ISSN 2278-3091
Volume 9, No.5, September - October 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse10952020.pdf
https://doi.org/10.30534/ijatcse/2020/10952020

Implementation of Artificial Intelligence to Predict Threats in Social Media Based on User's Behavior

Rebin A. Saeed
College of Engineering and Computer Science, IT Department, Lebanese French University. Erbil. Iraq
Shareef M. Shareef
College of Education and Languages. Lebanese French University. Erbil. Iraq

ABSTRACT

The online social network users are with faced multiple vulnerabilities threats that are strategically implementing the social engineering mechanisms. Cybercriminals targeting the social engineering technique often investigate the environment in which a user is subjected. However, current research is pegged on the technical measurement of how threats can be neutralized or prevented completely in the online social network environment. It, therefore, follows that the online social networks systems create characteristics and elements which can be investigated further to produce relevant models. Facebook in the recent past has worked so hard and invested heavily in developing algorithms that are able to determinate an imminent cyber-attack based on user's behavior and characteristics on the platform. As much as Facebook has done relevant technical measures to ensure that threats are minimized as much as possible there is still a gap of further investigations which seek to harness the automated algorithmic prediction using artificial intelligence to determine the possibility of an attack or a threat. This research uses the machine learning techniques to show how an AI-based algorithm of the user's behavioral characteristics, perceptions, and socio-emotions that would help in identifying features that further become very relevant in determining an individual's vulnerability to social engineering threats and attacks. The aim is to primarily study the habitual perspective and perpetual perspective reactions towards socially engineered threats daily. This research uses a comparative analysis of the theories and the findings from the primary data to show that certain behaviors of Facebook users are a threat to other users. Through machine learning techniques, the results have shown how A.I. algorithms work in identifying scamming messages and scammers.

Key words: social engineering, threats, cyber-attacks, A.I. algorithm, machine learning prediction, A.I., social media.

1. INTRODUCTION

The online social networking platform has transformed into an engagement platform for millions of users who share information on business and many other associated areas. It is therefore imperative to understand that the large amount of information circulating in these online social networks exposes the entire platforms into security risks which could be otherwise predicted and prevented [1]. Analytically, social engineering has been presented to be one of the most critical threat angles that most online social network users do face. Apparently, training online social network users and enhancing their awareness of potential threats that exist within their environment has proven to be a very essential model for preventing minor threats that may take a social engineering perspective [2]; [3]. However, identifying users who may face potential threats in online social networks based on their behavior has become a challenge for quite some time. Based on the data of these users and their regular online behavior in social platforms, there is a plausibility that the prediction of their day-to-day engagement in online social networks can help identify the potential risk-based threats [4];[5] and as such help the users through proper training and advanced awareness campaign through the same platforms as well. Few of the social network users have the capacity to determine their security and privacy effectively [6]. However, an advanced security threat issues may only be solved through proper intervention model through enhancement of a well-developed structure.

This research focuses on producing relevant structures of detecting [7] and preventing possible threats and attacks based on users' behavior on the platform. This is because an attacker is often targeting the users and not the system. As such it is very important to develop a strong structural model for identifying possible threats based on social engineering protocols, thereby paving way for relevant actions to be taken by the Online Social Network (OSN) platform [4]. As much as a few studies have been conducted to determine the vulnerability of users online this paper at bringing a novel mechanism for vulnerability prediction based on specific user characteristics. The research targets Facebook platform and the engagement of users into the network platform coupled with the fact that most of these networks have competent ways of dealing with threats on their own platforms. Objectively this research also finds that there is a need to predictively study the user vulnerability based on their behavior whether it is direct or indirect as presented by evidence of individuals' characteristics. This paper is organized as follows: From the introduction, the second section is the related works including the previous studies on OSN threats, the third section is a methodology for data collection and data analysis, followed by results and discussions and final section is the conclusion.

2. RELATED WORKS

A few studies have used machine learning models and artificial intelligence to develop models that would

help controlling threats related to scamming messages and malicious digital contents. According to [8], most industries in modern society are on the verge of or have faced a social media security risk, most which have left these organizations or institutions in the middle of controversies. [9] predicted security threats on the internet and social media platform through the spreading of rumors and false information. The Trio justified their study approach by arguing that the volume of digital contents shared on the internet and social media platforms have a significant impact on the lives of people. [9] developed prevention and a mitigation framework for malicious information shared over the social media platforms using artificial intelligence and machine learning techniques. The study revealed the potential and significance of these two technologies in controlling the malice through falsified information and rumors on the internet and social media. A study by [11] developed a microscopic diffusion model to assist in preventing risks and threats from social media users through rumors and leaked information.

Fake accounts are another form of social networks risk. It usually involves the process whereby attackers create a form of attack with a specific intent and masquerade it in form of a fake account. Once completed, the attackers send friend requests under the account and once accepted, the account undertakes actions such as collect information on individuals. In July 2010, a profile that was fake named Robin sage was actively sent out to request connections from personas, upon which multiple people accepted the request even without the knowledge of which the woman was [12]. After a while, the account had successfully connected to with hundreds of people, from institutions including security firms, government as well as military. With that, such a social media security threat must not be underscored.

In a recent survey of participants of the annual RSA security conference that takes place in San Francisco, a vendor associated numbers to the social media security threats. In his report on employees' social network major workplace risk with relation to passwords, he found out that over 50 percent of employees had failed to change their passwords in the past year while 20 percent of this number had never had their passwords changed [13]. Most enterprises have raised concerns at the degree upon which their employees converge both their professional together with personal lives on social media platforms. Whether with intent or not, these employees by doing so either directly or indirectly put their respective institutions at risk of a potential social media security threat. As such, these enterprises expression of concern is warranted, since they are exposed to quite several key social media methodological attacks as well as threats [14]. In their article, [15] suggested that social network use has increased over the years, with most people intending to expand their network of online friends. However, as social networks make everyday life more comfortable, so does the threat to the security and privacy of the user's increase. The article argues that Artificial Intelligence is one of the computer sciences fields that can help to curb cyber threats. Today, most cybercrimes cannot be solved optimally due to their complexity. However, the artificial intelligence techniques such as fuzzy sets, multi-agent systems, neural networks, clustering, pattern recognition, data mining and evolutionary computations can be successful in solving some of the privacy issues in social networks [15].

Besides, according to [16], social media has become a crucial part of most people's careers, businesses, and social life. It also contributes to a much larger spectrum and intensity to society. The article suggests that cybercrimes can be prevented by analyzing the behavioral changes and sentiment analysis of people by predicting their thoughts through their social media posts using iterative clustering [16]; [17]. This approach can be crucial in providing solutions to people in need of socio-emotional problems or carrying out criminal activities. The article analyzes the unsupervised learning technique and classifies the clusters in predefined categories. The article has further explained in detail on how to undertake the algorithm and how to interpret the data found. If a change occurs in the first threshold, the behavior is not harmful but if the change occurs in the second threshold, then there is a need for immediate help. This article is extensive enough, and I find it in alignment with my research as they both provide valuable information that can help curb the incidences of cybercrime using Artificial Intelligence.

3. METHODOLOGY

The aim of this research is to develop a relevant algorithm to help in studying the behavioral features of users to determine if the user has an imminent threat or not. The most suitable approach for this research is the use of unsupervised learning. In this algorithm, there is no need to have a target variable to predict the outcome. There is no need to supervise the model but instead, allow it to work on its own to discover the patterns that were undetected before. Although this approach is more unpredictable compared to other machine learning algorithms, it is suitable for this research because it involves complex processing tasks to analyze the social media feeds, posts, and updates of a given user over a while to identify their behavior patterns [16]. Analyzing the type of feeds and posts that a user receives can help determine if they have social-emotional issues like depression and anxiety or their historical engagements with potential cybercriminals [18]. Unsupervised learning will be the most effective approach to this study because it identifies the unknown patterns in data and features that can be useful in categorization. Besides, the approach takes place in real-time, which is appropriate for real-time behavior analysis of the users. Lastly, it is easier to get unlabeled data from the Facebook platform requiring less manual intervention [19]. The unsupervised learning algorithm used for this research was K-means clustering. Besides, supervised learning was also used as a substitute to analyze the primary data of Facebook users. The goal of this approach is to approximate the mapping function so that the input variables can predict the outcome [20]. Linear regression was the most appropriate supervised learning algorithm to reduce errors and make the most accurate results of the study [21]. The representation of the

linear regression helped to determine the relationship between the input and output variables by finding the specific weightings of the input variables.

3.1 The system architecture

In detecting threats [4] online, this paper aims at providing an understanding and the potential of the sentiments behind the words being used by the users [7]. Feeds given by the user can be analyzed using k-means clustering so that a properly developed system extracts the potential threat exposure and vulnerability associated with the user. K-means clustering helps in finding the highest value for every iteration. The data is then clustered in k groups where a larger k means there are smaller groups with more granularity, while a lower k means that larger groups have less granularity [22]. In this architecture, the algorithm proposes collecting social web data over a period for every user and analyzing to the tune of specificity of the user and the data provided. The system architecture uses k-means clustering where data is collected, processed, features are identified and extracted, semantics are applied on the data for further specificity extraction, the data is then classified appropriately based on predetermined models of the algorithm, and finally relevant action is taken by the system network management team or automatically prevented via an advanced system protection integration module as shown in Figure 1. Despite the user negligence on security issues, the system is still able to protect the user from common malicious threats and advanced attacks that they may not know about – mostly from fake accounts that have systematically mined [4]. These characteristic and behavioral study of a specific user is the core of the study.

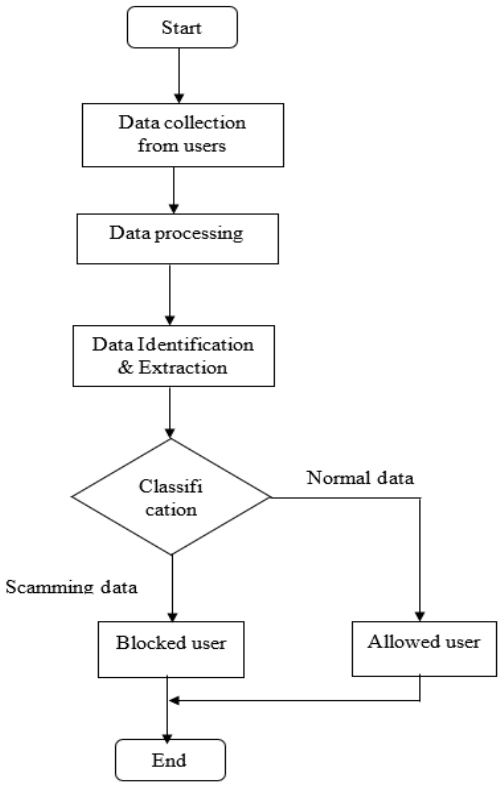

Figure 1: The flow chart showing the system architecture

4. ARTIFICIAL INTELLIGENCE IN SOCIAL MEDIA

Artificial intelligence has been widely appreciated in different angles on the internet of things. Most recently, artificial intelligence has been implemented in the online social networking platforms thereby providing ease of monitoring different behavioral and perception contexts of users. In modern technologically advanced social media platforms [16], there exist multiple and numerous technological threats in every dimension of Internet usage. Implementing artificial intelligence to incorporate widely used collected data to understand user behavior has helped in marketing and productivity prediction models that have proved very useful today. Prediction in marketing and managerial tasks that enhance productivity are not the only limits of artificial intelligence in online social networks [22]. One of the Major deployments of artificial intelligence in cybersecurity and user protection. Cybersecurity is another advanced and wide area in every internet-based application. However, determining threats and attacks in the online platform requires a heavy investment of resources and properly developed algorithms. The artificial intelligence that targets the prediction of threats and prevention of attacks has so far been implemented successfully by Facebook. However, Facebook has its own limits which are based on its user's privacy reasons and international laws that protect users from privacy rights infringement [6].

The online social networking platforms face daily cyber threats both from external parties as well as from the users themselves [18]. Users have been a common target for most online scammers and malicious application developers. The hacking community is currently targeting users to gain access to the databases of various social media platforms [16]. Just like common web-based applications online social networks face multiple threats because they host millions of users and millions of web visits monthly. Online social networks no longer support the concept of fun only but also have found their roots into businesses networking solutions as well as the greater context of social network aspects in human lives. The unprecedented developments in the information technology age have enhanced the spread of online social networks rapidly [22]. Millions of internet users' today is to find themselves in one or more social media networks for business or social reasons [16]. It is therefore important to take care of the online social networks by providing a proper security framework which predicts the viability of a threat taking place based on the user behavior and thereby suggesting a favorable mode of action to be taken. To predict how users in social networks behave, it is imperative to completely understand the underlying structures that are favorable for the hacking community.

Cybercriminals [4] are targeting every single aspect of weakness from specific social network platforms to harness information and cause data breaches. It is imperative to understand that social networking platforms need an advanced algorithmic module that will help study users' behavior to provide possible analytics of threat prevention mechanisms. Phenomenally, it has been found that most users fall in the trap of socially engineered

threats and attacks. In the recent past, social engineering attacks have been the center of attacks in major online social networks today [22]. Apart from data-stealing the cybercriminals often take over individual user's accounts and commit more criminal activities while the real user is locked out of their accounts. The effects of socially engineered threats are so many, but the conceptual prevention modality can take care of almost every single problem most people experience is online [18].

Traditionally studies were particularly useful in understanding and determining the technical perspective approach of threats and further prevention mechanisms that are only relevant to the old and less advanced internet-based devices. The advancement of technology and farther inclusion of specific laws that target protecting user's privacy, has made the concept of real-time feeds analysis so easy [6]. Well-engineered algorithms can help protect through the prediction of possible threats by studying the behavior of a user. The behavior of a user can be studied over time to provide concrete metadata for further analysis. Producing an automated artificially intelligent system has widely been implemented in Python for this study and takes the concept of code optimization to consume less processing resources and enhance efficiency during execution. Most online social network engineers face challenges of security module implementations since not every user has been trained and is aware of the potential threats that await them in the social platforms.

5. EXPERIMENTATION

According to [23] experimentation is a research method adopted in such a way that independent variable, also referred to us the cause of the study, is manipulated using the statistical tools and its effects on the dependent variable is measured. During the experiment, extraneous variables are controlled to allow the study to realize their objects. Nevertheless, [24] warn that the views and opinions of the researcher should not be incorporated in the experimental study because it might have negative effects on the results. The study adhered to this by ensuring that the results obtained and presented in this section were only based on the data collected from the study subjects. Furthermore, all extraneous variables were controlled to allow the researcher to observe, record and analyze the effects of predictor variables on the dependent or response variable.

This research also used experimentation to try and establish the efficacy of machine learning in the detection of online threat in social media. Through a series of predictive techniques, one is exposed to a few ways through which the behavior of people can be predicted using the machine learning algorithms [25]. For a better understanding of the nature of the experiment that this paper used in the collection of crucial experimental information for this research, it is imperative to understand the classification, regression, clustering, and the dimensionality reduction elements in machine learning behavioral prediction. This experiment was based on Scikit-learn platform, which executes a machine learning algorithm using Python language. The Scikit-learn was used because of its importance in machine learning within the Python language. The library was deemed suitable because it includes machine learning tools and statistical models for regression, classification, and clustering as well as for dimensionality reduction [25]. The study adopted both supervised and unsupervised machine learning methods to analyze the data collected from participants. The regression model was used as the supervised machine learning for predictive analysis while k-means was used as the unsupervised machine learning techniques for clustering.

Classification, in machine learning, is imperative in the identification of the most idyllic category in which a given parameter belongs. In the case of this research, the classification was centered on facial recognition as well as the detection of a spam message [25]. Image recognition is an essential security measure as Facebook can use it to authenticate account owners as well as their close associates or friends for that matter. Spam messages and accounts are a big threat as some of them contain malicious or even obscene messages that can impact the user experience online. To ensure the prediction of behaviors attached to spam detection and image recognition, [25] explain that algorithms like the nearest neighbors and the random forest are effective [26] and therefore were used as shown in Figure 2. Using the k-Nearest Neighbors and random forest made it possible to visualize the different categories of data or information shared on the Facebook by creating feature and target variables and splitting the data into training and test datasets [25].

As visualized in Figure 2, the first column represents the nature of input data, with the colors showing the different features of the data population to be tested. This is analogous to the different messages and other forms of digital information shared on Facebook and other social media platforms. Through k-Nearest Neighbors and random forest analyses, which are non-parametric, these input data are grouped according characteristics and the new data is categorized into a group which is nearest to it [25]. The second column visualizes the support vector machine (SVM) for regression to show how the data input is categorized based on their linear relations. Other categorization techniques are radial basis function (RBF) SVM and Gaussian process.

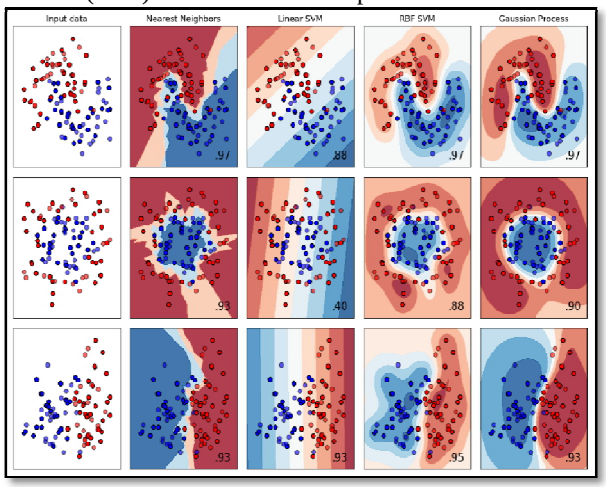

Figure 2: The plots showing comparison of training points in solid colors and testing points semi-transparent using Nearest neighbor and Random forest algorithm.

Regression entails the prediction of a significantly continuous-valued behavior that is pegged to a given user or object. The prediction of the behavior is done using the variations of the independent variables. The rationale behind the regression model is that there are independent factors who varied values cause proportional variation in the value of the predicted factor, which in this case is the behavior of Facebook users. In machine learning, the regression framework is most preferred when it comes to the prediction of the patterns of behavior through algorithms powered by Support Vector Regression (SVR), random forest, and the nearest neighbors [25]. As illustrated in Figure 3, there is a fluctuation in a variation of the target variable which is the behavior and data collected from the Facebook users. The pattern shows a negative effect of the data on the target behavior showing that the users have negative perceptions about the growing number of spam messages and vice versa.

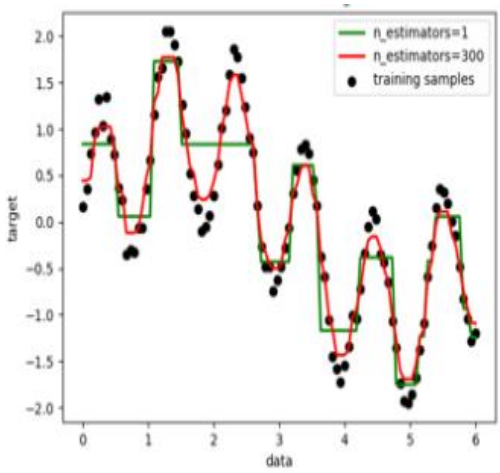

Figure 3: A boosted decision tree regression for predicting continuous-valued attribute associated with an object.

Clustering, as the name suggests, entails the grouping of homogenous patterns or parameters into sets with certain similarity indices. Through the grouping of similar behaviors into various discernible sets, clustering in machine learning is idyllic in the segmentation of user security classes or risk class [25]. To achieve reliable outcomes, the algorithms used in such cases are powered by k-Means, mean-shift, and spectral clustering as presented in the Figure 4. The classification is essential in discerning spam messages from the normal ones based on their features which the algorithm detect from the features of their content as shared by the Facebook users.

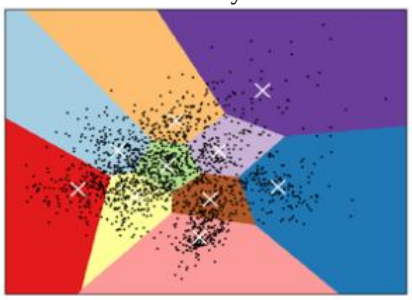

Figure 4: k-means clustering on digits data set, where white cross marks the centroids

Machine learning can also reduce the size of the variables that are random within a given dataset, a process that is referred to as dimensionality reduction. Based on the nature of this process, the application is best suited for visualizations and in cases where efficiency of the outcomes is given more priority. As such, the algorithms that are used for this purpose use feature selection method, k-Means [25], and the non-negative matrix factorization as depicted in Figure 5 which shows a three-dimensional result.

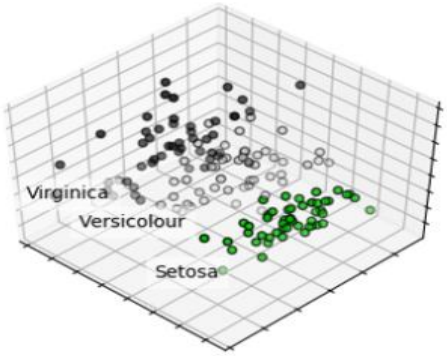

Figure 5.:k-means and non-negative matrix factorization in 3D diagram

For this experiment, this research focused on image recognition as a potential measure that can be used as a security tool on Facebook. This process exploited the use of a multi-output sensor estimator as the core tool in the identification of the images. In the case of Facebook, this security feature can be introduced when one is logging in to their accounts. As part of a two-step verification process, the user can use his or her password as the first security measure. Once the password was typed correctly and verified, the user was redirected to the second step, which was purely AI-guided. A set of pictures previously selected by the user were posted with the lower parts blurred. The users were then required to match the lower facial parts to the upper facial's parts. Most of these pictures were those of the user's choices like family members, schoolteachers or even friends. This framework was also used in the detection of potential threats in the event where certain users were either flagged down or put on the watch list for various cybersecurity crimes or threats for that matter. Once flagged, users would tend to alter their looks through either photo editing filters or software, something that posed a daunting task for the human force to single out.

This experiment used four Facebook photos of the respondents that were used in the questionnaire to substantiate the efficacy of A.I. in the detection of threats through image recognition. Figure 6 shows how various algorithms strived to complete the lower part of the faces with a clear comparison to the original photos of the people used in the experiment.

Figure 6. Face recognition through AI-guided algorithm

From Figure 6, it is evident that extra trees give the closest resemblance to the true photos of the users. The other algorithms, though they try to complete the lower facial features, are a bit shaky. Through the comparison of the outcomes, the extra tress algorithm is the most viable to use. However, the other algorithms were included in the machine learning process to ensure that any forms of image peculiarity are internalized. This is evident in the linear regression algorithm that tends to put more emphasis on facial hair, something that extra trees tend to disregard in the learning process. The code of the learning process is a prototype A.I. that can be used in the facial recognition of the image parameters loaded to it. The machine learns the faces associated with a given social media account and establishes a list of fit estimates. The two are compared to enable the completion of the faces, something that authenticates the log in process.

6. RESULTS AND DISCUSSION

The results and discussion section discusses the critical research data results that was collected in this research data. The questionnaire response rate is critically analyzed together with the corresponding survey research so that the relevant conclusions can be drawn. These conclusions are data based and thus they are valid.

6.1 Participants response

Online social network users face numerous threats [21] daily. Some of the threats are developed by fake attack accounts that are primarily targeting the users themselves. The social networking platforms have developed various methods for combating such problems. Facebook, for instance has invested heavily in securing its users and their social accounts effectively. It is therefore commendable that Facebook has developed AI-based algorithms that helped determine the behavior of a user and shield them from potential threats and attacks as well as eliminate fake accounts from attackers [21]. Such security modulation and presentation has been made possible through automated AI-based systems of complex algorithmic structures. However, this paper has specifically targeted cross-platform online social networks and thereby developing a common structural algorithm that can help protect users from various threats that they may face even without knowing that they are protected. For instance, one of the most common models of presenting this issue is by automatically identifying if a user account is fake or being watched over by malicious applications. Other examples include advising the users to automatically implement a second authentication factor to help secure them even further. Training and awareness models, for example, by asking them never to share their passwords or account details, is one method that has been traditionally existing ever since the social networking platforms, are made. The social networking platforms have proved to be very productive in terms of designing automatically pre-installed threat protection mechanisms in their systems.

In our study, a quantitative methodology was used in the form of a questionnaire to at least 100 participants to support the conclusion of the study. This is because questionnaires gave us a chance to get feedback directly from the research respondents. Questionnaires were also cheap and convenient as they could be emailed through google forms.One hundred questionnaires, with a total of 15 questions, were used to meet the needs of the study. The participants were then divided into two groups, one sample included victims of cybercrimes, and the other sample was on professionals. Both groups then gave their opinions of A.I. use as a means of curbing cybercrimes. On gender composition, 40 of the participants were female, while 60 were male. Besides, Facebook is a social platform that does not restrict the minimum age requirement. However, the study did not focus on the younger generation due to their level of inexperience. Sixty participants were between 18-28 years, representing 60% of all participants. Twenty participants were between 28-38 years, while there wereten participants both below 18 years and over 38 years. From the participant age composition, we can conclude that most of the Facebook users prone to cyber-attacks are between 18 to 28 years. Nonetheless, all the questionnaires were returned, representing a 100% response rate of both samples. The results of the questionnaire are provided in Table 1.

Table 1: Descriptive summary of the survey output

	Percentage of Respondents				
Question Item	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Artificial intelligence via social media could aid in building and protection of a brand.	40%	30%	0%	30%	0%
AI improves user experience in social media.	50%	30%	0%	10%	10%
AI is also used to observe resources in social media	10%	80%	0%	10%	0%
AI is a boon to social media cybersecurity	70%	20%	0%	10%	0%
AI has presented tools such as chatbots together with virtual assistants, which help many enterprises improve their marketing strategies by making good use of social media.	30%	60%	0%	10%	0%
Machine learning is one way to detect cyber threats in social media.	50%	20%	0%	20%	10%
Another means of threat detection in social media by use of AI is use of AI authentications and password protection systems.	60%	20%	0%	10%	10%

Our research found that Artificial Intelligence has a significant impact on promoting brands and protecting users from cyber-attacks. Contrary to the belief that A.I. can lead to more cyber-crimes, most participants disagreed on the issue contributing to the conclusion that Artificial Intelligence can instead help in reducing social network crimes. Besides, over time, social media platforms have improved the user experience by using algorithms to understand user behavior and, as a result, make recommendations on the relevant content. The same algorithms to study user behavior can also help identify potential threats and act immediately to protect the user's privacy. From these findings, we can carry out experimentation on how organizations and other users of the social media platform can use Artificial Intelligence as a tool to reduce cyber-attacks.

7. FUTURE WORK

In future, the algorithm proposes a standard model through which there is an automated decision-making process through integration with the decision support system. This study proposes an algorithmic process for designing a modern AI-based mechanism that will help in identifying threats through user behavior and thereby reporting such issues for relevant actions. In an advanced futuristic development, the same system model will be able to automatically stop an imminent threat targeting the specific users.

8. CONCLUSION

As organizations increasingly depend on computers and the internet to complete important tasks especially through communication and data sharing there is a risk of threats based on user behaviors, especially in the online social networks. Based on this concept the cybersecurity issue has become a very significant and essential aspect of every technological industry today. The online social network not being targeted by cybercriminals for quite a long time. However, the security practitioners in every department have consistently been approaching the issue through a technical measure to provide protection. According to the dynamism in social engineering, online threats have changed and cybercriminals today at targeting weaknesses among users based on social behavior. Considering such vulnerability existence, the study has developed an algorithm that aims at predicting the extent to which a combination and integration of user-related factors are dimensionally put together to help predict the users' vulnerability towards the socially engineered threats. The algorithm is implemented in Python programming language which has currently scored better in data mining mechanisms.

REFERENCES

[1] Alqatawna, J., Madain, A., Al-Zoubi, A.M., and Al-Sayyed, R.,**Online social networks security: Threats, attacks, and future directions**. In the book "Social Media Shaping e-Publishing and Academia" (Editors: N. Taha, R. Al-Sayyed, J. Alqatawna, and A. Rodan), Springer. Berlin, Germany. pp. 121-132, 2017.

[2] Fonseka, T.M., Bhat, V., and Kennedy, S.H., "**The utility of artificial intelligence in suicide risk prediction and the management of suicidal behaviors**", Australian & New Zealand Journal of Psychiatry Vol.53, no.10, pp.954-964, 2019.

[3] Ahmad, F., Khairunesa, I.S.A., Jamin, J., Rosni, N., and ThulasiPalpapanadan, S. "**Social media usage and awareness of cyber security issues among youths**", International Journal of Advanced Trends in Computer Science and Engineering vol.9, no.3, pp. 3090-3094, 2020.

[4] Ghari, W., "**Cyber threats in social networking websites",** International Journal of Distributed and Parallel Systems Vol.3, no.1, pp. 119-126, 2012.

[5] Almeida, H., Briand, A. and Meurs, M.J., **Detecting Early Risk of Depression from Social Media User-generated Content**. In the book"*CLEF (Working Notes)*". pp. 1-12, 2017.

[6] Raad, E. andChbeir, R.,**Privacy in online social networks**. In the book "Lecture Notes in Social Networks" (Editors: R. Chbeir and B. Al Bouna), Springer. Vienna, Austria. pp. 3-45, 2013.

[7] Kirichenko, L., Radivilova, T., and Anders, C. "**Detecting cyber threats through social network analysis: Short survey",** Socio-Economic Challenges Vol.1, pp. 20-34, 2017.

[8] Alguliyev, R., Aliguliyev, R. and Yusifov, F., **MCDM Model for Evaluation of Social Network Security Threats**. In the book "ECDG 2018 18th European Conference on Digital Government" (Editors: R. Bouzas-Lorenzo and A. Cernadas Ramos), University Santiago de Compostela. Spain, pp. 1-7, 2018.

[9] Wentao, C.H.U., Kuok-Tiung, L.E.E., Wei, L.U.O., Bhambri, P., andKautish, S. "**Predicting the security threats of internet rumors and spread of false information based on sociological principle",** Computer Standards & Interfaces Vol.73, pp. 1-7, 2021.

[10] Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... and Anderson, H.,**The Malicious Use of Artificial Intelligence : Forecasting, Prevention, and Mitigation**, 2018, available at https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf

[11] Wu, Y., Huang, H., Wu, Q., Liu, A., and Wang, T., "**A risk defense method based on microscopic state prediction with partial information observations in social networks**", Journal of Parallel and Distributed Computing Vol.131, pp. 189-199, 2019.

[12] Reischer, A.J., Orrange, J., Brightwell, S., Riemer, L. and Conahan, N., Social Sentinel Inc., **Systems and Methods for Identifying Safety and Security Threats in Social Media Content**. U.S. Patent Application 16/079,023, 2019.

[13] Chen, L., Gong, T., Kosinski, M., Stillwell, D., and Davidson, R. L.,"**Building a profile of subjective well-being for social media users**",PloSOne Vol.12, no.11, pp. 1-15, 2017.

[14] Dorofeev, A., Markov, A. and Tsirlov, V., **Social Media in Identifying Threats to Ensure Safe Life in a Modern City**. In the book"International Conference on Digital Transformation and Global Society" (Editors: A. Chugunov, A., R. Bolgov, Y. Kabanov, G. Kampis, and M. Wimmer), Springer. Cham, pp. 441-449, 2016.

[15] Sattikar, A.A. and Kulkarni, R.V., "**A role of artificial intelligence techniques in security and privacy issues of social networking**", International Journal of Computer Science Engineering & Technology Vol.2, no.1, p. 792, 2012.

[16] Jindal, S., and Sharma, K.,"**Intend to analyze social media feeds to detect behavioral trends of individuals to proactively act against social threats**", Procedia Computer Science Vol.132, pp. 218-225, 2018.

[17] Nie, D., Guan, Z., Hao, B., Bai, S. and Zhu, T., **Predicting Personality on Social Media with Semi-Supervised Learning**. In the book "*2014 IEEE/WIC/ACM International Joint Conferences on Web Intelligence (W.I.) and Intelligent Agent Technologies (IAT)*", IEE. Warsaw, Poland, pp. 158-165, 2014.

[18] Feng, B., Li, Q., Ji, Y., Guo, D., and Meng, X.,"**Stopping the cyberattack in the early stage: Assessing the security risks of social network users**", Security and Communication Networks Vol.2019, pp. 1-14, 2019.

[19] Luceri, L., Braun, T. and Giordano, S., "**Analyzing and inferring human real-life behavior through online social networks with social influence deep learning**", Applied Network Science Vol.4, no.1, p.34, 2019.

[20] Ghahramani, Z., **Unsupervised Learning**. In the book "Summer School on Machine Learning" (Editors: O. Bousquet, U. von Luxburg, and G. Ratsch), Springer, Berlin, Heidelberg, Germany. pp. 72-112), 2003.

[21] Barlow, H.B., "**Unsupervised learning**", Neural Computation Vol.1, no.3, pp.295-311, 1989.

[22] Fire, M., Goldschmidt, R. and Elovici, Y., "**Online social networks: threats and solutions**", IEEE Communications Surveys & Tutorials Vol.16, no.4, pp.2019-2036, 2014.

[23] Yu, D., Chen, N., Jiang, F., Fu, B. and Qin, A., "**Constrained NMF-based semi-supervised learning for social media spammer detection**", Knowledge-Based Systems Vol 125, pp.64-73, 2017.

[24] Dorofeev, A., Markov, A. and Tsirlov, V., **Social Media in Identifying Threats to Ensure Safe Life in a Modern City**. In the book "International Conference on Digital Transformation and Global Society: First International Conference, DTGS 2016" (Editors: A.V. Chugunov, R., Bulgov, Y. Kabanov, G. Kampis, and M. Wimmer), Springer. Cham, pp. 441-449, 2016.

[25] Fonseka, T.M., Bhat, V., and Kennedy, S.H., "**The utility of artificial intelligence in suicide risk prediction and the management of suicidal behaviors**", Australian & New Zealand Journal of Psychiatry Vol.53, no.10, pp.954-964, 2019.

[26] Villanueva, J.A., Lacatan, L.L., and Vinluan, A.A. "**Information technology security infrastructure malware detector system**", International Journal of Advanced Trends in Computer Science and Engineering Vol.9, no.2, pp. 1583-1587, 2020.