Contemporary Mathematics
http://ojs.wiserpub.com/index.php/CM/

UNIVERSAL WISER PUBLISHER

Research Article

Identifying Fake Digital Information Using Machine Learning Algorithms: Performance Analysis and Recommendation System

Ashish Patel[1], Yogesh Jadhav[2], Rutvij Jhaveri[3*], Roshani Raut[4], Faisal Mohammed Alotaibi[5], Dhavalkumar Thakker[6]

[1]Department of Computer Engineering, SVM Institute of Technology, Bharuch, India
[2]Computer Engineering, School of Technology Management and Engineering, SVKM's NMIMS University, Navi Mumbai, India
[3]Pandit Deendayal Energy University, Gandhinagar, India
[4]Pimpri Chinchwad College of Engineering, Savitribai Phule Pune University, Pune, India
[5]University of Liverpool, Liverpool, United Kingdom
[6]School of Computer Science, University of Hull, United Kingdom
Email: rutvij.jhaveri@sot.pdpu.ac.in

Received: 15 April 2023; **Revised:** 7 May 2023; **Accepted:** 26 May 2023

Abstract: This work focuses on the detection of fake digital information using various machine learning and deep learning algorithms to prevent its spread through Internet of Things (IoT) devices and systems. The research highlights the significance of detecting and preventing false or misleading information in critical areas such as healthcare, public safety, and emergency response. The study compares the performance of several supervised machine learning algorithms and identifies logistic regression as the most accurate (98.03%). The empirical analysis used data from The Indian Express, PolitiFact, and Kaggle and leveraged natural language processing (NLP) to prepare, clean, and model the data. To detect fraudulent posts, the study employed random forest, a supervised machine learning algorithm, which achieved an impressive accuracy rate of 99.71% on a Kaggle dataset. The research also developed a model for detecting false reporting related to COVID-19, utilizing the support vector machine technique, which achieved an accuracy rate of 78.69%. The presented work also determined the authenticity of images through convolutional neural networks (CNNs). Lastly, a content-based recommendation system was developed to enhance people's security and confidence.

***Keywords*:** COVID-19, deep learning, Google Colab, image processing, Kaggle

MSC: 92B20, 93C41, 93C62, 93C95

1. Introduction

From an Internet of Things (IoT) perspective, the proliferation of "fake news" can have severe consequences for connected devices and systems. Misinformation, defined as inaccurate or incorrect information unintentionally made or distributed, can spread rapidly through IoT devices, leading to false assumptions and misguided actions [1, 2]. Meanwhile, the intentional creation and dissemination of disinformation can manipulate public opinion and obstruct factual evidence, potentially causing damage to the IoT system's trust and the government's ability to make informed decisions. In such cases, it becomes crucial to employ techniques like fake digital information detection to prevent the

DOI: https://doi.org/10.37256/cm.4420232851

spread of false or misleading information through IoT devices, ensuring that decisions are based on accurate and factual evidence [3, 4]. Misinformation and disinformation can be broken down into seven distinct categories, which are as follows:

1. Satire or parody: The use of satire or parody is risky, even though the author does not intend to cause harm to anyone.
2. Misleading content: Misleading content is characterized by the inappropriate use of facts to present a topic or a person in an unfavorable light.
3. Imposter content: Imposter content is created when genuine sources are misrepresented as being something else.
4. Fabricated content: Recently fabricated content is wholly untrue, and its creators intend it to mislead and harm people.
5. False connection: This is what happens when the headlines, photos, or captions do not adequately support the content.
6. Context: This occurs when authentic content is distributed together with contextualized fake information.
7. Manipulated content: It can be defined as changing truthful information or imagery to trick someone into believing something untrue.

Websites that specialize in creating or sensationalizing stories are frequently the ones responsible for the dissemination of fake news [5]. It often employs controversial and provocative headings. Its growth poses a significant obstacle to the functioning of democratic societies in the modern world [6]. Fact-checkers are people who investigate the claims made in the media to ensure that they are accurate. These professionals debunk false claims made in fake news by pointing out why they are false. The use of machine learning and natural language processing (NLP) techniques, as shown in [7, 8], can now be used to supplement the manual fact-checking procedure that has traditionally been used. An application of artificial intelligence known as machine learning allows a computer to learn independently without being specifically programmed to do so. It not only processes but also learns from the data. We provide machine learning with the dataset, and the software generates the algorithm independently. There are three different ways of acquiring knowledge: (i) supervised learning (ii) unsupervised learning (iii) reinforcement learning.

"What we see is what we believe". A person cannot readily think of a made-up truth without first validating it, which results in its dissemination to others. Individuals begin to feel something is proven only after it has been exposed several times, which explains the illusory truth effect. The repetition effect persuades us to think previously incorrect information is true; this is the impact's strength. The illusory truth effect is one of the factors that contributes to misleading news reports gaining traction and drawing an audience. [9, 10]

A tremendous amount of image data has been generated by social networking platforms such as Facebook and Instagram. GANs (generative adversarial networks) are a burgeoning topic in machine learning/artificial intelligence that generate a lot of fake images. Many people have fallen victim to picture counterfeiting using image and video processing software like GNU Gimp, Adobe Photoshop, etc. Fake news and mob provocation rely heavily on photos like this, which are excellent targets for malicious manipulation [11-13].

Several techniques for facial manipulation in videos, including deepfake and faceswap, have been developed in the last several years, allowing anyone to easily change faces in video sequences with amazingly realistic results and no effort [14-18]. Modern technology, powerful smartphone cameras, and the widespread availability of high-speed internet connections have enormously boosted social media's ever-growing reach. Technological advancements, increased network access, and improved peer-to-peer connectivity have simplified the creation and transmission of digital videos across media sharing platforms. Deep learning has become extremely powerful as processing power has increased, which was thought to be unachievable only a few years ago [19]. However, this disruptive technology has introduced some new obstacles. Free deep learning-based software tools have made it possible to create credible face exchanges in films that leave minimal indications of manipulation, dubbed deepfake (DF) videos or artificial intelligence-generated media. The proliferation of DF on social media platforms has resulted in spamming and the propagation of false information [20]. DF detection is critical for resolving such a problem.

Supervised learning entails training the model with labeled samples, after which the machine performs the task on unseen data [21-23]. Our study will utilize a supervised learning algorithm to detect bogus news. Supervised learning applies to two distinct sorts of problems: classification and regression [24-26]. In this endeavor, we classify news

as ‘false’ or ‘real’. The optimal classification method for the false news detector is chosen based on the maximum accuracy achieved after comparing various classification algorithms [27, 28]. An approach based on deep learning can successfully distinguish artificial intelligence-generated false videos (DF videos) from real videos [29-32]. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs) are used to identify DF. The system uses a CNN at the frame level to extract features from the CNN. These features are used to train a RNN that learns to classify whether a video has been manipulated or not and whether detection of temporal inconsistencies between frames introduced by the DF creation tools is possible [33-35].

1.1 *Motivation*

From Amazon to LinkedIn, Uber Eats to Spotify, and Netflix to Facebook, recommender systems are widely used to offer “similar things,” “related employment,” “preferred cuisines,” “interesting movies or series,” and “songs to try based on interest” to their customers. The number of press releases has expanded significantly, and it has become difficult for one to go through all online news resources in search of relevant news stories. Search engines assist consumers in navigating the massive amounts of information available online. Since then, recommendation systems have evolved to address various issues and provide users with information relevant to their requirements, either based on their preferences or on content similarity [36-38]. Each online news publisher controls its content and employs various strategies to propose stories to users based on shared interests. In a very dynamic environment, it becomes difficult to propose news articles due to various obstacles, including frequent changes in the set of news articles, the set of users, and rapid changes in user preferences. As a result, recommendation systems must be capable of continuously processing incoming news streams in real-time [39, 40]. There are two kinds of recommendation methods:

- Content-based recommendation
- Collaborative filtering

A content-based recommendation system uses similarities between users or objects as determined by their qualities [41-43]. It uses additional information (metadata) about people or products, i.e., it uses already-existing content. This metadata may include the user’s age, gender, occupation, location, and skill sets. It comprises the item’s name, specs, category, and registration date. In this article, we develop a content-based recommendation system to recommend news articles comparable to previously read articles based on article headline, category, author, and publishing date [44, 45].

1.2 *Contribution*

In this paper, we provide the results of an empirical study to identify fake news, as shown in Figure 1. The accuracy of the detection has been measured using a variety of machine learning and deep learning methodologies. Immediately after detecting fake information, we introduced the concept of a recommended system. This approach boosts the user’s confidence when working with digital media, which is beneficial. The key contributions to this work are:

- We propose an intelligent approach to dealing with fake digital information.
- We conduct experiments to evaluate our approach to detecting fabricated news stories, job listings, COVID-19 information, and manipulated images online.
- We propose a trustworthy recommendation system to increase users’ confidence in consuming digital media online.

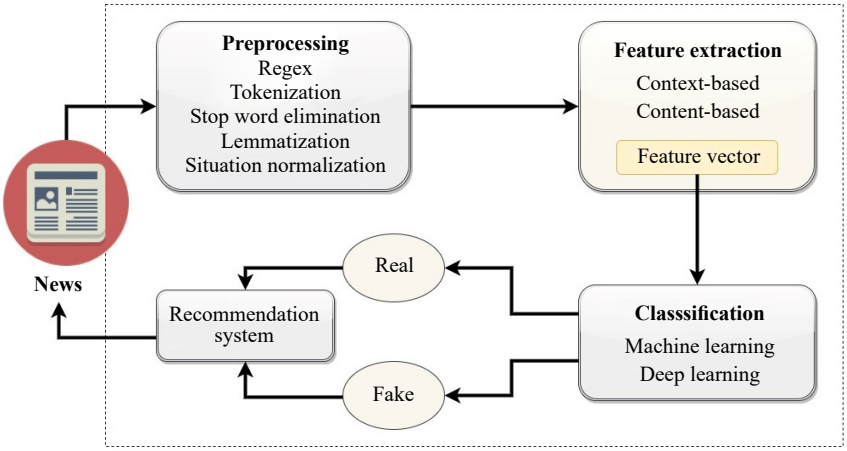

Figure 1. Fake news detection and recommendation approach

1.3 *Outline*

The organization of the paper is as follows: the first section overviews bogus digital information, its influence on society, and work requirements. The second section of the article describes the current condition of the field. Section 3 provides a detailed evaluation of the empirical inquiry. The fourth section addresses the analysis of the empirical study's results. Section 5 suggests a method for suggesting to the user that they maintain their faith while ingesting digital information. Section 6 concludes with a synopsis of the work and its potential scope.

2. Related work

A significant number of academics have made important contributions to the ongoing quest to locate and recognize reliable sources of digital information. In this section, we will talk about the numerous reviews that have been done and the research proposals that have been suggested by a variety of experts. Articles were obtained and examined from both online and offline archives using keywords such as fake news, bogus COVID-19 articles, fraudulent job advertisements, fake photos, and recommendation algorithms from the fake digital information domain.

Kesarwani at el. [46] demonstrated a straightforward method for detecting fake news on social media using the K-Nearest Neighbor (KNN) classifier, with a 79% accuracy rate. The KNN algorithm is a supervised machine learning algorithm that addresses classification and regression issues. The article attempts to assess fake news using the KNN classification algorithm by collecting users' implicit and explicit n characteristics across many dimensions. According to the article, KNN becomes slower as the model size increases. As indicated in the paper, the dataset for the model was obtained from Buzz Feed News (BFN), and it was utilized to train and test the model in this research. BFN uses the social analytics platform BuzzSumo to determine the best-performing Facebook content among 167 websites that post articles consistently. This dataset collected data on Facebook posts, each representing a news article. The authors culled these news pieces from Politico, ABC News, and CNN. The dataset contained the following four categories: "mainly true," "primarily false," "combination of true and false," and "no factual material." Apart from this, information on user social activity is collected via the Facebook API (application programming interface), including the number of shares, comments, and reactions to each post. After testing the model with various values of K, the study determined that the value of K provided the greatest accuracy. On the test set, the proposal achieved an approximate 79% classification accuracy for this model. The model's average weight precision was 0.75, and its recall was 0.79. This article offered a framework for predicting bogus news on social media. The method of extracting features from datasets was deemed critical due to their application in the data mining algorithm KNN for classifying news articles on social media.

The purpose of [47] is to categorize news stories as genuine or fabricated. The authors identify fake news using various models and classifiers and then forecast the model's accuracy using the Kaggle dataset. They constructed models using NLP, machine learning, and deep learning approaches and compared them to ensure optimum accuracy. The study analyzed results swiftly using an Nvidia DGX-1 supercomputer. This investigation examined several different models,

including CNN, KNN, LSTM (long short-term memory), decision tree, random forest, and naive Bayes theorem, as well as deep learning networks, including shallow convolutional neural networks (SCNNs), very deep convolutional neural networks (VDCNNs), LSTM networks, gated recurrent unit (GRU) networks, and a combination of CNNs with LSTM (CNN-LS; CNN-GRU). We investigated feature extraction and features such as the n-gram. The model was constructed using term frequency-inverse document frequency (TF-IDF) features that were extracted. Additionally, they discovered features such as word embedding and word2vec in deep neural networks. For feature extraction in the machine learning model, the proposal used pick k best and chi^2.

The study presented by [48] develops a model for classifying Instagram photographs in order to identify potential threats and fake images. The model is constructed utilizing deep learning methods, CNNs, the AlexNet network, and AlexNet transfer learning. According to the findings model, the AlexNet network had a higher accuracy rate of 97% than the other networks. This research presents a method for classifying images by taking them as input and classifying them using a practical system (the CNN model). The training phase will use a label or classification assigned to the input sample. Two tags are used: one for the original image class and another for the fictitious image class. The target photographs were collected from the Instagram program, and they represent the dataset, which is necessary to answer the research questions, test the hypothesis, and evaluate the results. The convolutional layer was developed with typical mathematical methods to extract visual features. These convolutional processes operate as two-dimensional digital filters. Following that, the activation function was created. Because picture data is nonlinear, a nonlinear activation function called the Rectified Linear Unit (ReLU) was applied. A technique called max pooling was used to minimize the array's size.

The authors of [49] presented a solution for detecting misleading information about COVID-19. A model is developed using World Health Organization (WHO), United Nations International Children's Emergency Fund (UNICEF), and United Nations data. The study constructed a voting ensemble classifier using seven feature extraction approaches and ten distinct machine-learning algorithms. To ensure the validity of the acquired data, the proposal used fivefold cross-validation and then produced an evaluation technique. The detection technique used ensemble learning to train ten machine learning classifiers on the acquired ground truth data. The author collected COVID-19 ground truth by scraping the websites of the WHO and its regional branches, UNICEF, related organizations, and the United Nations. It gathered all information about the COVID-19 outbreak from these organizations' daily situation updates, the WHO Director-General's briefing on COVID-19, and news published in their newsrooms on their websites. The Google Fact Check Tools API was used, which enables users to browse and search for facts from a variety of fact-checking websites worldwide, including opensecrets.org, snopes.com, factcheck.afp.com, washingtonpost.com, factcheck.org, and politifact.com. The results established the veracity of the gathered ground truth data and yielded favorable results. The neural networks, decision trees, and logistic regression classifiers produced the best results in the empirical study. Another good study about COVID-19-related analysis can be found in [50].

The article [51] described a new deep-learning method that can distinguish AI-generated fake videos from real videos. To detect the DF, it is necessary to grasp the GAN. GAN is fed a video and an image of a specific target. It generates further films in which the target's face is replaced by another individual who serves as a source. GAN divides video into frames and outputs the input image at the end of each frame. Additionally, it reconstructs and utilizes additional autoencoders. Due to resource constraints and production time constraints, the DF method can only generate face images of a given size. They must undergo affinal warping in order to match the source's face configuration. The approach discussed here detects such abnormalities by dividing the movie into frames and comparing the resulting face regions to their surrounding areas. The features are then extracted using a ResNExt CNN, a RNN with LSTM, and by recording the GAN-induced temporal discrepancies between frames. It uploaded and classified videos using a web-based platform; the primary purpose was to assess performance, security, user friendliness, correctness, and reliability [52-54].

The primary goal of [55] was to determine whether or not a job posting was phony using the Kaggle dataset. There were 17,880 job postings in the dataset. Prior to using this data in the classifier, it is pre-processed to eliminate stop words, superfluous attributes, and excessive spaces. The decision tree classifier outperformed the naive Bayes, multi-layer perceptron, and KNN classifiers. The technique evaluated the ensemble approach method in order to determine whether it might improve the model's performance or not. We implement and compare random tree classifiers, AdaBoost classifiers, and Gradient Boost classifiers. The investigation demonstrated that the random tree classifier outperformed

the others. The random forest classifier achieved an accuracy of 98.27%, a Cohen-Kappa score of 0.74, an $F1$-score of 0.97, and an a mean squared error (MSE) of 0.02, indicating that it was the most accurate approach.

In its simplest form, a metadata analyzer is a tag search algorithm. Assume that terms such as Photoshop, Gimp, and Adobe are discovered in the text, maybe at a higher rate. The technique provided in [56] resulted in the creation of two distinct variables, dubbed fakeness and realness. Each variable describes the probability of an image being genuine or a forgery. After the tag is assigned, it is assessed, and the relevant variables are incremented by a specified weight. Metadata analysis revealed encouraging results in the field of non-shared photos. Under minimal processing, it can detect anomalies in all 'photoshopped' photographs. However, it did not work with pictures posted on WhatsApp, Google+, or other social media platforms. When the system provides photos with modified metadata, it generates an error. They trained the neural network successfully, utilizing error-level analysis on 4,000 fake and 4,000 true photos. The image was classified as false or real using a neural network trained to a maximum success rate of 83 percent. Using this program on mobile devices will almost certainly result in a decrease in the propagation of fraudulent photographs via social media. A reliable false picture identification algorithm is created and evaluated by combining metadata analysis (40%), neural network output (40%), and findings (60%). The concept used in [57] explored the malicious URL detection method.

The system they develop in [58] learns from sentences how to identify bogus news. The initial step was to amass datasets. They gathered data from a variety of online sites. The acquired data was then labeled training data. 30% of that data was used for validation purposes. The data was then processed using the processes detailed in the flowchart below. Following the implementation of the method, the data were further processed using the bidirectional LSTM model. Two stages are required for the bi-LSTM architecture. In the first stage, after encoding headlines and bodies into input before passing them to the classifier based on terms that have been sub-worded, 28 headlines will be entered based on the largest number of words in the real headline. Simultaneously, 1,000 words will be fed into the body to ensure that it does not consume an excessive amount of memory. It retains the article's text, with a vector dimension of 300 for each word entered in the headline or news body. They then utilized a Softmax activation function to determine class opportunities in the second stage.

According to the observed findings in [59], KNN is the weakest algorithm in terms of predictive capacity, with a mean accuracy of 75% (EN-English), 89% (PT-Portuguese), and 75% (ES-Spanish). The ensemble algorithms random forest and extreme gradient boosting (XGB) produced comparable and steady results, with random forest achieving 79.9% (EN), 93.9% (PT), and 82.3% (ES), while XGB achieved 80.3% (EN), 94.7% (PT), and 82.3% (ES). Support vector machines showed the second-worst prediction performance on EN (79%) but the highest on PT (95%) and tied with ensemble algorithms on ES (82%). According to the results, the PT and ES collections are more linearly separable than the EN collection, with PT exhibiting slightly more linear behavior. Identifying false news is crucial in light of the increased news consumption via online social media (OSM), which allows for unregulated content streaming. Due to the rapid expansion of OSM, detection requires an automated method. The concept proposed a comparative examination of language-independent characteristics, stylometric complexity, and psychological types in a multilingual setting.

3. Empirical study: Fake information detection

The following sections detail the procedures we took to identify fake news. The step-by-step explanation will assist readers in comprehending the use of machine learning algorithms.

3.1 *Data collection, assembling, and platform*

A web scraper was used for the collection of data. The dataset for fake news detection was made by scraping data from websites like PolitiFact and The Indian Express. GitHub was also used for obtaining data. Data collected from various sources was arranged together depending on the four columns for fake news detection, which were title, author, text, and label. Google Colaboratory (Colab) Notebooks were used for the implementation of our model. For performing deep learning tasks, Google Colab has proven to be an excellent tool. It is a hosted Jupyter notebook that requires no setup and has an excellent free version, giving free access to Google computing resources such as GPUs and TPUs.

3.2 *Importing libraries*

Our model made use of the Natural Language Toolkit (NLTK), Pandas, NumPy, Matplotlib, Wordcloud, Regex, and Sklearn packages. NLTK provides a systematic foundation for developing systematic Python programs for working with human language data. The interfaces include over 50 corpora and lexical resources, such as WordNet, as well as text-processing libraries for classification, tokenization, stemming, lemmatization, tagging, parsing, and semantic reasoning wrappers. Pandas is a tool for manipulating large amounts of data at a high level. Constructed using the NumPy package and utilizing the DataFrame as the primary data structure.

The NumPy library contains multidimensional array objects and a plethora of algorithms for processing them (Numerical Python). NumPy is used to conduct mathematical and logical operations on arrays. Matplotlib is a powerful Python package that enables the creation of static, interactive, and animated displays. We created a data visualization using WordCloud to represent textual data. This library aids in visualizing the significance of each word based on its size, which corresponds to its frequency in the dataset. Regular expressions (abbreviated REs, regexes, or regex patterns) are a small, highly specialized computer language that is integrated into Python and imported via the re-module. It is a string that has a sequence of characters that defines a search pattern. It can be used to determine whether a string contains the defined search pattern. Scikit-learn (Sklearn) is the most efficient library, providing a well-organized collection of methods for machine learning and statistical modeling, including classification, regression, clustering, and dimensionality reduction, via a logical Python interface.

3.3 *Information about the datasets*

Kaggle is used to provide a comprehensive training dataset with the following attributes: (i) id: a unique identifier for a news item, (ii) title: a news article's title, (iii) author: the news article's author, and (iv) text: the article's text; it may be incomplete. The training dataset is 20,800 rows long and has five columns, whereas the testing dataset is 5,988 rows long and has four columns. A label of 1 in training data indicates that the news is authentic, whereas a label of 0 suggests that the item is false, as illustrated in Figure 2.

```
1 train.head()
```

	id	title	author	text	label
0	0	House Dem Aide: We Didn't Even See Comey's Let...	Darrell Lucus	House Dem Aide: We Didn't Even See Comey's Let...	1
1	1	FLYNN: Hillary Clinton, Big Woman on Campus - ...	Daniel J. Flynn	Ever get the feeling your life circles the rou...	0
2	2	Why the Truth Might Get You Fired	Consortiumnews.com	Why the Truth Might Get You Fired October 29, ...	1
3	3	15 Civilians Killed In Single US Airstrike Hav...	Jessica Purkiss	Videos 15 Civilians Killed In Single US Airstr...	1
4	4	Iranian woman jailed for fictional unpublished...	Howard Portnoy	Print \nAn Iranian woman has been sentenced to...	1

```
1 test.head()
```

	id	title	author	text
0	20800	Specter of Trump Loosens Tongues, if Not Purse...	David Streitfeld	PALO ALTO, Calif. â€" After years of scorni...
1	20801	Russian warships ready to strike terrorists ne...	NaN	Russian warships ready to strike terrorists ne...
2	20802	#NoDAPL: Native American Leaders Vow to Stay A...	Common Dreams	Videos #NoDAPL: Native American Leaders Vow to...
3	20803	Tim Tebow Will Attempt Another Comeback, This ...	Daniel Victor	If at first you donâ€™t succeed, try a differe...
4	20804	Keiser Report: Meme Wars (E995)	Truth Broadcast Network	42 mins ago 1 Views 0 Comments 0 Likes 'For th...

Figure 2. Top five rows of training and testing data

3.4 *Cleaning and pre-processing*

Typically, material scraped from websites is in raw textual format. Prior to analyzing or fitting a model to this data, it must be cleaned. Cleaning (or pre-processing) is the process of converting data to a format that a computer can interpret. This stage entails the removal of superfluous data. Stop words are meaningless words (data) in NLP. Regex, which is based on a context-free grammar approach, is beneficial for reducing superfluous punctuation.

- Tokenization: For English, we utilized the software Punkt tokenizer. An unsupervised algorithm divides a text into a list of sentences in order to create a model for abbreviated words, collocations, and words that begin sentences.

- Stop words elimination: These are frequently used terms (such as "the," "a," "an," and "in") that a search engine has been trained to ignore, both when indexing entries for searching and when retrieving them in response to a search query. To avoid clogging up our database or wasting precious processing time, stop words must be removed. This is accomplished by keeping a list of words deemed to be stop words. Subsequently, the dataset will be cleaned of stop words.
- Lemmatization is the process of gathering together the various versions of a word so that they can be studied as a single item. This method grasps the term in its base form, called a lemma, i.e., in its dictionary form. This procedure preserves contextual information. The pre-processing of text entails both stemming and lemmatization. Wordnet is a freely accessible lexical database containing over 200 languages that was created primarily for NLP. It contains semantic associations (e.g., synonyms) between its terms. It is a frequently used lemmatizer approach. Synsets are a way for WordNet to organize synonyms. Synsets are a collection of semantically identical data components. After removing stop-words from our dataset, we employed a WordNet lemmatizer.
- Situation normalization of items: In this case, we are just turning all characters in the text to lowercase. Because Python is a case-sensitive language, it distinguishes between nlp and NLP. The .lower() method can be used to transform a string to lowercase.

3.5 *Applying feature extraction techniques*

The conversion of document corpora into a numerical structure is required to make them more intelligible to computers. To do this, a vector space model, commonly known as a bag-of-words (BoW) model, is used. Vectorization is the process of transforming a collection of textual texts into numerical feature vectors. The BoW, or "Bag of N-grams," representation is the methodological approach for tokenization, counting, and normalizing. The bag-of-words technique entails the following:

- Splitting of the documents into tokens.
- Giving weights to each token proportional to the frequency with which it arises in the document and/or corpora.
- Creating a document-term matrix with every row showcasing a document and each column addressing a token.

This approach involves describing documents in terms of word occurrences while fully disregarding the document's relative location information for the words. The most frequently used feature extraction algorithms from the SKLearn.feature extraction. text classes are CountVectorizer and TfidfVectorizer. CountVectorizer converts text documents to a matrix of token counts, taking into account the occurrences of tokens in each document. As a result, a sparse representation of the counts is obtained.

The location of tokens or words is completely ignored when this technique is used in corpora. If a word is the entirety of a phrase, it will still be assigned a frequency of one; this is a significant disadvantage of the count vectorizer. As a result, the introduction of tfidf is necessary. A count matrix is transformed into a normalized tf: term-frequency or tf-idf: term-frequency times matrix. The inverse document-frequency representation is accomplished using the TfidfTransformer. Equation 1 specifies the formula for calculating the tf-idf for a term 't' in a document 'd' in a document collection.

$$tf\text{-}id(t,d) = tf(t,d) * log\left(\frac{n}{df(t)+1}\right) \tag{1}$$

3.6 *Data modelling*

The present work makes use of supervised machine-learning classification techniques. The accuracy, $F1$-score, F_β-score, precision, specificity, AUCROC, and recall of several models are compared.

- Logistic regression: When the dependent variable or target is categorical, logistic regression is utilized. Here, we're forecasting if our news is phony, whether it's real, or whether it's a 1. Because there are only two possible outcomes, binary logistic regression will be employed. The logistic regression value must be between 0 and 1 and cannot exceed this number to produce a curve in the 'S' shape referred to as the sigmoid function or logistic function. The logistic sigmoid function transforms the output, producing a probability value that

may then be mapped to two or more discrete classifications. It will be beneficial to investigate a model's nonlinearity. A logit function is used in logistic regression. The model becomes non-linear as a result of this logic function. In logistic regression, the concept of a threshold value is used to determine the probability that a value is either 0 or 1. Values greater than the threshold value are assigned a value of 1, while values less than the threshold value are assigned a value of 0.

- KNN is a supervised machine learning technique that may be used to handle classification and regression problems. Due to the fact that it does not immediately learn from the training set, it is often referred to as a lazy learner algorithm. Rather than that, a dataset is stored, and action is performed on it during categorization. KNN can estimate which of two categories, Category A, real, and Category B, fake, a new data point will fall into.
- Random forest: This is a commonly used machine learning algorithm that falls under the category of supervised learning. It is utilized for both classification and regression issues in machine learning. Random forest is a machine learning algorithm that is based on the concept of ensemble learning. It solves a complex problem by combining numerous classifiers and optimizing the model's performance. The ultimate forecast is formed by integrating all of the trees' projections. Ensemble approaches are a method for collecting data in order to reach a final conclusion.
- Decision tree: A decision tree is a subset of supervised machine learning in which data is continually partitioned by a defined parameter. A decision tree's internal nodes reflect dataset properties; branches indicate decision rules, and a leaf node represents the outcome. The tree is divided into two sections, which we refer to as decision nodes and leaves. The leaves denote the final outcomes, and the decision nodes denote the data splitting points. The tests are run in accordance with the data's properties. After posing a question, the tree is separated into yes or no responses. It is a graphical depiction that is used to determine all viable solutions to a problem/decision given certain conditions. The CART algorithm is utilized. CART stands for classification and regression tree algorithm.
- Support vector machine (SVM): SVM is a supervised machine learning technique that is used to solve classification and regression problems. Its objective is to determine the ideal line or decision boundary (hyperplane) for classifying n-dimensional space. A hyperplane is a mathematical term for this optimal choice boundary. The SVM algorithm determines the hyperplane's extreme points/vectors. This type of vector is referred to as a support vector. The figure below depicts how a decision boundary, or hyperplane, is used to classify two distinct groups. Our dataset is referred to as linearly separable data since it can be divided into two groups using a single straight line, and the classifier utilized is a linear SVM classifier.

4. Result analysis

Binary classification has four possible types of results, given by a confusion matrix: (i) True Negatives (TN): correctly predicted negatives (zeroes); (ii) True Positives (TP): correctly predicted positives (ones); (iii) False Negatives (FN): incorrectly predicted negatives (zeros); and (iv) False Positives (FP): incorrectly predicted positives (ones). For the dataset we employed, the following result is obtained: (i) TP: Out of 5,200 samples, 2,502 were real and were predicted to be real; (ii) TN: 2,496 samples were fake and were predicted to be fake; (iii) FP: 62 samples were fake and were predicted to be real; and (iv) FN: 40 samples were real and were predicted to be fake. To measure the performance of various machine learning algorithms, we used the following indicators of binary classifiers:

- Accuracy (equation 2): It is the most often used categorization metric, and it is straightforward to grasp.

$$\text{Accuracy} = (TP + TN)/(TP + FP + FN + TN) \tag{2}$$

- Precision (equation 3): The precision of a forecast is an acceptable option as an evaluation metric when we want to be certain about our prediction.

$$\text{Precision} = (TP)/(TP + FP) \tag{3}$$

- Recall (equation 4): When it comes to diagnostic accuracy, recall, also known as sensitivity or TP rate, is

defined as the ratio of TP to actual positives.

$$\text{Recall} = (TP)/(TP + FN) \tag{4}$$

- $F1$-score (equation 5): It is a number between 0 and 1, and it is also referred to as the harmonic mean of precision and recall, among other things. The $F1$-score assigns equal importance to precision and recall, resulting in significant difficulty.

$$F1\text{-score} = (TP)/(TP + 1/2(FP + FN)) \tag{5}$$

- F_β-score (equation 6): It creates a weighted $F1$ metric as below, where beta manages the trade-off between precision and recall.

$$F_\beta\text{-score} = (1 + \beta 2) * (\text{precision} * \text{recall})/ ((\beta 2 * \text{precision}) + \text{recall}) \tag{6}$$

- Specificity (equation 7): The specificity (or rate of TN) is the ratio of TN to actual negatives.

$$\text{Specificity} = TN/FN + TN \tag{7}$$

- AUC-ROC curve: Area under the curve (AUC)-receiver operating characteristics (ROC) curve is a performance statistic for classifying problems over several thresholds. The receiver operating characteristic curve (ROC) represents the probability curve, whereas the area under the curve (AUC) represents the degree or measure of separability. It demonstrates the model's capacity to distinguish between classes. The greater the AUC, the more accurate predictions for identifying 0s as 0s and 1s as 1s are made.

For the purpose of automating machine learning workflows, a machine learning pipeline is utilized. Their business model incorporates the process of transforming a sequence of data and correlating them with one another in a model that is capable of being tested and evaluated in order to arrive at a result, which may be positive or negative. The process of training a model typically takes place in a series of stages known as a pipeline. They are carried out over and over again in order to develop an effective algorithm and continually improve the model's precision. Joblib is a SciPy module that assists with pipelining. Additionally, it facilitates the saving and loading of objects that make use of NumPy data. The joblib API serializes Python objects to NumPy arrays efficiently. joblib.dump() and joblib.load() acts as replacements for pickle when dealing with large amounts of data, most notably large NumPy arrays. Front-end web development was carried out using HTML and CSS, while back-end web development was carried out using Python. Flask was used to deploy the website.

4.1 *Fake news detection*

As shown in Table 1, logistic regression achieves the highest accuracy, 98.03%. SVM came in second with an accuracy of 97.92%.

Table 1. Fake news performance parameters

Model	Accuracy (%)	$F1$-score	F_β-score	AUC	Specificity	Recall	Precision	Log loss
Logistic regression	98.03	81.90	91.68	84.63	69.53	100	76	5.38
KNN	80.84	80.78	81.61	85.71	79.43	95.24	93.65	6.61
Random forest	82.82	82.83	83.51	81.93	81.71	95.24	93.65	5.93
Decision tree	95.67	95.75	95.54	95.66	96.09	95.24	93.65	1.49
SVM	97.92	97.95	97.71	97.91	98.36	97.46	96.79	0.71

4.2 *Fraudulent job-postings detection*

Datasets from Kaggle's datasets were used to predict fraudulent job postings. In the CSV file, the following categories were used to group the data for job postings: job ID, title, location, department, salary range, company profile, description, requirements, benefits, telecommuting, company logo (if present), questions (if present), employment type, required experience, required education, industry, function, and fraudulent. Our concept was put into practice using Google Colab Notebooks. The dataset has 18 columns and 17,880 rows. All fraudulent job profiles have a value of 1, while all legitimate job profiles have a value of 0.

Table 2. Fraudulent job-postings performance parameters

Model	Accuracy (%)	$F1$-score	F_β-score	AUC	Specificity	Recall	Precision	Log loss
Logistic regression	69.08	69.21	68.57	69.62	70.31	67.88	62.59	10.07
KNN	93.30	93.65	90.22	92.52	100	86.76	88.07	23.24
Random forest	99.71	99.71	99.54	100	100	99.43	99.42	9.84
Decision tree	97.72	99.71	99.54	53.56	100	99.43	99.42	9.82
SVM	73.50	73.57	71.98	76.53	76.40	70.79	65.60	9.15

From Table 2, it is noted that the random forest supervised classification algorithm has the greatest accuracy of 99.71%. In comparison to other algorithms, several evaluation criteria were also higher. With other criteria like $F1$-score, F_β- score, specificity, recall, precision, and log loss having the same value, decision trees provided the next-best accuracy of 97.72%.

4.3 *Fraudulent COVID-19 information detection*

Datasets from Kaggle were gathered for the COVID-19 and fraudulent job posting predictions.

The data for the COVID-19 dataset was organized into the following categories in the CSV file: title, text, source, and label. Our concept was put into practice using Google Colab Notebooks. There are 4 columns and 1,164 rows in the dataset. Title, text, source, and label are the many columns of data. The website data that has been scraped is available in raw text form. Prior to analysis or model fitting, this data needs to be cleaned. As was done earlier in "Fake News Detection", this entails using the regex library, performing tokenization, deleting stop words, lemmatization, and case normalization.

From Table 3, it is noted that the SVM-supervised classification algorithm has the greatest accuracy of 78.69%. $F1$-score and F_β-score were two additional evaluation measures that outperformed existing methods. With other measures, such as recall and precision, having a greater value than SVM, KNN provided the next-best accuracy of 73.88%.

Table 3. Fraudulent COVID-19 information performance parameters

Model	Accuracy (%)	$F1$-score	F_β-score	AUC	Specificity	Recall	Precision	Log loss
Logistic regression	54.98	54.98	54.98	100	100	53	62.59	10.07
KNN	73.88	73.88	73.88	100	95	83	88.07	23.24
Random forest	63.57	63.57	63.57	100	90	71	99.42	9.84
Decision tree	60.82	60.82	60.82	100	90	71	99.42	9.82
SVM	78.69	78.69	78.69	100	70.79	65.60	65.60	9.15

4.4 *Forged image detection*

Datasets from GitHub and Kaggle were used to gather information for faked image detection. The data were separated into training and testing folders. Two folders — one containing phony photographs and the other real images — were contained inside the training folder. Comparably, the testing folder contained phony images and a separate folder of real images.

CNNs, or ConvNet, were used in this study to classify images as fake or real. CNN classifications of images start with an input image, process it, and assign it to one of several categories. It is a deep learning system that recognizes photos, groups them based on shared characteristics, and then identifies objects in the images. CNN employs a distinctive aspect of an image to identify it. CNN is superior to older neural networks for image processing. CNN and artificial neural network (ANN) are comparable. CNN first gathers information using layers before using ANNs to extract some of the image's properties. A high-level neural network API called Keras runs on top of TensorFlow. The implementation of that algorithm is provided by the Python module multi-task cascade CNN (MTCNN). We will utilize MTCNN, which is based on deep learning, because it is thought to be the best method for detecting faces in images.

First, we go through the folder iteratively, find and crop faces, and then save them in the appropriate folder. In this case, we'll be using the image-processing library Pillow. The most crucial module of PIL (Python Image Library) is a library named Pillow that operates on top of PIL. But since 2011, the PIL module has not been used. Pillow offers a variety of features that are compatible with all popular operating systems and even support Python 3. It is compatible with a wide range of image formats, including "bmp", "gif", "ppm", "tiff", "jpeg", and "png". The pillow library utilizes an image class to display the image. The image module in Pillow comes with built-in features, including the ability to load or generate new images, among others.

The code that begins with "from PIL import Image" imports the image module from the pillow before calling Image.open() and supplying the image filename as a parameter. Fake photos can be identified by executing the detect faces() function once the model has been loaded and configured. This gives a list of dictionary objects that each have a number of keys for the information about each face that was detected. For example, the dictionary object "box" has the x and y coordinates of the bottom left corner of the bounding box, along with its width and height. and the image will then be cropped. A function in the pillow named crop() is used to crop a picture's rectangular section. It takes a four-element tuple as input and returns the cropped rectangle portion of the image. We are transforming the created image from an array back to a NumPy array and saving it.

Three convolutional (CONV) layers, three max-pool layers, one flattening layer, and ultimately an output layer with sigmoid activation are included in this classifier. With the sequential API, a model is built. Sequential is one of the most used Keras models. The sequential API allows us to stack layers one on top of the other. A sequential object is made, then layers are added using the add function to form a convolutional neural network. The method above builds a sequential object first, then adds some convolutional, maxpooling, and dropout layers. It then flattens the output and sends it to a final dense layer before sending it to our output layer. The CONV layer is used to compute the result of neurons connected to local regions in the input. Each neuron computes a dot product between its weights and the local area in the input volume that it is connected to. The downsampling operation for the POOL layer is carried out along the spatial dimensions (width, height). Breaking up linearity is done with an activation function. We will employ the activation functions of sigmoid and ReLU.

- Padding: Convolutional operations, as mentioned above, decrease the size of the image, which is why we apply padding to preserve our input size.
- Pooling: This layer is used for reducing parameters and the computation process. In this pooling process, max pooling will be used.
- Flattening: Flattening is taking a matrix from convolutional and pooling processes and turning it into a one-dimensional array. This is important because the input of a fully connected layer, or ANN, consists of a one-dimensional array.

We set up the learning process before we began training the model. The optimizer, a loss function, and, optionally, certain metrics like accuracy, must all be specified. Because optimizers employ gradients to update the weights, they can reduce the loss function, which assesses how effectively our model meets the specified objective. The Adam Optimizer has been utilized. Adam is an optimization technique that dynamically modifies the learning rate. By combining multiple orientations of existing data, augmentation produces new information; overfitting is avoided. Before supplying

the photos to the model as input during training or model evaluation, the pixel values in the image should be scaled. Image augmentation is possible using the imageDataGenerator function. Before modeling, the ImageDataGenerator class in Keras provides a variety of methods for scaling variables in the image dataset. The class encapsulates the picture collection before returning photos in batches and performing the necessary scaling operations as needed.

Our model is now prepared for training. In order to train the model, we used a fit generator and gave train data, the number of epochs, and the batch size to our generator. To track the loss and accuracy on both sets, we also handed it a validation set, which is currently test data. It will also pass if steps per epoch, a requirement when using a generator, are set to the length of the training set and validation steps are set to the length of the test data. Epoch refers to the overall quantity of times the algorithm examines the full data set. We can split up an epoch into smaller pieces if it is too big to run all at once. A collection of these pieces is referred to as a batch.

For describing any model in JSON format, Keras provides the to json() function. A function named model from json() is used to load this information once it has been saved to a file and create a new model from the JSON file. The weights are then immediately saved using the load weights() symmetrical function and saved directly using the save weights() method. The complete model is then written to model.json in JSON format. A new model is built when the model and weight information are loaded from the saved files. Later, the model can be loaded by executing the load model() function with the filename as an argument. The model with the same architecture and weights is returned by the function. By using the Image.open() function, which returns a value of the picture object data type, the image is loaded. It recognizes the file type automatically. Figure 3 shows the accuracy over a number of epochs, and Figure 4 shows the loss over a number of epochs. The dataset comprises real and fake images, as shown in Figure 5. We achieved an accuracy of 97.69% with the use of MTCNN.

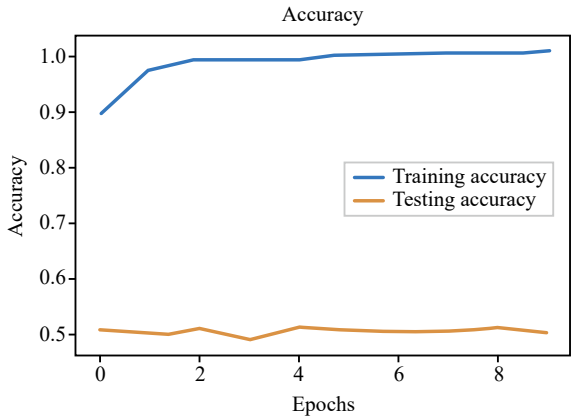

Figure 3. MTCNN: Variation of accuracy over number of epochs

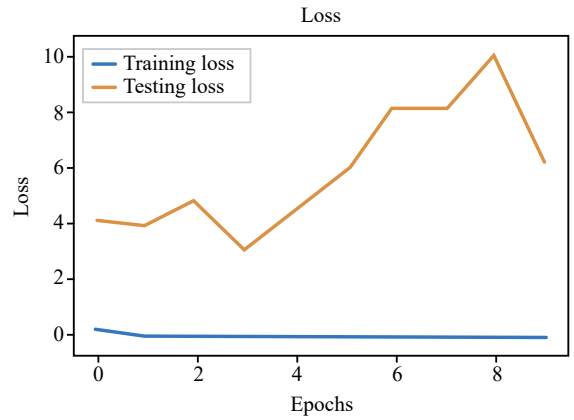

Figure 4. MTCNN: Variation of loss over number of epochs

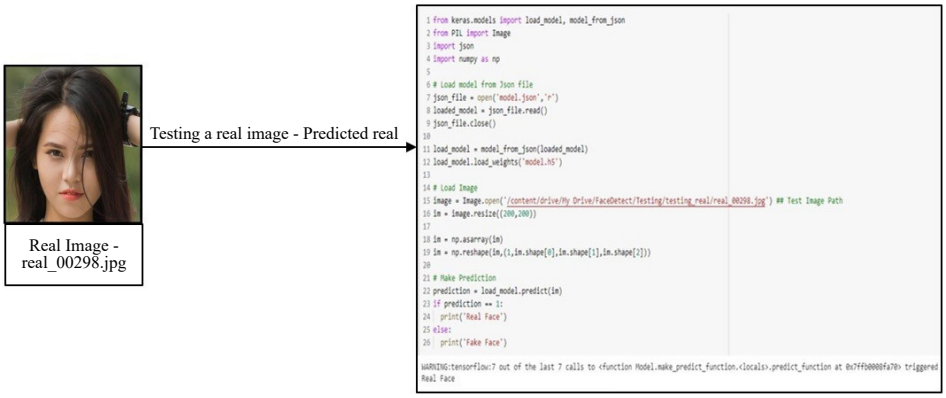

Figure 5. MTCNN: Testing a real image - Predicated real

5. Recommendation system

Kaggle datasets were used for the data collection for the recommendation algorithm. The link, text, title, date, keywords, summary, and title summary columns of the recommendation were used to group the data together. The application of our concept was carried out using Google Colab Notebooks. Imported packages included Sklearn, NumPy, Pandas, Matplotlib, NLTK, Regex, Random, and String. By adding a new column ID, eliminating duplicates, and deleting any null values that were previously included in the dataset, the dataset is transformed. ID, date, title, text, and link are some of the columns in the modified dataset, which has 1,496 rows and 5 columns. By invoking the modules in the NLTK library, the cleaning and pre-processing stage entails changing the data in the "text" column to lowercase and eliminating stop words and punctuation. By first compiling the HTML tag patterns using the regex library's compile function and then replacing any occurrences with spaces, HTML tags are eliminated from the dataset.

The TF-IDF encoding method was the one that we decided to employ for our dataset since it assigns a weight to each term that is proportional to how essential the term is to the document. The more frequently a term appears, the greater the weight it carries. Additionally, it provides an inverse that is weighted based on the frequency with which a given term appears in the dataset for each item. Therefore, it calls attention to uncommon terms throughout the entirety of the dataset that are nonetheless significant to the text at hand. The parameters for the TF-IDF vectorizer are:

- Analyzer: The analyzer is used to decide if the feature should be made up of n-grams of individual words and characters. In our case, the thing is words.
- ngram_rangetuple (min_n, max_n): The lower and upper limits of the range of n-values to be extracted for different n-grams. All n values between min_n and max_n are used. In our case, it's in the ballpark (1, 3).
- max_dffloat or int: When building the vocabulary, don't include words that appear in a document more than the given threshold. In this case, the threshold is 0.8.
- min_dffloat or int: When building the vocabulary, don't include words that appear in fewer than the given number of documents. This number is also known as the cutoff. Here, its value is 0.0.
- use_idfbool, default = True: Turn on inverse-document-frequency reweighting.

Now, we calculated how relevant or similar one document was to another. Here, each item is stored as a vector of its attributes (also vectors) in an n-dimensional space, and the angles between the vectors are used to figure out how similar they are. The user's likes and dislikes are measured by taking the cosine of the angle between the user profile vector (Ui) and the document vector. In our case, it's the angle between two document vectors. The reason for using cosine is that the cosine value increases as the angle between two vectors decreases, which means that the vectors are more alike. When making suggestions for a user, a recommender system has to choose between two ways to send information:

- Exploitation: The system picks documents that are similar to the ones the user has already chosen.
- Exploration: The system picks documents for which the user profile doesn't give enough information to predict how the user will react.

We used the exploitation technique as shown in Figures 6 and 7. A machine learning method for spotting

bogus news was discussed here. We presented a suggestion mechanism as soon as we discovered the bogus news. Increased confidence in online digital media consumption can be achieved through the deployment of a user-friendly recommendation system.

Figure 6. Recommended articles in case of min_df = 0.1

Figure 7. Recommended articles in case of min_df = 0.2

6. Conclusion and future scope

It is crucial to follow basic rules and regulations when consuming information through digital media to ensure the safety and security of IoT systems. The affordability, convenience, and rapid transmission of information through social media have made it a popular source for news consumption. However, this convenience also makes spreading "fake news easier," which includes deliberately misleading and deceptive material. The widespread dissemination of false information can be detrimental to individuals and society, potentially leading to incorrect decisions and actions by IoT systems and devices. Consequently, detecting false news on social media has emerged as a critical research topic, requiring unique machine learning and deep learning techniques that can identify and mitigate these threats. In this article, we have discussed various methods for identifying fake news on social media, focusing on enhancing trust in digital media sources. Additionally, we have suggested a recommendation system to promote informed decision-making and enhance the security of IoT devices and systems. In the future, we will focus on the following aspects:

- The models of the work are based solely on English, which is one of its significant constraints. Other languages are not taken into account. Therefore, our strategy will be to create a model to identify fake news using multilingual data. We'll strive to use a variety of tongues, such as French, Greek, Sanskrit, Hindi, German, and

Spanish.

- Since predetermined datasets are typically used for detection, we built a dynamic dataset that would gather all real-time news and refresh the dataset with the most recent information. In the future, accuracy predictions will be based on a different algorithm.
- We will create a cross-platform, hybrid application based on our website (Android and iOS).
- Plans include creating fake video detection models and the online deployment of video and picture detection models.
- We aim to implement the recommendation algorithm online as a dashboard to display various news categories based on the user's interests.
- Additionally, a methodology for spotting fake news produced by social media platforms (WhatsApp, Twitter, Facebook, and Instagram) will be developed.

Conflict of interest

The authors declare no conflict of interest.

References

[1] Shu K, Sliva A, Wang S, Tang J, Liu H. Fake news detection on social media: A data mining perspective. *ACM SIGKDD Explorations Newsletter*. 2017; 19(1): 22-36. Available from: https://doi.org/10.1145/3137597.3137600.

[2] Jain A, Kasbe A. Fake news detection. In: *2018 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*. Bhopal, India: IEEE; 2018. Available from: https://doi.org/10.1109/SCEECS.2018.8546944.

[3] Shu K, Wang S, Liu H. Beyond news contents: The role of social context for fake news detection. In: *Proceedings of the Twelfth ACM International Conference on Web Search and Data Mining*. New York, US: Association for Computing Machinery; 2019. p.312-320. Available from: https://doi.org/10.1145/3289600.3290994.

[4] Pérez-Rosas V, Kleinberg B, Lefevre A, Mihalcea R. Automatic detection of fake news. In: Bender EM, Derczynski L, Isabelle P. (eds.) *Proceedings of the 27th International Conference on Computational Linguistics*. Santa Fe, USA: Association for Computational Linguistics; 2018. p.3391-3401.

[5] Zhou X, Zafarani R, Shu K, Liu H. Fake news: Fundamental theories, detection strategies and challenges. In: *Proceedings of the Twelfth ACM International Conference on Web Search and Data Mining*. New York, US: Association for Computing Machinery; 2019; p.836-837. Available from: https://doi.org/10.1145/3289600.3291382.

[6] Zhang X, Ghorbani AA. An overview of online fake news: Characterization, detection, and discussion. *Information Processing & Management*. 2020; 57(2): 102025. Available from: https://doi.org/10.1016/j.ipm.2019.03.004.

[7] Zhou X, Zafarani R. A survey of fake news: Fundamental theories, detection methods, and opportunities. *ACM Computing Surveys*. 2020; 53(5): 1-40. Available from: https://doi.org/10.1145/3395046.

[8] Oshikawa R, Qian J, Wang WY. A survey on natural language processing for fake news detection. In: *Proceedings of the Twelfth Language Resources and Evaluation Conference*. France: European Language Resources Association; 2020. p.6086-6093.

[9] Ogundokun RO, Arowolo MO, Misra S, Oladipo ID. Early detection of fake news from social media networks using computational intelligence approaches. In: Lahby M, Pathan A-SK, Maleh Y, Yafooz WMS. (eds.) *Combating fake news with computational intelligence techniques*. Cham: Springer; 2022. p.71-89. Available from: https://doi.org/10.1007/978-3-030-90087-8_4.

[10] Prasad R, Udeme AU, Misra S, Bisallah H. Identification and classification of transportation disaster tweets using improved bidirectional encoder representations from transformers. *International Journal of Information Management Data Insights*. 2023; 3(1): 100154. Available from: https://doi.org/10.1016/j.jjimei.2023.100154.

[11] Abayomi-Alli A, Abayomi-Alli O, Misra S, Fernandez-Sanz L. Study of the yahoo-yahoo hash-tag tweets using sentiment analysis and opinion mining algorithms. *Information*. 2022; 13(3): 152. Available from: https://doi.

org/10.3390/info13030152.
[12] Olaleye T, Abayomi-Alli A, Adesemowo K, Arogundade OT, Misra S, Kose U. Sclavoem: Hyper parameter optimization approach to predictive modelling of COVID-19 infodemic tweets using smote and classifier vote ensemble. *Soft Computing*. 2022; 27: 3531-3550. Available from: https://doi.org/10.1007/s00500-022-06940-0.
[13] Peter A, Omole R, Misra S, Garg L, Oluranti J. Machine learning approaches for classifying the peace-war orientations of global news organizations' social media posts. In: *Information Systems and Management Science: Conference Proceedings of 4th International Conference on Information Systems and Management Science (ISMS) 2021*. Cham: Springer; 2022. p.301-317. Available from: https://doi.org/10.1007/978-3-031-13150-9_26.
[14] Shu K, Cui L, Wang S, Lee D, Liu H. dEFEND: Explainable fake news detection. In: *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining.* New York, US: Association for Computing Machinery; 2019. p.395-405. Available from: https://doi.org/10.1145/3292500.3330935.
[15] Parikh SB, Atrey PK. Media-rich fake news detection: A survey. In: *2018 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR).* Miami, FL, USA: IEEE; 2018. p.436-441. Available from: https://doi.org/10.1109/MIPR.2018.00093.
[16] Granik M, Mesyura V. Fake news detection using naive Bayes classifier. In: *2017 IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON)*. Kyiv, UKraine: IEEE; 2017. p.900-903. Available from: https://doi.org/10.1109/UKRCON.2017.8100379.
[17] Thota A, Tilak P, Ahluwalia S, Lohia N. Fake news detection: A deep learning approach. *SMU Data Science Review*. 2018; 1(3): 10.
[18] Abiodun EO, Alabdulatif A, Abiodun OI, Alawida M, Alabdulatif A, Alkhawaldeh RS. A systematic review of emerging feature selection optimization methods for optimal text classification: The present state and prospective opportunities. *Neural Computing and Applications*. 2021; 33(22): 15091-15118. Available from: https://doi.org/10.1007/s00521-021-06406-8.
[19] Taofeek OT, Alawida M, Alabdulatif A, Omolara AE, Abiodun OI. A cognitive deception model for generating fake documents to curb data exfiltration in networks during cyber-attacks. *IEEE Access*. 2022; 10: 41457-41476. Available from: https://doi.org/10.1109/ACCESS.2022.3166628.
[20] Ahmed U, Jhaveri RH, Srivastava G, Lin JC-W. Explainable deep attention active learning for sentimental analytics of mental disorder. *ACM Transactions on Asian and Low-Resource Language Information Processing*. New York, US: Association for Computing Machinery; 2022. Available from: https://doi.org/10.1145/3551890.
[21] Patel A, Shah J. Sensor-based activity recognition in the context of ambient assisted living systems: A review. *Journal of Ambient Intelligence and Smart Environments*. 2019; 11(4): 301-322. Available from: https://doi.org/10.3233/AIS-190529.
[22] Patel A, Shah J. Real-time human behaviour monitoring using hybrid ambient assisted living framework. *Journal of Reliable Intelligent Environments*. 2020; 6(2): 95-106. Available from: https://doi.org/10.1007/s40860-020-00100-7.
[23] Patel AD, Shah JH. Performance analysis of supervised machine learning algorithms to recognize human activity in ambient assisted living environment. In: *2019 IEEE 16th India Council International Conference (INDICON)*. Rajkot, India: IEEE; 2019. Available from: https://doi.org/10.1109/INDICON47234.2019.9030353.
[24] Jadhav Y, Mathur H. Detection of breast cancer by using various machine learning and deep learning algorithms. In: Jain V, Juneja S, Juneja A, Kannan R. (eds.) *Handbook of machine learning for computational optimization*. CRC Press; 2021. p.51-70.
[25] Jadhav Y, Patil V, Parasar D. Machine learning approach to classify birds on the basis of their sound. In: *2020 International Conference on Inventive Computation Technologies (ICICT)*. Coimbatore, India: IEEE; 2020. p.69-73. Available from: https://doi.org/10.1109/ICICT48043.2020.9112506.
[26] Khan A, Worah G, Kothari M, Jadhav YH, Nimkar AV. News popularity prediction with ensemble methods of classification. In: *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. Bengaluru, India: IEEE; 2018. Available from: https://doi.org/10.1109/ICCCNT.2018.8494095.
[27] Ruchansky N, Seo S, Liu Y. CSI: A hybrid deep model for fake news detection. In: *Proceedings of the 2017 ACM on Conference on Information and Knowledge Management*. New York, US: Association for Computing Machinery; 2017. p.797-806. Available from: https://doi.org/10.1145/3132847.3132877.

[28] Ahmad I, Yousaf M, Yousaf S, Ahmad MO. Fake news detection using machine learning ensemble methods. *Complexity*. 2020; 2020: 8885861. Available from: https://doi.org/10.1155/2020/8885861.
[29] Khattar D, Goud JS, Gupta M, Varma V. MVAE: Multimodal variational autoencoder for fake news detection. In: *The World Wide Web Conference*. New York, US: Association for Computing Machinery; 2019. p.2915-2921. Available from: https://doi.org/10.1145/3308558.3313552.
[30] Gravanis G, Vakali A, Diamantaras K, Karadais P. Behind the cues: A benchmarking study for fake news detection. *Expert Systems with Applications*. 2019; 128: 201-213. Available from: https://doi.org/10.1016/j.eswa.2019.03.036.
[31] Singhania S, Fernandez N, Rao S. 3HAN: A deep neural network for fake news detection. In: Liu D, Xie S, Li Y, Zhao D, El-Alfy E-SM. (eds.) *Neural information processing*. Cham: Springer; 2017. p.572-581. Available from: https://doi.org/10.1007/978-3-319-70096-0_59.
[32] Alkhodhairi RK, Aljalhami SR, Rusayni NK, Alshobaili JF, Al-Shargabi AA, Alabdulatif A. Bitcoin candlestick prediction with deep neural networks based on real time data. *Computers, Materials and Continua*. 2021; 68(3): 3215-3233. Available from: https://doi.org/10.32604/cmc.2021.016881.
[33] Yang Y, Zheng L, Zhang J, Cui Q, Li Z, Yu PS. TI-CNN: Convolutional neural networks for fake news detection. *arXiv* [Preprint] 2018. Version 3. Available from: https://doi.org/10.48550/arXiv.1806.00749.
[34] Wani A, Joshi I, Khandve S, Wagh V, Joshi R. Evaluating deep learning approaches for covid19 fake news detection. In: Chakraborty T, Shu K, Bernard HR, Liu H, Akhtar MS. (eds.) *Combating online hostile posts in regional languages during emergency situation*. Cham: Springer; 2021. p.153-163. https://doi.org/10.1007/978-3-030-73696-5_15.
[35] Yang S, Shu K, Wang S, Gu R, Wu F, Liu H. Unsupervised fake news detection on social media: A generative approach. *Proceedings of the AAAI Conference on Artificial Intelligence*. 2019; 33(1): 5644-5651. Available from: https://doi.org/10.1609/aaai.v33i01.33015644.
[36] Chen X, Jia S, Xiang Y. A review: Knowledge reasoning over knowledge graph. *Expert Systems with Applications*. 2020; 141: 112948. Available from: https://doi.org/10.1016/j.eswa.2019.112948.
[37] Sengupta S, Basak S, Saikia P, Paul S, Tsalavoutis V, Atiah F, et al. A review of deep learning with special emphasis on architectures, applications and recent trends. *Knowledge-Based Systems*. 2020; 194: 105596. Available from: https://doi.org/10.1016/j.knosys.2020.105596.
[38] Han K. Personalized news recommendation and simulation based on improved collaborative filtering algorithm. *Complexity*. 2020; 2020: 8834908. Available from: https://doi.org/10.1155/2020/8834908.
[39] Gong W, Zhang W, Bilal M, Chen Y, Xu X, Wang W. Efficient web APIs recommendation with privacy-preservation for mobile app development in industry 4.0. *IEEE Transactions on Industrial Informatics.* 2022; 18(9): 6379-6387. Available from: https://doi.org/10.1109/TII.2021.3133614.
[40] Wang Z, Wang W, Yang Y, Han Z, Xu D, Su C. CNN-and GAN-based classification of malicious code families: A code visualization approach. *International Journal of Intelligent Systems*. 2022; 37(12): 12472-12489. Available from: https://doi.org/10.1002/int.23094.
[41] Javed U, Shaukat K, Hameed IA, Iqbal F, Alam TM, Luo S. A review of content-based and context-based recommendation systems. *International Journal of Emerging Technologies in Learning*. 2021; 16(3): 274-306. Available from: https://doi.org/10.3991/ijet.v16i03.18851.
[42] Khanal SS, Prasad PWC, Alsadoon A, Maag A. A systematic review: Machine learning based recommendation systems for e-learning. *Education and Information Technologies*. 2020; 25(4): 2635-2664. Available from: https://doi.org/10.1007/s10639-019-10063-9.
[43] Lops P, de Gemmis M, Semeraro G. Content-based recommender systems: State of the art and trends. In: Ricci F, Rokach L, Shapira B, Kantor PB. (eds.) *Recommender systems handbook.* Boston: Springer; 2011. p.73-105. Available from: https://doi.org/10.1007/978-0-387-85820-3_3.
[44] Djenouri Y, Belhadi A, Srivastava G, Lin JC-W. An efficient and accurate GPU-based deep learning model for multimedia recommendation. *ACM Transactions on Multimedia Computing, Communications, and Applications*. 2022; 20(2): 40. Available from: https://doi.org/10.1145/3524022.
[45] Djenouri Y, Belhadi A, Srivastava G, Lin JC-W. Advanced pattern-mining system for fake news analysis. *IEEE Transactions on Computational Social Systems*. [Early Access] 2023. Available from: https://doi.org/10.1109/TCSS.2022.3233408.

[46] Kesarwani A, Chauhan SS, Nair AR. Fake news detection on social media using K-nearest neighbor classifier. In: *2020 International Conference on Advances in Computing and Communication Engineering (ICACCE)*. Las Vegas, NV, USA: IEEE; 2020. Available from: https://doi.org/10.1109/ICACCE49060.2020.9154997.

[47] Kaliyar RK. Fake news detection using a deep neural network. In: 2*018 4th International Conference on Computing Communication and Automation (ICCCA)*. Greater Noida, India: IEEE; 2018. Available from: https://doi.org/10.1109/CCAA.2018.8777343.

[48] AlShariah NM, Khader A, Saudagar J. Detecting fake images on social media using machine learning. *International Journal of Advanced Computer Science and Applications*. 2019; 10(12): 170-176. Available from: http://dx.doi.org/10.14569/IJACSA.2019.0101224.

[49] Elhadad MK, Li KF, Gebali F. Detecting misleading information on COVID-19. *IEEE Access*. 2020; 8: 165201-165215. Available from: https://doi.org/10.1109/ACCESS.2020.3022867.

[50] Iwendi C, Mahboob K, Khalid Z, Javed AR, Rizwan M, Ghosh U. Classification of COVID-19 individuals using adaptive neuro-fuzzy inference system. *Multimedia Systems*. 2022; 28: 1223-1237. Available from: https://doi.org/10.1007/s00530-021-00774-w.

[51] Güera D, Delp EJ. Deepfake video detection using recurrent neural networks. In: *2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*. Auckland, New Zealand: IEEE; 2018. p.1-6. Available from: https://doi.org/10.1109/AVSS.2018.8639163.

[52] Patel C, Bashir AK, AlZubi AA, Jhaveri R. EBAKE-SE: A novel ECC-based authenticated key exchange between industrial IoT devices using secure element. *Digital Communications and Networks*. 2022; 9(2): 358-366. Available from: https://doi.org/10.1016/j.dcan.2022.11.001.

[53] Ramani S, Jhaveri RH. ML-based delay attack detection and isolation for fault-tolerant software-defined industrial networks. *Sensors*. 2022; 22(18): 6958. Available from: https://doi.org/10.3390/s22186958.

[54] Panigrahi R, Borah S, Bhoi AK, Ijaz MF, Pramanik M, Jhaveri RH, et al. Performance assessment of supervised classifiers for designing intrusion detection systems: A comprehensive review and recommendations for future research. *Mathematics*. 2021; 9(6): 690. Available from: https://doi.org/10.3390/math9060690.

[55] Dutta S, Bandyopadhyay SK. Fake job recruitment detection using machine learning approach. *International Journal of Engineering Trends and Technology*. 2020; 68(4): 48-53. Available from: https://doi.org/10.14445/22315381/IJETT-V68I4P209S.

[56] Villan MA, Kuruvilla A, Paul J, Elias EP. Fake image detection using machine learning. *International Journal of Computer Science and Information Technology & Security (IJCSITS)*. 2017; 7(2): 19-22.

[57] Afzal S, Asim M, Javed AR, Beg MO, Baker T. URLdeepDetect: A deep learning approach for detecting malicious URLs using semantic vector models. *Journal of Network and Systems Management*. 2021; 29: 21. Available from: https://doi.org/10.1007/s10922-021-09587-8.

[58] Ghinadya, Suyanto S. Synonyms-based augmentation to improve fake news detection using bidirectional LSTM. In: *2020 8th International Conference on Information and Communication Technology (ICoICT)*. Yogyakarta, Indonesia: IEEE; 2020. p.1-5. Available from: https://doi.org/10.1109/ICoICT49345.2020.9166230.

[59] Abonizio HQ, de Morais JI, Tavares GM, Junior SB. Language-independent fake news detection: English, Portuguese, and Spanish mutual features. *Future Internet*. 2020; 12(5): 87. Available from: https://doi.org/10.3390/fi12050087.