QALAAI ZANISTSCIENTIFIC JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil, Kurdistan, Iraq
Vol. (6), No (1), Winter 2021
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

Prediction of The Security Threats in Social Media Using Artificial Intelligence

Rebin A. Saeed
Department of IT, College of Engineering and Computer Science, Lebanese French University. Erbil, Kurdistan Region, Iraq
rebin.abdullah88@gmail.com

Shareef M. Shareef
College of Education and Languages, Lebanese French University, Erbil, Kurdistan Region, Iraq
s.shareef@lfu.edu.krd

ARTICLE INFO

Article History:
Received: 2/12/2020
Accepted: 4/1/2021
Published: Winter 2021

Keywords: *social engineering, threats, cyber-attacks, AI algorithm, machine-learning prediction, AI, social media.*

Doi:
10.25212/lfu.qzj.6.1.38

ABSTRACT

The online social network clients are exposed to various weaknesses dangers deliberately by actualizing social designing systems. Cyber-Criminals are focusing on the social designing method regularly explore the climate of a client. Nonetheless, ebb and flow research centers around the specialized estimation of how to kill or forestall dangers totally in the online informal community climate. Along these lines, the online informal organization frameworks utilize pertinent models to make highlights for additional examination. Facebook, in the ongoing past, has buckled down and put intensely in creating calculations that can decide an up-and-coming digital assault dependent on client's conduct and qualities on the stage. Despite the fact that Facebook has done important specialized measures to limit dangers however much as could be expected, there is as yet a hole for additional examinations, which try to outfit the mechanized algorithmic forecast utilizing man-made consciousness to decide the chance of an assault or a danger. This exploration utilizes AI strategies to show how an AI-based calculation of the client's conduct attributes, insights, and human science feelings would help recognize

QALAAI ZANISTSCIENTIFIC JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil, Kurdistan, Iraq
Vol. (6), No (1), Winter 2021
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

highlights that further gotten extremely significant in deciding a person's weakness to social designing dangers and assaults. The point is to; fundamentally study the conventional viewpoint and never-ending viewpoint responses towards socially designed dangers day by day. This exploration utilizes a near examination of the speculations and the essential information discoveries to show that specific practices of Facebook clients are a danger to different clients. The outcomes have demonstrated how AI calculations work in distinguishing misleading messages and con artists through AI methods.

I. INTRODUCTION

The online long range interpersonal communication stage has changed into a commitment stage for a great many clients who share business data and other social associations. Accordingly, comprehend that the enormous measure of data circling in these online informal organizations uncovered the whole stage to security hazards, which are generally unsurprising and potentially preventable [1]. Logically, social designing has been one of the most basic danger points that most online informal organization clients face. Preparing on the web interpersonal organization clients and upgrading their consciousness of expected dangers inside their current circumstance has demonstrated to be a fundamental model for forestalling minor dangers that may take a social designing viewpoint [2]; [3]. Notwithstanding, recognizing clients who may confront likely dangers in online informal communities dependent on their conduct has become a test for a long while. In light of these clients' information and their ordinary online conduct in social stages, there is a believably that the forecast of their everyday commitment in online interpersonal organizations can help recognize the potential danger-based dangers [4];[5]. That permits the clients through legitimate preparing and progressed mindfulness crusade through similar stages also. Not many of the interpersonal organization clients can decide their security and protection practically [6]. Be that as it may, progressed security danger issues may just be dis-solvable through an appropriate intercession model by upgrading a very much created structure.

This examination centers around creating significant structures for distinguishing [7] and forestalling potential dangers and assaults dependent on clients' conduct on the stage. It is on the grounds that an aggressor is regularly focusing on the clients and not the framework. Accordingly, it is basic to build up a vigorous underlying model for

QALAAI ZANISTSCIENTIFIC JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil, Kurdistan, Iraq
Vol. (6), No (1), Winter 2021
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

distinguishing potential dangers dependent on social designing conventions, consequently making ready for important moves to be made by the Online Social Network (OSN) stage [4]. A couple of studies have been directed to decide the weakness of clients on the web. This paper brings a novel system for weakness forecast dependent on explicit client attributes. The exploration focuses on the Facebook stage and the commitment of clients into the organization stage, combined with the way that the vast majority of these organizations have insightful methods of managing their media dangers. Impartially, this exploration additionally finds a need to; predicatively study client weakness dependent on their conduct, regardless of whether immediate or aberrant, as introduced by proof of people's qualities. This paper is coordinated as follows: From the presentation, the subsequent area is the connected works, remembering the past investigations for OSN dangers, the third segment is an approach for information assortment and information examination, trailed by results and conversations, and the last segment is the end.

II. RELATED WORKS

A few studies have used machine learning models and artificial intelligence to develop models to control threats related to scamming messages and malicious digital content. According to the current study [8], modern organizations are on the verge of, or are faced with a social media security risk. Most of which have left these organizations or institutions in the middle of controversies. The study by [9] predicted security threats on the internet and social media platforms through the spreading of rumors and false information. The Trio justified their study approach by arguing that the volume of digital content shared on the internet and social media platforms significantly affect the lives of people. In the recent study, [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 malice through falsified information and rumors on the internet and social media. A study by [11] developed a microscopic diffusion model to prevent risks and threats from social media users through rumors and leaked information.

Fake accounts are another form of social network risk. It usually involves the process whereby attackers create a state of attack with a specific intent and masquerade it in the way of a fake account. Once completed, the attackers send friend requests under the account, and once accepted, the account undertakes actions such as collect

QALAAI ZANISTSCIENTIFIC JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil, Kurdistan, Iraq
Vol. (6), No (1), Winter 2021
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

information on individuals. In July 2010, a fake profile 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 with hundreds of people, from institutions including security firms, government, and military. With that, such a social media security threat has a significant impact on users.

A recent survey focused on participants in the annual RSA security conference in San Francisco, a vendor associated numbers with social media security threats. In his report on employees' social network significant workplace risk regarding 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 their protection and 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 several critical social media methodological attacks and risks [14]. In their article, [15] suggested that social network use has increased over the years, with most people intending to expand their online friends' network. 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 curb cyber threats. Today, most cybercrimes are not solvable optimally due to their complexity. However, artificial intelligence techniques such as fuzzy sets, multi-agent systems, neural networks, clustering, pattern recognition, data mining, and evolutionary computations can help solve some of the privacy issues in social networks [15].
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 broader spectrum and intensity to society. The article suggests that cybercrimes are preventable by analyzing people's behavioral changes and sentiment analysis by predicting their thoughts through their social media posts using iterative clustering [16]; [17]. This approach can be crucial in providing solutions to socio-emotional problems or carrying out criminal activities. The article analyzes the unsupervised learning technique and classifies the clusters into predefined categories. The research has further explained how to undertake the algorithm and how to interpret the data

QALAAI ZANISTSCIENTIFIC JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil, Kurdistan, Iraq
Vol. (6), No (1), Winter 2021
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

found. If a change occurs in the first threshold, the behavior is not harmful, but if the change occurs in the second threshold, immediate help is needed. This article is extensive enough, and I find it in alignment with my research. They both provide valuable information that can help curb the incidences of cybercrime using Artificial Intelligence.

III. METHODOLOGY

This research aims to develop a relevant algorithm to study users' behavioral features to determine if the user has an imminent threat. The most suitable approach for this research is the use of an unsupervised machine learning technique. 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 undetected patterns beforehand. Although this approach is more unpredictable than 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 commands that a user receives can help determine if they have social-emotional issues like depression and anxiety or their historical engagements with potential cyber criminals [18]. Unsupervised learning techniques are the most suitable for data categorization in this study. It is because it identifies the unknown patterns in data and categorization. Besides, the procedure takes place in real-time, which is appropriate for the users' real-time behavior analysis. 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. The study also adopted a supervised learning technique as a substitute to analyze Facebook users' primary data. This approach aims 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 study's most accurate results [21]. The linear regression representation helped determine the relationship between the input and output variables by finding the specific weightings of the input variables.

A. The system architecture

Detecting security threats online [4] has been addressed in this paper to understand the magnitude and potential of user vulnerability and prevention mechanisms. The

QALAAI ZANISTSCIENTIFIC JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil, Kurdistan, Iraq
Vol. (6), No (1), Winter 2021
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

user's behavior is gauged by the sentiments behind the words being used by the users [7]. The user's feeds 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 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 the user's specificity and the data provided. The system architecture uses k-means clustering where data is collected, processed, features are identified and extracted, and semantics are applied to the data for further specificity extraction. The information is then classified appropriately based on the algorithm's predetermined models. Finally, the team that manages system network has taken relevant action or automatically prevented via an advanced system protection and integration module, as shown in Figure 1. Despite user negligence on security issues, the system can still 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 characteristics and behavioral study of a specific user is the core of this study.

QALAAI ZANISTSCIENTIFIC JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil, Kurdistan, Iraq
Vol. (6), No (1), Winter 2021
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

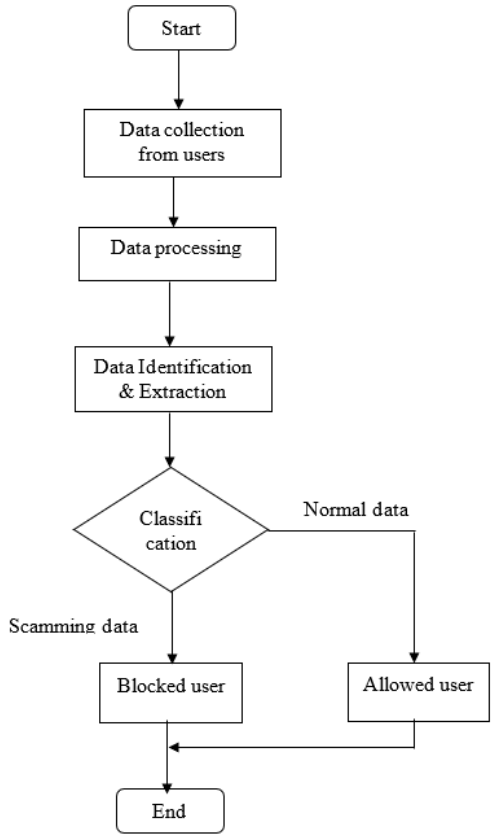

Figure 1. The flow chart showing the system architecture

IV. ARTIFICIAL INTELLIGENCE IN SOCIAL MEDIA

Artificial intelligence has been widely appreciated from different angles on the internet of things. 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 is not the only limit of artificial intelligence in online social networks [22]. The Major deployment of artificial

QALAAI ZANISTSCIENTIFIC JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil, Kurdistan, Iraq
Vol. (6), No (1), Winter 2021
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

intelligence is cybersecurity and user protection. Cybersecurity is another advanced and comprehensive area in every internet-based application. However, determining threats and attacks in the online platform requires a massive investment of resources and adequately developed algorithms. Facebook has successfully implemented artificial intelligence that targets the prediction of threats and prevention of attacks. However, Facebook has its limits 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 from both external parties and 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 access the databases of various social media platforms [16]. Like typical web-based applications, online social networks face multiple threats because they host millions of users and millions of monthly web visits. Online social networks no longer support the concept of fun only. However, they have found their roots in business networking solutions and the greater context of social network aspects in human lives. The unprecedented developments in the information technology age have rapidly enhanced the spread of online social networks [22]. Today's millions of internet users are to find themselves in one or more social media networks for business or social reasons [16]. Therefore, it is essential to take care of the online social networks by providing a proper security framework that predicts the viability of a threat happening based on the user behavior, thereby suggesting a favorable mode of action. It is imperative to understand the underlying structures favorable for the hacking community thoroughly.

Cybercriminals [4] target every 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 to help study users' behavior to provide possible analytics of threat prevention mechanisms. Phenomenally, it has been found that most users fall into 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, cybercriminals often take over individual user's accounts and commit activities that are more criminal 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].

QALAAI ZANISTSCIENTIFIC JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil, Kurdistan, Iraq
Vol. (6), No (1), Winter 2021
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

Traditionally studies were particularly useful in understanding and determining the technical perspective approach of threats and other prevention mechanisms relevant to the old and less advanced internet-based devices. The advancement of technology and the further 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 action of a user can be analyzed over time to provide concrete metadata for further analysis. Producing an automated artificially intelligent system has widely been implemented in Python for this study. It takes the concept of code optimization to consume less processing resources and enhance efficiency during execution. Most online social network engineers face security module implementations' challenges since not every user has been trained and is aware of the potential threats that await them in the social platforms.

V. EXPERIMENTATION

According to [23], experimentation is a research method adopted in such a way that the independent variable, also referred to as the cause of the study, is manipulated using the statistical tools, and its effects on the dependent variable are 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.

A. Machine Learning Efficacy in Threat Detection

This research also used experimentation to establish the efficacy of machine learning in detecting online threats in social media. Through a series of predictive techniques, one is exposed to a few ways through which people's behavior can be predicted using machine learning algorithms [25]. To better understand 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 dimensionality reduction elements in machine learning behavioral prediction. The

QALAAI ZANISTSCIENTIFIC JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil, Kurdistan, Iraq
Vol. (6), No (1), Winter 2021
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

experiment was based on the 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, and 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 influence 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 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 for testing. It is analogous messages and other forms of digital information shared on Facebook and other social media platforms. These input data are grouped according to characteristics through k-Nearest Neighbors and random forest analyses, which are non-parametric. The new data is categorized into the nearest group [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.

QALAAI ZANISTSCIENTIFIC JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil, Kurdistan, Iraq
Vol. (6), No (1), Winter 2021
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

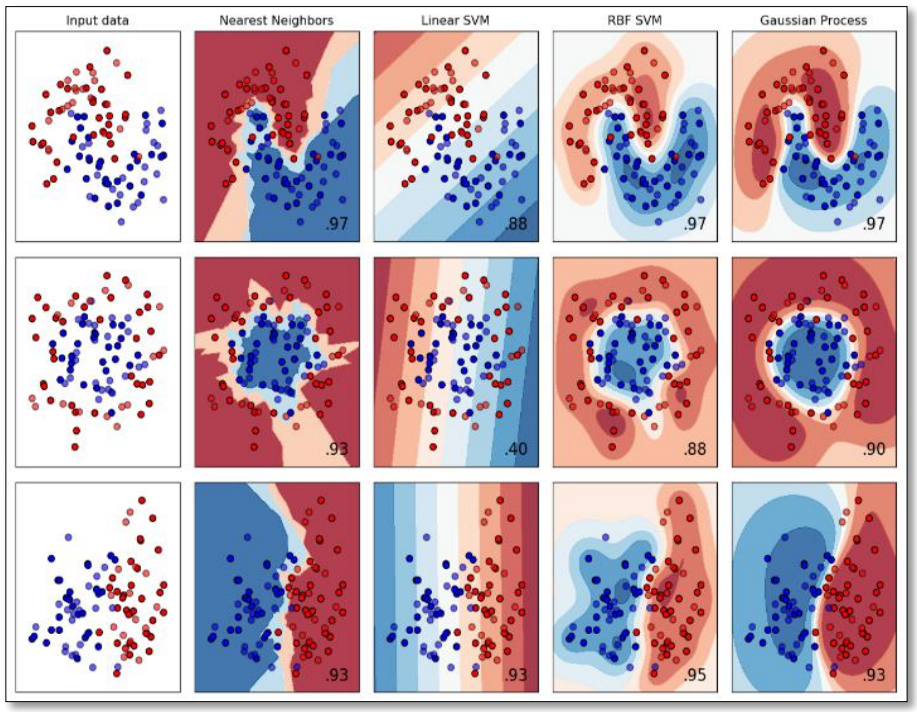

Figure 2. Plots comparing training points in solid colors and testing points semi-transparent using nearest neighbor and Random forest algorithm.

Regression entails the prediction of a significantly continuous-valued behavior that is pegged to a given user or object. The prediction of the action is made using the variations of the independent variables. The rationale behind the regression model is that there are independent factors whose varied values cause proportional variation for the factor, which is the behavior of Facebook users. In machine learning, the regression framework is most preferred when it comes to predicting 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 the target variable's variation, which is the behavior and data collected from Facebook users. The pattern shows an adverse effect of the target behavior of data

QALAAI ZANISTSCIENTIFIC JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil, Kurdistan, Iraq
Vol. (6), No (1), Winter 2021
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

showing that the users have negative perceptions about the growing number of spam messages and vice versa.

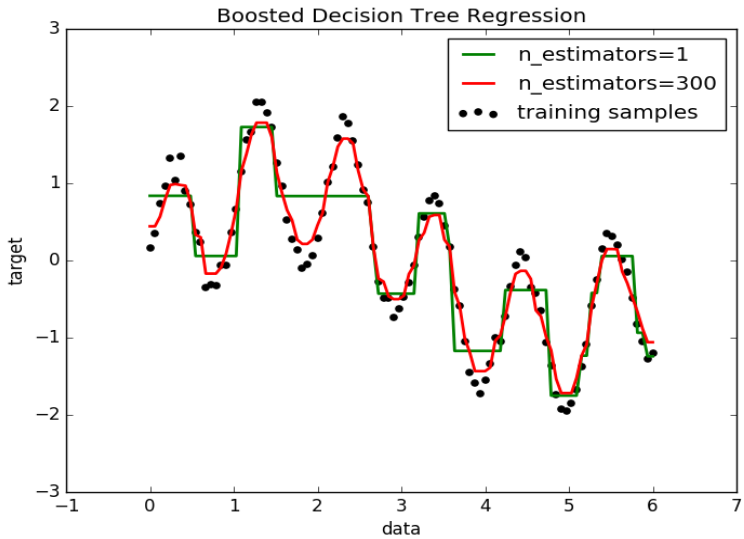

Figure 3. A boosted decision tree regression for predicting continuous-valued attributes associated with an object.

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 Figure 4. The classification is essential in discerning spam messages from the normal ones based on their features, which the algorithm detects from the features of their content as shared by the Facebook users.

QALAAI ZANISTSCIENTIFIC JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil, Kurdistan, Iraq
Vol. (6), No (1), Winter 2021
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

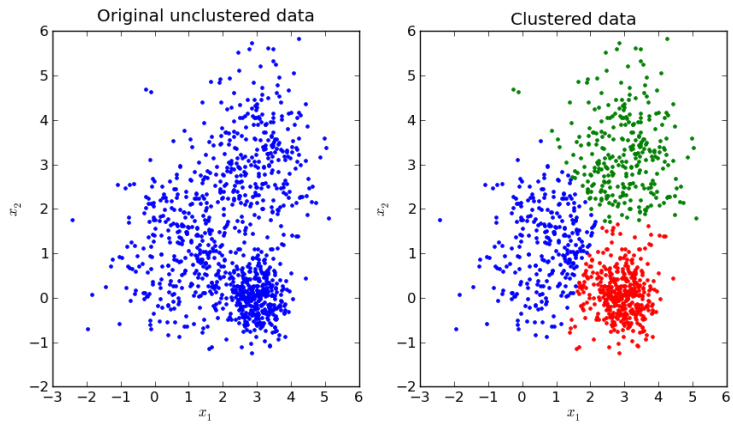

Figure 4. Using K-means clustering to group similar non-labeled data into 3 clusters.

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 the feature selection method, k-Means [25], and the non-negative matrix factorization as depicted in Figure 5, which shows a three-dimensional result.

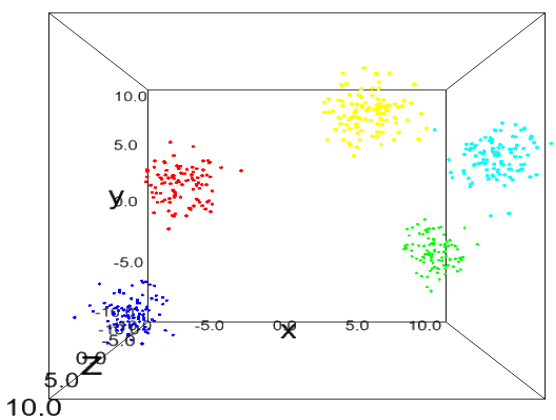

Figure 5. The k-means and non-negative matrix factorization in the 3D diagram

QALAAI ZANISTSCIENTIFIC JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil, Kurdistan, Iraq
Vol. (6), No (1), Winter 2021
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

B. Image Recognition as Security Measure

For this experiment, this research focused on image recognition as a potential measure used as a security tool on Facebook. This process exploited the use of a multi-output sensor estimator as the core tool in identifying 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 their 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 to detect potential threats in the event where certain users were flagged either down or put on the watch list for various cybersecurity crimes or threats, for that matter. Once flagged, users would alter their looks through either photo editing filters or software, which 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 AI in the detection of threats through image recognition. Figure 6 shows how various algorithms strived to complete the lower part of the faces with an exact comparison to the original photos of the people used in the experiment.

QALAAI ZANISTSCIENTIFIC JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil, Kurdistan, Iraq
Vol. (6), No (1), Winter 2021
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

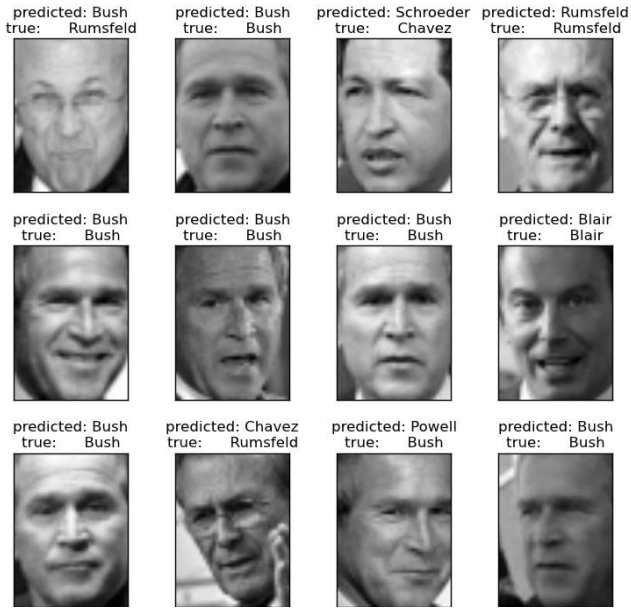

Figure 6. Face recognition through AI-guided algorithm in Scikit-Learn

From Figure 6, it is evident that extra trees give the closest resemblance to the actual 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 different tress algorithm is the most viable to use. However, the other algorithms were included in the machine learning process to ensure that any image peculiarity forms are internalized. It is evident in the linear regression algorithms that emphasize facial hair, something that extra trees tend to disregard in the learning process. The learning process code is a prototype AI 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, which authenticates the log in process.

VI. RESULTS AND DISCUSSION

The results and discussion section discusses the critical research data results that were collected in this research data. The questionnaire response rate is critically

QALAAI ZANISTSCIENTIFIC JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil, Kurdistan, Iraq
Vol. (6), No (1), Winter 2021
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

analyzed together with the corresponding survey research so that the relevant conclusions can be drawn. These conclusions are databased, and thus they are valid.

A. Threat Detection Using AI based Algorithm

Online social network users face numerous threats [21] daily. Some of the risks are developed by fake attack accounts that are primarily targeting the users themselves. 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. Therefore, it is 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, thereby developing a standard structural algorithm that can help protect users from various threats that they may face even without knowing that they are protected. 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 secure them even further. For example, training and awareness models, by asking them never to share their passwords or account details, is one method that has traditionally existed 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.

B. Opinion of Social Media about AI based Security

In our study, a quantitative methodology was used in the form of a questionnaire to at least 100 participants to support the course's conclusion. It 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 15 questions, were used to meet the study's needs. 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 on AI use as a means of curbing cybercrimes. On gender composition, 40 of the participants were female, while 60

QALAAI ZANISTSCIENTIFIC JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil, Kurdistan, Iraq
Vol. (6), No (1), Winter 2021
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

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 were ten participants between 28 and 38 years, while there were ten participants 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.

Our research found that Artificial Intelligence has a significant impact on promoting brands and protecting users from cyber-attacks. Contrary to the belief that AI can lead to more cyber-crimes, most participants disagreed on the issue contributing to the conclusion that Artificial Intelligence can reduce 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 users' privacy. From these findings, we can experiment with how organizations and other users of the social media platform can use Artificial Intelligence as a tool to reduce cyber-attacks.

VII. FUTURE WORK

In the 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 specific users.

VIII. CONCLUSION

As associations progressively rely upon PCs and the web to finish fundamental assignments essentially through correspondence and information sharing, there is a danger of dangers dependent on client practices, particularly in online interpersonal organizations. In light of this idea, the online protection issue has become an extremely huge and fundamental part of each innovative industry today. The online

informal community not being focused by digital hoodlums for a significant long time. Be that as it may, each office's security professionals have reliably been moving toward the issue through a specialized measure to give insurance. As per social designing dynamism, online dangers have changed, and digital crooks today focus on clients' shortcomings dependent on social conduct. Therefore, the examination has built up a calculation that targets anticipating the degree to which a mix and incorporation of client related elements are dimensional assembled to help foresee the clients' weakness towards the socially designed dangers. The calculation is actualized in Python programming language, which has as of now scored better in information mining systems.

REFERENCES:

[1] Alqatawna, J., Madain, A., Al-Zoubi, A. M., & Al Sayyed, R.. (2017). Online social networks security: Threats, attacks, and future directions. Springer, 3(4), pp. 121-132.

[2] Fonseka, T.M., Bhat, V., & Kennedy, S.H.. (2019). The utility of artificial intelligence in suicide risk prediction and the management of suicidal behaviors. Australian & New Zealand Journal of Psychiatry, 53(10), pp. 954-964.

[3] Ahmad, F., Khairunesa, I.S.A., Jamin, J., Rosni, N., & Thulasi Palpapanadan, S.. (2020). Social media usage and awareness of cyber security issues among youths. International Journal of Advanced Trends in Computer Science and Engineering, 9(3), pp. 3090-3094.

[4] Ghari, W.. (2012). Cyber threats in social networking websites", International Journal of Distributed and Parallel Systems, 3(1), pp. 119-126.

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

[6] Raad, E. & Chbeir, R.. (2013). 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.

[7] Kirichenko, L., Radivilova, T., & Anders, C.. (2017). Detecting cyber threats through social network analysis: Short survey. Socio-Economic Challenges, 1(2), pp. 20-34.

[8] Alguliyev, R., Aliguliyev, R. & Yusifov, F.. (2018). 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.

[9] Wentao, C.H.U., Kuok-Tiung, L.E.E., Wei, L.U.O., Bhambri, P., & Kautish, S.. (2020). Predicting the security threats of internet rumors and spread of false information based on sociological principle. Computer Standards & Interfaces, 73(1), pp. 1-7.

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

[11] Wu, Y., Huang, H., Wu, Q., Liu, A., and Wang, T.. (2019). A risk defense method based on microscopic state prediction with partial information observations in social networks. Journal of Parallel and Distributed Computing, 131(1), pp. 189-199.

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

[13] Chen, L., Gong, T., Kosinski, M., Stillwell, D., & Davidson, R. L.. (2017). "Building a profile of subjective well-being for social media users", PloS One, 12(11), pp. 1-15.

[14] Dorofeev, A., Markov, A. & Tsirlov, V.. (2016). 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.

[15] Sattikar, A.A. & Kulkarni, R.V.. (2012). A role of artificial intelligence techniques in security and privacy issues of social networking. International Journal of Computer Science Engineering & Technology, 2(1), p. 792 - 806.

[16] Jindal, S., & Sharma, K.. (2018). Intend to analyze social media feeds to detect behavioral trends of individuals to proactively act against social threats. Procedia Computer Science, 132(3), pp. 218-225, 2018.

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

[18] Feng, B., Li, Q., Ji, Y., Guo, D., & Meng, X.. (2019). "Stopping the cyberattack in the early stage: Assessing the security risks of social network users. Security and Communication Networks, 4(6), pp. 1-14.

[19] Luceri, L., Braun, T. & Giordano, S.. (2019). Analyzing and inferring human real-life behavior through online social networks with social influence deep learning. Applied Network Science, 4(1), p. 34, 2019.

[20] Ghahramani, Z.. (2003). 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).

[21] Barlow, H.B.. (1989) Unsupervised learning. Neural Computation, 1(3), pp. 295-311, 1989.

[22] Fire, M., Goldschmidt, R. & Elovici, Y.. (2014). "Online social networks: threats and solutions", IEEE Communications Surveys & Tutorials, 16(4), pp. 2019-2036.

QALAAI ZANISTSCIENTIFIC JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil, Kurdistan, Iraq
Vol. (6), No (1), Winter 2021
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

[23] Yu, D., Chen, N., Jiang, F., Fu, B. & Qin, A.. (2017). Constrained NMF-based semi-supervised learning for social media spammer detection. Knowledge-Based Systems, 125(2), pp. 64-73.

[24] Dorofeev, A., Markov, A. & Tsirlov, V.. (2016). 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.

[25] Fonseka, T.M., Bhat, V., & Kennedy, S.H.. (2019). "The utility of artificial intelligence in suicide risk prediction and the management of suicidal behaviors. Australian & New Zealand Journal of Psychiatry, 53(10), pp. 954-964.
Villanueva, J.A., Lacatan, L.L., & Vinluan, A.A.. (2020). Information technology security infrastructure malware detector system. International Journal of Advanced Trends in Computer Science and Engineering, 9(2), pp. 1583-1587.

پووختەی توێژینەوە

لەمیانەی جێ بەجێکردنی میکانیزمەکانی ئەندازیاری کۆمەڵایەتی بەکاربەرانی تۆڕە کۆمەڵایەتییەکان ڕووبەڕووی هەڕەشەی ستراتیژی بوونی خاڵی لاوازی دەکەنەوە. چەتەکانی ئینتەرنێت ئامانجیان تەکنیەکەکانی ئەندازیاری کۆمەڵایەتییە کە تێیدا زۆرجار لێکۆڵینەوە لەبارەی ژینگە بەکاربەران دەکەن. بەڵام، ئەم توێژینەوە تیشك دەخاتە سەر پێوەرسازی تەکنیکی چۆنیەتی پووچەڵکردنەوە یان ڕێگەگرتن لە هەڕەشەکانی بەشێوەکی گشتگیری لە ژینگەی تۆڕە کۆمەڵایەتییەکاندا. سەرەنجام، سیستەمەکانی تۆڕە کۆمەڵایەتییەکان پەنا بۆ بەکارهێنانی ڕێگا و مۆدڵی پێوەندیدار دەبەن بۆ دروستکردنی تایبەتمەندییەکان بۆ مەبەستی لێکۆڵینەوە زیاتر .

لەم ساڵانەی دواییدا فەیسبووك بە چڕی دەستی کرد بە کاکردن و وەبەرهێنانی فراوان لە بواری گەشەپێدانی سیستەمی چارەسەر ئەژمارەیی دە توانای بڕیاردانی هەبێت لە ئەگەری بوونی هەر هێرشێکی ئەلیکترۆنی بۆ سەر هەڵسوکەوتی بەکاربەران و دەستینشانکردنی کاراکتەری پلاتفۆرمەکە. لەگەڵ ئەوەی فەیسبووك چەندین پێوەری پێوەندیداری تەکنیکی ئەنجام دا بۆ کەمکردنەوەی هەڕەشەکان تا ئەوەی توانی ئەنجامی بدات، لەگەڵ ئەوەشدا، تا ئێستا بۆشایی هەیە بۆ ئەنجامدانی

QALAAI ZANISTSCIENTIFIC JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil, Kurdistan, Iraq
Vol. (6), No (1), Winter 2021
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

لێکۆڵینەوەی زیاتر کە بوونەتە سەرئێشە بۆ پێشبینی ئۆتۆماتیکی سیستەمی چارەسەری ئەژمارەیی بە بەکارهێنانی ژیری دەستکرد بۆ دەستنیشانکردنی ئەگەری بوونی هەی هێرشێك یان هەڕەشەیەك. ئەم توێژینەوەیە تەکنیەکەکانی ئۆتۆماتیکی بەکار دەهێنێت بۆ خستنەڕووی ئەوەی کە ئایە چۆن ژیری دەستکرد لەسەر بنەمای سیستەمی چارەسەری ژمارەیی سەر کاراکتەری هەڵسوکەوتی بەکاربەران و درك و تێڕوانینەکانی بەکاربەران و لایەنی هەستی کۆمەڵایەتی کە یارمەتی دەستنیشانکردنی ئەو تایبەتمەندییانە دەدات کە زیاتر پێوەندیدارن لە ڕووی دەستنیشانکردنی هەڕەشەی سەر هەر تاکێك لە ڕووی هەڕەشە و هێرشی سەر ئەندازیاری کۆمەڵایەتی. مەبەستەکە بریتییە لە ئەنجامدانی توێژینەوە لەبارەی کاردانەوەی تێڕوانینی ئۆرسۆدۆکس و تێڕوانینی بەرەوپێشچوونی هەمیشەیی بەرامبەر هەڕەشەکانی ڕۆژانەی سەر ئەندازیاری کۆمەڵایەتی. ئەم توێژینەوەیە شێوازی شیکاری بەراوردکاری تیۆرەکان بەکار دەهێنێت، و دەرئەنجامە بەدەستهاتووەکانیش بۆ خستنەڕووی ئەوەی کە ئایە هەڵسوکەوتی دیاریکراوی بەکاربەرانی فەیسبووك بریتین لە هەڕەشە بۆ سەر بەکاربەرانی دیکە. دەرئەنجامەکان ئەوەیان نیشان دا کە ئایە ژیری دەستکرد چۆن کار دەکات لە دەستنیشانکردنی نامە فێڵکارییەکان و خودی فێڵکارەکانیش لە ڕێگەی تەکنیکەکانی ئۆتۆماتیکی.

ملخص البحث

بشكل استراتيجي يتعرض مستخدمو الشبكات الاجتماعية عبر الإنترنت للعديد من تهديدات و نقاط الضعف، ذلك من خلال تنفيذ آليات الهندسة الاجتماعية. غالبًا ما يقوم مجرمو الإنترنت الذين يستهدفون تقنية الهندسة الاجتماعية بالتحقيق في بيئة المستخدم. مع ذلك، يركز البحث الحالي على القياس التقني لكيفية تصدي أو منع التهديدات بالكامل في بيئة الشبكات الاجتماعية عبر الإنترنت، و تستخدم أنظمة الشبكات الاجتماعية عبر الإنترنت النماذج ذات الصلة لإنشاء مميزات لمزيد من التحقيق. في سنوات الماضية عمل فيسبوك، بجد واستثمر بشكل كبير في تطوير خوارزميات يمكنها تحديد هجوم إلكتروني وشيك استنادًا إلى سلوك المستخدم وخصائصه على النظام الأساسي. على الرغم من أن فيسبوك قد اتخذ التدابير الفنية ذات الصلة لتقليل التهديدات قدر الإمكان، إلا أنه لا تزال هناك فجوة لمزيد من التحقيقات، والتي تسعى إلى تسخير التنبؤ الخوارزمي الآلي باستخدام الذكاء الاصطناعي لتحديد إمكانية حدوث هجوم أو تهديد. يستخدم هذا البحث تقنيات التعلم الآلي لإظهار كيف أن الخوارزمية القائمة على الذكاء الاصطناعي للخصائص السلوكية للمستخدم، والتصورات، والعواطف الاجتماعية ستساعد في تحديد الميزات التي تصبح أكثر أهمية في تحديد تعرض الفرد لتهديدات وهجمات الهندسة الاجتماعية. والهدف و يقوم بدراسة المنظور الأرثوذكسي و ردود الفعل الدائمة تجاه التهديدات الاجتماعية المهندسة يوميًا.

QALAAI ZANISTSCIENTIFIC JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil, Kurdistan, Iraq
Vol. (6), No (1), Winter 2021
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

يقوم هذا البحث بأستخدام تحليل مقارنات للنظريات ونتائج البيانات الأولية لإظهار أن سلوكيات معينة لمستخدمي فيسبوك تشكل تهديدًا للمستخدمين الآخرين. أظهرت النتائج كيفية عمل خوارزميات الذكاء الاصطناعي في تحديد الرسائل الخادعة والمحتالين من خلال تقنيات التعلم الآلي.