International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 05 May 2024, pp: 924-931 www.ijaem.net ISSN: 2395-5252

Social Networking Attacks detection using Machine Learning Approaches

Ayushi[1], Aditi[2], Simranjot Kaur[3]

[1, 2] student, IV SEM ,M.C.A, DAV Institute of Engineering and Technology, Jalandhar, Punjab, India
[3]Assistance Professor , M.C.A, DAV Institute of Engineering and Technology, Jalandhar, Punjab,India

Date of Submission: 18-05-2024 Date of Acceptance: 28-05-2024

ABSTRACT
As social networking sites improve, protecting private information online has been an important and serious research topic. Thanks to the development and ease of the website, the number of users of social networks and social communities has grown considerably. Despite the fact that social networks are used worldwide, there is a growing lack of knowledge about OSN studies have shown that online community users disclose theirpersonal information such as phone numbers, email addresses, etc. This article discusses various attacks that are possible in social networks and can be detected using machine learning methods.

Keyword: OSN, Machine Learning, Deep Learning, Attacks, DDos, XSS, ELM, SVM, K means, KNN, BEC.

I. INTRODUCTION

As more and more people around the world use social networks to communicate and socialize with others, network development and the development of smart mobile devices have made it easier than ever to communicate and communicate with others. This convenience has also led to new kinds of network security issues, such as personal information leakage and even national security issues that can put our lives in danger. Network security encompasses many aspects, such as policies and best practices for preventing and detecting malicious node activity. With the amount of knowledge being shared and exchanged online, social network security is more critical than ever. The world has become more interconnected than ever before, and while this is good news for people and businesses, it also means that everyone has access to information. When hackers get involved, they can do a lot of nasty things. This paper will discuss some of the attacks that can be done with machine learning.There are hundreds of ML algorithms and methods that can be broken down into unsupervised learning andsupervised learning. Unsupervised learning involves classification when input matches a source orregression when data is converted into a constant output. supervised learning involves the classification of information. It is mainly done by grouping data and is used to measure discovery and to-dimensional. In cyber security, these two techniques can be used in near real time to detect malware and address the gaps in traditional security measures.

II. ATTACKS ON SOCIAL MEDIA

A. PHISHING ATTACKS

Phishing campaigns take advantage of social media platforms to trick users into giving up personal information (e.g. financial information, passwords or business information). There are several types of phishing campaigns that take place on social media platforms:

1) **C2 Infrastructures:** While the misuse of short URLs is not new, phishing assaults on Twitter have seen an increase in their use. Threatened actors even host their C2 infrastructure on the network by other threatening actors, such as penters, and employ a combination of shorter URLs on Twitter to hide dangerous links.

2) **Impersonation:**Due to the poor use of social engineering, phishing is a significant factor in the success of an attack. By pretending to be someone in a position of power, it is simple to harm this man, the name that goes along with it, and coerce others into doing such things. This excludes occurrences that negatively affect users as well as humorous accounts that are usually labeled. One of the most prevalent instances is when a threat agent responds to a celebration via Twitter, claiming to be that person, and offers free Bitcoins. A hint: they're not.

3) **Credential Theft and Propagation:**In addition to distributing phishing assaults on social media, threat actors also trick users into signing onto phony landing pages, which essentially divulges their credentials. In the event that this occurs, vulnerabilities may be acquired by a danger team, and efforts may be made to get new users to trade passwords or act more like a BEC attack in order to initiate a wire transfer.

4) **Data Dumps:** Damaged network dumps frequentlymake the rounds on the internet. That might be advertised on the dark web or other places, as well as on dumpsites and blogs.

5) **Data Collection:**What was the name of the original pet? Did she not have fluff? Alright, so ten years ago you posted on social media about using knowledge to reset passwords. What private details about your life beyond the essentials are there?

An individual with a hazard can also think of something and utilize it to create a customized, intricate software.

B. MALWARE

Malware, or malicious software, is the same thing. It's a word for general intrusion. It is obtrusive. It is intended to be used on a computer to log in and view personal data. Compared to other online services, social networks are less vulnerable to malware attacks due to their nature and the links among members. The worst case for ransomware is when it gets to users' credentials and starts sending messages. One exampleof malware that spread using OSNs is Koobface, which was shared on Facebook, LinkedIN, and Twitter. Link identifiers were gathered, and thetarget-infected computer's botnet was rendered operational. An OSN serves a variety of functions, but one important one is entertainment and publicity. However, it exposed its users to risky activities.

C. ATTACK OF SPAM

Spam on OSNs in the form of updates or direct emails is known as unsolicited messaging. Messages that are spam are spam. Because consumers spend so much time on OSNs, spam on these platforms is more dangerous than typical spam emails. Spam sometimes consists of links to malware, phishing, or fraudulent adverts. Usually, spammers use phony accounts or spam programs to create spam. An identity created in the name of a well-known person typically broadens the bogus profile. Usually, spam bots and compromised accounts send out spam reports. But the majority of spam originates from compromised accounts.Spam-filtering techniques detect dangerous language or URLs inemails and redirect them before sending them to a target system.

D. Scripting on the Web: XSS

One of the most prevalent and dangerous flaws in online security threats is cross-site scripting, which is negatively impacted by web-based programs. Through the use ofXSS exploitation, a hacker can install malicious software on the target user's web browser, compromising cookies, credit card numbers, and password information. As a result, an attacker may utilize XSS to create XSS worms, which have the ability to quickly propagate OSNs using social network infrastructure.

E. The clickjacking

Through clickjacking, a user clicks on something that is hidden or misidentified as another website element. Users may inadvertently download viruses, visit dubious websites, divulge passwords or sensitive information, transmit money, or make purchases online as a result. An invader will take control of OSN users by clicking on the assault and unintentionally sending requests and posting spam on their timelines. Clickjacking attacks will also incentivize hackers to capture their activities via the users' PCs' hardware, including the microphone and camera.

F. De-Identification Assaults

De-anonymization is a data-mining process that allows for the re-identification of an individual by comparing confidential archived details with readily available and established data outlets. OSNs offer excellent means of exchanging information, resources, and contacts. Deanonymization attacksare an easy target since the data shared by OSNs is made publicly accessible by default. In order to protect user privacy, existing internet services employ pseudonyms to reveal personal information. However, a number of deanonymization techniques allow for the re-identification of an individual.

G. Attacks using Fake Profiles

On most social networks, a phony attack is a typical assault. In this kind of attack, the attacker creates a profile using a fictitious social network credential and uses it to send messages on behalf of actual users. It delivers spam as soon as friendship is received. Usually programmed or semi-automatic, fake profiles mimic real people. The goal of the fictitious profiles is to collect and disseminate personally identifiable information that OSN users have access to only their friends. The phony profile attack, which uses an online social network service provider's capacity, is another issue.

H. Inference-Based Attacks

In contrast to attacks on social networks, it is intended that significant and private information, such as age, ethnicity, religious affiliation, or political affiliation, will not be made public. Although the specifics or attributes made public within the network ought to remain confidential, users could exploit data mining techniques to predict user privacy by utilizing OSN knowledge leaks. Machine-learning algorithms can be used to carry out inference attacks, such as merging publicly accessible social network data with the network's topology and user content. Any two users can utilize a mutually-friends-based attack to find their shared neighbour.A proposal for an inference attack to deduce a user's attributes from their publicly available data attributes was made in Reference. Facebook's approach for determining various user traits, including geography, interests, and educational background, was examined.

I. Information Violating

Social media is available for peer engagement and open information exchange. Anyone can freely disseminate their personal information, including medical records. Unfortunately, a few of them reveal far toomuch personalinformation about products, businesses, organizations, or any other type of confidential information. The disclosure of this sensitive personal data may not be well received by OSN users. An insurance company, for instance, can utilize OSN data to determine which customers are risky

J. Exposure of the Location

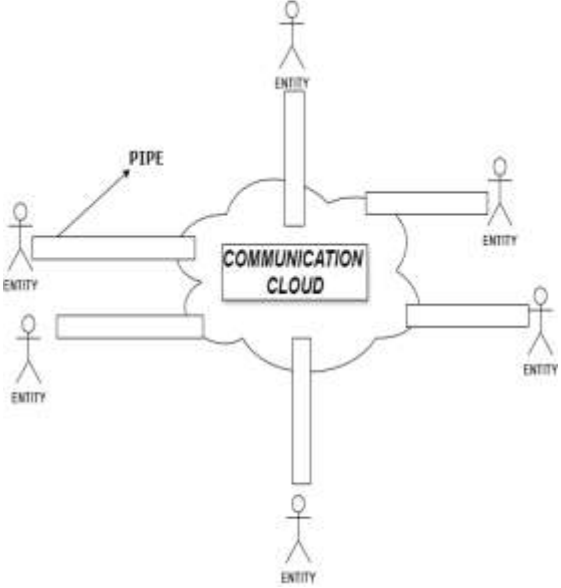
The possibility of location leaks is one type of data breach. Different people browse social media networks using different mobile device patterns. Applications are typically utilized to access an internet smartphone source.Since mobile devices are utilized for online access, position leaks violate modern privacy. Users can communicate their location information with others by using electronic mobile devices. As a result, attackers can harm users by using the regional information that is exposed on social networking sites.

K. Bullying online

Threatening a target through text messages and emails is known as cyberbullying. OSN users also utilize their photos to display location-based information. A rival can gather data using content-based methods, but then take use of it to launch risky attacks.

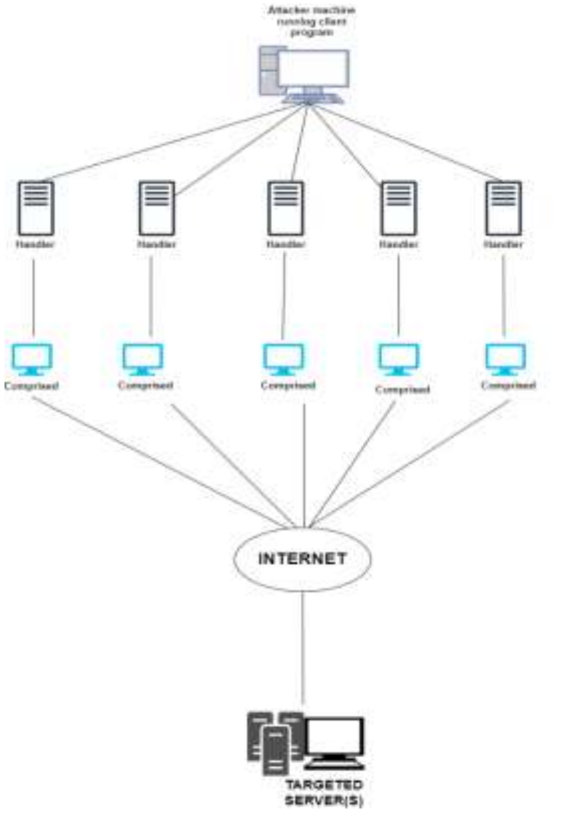
L. Attack of Sybil

The hacker employs multiple aliases in this kind of assault in order to increase their influence. Sybil attacks are associated with the way individuals create their identities or sign documents. Due to the OSN's structure and the system's accessibility, it is anticipated that widespread Sybil assaults will be feasible.



M. Denial-of-service Attack

The DDoS attack is a multi-source incursion that takes control of client resources and prevents users from providing support to actual clients. Attackers of DDoS are exploiting open source networks (OSNs) to target massive DDoS attacks. For instance, individuals can carry out this attack by adding {img¿ tags to Facebook notes. Facebook saves the image from the external server and scrolls it whenever this attribute is used.

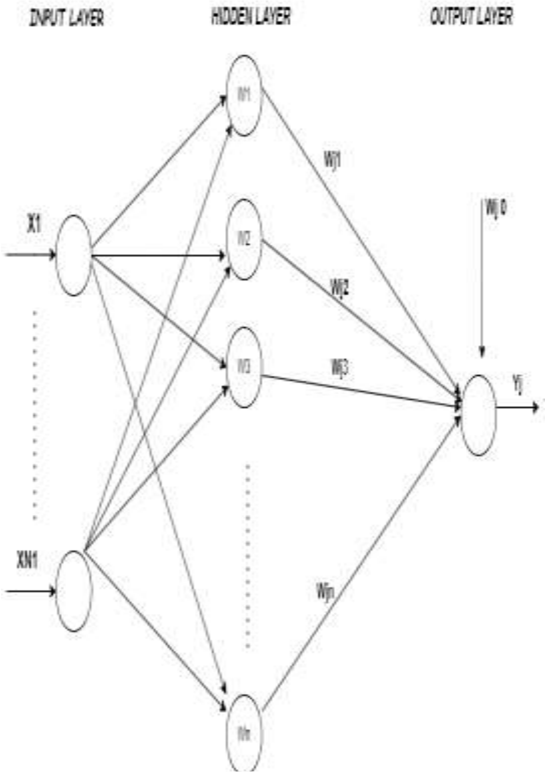


Facebook users frequently use any image and even specific text with intricate specifications.
Eventually, Facebook servers must repeatedly open the same file in one-page view.

III. MACHINE LERANING APPROACHES

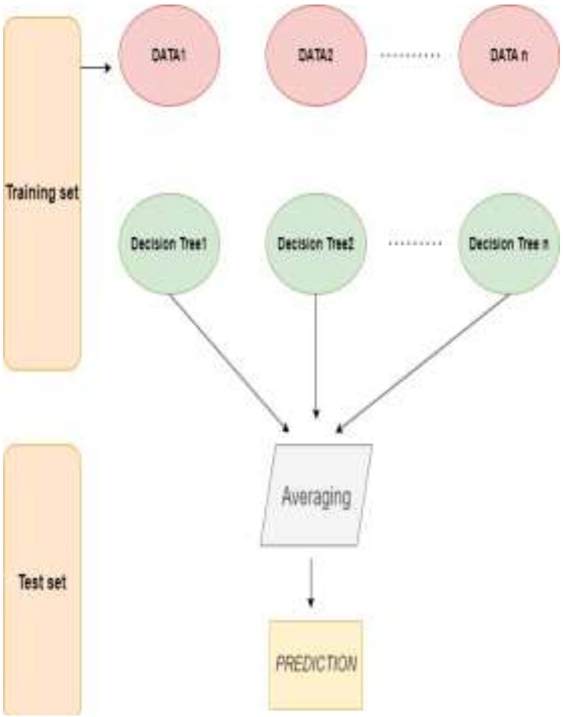
A. EXTREME LERANING MACHINE

The ELM algorithm is used to exploit feed-forward neural networks with one or more layers of secret nodes. These hidden nodes are arbitrarily balanced and the algorithm determines the appropriate performance weights analytically. According to the algorithm's designer, it can train neural networks several thousand times faster than traditional learning algorithms and produce excellent consistent results.



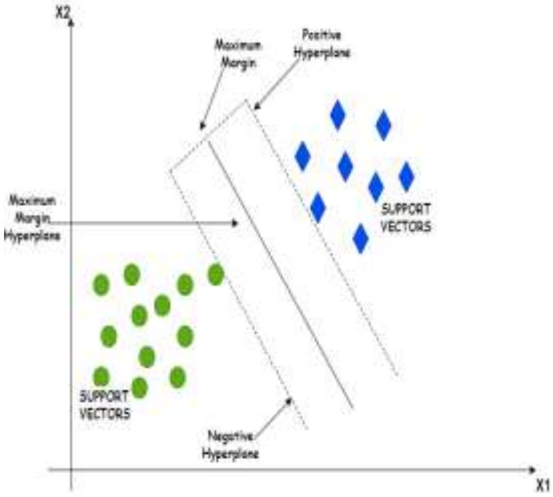
B. THE RANDOM FOREST

The machine learning algorithm supervises a number of decision trees used in the Random Forest technique for classification and regression tasks . Because the Random Forest method incorporates the concept of several trees voting based on a majority basis, it serves as a learning algorithm for the ensemble. The cumulative product of all tree groupings determines the algorithm's efficiency, which is expressed as a class prediction. Recent research has focused on the usefulness of radiofrequency (RF) for safety assaults, specifically in the areas of spam filtering, malware detection, injection attacks, etc.



C. SUPPORT VECTOR MACHINE

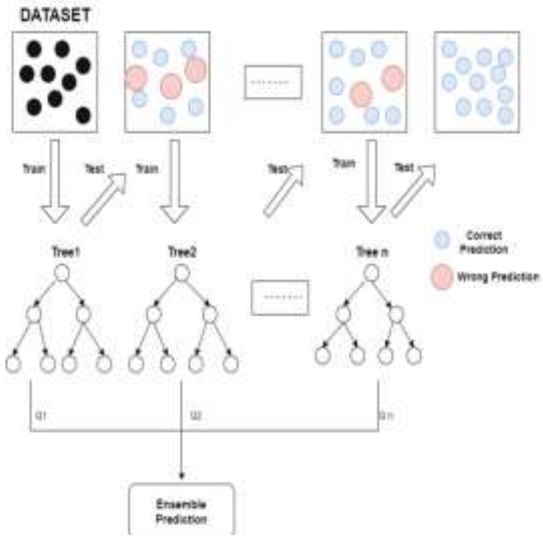
The Support Vector Machine (SVM) is a supervised learning model utilized in regression and classification analyses. It was highly sought to have great precision with lesscomputational power and sophistication. SVM is also utilized in computer security to identify intrusions. For instance, data based on a contemporary kernel function and the specific categorization of internet traffic have been evaluated using one class SVM. Finding the best hyperplane to accurately discriminate between distinct class data points is the primary objective of support vector machines (SVM). The hyperplane's height and input feature ratios are both less than one. (For instance, when dealing with three features, the hyperplane is two-dimensional.)Data dots on one side of the hyperplane (green and purple, as in Figure) are classified into one class, whereas data dots on the other side are classified into a different class. The difference between the hyperplane and the initial point (for all classes) on either side of the hyperplane serves as a check to see if the algorithm correctly handles its categorization decision. The right choice is made the wider the distance and the more precise our SVM is taken.



SVM

D. Boosting with a gradient

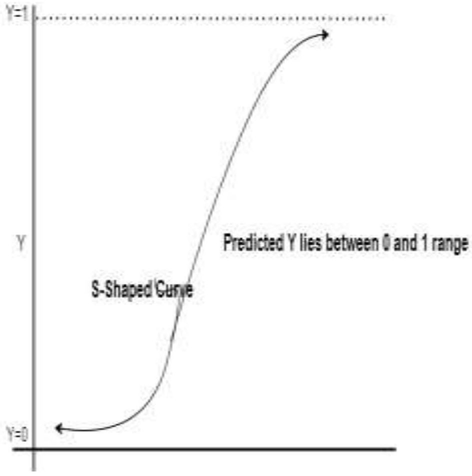
This approach, which combines classification and regression, creates the decision tree using a sequence of weighted prediction models. This combines the features of a loss function, an additive model, and a weak learner. This model adds the weak learners in order to minimize the loss function. Gradient boost works under the core premise that a weak-predicted model will be enhanced and residual trends will be used on a regular basis.The simulation of residues is terminated when it reaches a point where there is no configuration for the residuals (otherwise it could contribute tooverfitting).It involves loweringthe failure function mathematically in order to lower the likelihood of the test failing.



GRADIENT BOOSTING ALGORITHM

E. LOGISTIC REGRESSION

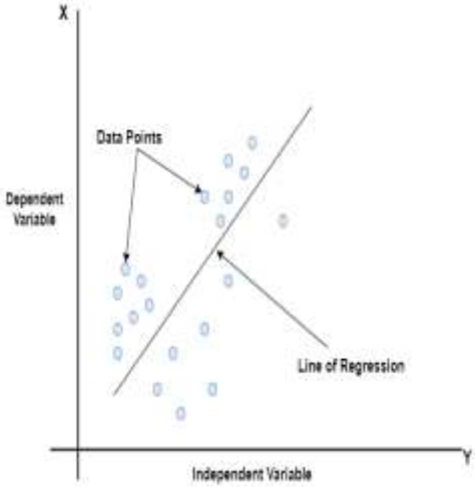
Although there are many more intricate extensions, logistic regression is a statistical model that uses a logistic equation as its fundamental form to predict a discrete dependant variable. Regression analysis is used to calculate logistic regression (also known as logit regression) as a logistical model parameter (a binary regression form). Logistic regression is a useful tool for identifying potentially dangerous network traffic.



LOGISTIC REGRESSION

F. Linear Regression

One type of supervised learning machine algorithm is linear regression. This carries out a regression function. A target value is predicted using regression using a variety of variables. The primary purpose of the interaction between factors and forecasting is identification. The type of interaction between the independent and dependent variables, the number of independent variables included, and their consideration all influence the differences across regression models.



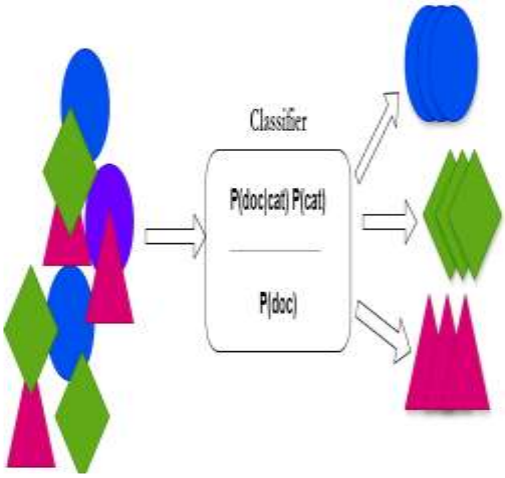
Linear Regression

G. Naive Bayes

This classification technique uses autonomous predictors, or Bayes theorem, as its foundation. To put it simply, the Naive Bayes Classifier makes the assumption that a given category has no additional functions in any class. Originally, a fruit with a round shape, a diameter of 3 cm, and a red tint may be referred to as an apple. Despite the fact that thesequalities vary and contain specific qualities.

The Naive Bayes grouping can view characteristics independently, which increases the likelihood that the fruit would be an apple.

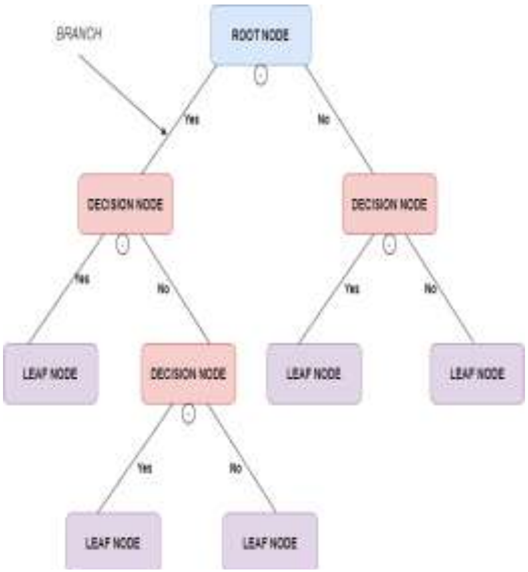
For really large data sets, the naive Bayesian model is especially helpful and easy to build. Naive Bayes is designed to perform highly complex classification tasks in addition to being simple.



NAIVE BAYES THEOREM

H. DECISION TREE

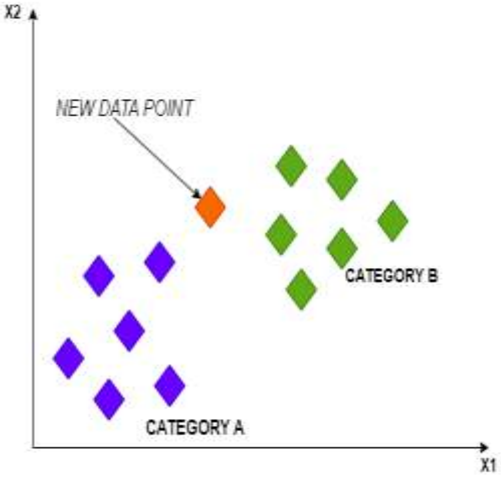
The learning algorithm is a type of supervised algorithm that is mainly applied to classification tasks. This works incredibly well with both continuous and categorical variables. We split individuals into two or more regular groups using this strategy. The most important characteristics and independent factors enable the rendering of various classes



DECISION TREE

I. KNN, or "k-Nearest Neighbours,"

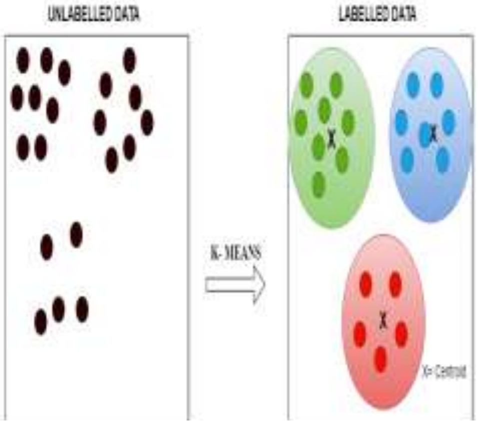
Both classification and regression issues are important. Nonetheless, it is most widely used in marking in the field. K The closest neighbours are a simple algorithm which stores all possible cases and classifies the new cases by majority of votes of their neighbours. The case of the class is most commonly determined by a distance function among its nearest K neighbours.Manhattan, Hamming ,Euclidean and Minkowski can be used as the distance functions. The first 3 functions and the fourth as categorical variables (hamming) are used for continuous function. The case is given simply to the next class of the neighbour if K = 1. At times, choosing K is a difficulty during the design phase of kNN.



KNN

J. K-Means

With each data point belonging to a single set, the K-means method is an iterative process that divides the dataset into preset non-overlapping subgroups (clusters). This seeks to maintain cluster distinctness (without bias) while bringing the data points between the clusters as close together as feasible. Data points are assigned to clusters so that the squared difference between the cluster centroid (the arithmetic mean of all the data points in the cluster) and the data points is as small as possible. The homogeneity of data points within a cluster increases with decreasing variance between clusters.



K- MEANS

IV. METHODOLOGY

a) Datasets

For our project we have taken a specific social media platform e.g. Facebook which is a multivariate dataset from Kaggle. This dataset have five attributes including username, channel name, country, main topics and likes. The main objective is to understand, simulate, and identifying vulnerabilities in social media networks through machine learning approaches.

b) Experimental Setups

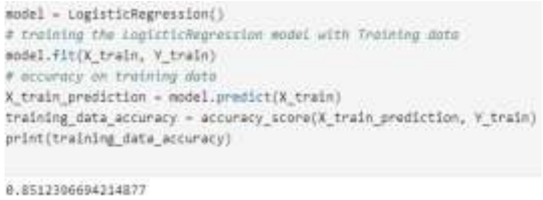
The Facebook dataset, which we gathered, has 150 tuples with the five attributes including username,channel name, country, main topics and likes. The username, channel name, and main topic is the three that are featured.

About 70% of the current dataset is made up of training data, while the remaining 30% is testing data.

Four distinct machine learning algorithms are used to acquire accuracy ,with a maximum accuracy of 0.85%.

The algorithms we have used is Logistic Regression followed by Random Forest , K – Nearest Neighbor and Confusion matrix.

After entering the input values researchers and security professionals can leverage machine learning to identify and mitigate social media networking attacks, enhancing the overall security of social media platforms.



```
model = LogisticRegression()
# training the LogisticRegression model with Training data
model.fit(X_train, Y_train)
# accuracy on training data
X_train_prediction = model.predict(X_train)
training_data_accuracy = accuracy_score(X_train_prediction, Y_train)
print(training_data_accuracy)

0.8512306694214877
```

V. CONCLUSION

People are the primary cause of security and privacy issues, despite the fact that advancements in relevant technology enable attackers to commit even more harmful security violations on social network websites. The cumulative information gleaned from our conversation will provide scholars and practitioners with a clear and accurate understanding of the reasons why privacy and protection challenges persist. Additionally, many approaches of using machine learning to solve the problems on networking sites are presented.

Ⅵ.ACKNOWLEDGEMENT

We would like to thank our supervisor, Miss Simranjotkaur, for their guidance and support throughout this research. Special thanks to our H.O.D MR.Vinay Chopra, Department of Computer Applications for their valuable feedback andDAV Institute of Engineering and Technology for their constant support ,suggestions and modifications to improve the quality of the paper.

REFRENCES

[1]. Sagar Dhanraj pandey, Neha Yadav and Nikhil karale,"Social networking attacks detection using machine learning approaches"available at https//www.researchgate.net/publication/350513726.

[2]. Ali, S.; Islam, N.; Rauf, A.; Din, I.U.; Guizani, M.; Rodrigues, J.J.P.C. Privacy and Security Issues in Online Social Networks. Future Internet 2018.

[3]. Asma A. Alsufyani Ama A. Alsufyani et al./ Indian Journal of Computer Science and Engineering (IJCSE) "Social Engineering Attack Detection UsingMachine Learning: Text Phising Attack."

[4]. Fire, M.; Katz, G.; Elovici, Y. Strangers intrusion detection-detecting spammers and fake profiles in social networks based on topology anomalies. Human J. 2012.