table 3. First, participants were asked if they talked regularly on their mobile phones in public places. In 2010, 73% of participants indicated that they did, and in 2023, this percentage has increased by 22%. This indicates a clear majority participating in this behavior, with 95% of participants in the current study noting that they talk on the phone regularly in public places. In the current study, participants were also asked whether they believe it is socially acceptable to talk on their mobile phone in public. The majority, 87%, answered yes, while only 13% answered no. These results point to a cultural shift where it is now socially acceptable to talk on mobile phones in public places.

Further, a majority of participants in both studies have taken a work call while on vacation, 73% in 2010 and 89% in 2023. This increase in willingness to take work-related calls while on vacation serves as evidence that there are blurred lines between work and private life, and could indicate potential problems with work-life balance.

Finally, in this section, participants were also asked if they use text messaging as a form of communication and if they prefer texting to making a phone call. There was a slight decrease (-5%) from 2010 to 2023 in participants who noted that they use text messaging. While this result is a bit surprising, there could be other reasons that this response decreased. For instance, many people use social media apps for text or video communication in 2023 and may not consider these communication methods as text messaging. Further, there was a large increase in responses between the studies (+39%) when participants were asked whether they preferred texting to making a phone call. In 2010, 53% preferred texting and in 2023, 92% preferred texting. With this increase, it is clear that text messaging is a preferred method of communication in 2023.

Receive the majority of phone communications by:	2010	2023	% Change
Mobile phone via voice	75%	71%	-4%
Text message	16%	21%	+5%
Landline	9%	7%	-2%

Table 4: Comparison of participants' primary phone communication methods

The next set of questions probed deeper into how participants communicate using their mobile phones by asking whether they receive the majority of their phone communications via voice calls on a mobile phone, text messages, or on a landline. The majority of participants indicated that they receive most communications via voice calls on a mobile phone (75% in 2010 and 71% in 2023), while a fair number of participants indicated they receive most communications via text messaging (16% in 2010 and 21% in 2023), and a consistently low number indicated their majority of communications are received via landlines (9% in 2010 and 7% in 2023). Table 4 shows the differences in responses between the two studies.

Another set of questions delved into the usage of mobile phones while driving. Talking on the phone and texting while driving can be extremely dangerous and are illegal in most U.S. states without the use of hands-free technology. Hands-free technology was not prevalent in use in 2010, and only the current study asked participants if they used this technology while driving.

Based on the responses, shown in Table 5, there has been a dramatic decrease (-40%) in talking on the phone while driving from 2010 to 2023 (without hands-free technology). However, 51% is still an alarmingly high percentage for participants to indicate they participate in this dangerous behavior. Similarly, there was very little change for texting on a mobile phone while driving from 2010 to 2023 (+1%). This result (50% in 2010 and 51% in 2023) also indicates that more than half of the participants text while driving, which is concerning because studies have shown that driving while texting may be more dangerous than driving under the influence of alcohol (Madden & Lenhart, 2009).

While Driving:	2010	2023	% Change
Talk on phone	91%	51%	-40%
Talk on phone (hands-free)	-	58%	-
Text on phone	50%	51%	+1%
Text on phone (hands-free)	-	51%	-

Table 5: Comparison of participants' mobile phone use habits while driving

The 2010 study asked participants whether they thought it was rude if someone took a phone call while meeting or speaking with them. This question was repeated in the current study and the results were very close, with 63% responding that they think it's rude in 2010 and 67% responding that they believe it's rude in 2023, a difference of only 4%. Two additional questions in this same area were added for the 2023 study. Participants were asked if they talked on speaker phone while in public. Of the respondents, 67% indicated that they do use speaker phone in public. Further, they were asked if they think it's rude if someone talks on speaker phone in public and 62% indicated that they find it rude. This is an interesting result that seems to indicate that while the majority of people find it rude when someone talks on speaker phone in public, they still participate in this activity.

Another new question asked in the current study focused on whether the participant had ever been out to a meal with friends where everyone at the table was on their mobile phone. In 2023, 79% of participants said they had experienced this situation, while only 21% had not. The final new question in the current study asked if the participant could make it through the day without using or checking their mobile phone. The majority of participants, 65%, responded yes, while 35% answered no.

In the 2010 study, there were several statistically significant relationships found between age and various behaviors and opinions about mobile phones. For instance, significance was found between age and each of the following: (1) preferring text over voice calls, (2) number of texts sent on average each day, (3) taking a work-related phone call while on vacation, and (4) whether or not the participant felt that it was rude to be interrupted by a phone call when meeting with someone. In the current study, there were no significant relationships found between age and any of the various behaviors and opinions about mobile phones.

5. DISCUSSION

This study sought to determine how mobile phone acceptance and users' perceptions of socially acceptable styles of communication using mobile phones have changed from 2010 to 2023. In their original study, the authors found that standards of behavior in regard to use of mobile phones in various social settings were changing. Prior to the rise of mobile phone usage, there were different cultural standards that allowed for less interruption in places like meetings, movie theatres, places of worship, funerals, or even just meals with friends. In 2010, those cultural norms were changing as more and more people started to use their mobile phones for calls and texts while in those primary social situations (Pinchot, et.al, 2011).

Additionally, in the original study, a number of significant relationships were found between age and mobile phone usage behaviors and opinions. It was clear in that study that younger people were more likely to send more text messages on average per day and to prefer texting over voice calls. They were also more likely to take work-related phone calls while on vacation. Interestingly, younger people were also more likely to find it rude for someone to take a phone call when meeting with someone (Pinchot, et.al, 2011).

In the 2023 study, the participants showed no significant difference in how age groups use mobile phones in social situations. This shows a clear difference from 2010 when younger people were more likely to use mobile phones and prefer text messaging. In 2023, people of all age groups use mobile phones regularly, and the majority of participants in this study prefer texting over voice calls even though they still receive the majority of their phone communication via voice calls on their mobile device.

Phone habits while driving have also changed over the past decade. In the original study, 91% of the participants said they talked on the phone while driving, holding the device. In the current study, this percentage has dropped to 51%, though this number is still alarmingly high for such a dangerous activity. Likewise, texting while driving, holding the device, was at 50% in 2010 and has held steady at 51% in 2023. The participants in the current study also noted that they use hands-free technology to both talk on the phone while driving (58%) and text while driving (51%). While this is generally regarded to be safer behavior, studies have also shown that any kind of mobile phone use, whether hands-free or not, can impact safety due to driver distraction (Lipovac et al., 2017).

This study sought to answer the research question: In what ways has social acceptance of mobile phone use changed from 2010 to 2023? The answer to that question seems clear. All social situations appear to be fair game for use of mobile phones, including settings such as places of worship or funerals which used to be places where most people would refrain from using their devices. Even though the 2023 study shows that people still find it rude when others take a call while speaking to them or talk on their speaker phone while in public, they do find using mobile phones in public to be socially acceptable. The majority even engage in some of those rude behaviors themselves.

The literature provides support for the idea that mobile phones have become a necessary utility for people in their daily lives, akin to their wallets and keys (Emanuel et al., 2015). Given more time, the mobile phone may even surpass the wallet and keys in importance and become the one daily utility that people need. Phones can already use apps to serve as a key for a digital lock on cars (Wardlaw, 2020) and hotel rooms (Dans, 2019), and they can also serve as a wallet for contactless mobile payments (Seiber, 2021).

It would be remiss not to mention the impact of the COVID-19 pandemic on the role of mobile devices over the past decade, as this study looks at the time period between 2010 to 2023, which includes the pandemic which started in 2020. For instance, there was a significant leap forward in the adoption of contactless mobile payments between 2020 and 2023, with 69% of retailers noting that they saw an increase during the pandemic (Seiber, 2021). The appeal of the contactless nature of the transaction was likely the driving factor in this increase in adoption.

Further, mobile devices became a primary source of support, comfort, and communication for people during the COVID-19 pandemic, when most people spent a significant amount of time quarantined in their homes (de Souza e Silva & Xiong-Gum, 2023). Many adults now use their mobile phones to help pass the time or relieve stress in situations where they would not have been used before, what Meluman and Pham (2020) call an "adult pacifier."

Due to the ubiquity of smartphones, the increased adoption of mobile phone use for more tasks and types of communication during the pandemic, and the shift in cultural acceptability of mobile phone use in various social settings as described by this study, it is clear that our culture has accepted the mobile phone as a daily utility.

6. LIMITATIONS

This research sought to compare the results of a survey on mobile phone communication behaviors and user perceptions about mobile phone usage in a comparison study between responses obtained in 2010 and then again in 2023. In the 2010 study, the sample was much smaller (n=88), and was obtained through convenience sampling of university students. In the current study, the sample was larger (n=293), but was obtained via Amazon MTurk. The respondents from MTurk were not limited to university students, which could limit the comparison.

7. CONCLUSIONS

Mobile phones have clearly provided modern conveniences, not the least of which is being the ability to stay in touch with family, friends, and work colleagues from anywhere around the globe. With the ubiquity of mobile phones and the continued growing usage of mobile apps, contactless mobile payments, and other mobile device technology, it would arguably be difficult in modern society to survive without a mobile phone. However, with the great power of mobile phone technology comes great responsibility. While many enjoy the benefits of mobile phones, there is a growing concern in regard to mobile phone dependence and addiction (Melumad et al., 2019; Rozgoniuk et al., 2019; Alter, 2017; Fullwood et al., 2017; Wilmer et al., 2017) and a continued impact on work-life balance (Arokiasamy & Fadzil, 2022; Schmucker, 2022).

Given the potential social and mental health problems that could be caused by overuse of mobile phones, more study is needed to determine the best path forward for responsible and healthy use of mobile phones.

8. REFERENCES

Al-Barashdi, H., Bouazza, A., & Jabur, N. (2015). Smartphone addiction among university undergraduates: A literature review. *Journal of Scientific Research and Reports, Vol. 4, no. 3*, pp. 210-225

Albrecht, U., Kirschner, N.E., & Grusser, S.M. (2007). Diagnostic instruments for behavioural addiction: An overview. *GMS Psycho-Social Medicine, 4*. Document 11

Alter, Adam (2017). Irresistible: The rise of addictive technology and the business of keeping us hooked. *New York: Penguin Press*

Arokiasamy, L., & Fadzil, A.F. (2022). Mobile technology use, work-life balance and employee's productivity: A literature review. *International Journal of Early Childhood Special Education, 14*(3), 248-266.

Beranuy, M., Chamarro, A., Graner, C., & Carbonell, X. (2009). Validation of two short scales to assess Internet addition and mobile abuse. *Psicothema, 21*-480-485.

Bianchi, A., & Phillips, J.G. (2005). Psychological predictors of problem mobile phone use. *CyberPsychology & Behavior, 8 (1),* 39-51

Centers for Disease Control and Prevention (2022). National health interview survey.

Retrieved from https://www.cdc.gov/nchs/nhis/releases.htm#wireless

Dans, E. (2019). Another use for the smartphone: Checking into a hotel. *Forbes.* https://www.forbes.com/sites/enriquedans/2019/07/29/another-use-for-the-smartphone-checking-into-ahotel/?sh=656f3aae26a1

De Souza e Silva, A., & Xiong-Gum, M. (2023). COVID-19 now and then: Reflections on mobile communication and the pandemic. *Mobile Media & Communication, 11*(2), 140-155.

Eadicicco, L. (2017). This is why the iPhone upended the tech industry. *Time*. https://time.com/4837176/iphone-10th-anniversary/

Emanuel, R., Bell, R., Cotton, C., Craig, J., Drummond, D., Gibson, S., Harris, A., Harris, M., Hatcher-Vance, C., Jones, S.m, Lewis, J., Longmire, T., Nash, B., Ryans, T., Tyre, E., Walters, D., & Williams, A. (2015). The truth about smartphone addiction. *College Student Journal, 49 (2*), 291-299

Fook, C.Y., Narasuman, S., Azia, N.A., Mustafa, S.M.S., Han C. T. (2021). Smartphone usage among university students. *Asian Journal of University Education (AJUE) Vol 17, No. 1*

Fullwood, C., Quinn, S., Kaye. L.K., & Redding, C. (2017). My virtual friend: A qualitative analysis of the attitudes and experiences of smartphone users: Implications for smartphone attachment. *Computers in Human Behaviou, 75*, 347-55

Kaysi, F., Yavuz, M., & Aydemir, E. (2021). Investigation of university students' smartphone usage levels and effects. *International Journal of Technology in Education and Science (IJTES), 5(3),* 411-426

King, A.L.S., Valenca, A.M., Silva, A.C., Sancassiani, F., Machado, S., & Nardi, A. E. (2014). Nomophobia: impact of cell phone use interfacing with symptoms and emotions of individuals with panic disorder compared with a control group. *Clinical practice and epidemiology in mental health: CP & EMH, 10, 28*

Lipovac, K., Deric, M., Tesic, M., Andric, Z., & Maric, B. (2017). Mobile phone use while driving – literary review. *Transportation Research Part F: Traffic Pyschology and Behaviour, 47*, 132-142.

Lovett, M., Bajaba, S., Lovett, M., & Simmering, M. (2018). Data quality from crowdsourced surveys: A mixed method inquiry into perceptions of Amazon's Mechanical Turk Masters. *Applied Psychology, 67*(2), 339-366. doi: 10.1111/apps.12124

Madden, M. & Lenhart, A. (2009, November 6) Teens and distracted driving. *Pew Internet & American Life Project*,

Matyszczyk, C. (2009, February 26). Facebook entry gets office worker fired. *CNET News*.

Melumad, S, Inman, J.J., & Pham, M.T. (2019). Selectively emotional: How smartphone use changes user-generated content. *Journal of Marketing Research, 56(2),* 259-275

Melumad, S. & Pham, M.T. (2020). The smartphone as a pacifying technology. *Journal of Consumer Research, Vol 47, Issue 2.* pp. 237-255

Ozkan, M., & Solmaz, B. (2015). Mobile addiction of generation Z and its effects on their social lives. *Prodecia – Social and Behavioral Sciences, Vol. 205*, pp. 92-98

Pew Research Center (2022). Mobile fact sheet. Retrieved from https://www.pewresearch.org/internet/fact-sheet/mobile/

Pinchot, J., Paullet, K., & Rota, D. (2011). How mobile technology is changing our culture. *Journal of Information Systems Applied Research (JISAR).* April 2011

Redmiles, E.M., Kross, S., & Mazurek, M.L. (2019). How well do my results generalize? Comparing security and privacy survey results from MTurk, web, and telephone samples. *2019 IEEE Symposium on Security and Privacy*, 1326-1343.

Rozgonjuk, D., Elhai, J.D., Ryan, T., & Scott, G.G. (2019). Fear of missing out is associated with disrupted activities from receiving smartphone notifications and surface learning in college students. *Computers & Education, 140*: 103590.

Schmucker, R. (2022). Blurring of boundaries in work's 'new normal'. *Social Europe*

Seiber, S. (2021). How the pandemic changed mobile payments. *Forbes.* ps://www.forbes.com/sites/scarlettsieber/2021/08/27/how-the-pandemic-changed-mobile-payments/?sh=9a9d84315459

Sondergaard, A., (2009, September 2). People are getting fired because of Facebook.

Statista (2022). Smartphones in the U.S. – statistics & facts. Retrieved from https://www.statista.com/topics/2711/us-smartphone-market/#topicOverview

Tosell, C., Kortum, P., Shepard, C., Rahmati, A., & Zhong, L. (2015). Exploring smartphone addiction: insights from long-term telemetric behavioral measures. *Int J Interact Mob Technol, 9, 37-43*

Vanhedi, Z., & Saiphoo, A. (2017). The association between smartphone use, stress, and anxiety: A metanalytic review. *Stress and Health, 34 (3),* 347-58

Wardlaw, C. (2020). What is a digital key for a car? *J.D. Power.* https://www.jdpower.com/cars/shopping-guides/what-is-a-digital-key-for-a-car

Wilmer, H.H. Sherman, L.E., & Chein, J.M. (2017). Smartphones and cognition: A review of research exploring the lins between mobile technology habits and cognitive functioning. *Frontiers in Psychology, 8*, 605

Yen, J., Ko, C., Yen, C., Cheng-Sheng, C. Cheng-Sheng, C. (2009). The association between harmful alcohol use and internet addiction among college students: Comparison of personality. *Psychiatry and Clinical Neurosciences, 63 (2*), 218-24

Yildirim, C., & Correia, A.P. (2015). Exploring the dimensions of nomophobia: Development and validation of a self-reported questionnaire. *Computers in Human Behavior, 49*,130-137.