Identification of Malicious Accounts in Facebook

Prasanta Kumar Sahoo, K. Lavanya

ABSTRACT: ***In this modern world of internet age social networking is becoming popular day by day for sharing of information and day to day communication. The social media has changed the way people pursue their life and made it a part of their life to get connected with friends, family, colleagues and with the society as a whole. Social networking can occur for social purposes, business purposes by the use of Facebook, Twitter, LinkedIn etc. Hence it has become the favorite spot for the cyber criminals. Facebook is a free social networking website that allows users to upload photos and video, send messages and keep in touch with friends, family and rest of the world. Unfortunately, spammers are also using this Facebook for their personal gain by creating fake profiles or comprising the other famous accounts. These accounts together are referred as malicious accounts. Hence it became important task to identify this spam for free communication over Facebook. However, some former researchers have proposed their work to identify these accounts but suffering from many limitations. In this paper a method is proposed called An unsupervised method to detect spam in Facebook using DBSCAN algorithm. This research work used Jaccard similarity and DBSCAN algorithm to detect spam messages. This research work is implemented using real time messages and evaluated. The experimental results show the methodology used is very efficient, having better accuracy and low false positive rate in detecting the spam messages in Facebook. This research work will help the common man in detecting malicious Facebook accounts in a great way.***

Related terms: Social networking, Facebook, malicious accounts

I. INTRODUCTION:

With the invention of internet technologies, the communication has become very fast and simple. The best and effortless way to communicate with the family, friends etc is through social networking. Social networking is a platform where people communicate with each other irrespective of physical locations by exchanging messages, images, video through social platforms like Facebook, Twitter, etc. Because of the quick increment inside the OSN clients, a large number of people have turned out to be snared on the use of Social system. Facebook alone vessels more than 500 million clients and has as of late outperformed Google as the most visited website on web [1][2]. Facebook is one of the biggest and arguably most powerful social network and free, as face book is a free and open communication channel with lot of attractive stuff like posts, calls etc. These favorable probabilities attracting cyber criminals to commit fraud online. Hence it became the honeypot for the cyber criminals to spread spam easily [3] Cyber criminals are those who has the intension to steal data, abuse the people for the sake of their happiness and intuitively pull down the name and fame of a popular persons etc.

Revised Manuscript Received on October 15, 2019

Dr. Prasanta Kumar Sahoo, Professor, Department of Computer Science and Engineering,
Sreenidhi Institute of Science and Technology, Yamnampet, Ghatkesar, Hyderabad-501301, Telangana, India

K. Lavanya, M. Tech. 2nd year, Dept of Computer Science and Engineering. Sreenidhi Institute of Science and Technology,
Yamnampet, Ghatkesar, Hyderabad-501301, Telangana, India.

So, it has become one of the most attractive media for cyber attackers. News channels, politicians, celebrities, business people, students, international groups are widely using Facebook for communication. Miserably attackers are also using the Face book to spread spam online. Generally for fraud activities hackers choose online accounts which have more number of friends/followers and online business but they are also focusing on the normal people like students, women to abuse them online[4].Cyber criminals are using different methods to spread the spam content online for a large number of people at a time. They are using fake or malicious and compromised accounts [5] to accomplish their tasks. Forged records are made for gainful malignant exercises, for example, spamming, click-extortion, malware circulation, and character misrepresentation, phishing. Phishers utilize various systems to mislead the clients and take their own and money related data [6] Compromised accounts are legitimate accounts that a malicious party takes control over, with the intention of gaining financial profit [7] or spreading misinformation. Malicious/Fake account in Face book are used to gain the access to a real account. Once the attacker ingress the legitimate account can commit the fraud or illegal activities by impersonating the real user with the help of messages, links, videos [8]. With this they can exploit trust connections between the authentic record owners and their companions [9] by means of links, messages and photos because social network users react to the posts coming from the trusted account [10][11]. Recent proof demonstrates that these believed networks can end up viable systems for spreading malware and phishing assaults. Prevalent system are progressively getting to be focus to spread spam propelled from enormous Botnets [12][13]. Ordinarily, client profiles are not open in Facebook, and the privilege to see a client's page is allowed simply subsequent to having built up a relationship of trust with the client so spammers are utilizing bargained accounts. When the user A wants to become friend with another user B in Facebook, first A needs to send a request to B, who has to acknowledge that she/he knows A. When B confirms the request, a friendship connection with A is established. Many a times cyber criminals are designing some fake and attractive games to access the user personal data. Then these accounts are used in multiple ways to send messages to the friends of legitimate user, images, warning them that their account was about to be disabled and instructing the users to click on a link to verify their account [14]. Then if a user clicks on that link it will be redirected to a false Face book page and ask them to enter login info and credit card etc. Ex: If user A's account is compromised then the attacker uses A's account to send spam messages to user C which direct to some malicious website. Once user C signs in the spam message will be displayed to C exposing to potential threats. Potential threats may include loss of valuable data in business, personal information which leads to financial threats, harassment etc. The principal use of these compromised accounts is to spoil relationships, earn money, abuse the legitimate user to let

him down in society etc. Since the detection is still exclusively a manual endeavor, this is often too late to mitigate the negative impacts of account compromises. As per a survey there are 500 Million Female accounts in Facebook, but the population of Female in world is nearly 300 Million [15]. That means we can assume how many fake accounts and unwanted data is being created.

A general step by step procedure how an attacker can spread spam over Face book using malicious accounts:

- First attacker creates fake account or compromise the legitimate account in face book by using his/her own techniques.
- At that point these records are utilized to send messages to different clients, ex: cautioning them that their record was going to be disable and request the clients to tap on a connect to check their record [14].
- Suppose if a user clicks on that link it will be redirected to a false Facebook page and ask them to enter login info and credit card etc.
- Using compromised accounts, the spam message can be sent to friends of compromised account to spoil relationship, earn money etc. [19].

II. OVERVIEW OF EXISTING SYSTEM:

1.Jince P. kuruvella et.al [2017] states that malevolent users utilize the well-founded connections and good interrelation between the real account users and friends, efficiently share out unsolicited advertisements, spoofing links (or) virus while protect themselves being obstructed by the service provisioner. They proposed a solution based on the user clicks and named it as a "Click Stream Method". This method gathers set of social behavioral features that characterizes the user activities and are stored in a database. Then it calculates the number of times the user clicks on particular link while surfing or by using software application. When a user clicks on particular webpage, this activity is recorded on the client side/web browser. These are compared with the data base to determine the spam [16].

2.Christo Wilson et.al [2010] defined online social network in the wrong hands are effective mechanisms for spreading attacks. They proposed a mechanism to identify this fraud based on "Wall messages" since these messages are one basic way to express interest online. First a collective unique class of posts enclosed in a complete set of Facebook messages are recognized. Every Facebook message is modeled as <Description, URL> pair. Here Uniform Resource Locator is target and Description is text in wall message (because any spammer cannot achieve the goal without URL). With this information the wall post similarity graph is constructed. All the similar wall posts are clustered into graph before that it identifies the wall posts containing URL's and extract URL's. To identify this URL's, click here keyword is used to search unclear URL's [17]

3. Hongyu Gao et.al [2010] determines that online social networks are effective tools for spreading spam for attackers. They proposed a measure to identify and named as "Spam filtering system". This system is deployed as a component in service provider side. All the messages are clustered to uncover connection among all the messages. Due to its computational overhead it's (Clustering) is not used in Spam filtering system. To address this incremental clustering and parallelization is used. Once deployed it inspects every message before rendering to recipient. Example if message 'A' is classified as spam it's dropped and then if message 'B' is legitimate it's stored in service provider [18].

4. Manuel Egele et.al [2017] elucidates that compromising social network networks is easy way to spread spam. They proposed a method to identify this and called it as "Compa". This system mainly focuses on the stream of messages that a user posted on social network. The number of messages considered are not to be less than 10. Then system extracts set of values from each message and trains a statistical model. Once the behavioral profile of a user is identified the system will be able to identify the new message and test to which extent it belongs to a legitimate user [19].

5. Quiang Cao et.al [2012] proposed a tool called Sybil Rank. Likelihood of being fake depends on the properties of social graph, based on these properties the compromised accounts are identified. The factors like inter arrival time and the click sequence in an account [20].

A. PROBLEMS WITH THE MALICIOUS ACCOUNTS:

1. Recently a fake account was created on the name of the Mumbai woman and attached loop of threatening internet sites then wrote disgusting statements on the latest account, in addition called her as a prostitute [21].
2. A fake face book account was created on the name of the Muslim woman and fraudster started celebrating success of BJP party and continuously appreciating the greatness of PM Modi [22].
3. A Gujarat based 22-year-old teenager created fake account on Harsh Vora, a 16-year-old boy from Ghatkopar and started chatting with the friends as Vora especially with girls [23].
4. A scammer gained an access to one of the Facebook user's account then posted a text to one of the account owner friends that his briefacse was missed somewhere while going to the destination and required $500 to come back to home [22].
5. A 18 year-old student created a malicious account on behalf of the regoinal manager and sent in unprofessional text [23].
6. A latest post by security specialists Amir Lakhani and Joseph Muniz encapsulated the ease with which they had compromised an American administration office by utilizing a beautiful profile, by using few civil engineering, malware they manipulated the council in such a way that they themselves provided the fictitious operations with a laptop and gmail account [24].

B. LIMITATIONS:

Although some former researchers offered the solutions to detect the spam from OSN's, they are suffering from the considerable limitations are:

- spam detection Methods are training data dependent
- Topic specific spam analysis not implemented
- Spam detection became complex operation
- results are suffering from false positives.

III. PROPOSED SYSTEM:

To address these limitations, in our paper we proposed "An unsupervised method to detect spam in Facebook using DBSCAN" which is becoming the platform to spread spam. Without any initial training phase, using unsupervised techniques, it efficiently inspects the stream of user generated messages, immediately dropping those messages identified as malicious before they reach the specified users. Our proposed method is complete offline, unsupervised and automatic, while detecting the spam messages from OSN's. With the help of DBSCAN clustering technique the anomalies are detected from offline messages before they are sending to all followers. Generic Spam Characters data set, Jaccard Similarities and other correlation techniques have been used to conquer the proposed spam detection method. In order to implement the proposed system, the whole system contains the below modules, which will be implemented in phases as mentioned below:

- Message Dataset Preprocessing
- Jaccard Similarity
- DBSCAN and Anomaly Detection
- Spam Reporting

A. SYSTEM ARCHITECTURE:

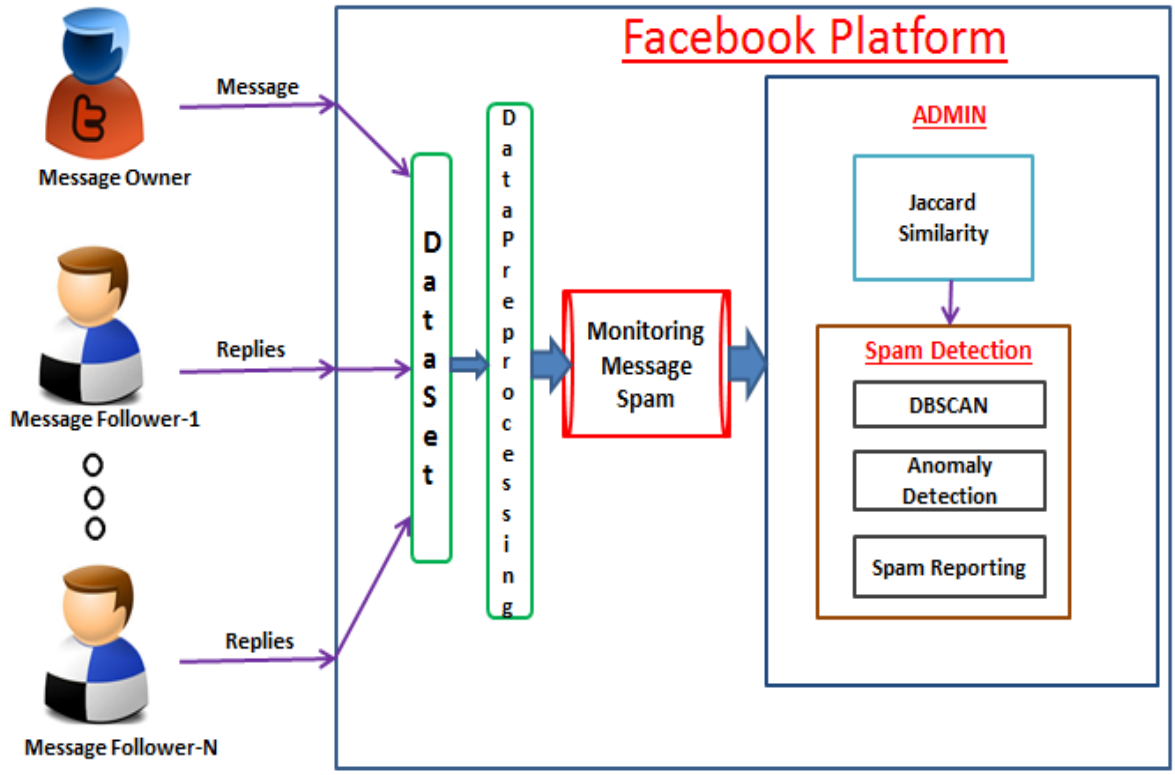

Fig 1: shows the system architecture.

B. MESSAGE DATASET PREPROCESSING:

As a part of this module project initially creates a simulation of admin model. In this model initially the data from social networks has been collected in the form of message dataset. This dataset contained raw messages are preprocessed with additional spaces trimming, De-duplication, data validation and some other formal preprocessing techniques. This preprocess helps to eliminate the unnecessary data from dataset to reduce the false record participation in spam detection process.

C. JACCARD SIMILARITY:

In general, first the account holder posts a message to its followers, then it will be read by the followers and interested will replies to it with their version. Jaccard Similarity is a text processing model, designed to filter the commonality in Facebook data including abusiveness, violence spreading, Anti-Social activities etc. Jaccard similarity is used to identify the similarity between two sets of data. So that we will be able to calculate the similarity percentage, it can be in between 0% to 100%. The higher the % value the more is the commonality between the two sets of data.

The Basic Formula to calculate the Jaccard similarity is:

J(A/B)=[AnB]/[AuB]

The above formula can be described as:

1. Identify the number of data points shared among both the sets.
2. Find the total data points present in both the sets.
3. Then divide the number of shared points found in 1 by Total number of data points found in 2.
4. Finally multiply the result from step 3 with 100 to get the percentage.

As part of the proposed model, all messages from dataset are filtered by this Jaccard similarity. Any unsatisfied messages with hateful content will be restricted at this stage without posting.

D. DBSCAN and ANOMALY DETECTION:

After Jaccard similarity detection the reply messages to main message must be scanned

for specific spam before they publish, our DBSCAN is exactly used for this. **Density-Based Spatial Clustering of Applications with Noise (**DBSCAN) is an efficient clustering method to deal even when noise data presented in messages. DBSCAN mainly depends on 2 parameters:

1. Eps (Ecludian Distance)
2. Min pts (Minimum Points)

Eps: This parameter us used to check if the particular data point can be included in a cluster or not. Suppose if we consider Eps value as 3, the distance between the points in a dataset which are below and 3 can be formed as a cluster.

Min pts: It determines how many data points must be present within a Eps distance so that a cluster can be formed. Suppose if we consider the min pts as 4, there must be 4 data points to form a cluster.

Variable evaluation:

Eps:

1.If we choose the Eps value too small then more number of data points are considered as outliers.

2. If we choose the Eps value too high then most of the data will be in same cluster so that they will merge and can create a confusion which leads to false result.

So we must be very careful while deciding the Eps value, one way to calculate the Eps value is using K-distance graph.

Min Pts: It can be estimated based on the Dimensions of a dataset(D) i.e,Minpts=(D+1).

1.If your dataset contains more noise, it's ideal to choose large value for better results.

2.Larger the dataset choose large minpts value to get more clusters which will leads to more positive result with better accuracy.

As part of this module reply messages are clustered using DBSCAN and the left-over noise elements are detected as anomalies.

E. SPAM REPORTING:

After DBSCAN clustering the anomalies relevant features are compared against the features of owner's message using correlating mining process with help of Jaccard similarity basic knowledge. The result values from DBSCAN and correlation process scrutinized against the threshold value for the spam confirmation.

Advantages:

The proposed spam detection method is having the notable advantages, which are the best solutions for the former research are:

- ❖ Unsupervised techniques made the spam detection process as training data independent.
- ❖ DBSCAN is used for efficient clustering and anomaly detection
- ❖ Empirical Studies exposes the reduction of false positives in results.

IV. CONCLUSION:

Now a day's social media is becoming a communication platform to connect with peers, friends, social groups and the society at large. As because it is very easy to access and not having enough security compliance mechanisms, fraudsters used social media frequently to cheat the common man. It is becoming the favorite spot for the cyber criminals to harass others and use it for personal gain by creating fake Facebook profiles. Compromised accounts are main source in social networks to spread spam or commit different kind of frauds. Hence it's important to identify the compromised the accounts in social networks to minimize the loss at a very early stage. The Proposed System able to identify the compromised accounts very efficiently using DBSCAN and Jaccard similarity. The system is being tested and results are evaluated and compared. The system is very useful in detecting compromised Facebook accounts with better accuracy. It will be a great help for the common man to protect their privacy by detecting properly compromised Facebook accounts.

REFERENCES

1. H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao, "Detecting and characterizing social spam campaigns," in Proc. 10th ACM SIGCOMM Conf. Internet Meas. (IMC), Melbourne, VIC, Australia, pp. 35–47,2010.
2. Christo Wilson, Bryce Boe, Alessandra Sala, "User Interactions in Social Networks and their Implications" in EuroSys'09, April 1–3, Nuremberg, Germany, ACM,2009.
3. K. Lee, J. Caverlee, and S. Webb, "Uncovering social spammers: Social honeypots + machine learning," in Proc. 33rd Int. ACM SIGIR Conf. Res. Develop. Inf. Retr. (SIGIR), Geneva, Switzerland, pp. 435–442,2008.
4. C. Grier, K. Thomas, V. Paxson, and M. Zhang, "@spam: The underground on 140characters or less," In Proc. ACM Conf. Comput. Commun. Security, pp. 27–37,2010.
5. Xin Ruan , Zhenyu Wu , Haining Wang ,and Sushil Jajodia,"Profiling Online Social Behaviors for Compromised Account Detection" IEEE Trans. Information Forensics and Security 11,1(2016),176–187,2016.
6. Prasanta Kumar Sahoo, "Data Mining a way to Solve Phishing Attacks," in IEEE International Conference on Current Trends towards Converging Technologies (ICCTCT-2018),Coimbatore,India,2018.
7. Chris Grier, Kurt Thomas, Vern Paxson, and Chao Michael Zhang, "@spam: the underground" , In Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS,2010.27–37,2010.
8. H. Xiong, P. Malhotra, D. Stefan, C. Wu, and D. Yao, "User-assisted host-based detection of outbound malware traffic," in Proc. 11th Int. Conf. Inf. Commun. Secur. (ICICS), Beijing, China, pp. 293–307,2009.
9. Xin Ruan, Zhenyu Wu, Haining Wang , and Sushil Jajodia, "Profiling Online Social Behaviors for Compromised Account Detection", IEEE Trans. Information Forensics and Security 11,176–187,2016.
10. C. Wilson, B. Boe, A. Sala, K. P. N. Putta swamy, and B. Y. Zhao, "User interactions in social networks and their implications," in Proc.4th ACM Eur. Conf. Comput. Syst. (EuroSys), Nuremberg, Germany, pp. 205–218,2009.
11. T. Jagatic, N. Johnson, M. Jakobsson, and T. Jagatif, "Social phishing," Commun, ACM, vol. 50, no. 10, pp. 94–100, 2007.
12. Users of social networking websites face malware and phishing attacks. Symantec.com Blog.
13. Zeus botnet targets facebook. http://blog.appriver.com/2009/10/ zeus-botnet-targets facebook.html.
14. https://www.thequint.com/news/webqoof/fake-social-media-profiles-muslim-identities-bolster-bjp-case-study-gini-khan-giniromet.
15. A. Graves, et. al "A Novel Connectionist System for Improved Unconstrained Handwriting Recognition". IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 31, 2009.
16. Jince P Kuruvilla, Kavitha P, and Dr.G. Kalpana, "Detection of compromised accounts on social networks based on anomalous user behavior", in the international Journal of Emerging Technology in Computer Science & Electronics (IJERCSE),2017.
17. H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen and B. Y. Zhao, "Detecting and characterizing social spam campaigns", in the proceedings of the 10th ACM SIGCOMM conference on Internet mea surement, IMC '10, Melbourne, Australia, pages 35–47,2010.
18. H. Gao, Y. Chen, and K. Lee, "Towards online spam filtering in social networks", in the symposium on network and distributed System Security, NDSS 12', San Diego, CA USA. Internet Society,2012.

19. M. Egele, G. Stringhini, C. Kruegel, and G. Vigna, "proposed system: Detecting compromised accounts on social networks," in proc. Symp. Netw. Distrib. Syst. Secur. (NDSS), San Diego, CA, USA, 2013.
20. Q. Cao, M. Sirivianos, X. Yang and T. Pregueiro, "Aiding the detection of fake accounts in large scale social online services", in the proceedings of the 9th USENIX conference on Networked Systems Design and Implementation, NSDI'12, San Jose, CA,2012.
21. https://www.hindustantimes.com/mumbai-news/cyberstalker-creates-fake-fb-account-of-mumbai-woman-posts-photos-obscene-material-on-it/storybarX2zsombAbNaYHeSJILP.html
22. https://socialnomics.net/2016/01/13/4-case-studies-in-fraud-social-media-and-identity-theft/
23. US agency was hacked and it's available online: https://freshmango.com/security-case-study-hacked-by-social engineering.
24. https://indianexpress.com/article/technology/sponsored/realme-2-is-the-best-budget-smartphone-available-in-the-sub-10k-category-5337122/

AUTHORS PROFILE

Dr. Prasanta Kumar Sahoo, Professor, Department of Computer Science & Engineering, Sreenidhi Institute of Science & Technology, Hyderabad. He completed his Ph.D. from Fakir Mohan University, Odisha in Computer Science Engineering. He has 17 years of teaching, research and administrative experience. He has earlier worked as Head of the Dept. in both CSE and IT dept. in various reputed Engineering Colleges. His Research interest includes Cyber Security, Information Security and Data Mining. He has published around 50 research papers in various reputed journals both at national and International level. His research papers were cited both at national and international level, so far by 41 citation and 1567 reads as per Google Scholar and research Gate report. Many times Dr. Prasanta Kumar Sahoo won the best teacher award in various colleges for his contribution to the teaching and learning process. He is Certified Professional from BalaBit, completed Electronic Contextual Security Intelligence exam Intermediate Level (ECSI). He has guided more than 50 projects both at UG and PG level. He has delivered more than 15 guest lecturers. He has organized three national conference and nine faculty development program with an immense success.

K. Lavanya, pursuing Masters Degree in computer Science & Engineering from Sreenidhi Institute of Science and Technology, Hyderabad. She has completed her B. Tech Degree from JNTU Hyderabad. She also published few papers in reputed journals.