ENHANCING COMPROMISED ACCOUNT DETECTION IN ONLINE SOCIAL NETWORKING USING FUZZY CLASSIFICATION AND BAUM WELCH ALGORITHM

[1]Darshana Chaudhari, [2]sayali revade, [3]Yogita sonje, [4]Yogita Jagtap, [5]Jyoti Deshmukh
[1]UG Student, [2]UG Student, [3]UG Student, [4]UG Student, [5]UG Student Guide
[1]computer engineering,
[1]JSPM,S BSIOTR, pune, India

Abstract*—Due to happening of malicious spam over the compromised accounts of online social network users. To overcome this problem some system needs to detect the compromised accounts of online social network users in early stages, for this purpose there are different methodologies are used. We study the social behavior of online social network users, captures the users behavior, users activity. Many system related to Characterizing User Behavior in Online Social Networks are having performance issues regarding compromised account detection. To enhance the process of compromised account detection in online social networking sites proposed system put forwards an idea of gathering all social networking behavior features that include extroversive posting and introversive browsing activity of the users, which is used by the process of Baum_ Welch Methodology to identify the hidden state of compromised account detection for early detection of account compromization and this is catalyzed by the process of Fuzzy C-means Clustering technique.

***Keywords*— OSNs, behavior,compromised accounts detection,classification Introduction**

A social networking sites have been risen in popularity , cyber criminals started to exploit these sites to spread malware and to carry out scams . Compromising social network accounts has become a profitable course of action for cybercriminals. By hijacking control of a popular media or business account , attackers can distribute their malicious messages or disseminate fake information to a large user base .The impact of these incidents range from a tarnished reputation to multi billion doller monetary losses on markets. So a fine grained system is required to detect compromised online accounts.

1. Extroversive Posting Collection**:** Here system collects all the online posting of the users and try to identify the features using NLP (Natural language processing). In this step system tries to identify the some features like numerical data, Proper nouns used and some most frequent words of the posting which helps to identify the hidden states ahead.

2.Introversive Browsing Collection: Here a system collects all the introversive activities of the browsing like time spend on home page, time spend on commenting activities etc..

3. Fuzzy C- Means Clustering :Here in this step all the data collected in above two steps are been formatted and collected in a list. And then this list is been subjected to labeling of the entities for numerical conversions and then based on this data is been converted into clusters of the desires facts by using Fuzzy C means process.

Here all the data that is been collected for the calming of insurance is clustered logically using c means clustering with the following technique. This algorithm works by assigning membership to each data point corresponding to each cluster center on the basis of distance between the cluster center and the data point. More the data is near to the cluster center more is its membership towards the particular cluster center. Clearly, summation of membership of each data point should be equal to one After each.

The proposed system can be design based on the following entities.

Compromisation of high profile accounts can cause major loss [1][2]. Plus recently there have been multiple incidents of mass account compromisation. Such experiences can make negative impression on legitimate users and can potentially harm the relationship between users and OSN service providers. The accounts which are solely created to spread spam can be easily spotted and removed. But this is not the case with benign account holders. The compromised normal account cannot be simply banned or removed because it may still being used by its true user.

To deal with such problem one solution is capture and analyze the user behavior on online social networks. Many previous attempts have been made to study such user behavior[3][4]. Mere study of online user behavior cannot detect the compromised account, for that the further analysis and preventive techniques are needed.

Once the user inputs the correct credentials the access is given to the user. As the user accesses his/her account the extroversive and introversive data are collected. Using fuzzy rules and distance measurement techniques these collected introversive and extroversive data are classified in different clusters. Fuzzy C-Means clustering is used for classification. Once the data is classified it is then observed for hidden states. The forward and backward algorithms are used in Baum-Welch algorithm to work on Hidden Markov Model to find its hidden states. Once the hidden states are observed it is then easy to determine whether the account is compromised or not.

The concepts used in this paper are fuzzy c-means clustering, Hidden Markov Model, User behavioral profiles and behavioral features.

User behavioral profiles are basically the detailed bio-data of each user. It tells how each user accesses his/her OSN account. It mainly contains the access pattern of a user. The used for extracting the user behavior are session time, clickstream; time the user spends on each page; usual posting time, type; usual platform used for accessing the account etc. User behavioral profile plays an important role in detection of compromised accounts. A fake user can't fully imitate the behavior of legitimate user and thus creates a huge difference between original and fake user leading to the easy detection of compromisation.

User behavioral profiles are formed with the help of behavioral features. The behavioral features are basically categorized into two types: introversive and extroversive behavioral features. Introversive behavioral features tell about the activities which include introversive access like just going through the status posted by friends and do not comment. Extroversive features tell

about the activity which includes the extroversive accesses such as commenting on friend's status updates and photos, messing a friend, liking the photos posted by friend, posting of friend's profile etc.

Fuzzy c-means (FCM) is a data clustering technique in which a dataset is grouped into n clusters with every data-point in the dataset belonging to every cluster to a certain degree. Fuzzy C-means clustering is used for classifying the user activities. Whenever a user accesses his account, the clickstream is observed to collect the features. These features are then classified into different clusters. Once all the introversive and extroversive data are collected then they need to be categorized and cluster based on the fuzzy rules according to the perspective of the attack detection. Here FCM is used because to add unique cluster elements, so this proves to be effective mechanism to isolate the user from bull of the collected data.

A hidden Markov model (HMM) is a statistical Markov model in which the system being modeled is assumed to be a Markov chain with unobserved (*hidden*) states. The Baum Welch algorithm is used to extract the hidden states from the k known parameters like introversive and extroversive entities.

I. LITERATURE SURVEY

[3] This paper proposed a method to detect compromised account in online social networks with the help of online social behavior. It uses introversive and extroversive behavioral features extracted from clickstream collection to form a social behavioral profile for each of the individual user. The deviation from these authentic profiles indicates the account compromisation act. Study with the help of 50 students on Facebook data for few weeks proved this system effective. Though this system collects the clickstream for each user every time he uses his accounts, but the profiles are updated periodically. This leads to the detection of account compromisation post the attack. The system can be updated to detect the account compromisation while the attacker is still attacking.

[4] Presents new kind of analysis for user workloads in online social networks. The study is based on detailed clickstream data, collected over a 12-day period, summarizing HTTP sessions of 37,024 users who accessed four popular social networks: Orkut, MySpace, Hi5, and LinkedIn. Analysis demonstrates power of using clickstream data in identifying patterns in social network workloads and social interactions. Browsing cannot be inferred from crawling publicly available data, accounts for 92% of user activities. However the amount of data for crawling is very huge and requires more optimized algorithms. This work can be extended to analyze the impact of friends on behavior of user of social networks. Social network workload generator and Markov model can be incorporated to improve the performance

[5] This article presents investigative work on how users' activity on Facebook relates to their personality, as measured by the standard Five Factor Model. Results show significant relationships between personality traits and various features of Facebook profiles. It also showed how multivariate regression allows prediction of the personality traits of an individual user given their Facebook profile. Data used may suffer from a self-selection bias. users were able to control the information stored regarding their profile, so we only had data for users who chose to let us access this information. The system can be further adapted for online advertising and recommender system.

[6] Proposed System uses the combination of statistical modeling and anomaly detection to identify accounts that experience a sudden change in behavior. Such behavior changes can be due to benign reasons, it is necessary to derive a way to distinguish between malicious and legitimate changes. They developed a tool called COMPA that implements above mentioned approach. Attacker who has knowledge of COMPA can prevent account compromisation from detection. Automated crawling slowing down such data gathering endeavors. COMPA can be easily extended with additional and more comprehensive similarity measures. Other similarity measures integration is scope of work.

[7] This paper explains a method to distinguish potentially bad behavior from normal behavior using unsupervised anomaly detection techniques over user behavior. For doing so they used a technique based on Principal Component Analysis that models the behavior of normal user accurately and identifies the significant deviation from it as anomalous. The demonstration on Ground truth data of from Facebook successfully detects attacker strategies like fake, compromised, and colluding Facebook identities. The application of this strategy to detect click spam in Facebook ads shows majority of clicks are from anomalous users.

[8] This article compares the performance of fuzzy C-means clustering algorithm with other clustering algorithms. It states that as compare to other clustering algorithms fuzzy c means is more efficient, reliable and robust than others in certain cases or applications by its performance. And also it concludes that as compare to other clustering algorithms fuzzy c means is more efficient, reliable and robust than others in certain cases or applications by its performance.

[9] This paper put forwards an improved fuzzy c-means algorithm and applies to deal with meteorological data on top of traditional fuzzy c-means algorithm. FCM has difficulty in selecting the initial cluster centers that is why it improves classical FCM by adopting a novel strategy for selecting the initial cluster centers. WEKA, the open source data mining platform does not have FCM option. This paper successfully implements the FCM algorithm and advanced FCM algorithm with the help of basic classes in WEKA. The comparison shows that this method generates better clustering results than those of K-means algorithm and traditional FCM algorithm.

[10] This paper explains an efficient K-means clustering algorithm and Fuzzy C-Means Algorithm under Morphological Image Processing (MIP) and accurate Fast Bounding Box Based Segmentation Method. This paper carried out image segmentation algorithm using various clustering algorithm for better performance. The segmentation techniques like thresholding and morphological operators are used.

[11] This paper surveys different the fuzzy c-means clustering algorithms. The algorithm it surveyed includes Fuzzy C-Means (FCM) algorithm, Probabilistic C-Means (PCM) algorithm, Fuzzy Probabilistic C-Means (FPCM) algorithm, Possibilistic Fuzzy C-Means (PFCM) algorithm.

[12] It provides a tutorial on learning and inference in Hidden Markov Models in the context of recent literature on Bayesian networks. It generalizes hidden markov model with multiple hidden state variables, multi-scale and mixed discrete & continuous variables. It also discusses the Bayesian methods for model selection in generalized HMMs.

[13] This paper derives a method similar to Baum-Welch algorithm for estimating the parameters of the HMM. This algorithm allows the observation PDF of each state to be defined and estimated using a different feature set. It maximizes the likelihood function for the standard parameterization of the HMM defined on input data space. It demonstrates that it is possible to parameterize the HMM using different features for each state.

[14] This paper proposes the incremental Hidden Markov Model (IncHMM) with an improved Baum-Welch algorithm. It uses β approximation. It shows β approximation used have been successful after statistical comparison between raw and IncHMM generated traces. It creates two Workload models; each with their own β approximation; which characterizes data traces incrementally.

[15] This paper presents a parallel version of Baum-Welch algorithm; because Baum-Welch algorithm is robust, but slow. It considers unidirectional procedures which in contrast with well known forward-backward algorithms, use the amount of memory that is independent of the observation sequence length.

[16] This paper invents the new algorithm based on Baum-Welch algorithm for estimating the parameters of a hidden markov model (HMM). Each state is observed using a different set of feature rather than relying on a common feature set. For discriminating a given state with white-noise state each feature set is chosen wisely. Experiments shows that it provides better results than conventional HMM.

[19] The paper introduces a method of Bayesian probability papers for estimating the reliability function of popular in reliability analysis location-scale life time distributions. It uses simulation examples to validate the method and a real engineering data example to illustrate its practical applications.

[18] This paper is a tutorial on parameter estimation. It has used the example of single stationary sinusoidal frequency. The basic rules for manipulating and assigning probabilities are used. The applications of Bayesian probability theory are explained in this paper. The applications are Parameter estimation problem and model selection problems.

III PROPOSED METHODOLOGY

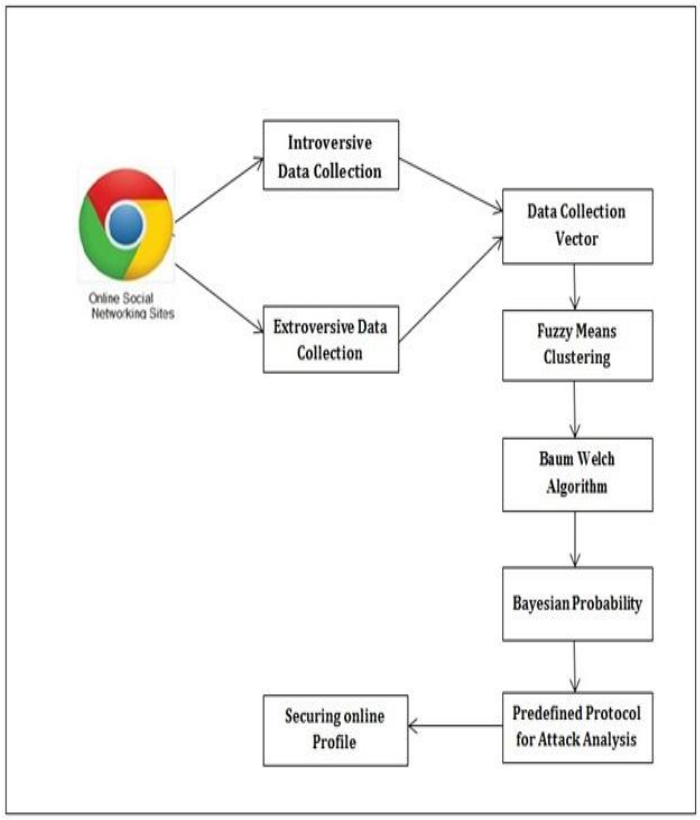

Figure 1: System overview for Compromised account detection

The proposed system is designed based on the following entities that explained in step by step

Step 1: Extroversive Posting Collection - Here system collects all the online posting of the users and try to identify the features using NLP (Natural language processing). In this step system tries to identify the some features like numerical data, Proper nouns used and some most frequent words of the posting which helps to identify the hidden states ahead.

Step 2: Introversive Browsing Collection- Here a system collects all the introversive activities of the browsing like time spend on home page, time spend on commenting activities etc..

Step 3: **Fuzzy C- Means Clustering -** Here in this step all the data collected in above two steps are been formatted and collected in a list. And then this list is been subjected to labeling of the entities for numerical conversions and then based on this data is been converted into clusters of the desires facts by using Fuzzy C means process.

The working flow of fuzzy C- Means Clustering can be depicted in figure 2.

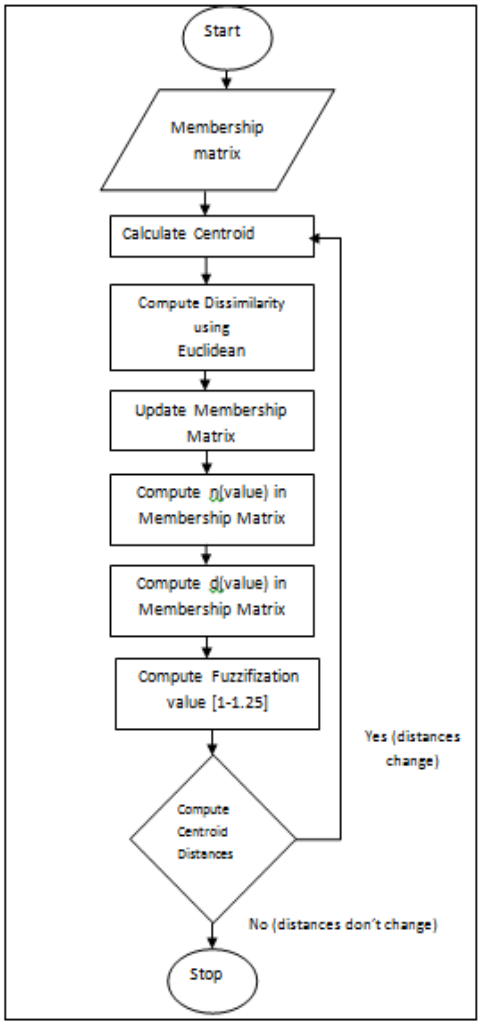

Figure 2: Working flow of Fuzzy C – Means Clustering

Step 4: Hidden Markov Model - The hidden markov model is been used based on the Baum Welch algorithm Here in this step the unknown parameters are identified from the Analysis of clusters formed in the prior steps using Baum Welch algorithm as mentioned below.

4.1 Forward Algorithm

Here each unique cluster elements are compared with the next elements of the other clusters to form a semantic association based on some predefined protocols and decisions and algorithm can be represent below

ALGORITHM 1:FORWARD ALGORITHM

// Input : Data Set **D**,
Observed States $\mathbf{O_s}$ = { O_{s1} , O_{s2},O_{s3}}
Step 0: **Start**
Step 1: Identify the Observed state Attribute $\mathbf{O_{si}}$
Step 2: **FOR** i=0 to size of **D**
Step 3: Identify Attribute $\mathbf{O_{si}}$ and put in separateList $\mathbf{O_{SL}}$
Step 4: END FOR
Step 5: FOR i=0 to size of $\mathbf{O_{SL}}$
Step 6: identify α using equation 1
Step 7: **END FOR**
Step 8: **Stop**

4.2 Backward Algorithm

Here each unique cluster elements are combined with the same clusters other elements and then this combination elements are form association with the other cluster elements based on some predefined protocols and decisions. and algorithm can be represent below

ALGORITHM 1:BACKWARD ALGORITHM

// Input : Data Set **D**,
Observed States $\mathbf{O_s}$ = { O_{s1} , O_{s2},O_{s3}}
Step 0: **Start**
Step 1: Identify the Observed state Attribute $\mathbf{O_{si}}$
Step 2: **FOR** i=0 to size of **D**
Step 3: Identify Attribute $\mathbf{O_{si}}$ and put in separateList $\mathbf{O_{SL}}$
Step 4: END FOR
Step 5: FOR i=0 to size of $\mathbf{O_{SL}}$
Step 6: identify β using equation2
Step 7: **END FOR**
Step 8: **Stop**

4.3 Baum-Welch Algorithm

This algorithm takes input from associated clusters formed through forward and backward algorithms, and then it evaluates hidden state based on the probability and frequency of the association. Hidden states can be evaluated using equation 1.

$$\gamma = \sum_{j=1}^{N} \alpha(j)\beta(j) \text{---------- (1)}$$

Where
α = Forward Probability
β = Backward Probability
γ=Probability of being at the state
N= Size of the Observed state List
Step 5: Here in this step by using Bayesian probability and predefined protocols compromised attacks are evaluated.

IV RESULTS AND DISCUSSIONS

To show effectiveness of the proposed system experiments are conducted by deploying the system in windows based java supporting machine. For deployment experiment is used Apache tomcat as the web server and Netbeans as the development IDE.

Precision and recall are considered as the best performance measuring parameters. Precision can be defined as the ratio of number of relevant attacks detected to the sum of number of relevant and irrelevant attacks detected. Relative effectiveness of the system is well expressed by using precision parameters.

Whereas the recall can be defined as the ratio of number of relevant attacks detected to the sum of relevant attacks not detected. Absolute accuracy of the system is well narrated by using recall parameters.

Precision and recall can be more clearly elaborated as follows.

- X = the number of relevant attacks detected,
- Y = the number of relevant attacks not detected, and
- Z = The number of irrelevant attacks detected.

So, Precision = (X/ (X+ Z))*100
And Recall = (X/ (X+ Y))*100

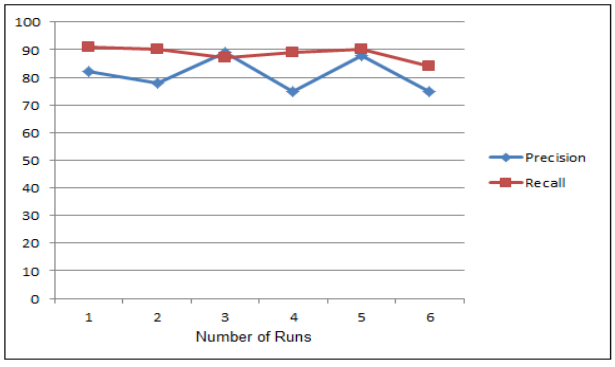

Figure 3: Performance Evaluation through precision and recall

On plotting the graph for precision and recall for different number of runs we found some facts that system yields 81.16 % of precision and 88.5 % of recall. This we can say that good for any system.

V CONCLUSION AND FUTURESCOPE

Now a days due to increasing popularity of online social networks, the users of OSN are always prone to attack. Compromised attacks are the worst in the form and they can steal the data from the user accounts or they can miss use the user profile.

So proposed methodology proposes an idea of using detecting compromise attack using machine learning technique. This process eventually yields the best results as it scrutinizes the past history of attack patterns.

This system can be explicitly implement for other attacks in real time OSN in internet in the future enhancements.

REFERENCES

[1] Barack Obama's tweets hacked. [Online] Available: http://money.cnn.com/2013/10/28/technology/barack-obama-twitter-hack/

[2] Russian Prime Minister's Twitter Account Hacked. [Online] Available: http://www.effecthacking.com/2014/08/russian-prime-ministers-twitter-account.html?m=0

[3] Ruan, X., Wu, Z., wang, H., & Jajodia, S. (2016). "Profiling Online Social Behaviors for Compromised Account Detection". Information Forensics and Security, IEEE Transactions on, 11(1), 176-187.

[4] F. Benevenuto, T. Rodrigues, M. Cha, and V. Almeida, "Characterizing user behavior in online social networks," in Proc. 9th ACM SIGCOMM Conf. Internet Meas. Conf. (IMC), Chicago, IL, USA, 2009, pp. 49–62..

[5] Q. Cao, M. Sirivianos, X. Yang, and T. Pregueiro, "Aiding the detection of fake accounts in large scale social online services," in Proc. 9th USENIX Conf. Netw. Syst. Design Implement. (NSDI), San Jose, CA, USA, 2012, p. 15.

[6] M. Egele, G. Stringhini, C. Kruegel, and G. Vigna, "COMPA: Detecting compromised accounts on social networks," in Proc. Symp. Netw. Distrib. Syst. Secur. (NDSS), San Diego, CA, USA, 2013M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[7] B. Viswanath et al., "Towards detecting anomalous user behavior in online social networks," in Proc. 23rd USENIX Secur. Symp., San Diego, CA, USA, Aug. 2014, pp. 223–238

[8] Singh, Tejwant, and Mr Manish Mahajan. "Performance comparison of fuzzy C means with respect to other clustering algorithm." International Journal 4.5 (2014).

[9] Lu, Yinghua, et al. "Implementation of the fuzzy c-means clustering algorithm in meteorological data." International Journal of Database Theory and Application 6.6 (2013): 1-18.

[10] Ghogge, Rajshekhar. "Fuzzy C-means Clustering Algorithm." Brain 3.7 (2014).

[11] Suganya, R., and R. Shanthi. "Fuzzy c-means algorithm-a review." International Journal of Scientific and Research Publications 2.11 (2012): 1.

[12] Ghahramani, Zoubin. "An introduction to hidden Markov models and Bayesian networks." International Journal of Pattern Recognition and Artificial Intelligence 15.01 (2001): 9-42.

[13] Baggenstoss, Paul M. "A modified Baum-Welch algorithm for hidden Markov models with multiple observation spaces." IEEE Transactions on speech and audio processing 9.4 (2001): 411-416.

[14] Chis, Tiberiu S., and Peter G. Harrison. "Incremental HMM with an improved Baum-Welch Algorithm." OASIcs-OpenAccess Series in Informatics. Vol. 28. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2012.

[15] Turin, William. "Unidirectional and parallel Baum-Welch algorithms." IEEE Transactions on Speech and Audio Processing 6.6 (1998): 516-523.

[16] Baggenstoss, Paul M. "A modified Baum-Welch algorithm for hidden Markov models with multiple observation spaces." IEEE Transactions on speech and audio processing 9.4 (2001): 411-416.

[17] Hsiao, Roger, Yik-Cheung Tam, and Tanja Schultz. "Generalized Baum-Welch algorithm for discriminative training on large vocabulary continuous speech recognition system." 2009 IEEE International Conference on Acoustics, Speech and Signal Processing. IEEE, 2009.

[18] Bretthorst, G. Larry. "An introduction to parameter estimation using Bayesian probability theory." Maximum Entropy and Bayesian Methods. Springer Netherlands, 1990. 53-79.

[19] Kaminskiy, M., and V. Krivtsov. "Bayesian probability papers." Reliability: Theory & Applications 1.2 (2006): 57-62.

[20] Stokes, Maura, Fang Chen, and Funda Gunes. "An introduction to Bayesian analysis with SAS/STAT® software." Proceedings of the SAS Global Forum 2014 Conference, SAS Institute Inc, Cary, USA (available at https:// support. sas. com/ resources/ papers/ proceedings14/ SAS400-2014. pdf). 2014.