THINK INDIA (Quarterly Journal)

ISSN: 0971-1260
Vol-22-Issue-2-April-June-2019

Inspecting The Social Networks Based On Eccentric Behavior Of User

Mrs. N.Ramya[1*], B.Nithya[2], K.L.Pavithra[2], R.Swetha [2]

Assistant professor, Computer Science Engineering., Sri Sai Ram Engineering college, Chennai, India India [1]

Student, Computer Science Engineering, Sri Sai Ram Engineering college, Chennai,India India [2]

ramya.cse@sairam.edu.in , bnithya97@gmail.com , pavithrakarthikeyan22@gmail.com

swethar2498@gmail.com

ABSTRACT:
A risk assessment based on the idea that the more a user behavior diverges from what it can be considered as normal behavior. Sybil attack which is considered as a single user will continuous post any content, more number friends in short period of time. We monitor group behavior of people based on their posts and likes. If there are any deviations misbehavior is identified. We deploy a centralized server for all kinds of Government Registrations, user has to provide three different mobile numbers and the sequence of feeding is also given by the user. In case of any New registrations like License / PAN Number / any where Aadhaar is used OTP will be generated to all the three numbers. If any other user tries to access the Main registered mobile number of the user then the automatic notification of Link is communicated to the main user for authentication, only after permission, the requested user can view the mobile number. This System will avoid any misbehavior particularly mobile based banking process.

Keywords— Sybil attack, Anomalous Behavior, Online social network(OSN), Clustering, Risk Analysis, Big Data, Hadoop, One Time Password(OTP)

INTRODUCTION:

ONLINE Social Networks (OSNs) allows the users to create a public or private profile, afford sharing of information and ideas, interests with other users promote communication. As a result, OSNs are gaining popularity in the recent times and are an integral part of life. People use OSNs for both personal and business purposes. The social media allows to build connections expanding to finally build a network. Although there is a dramatic increase in OSN usage— Face book, for instance, has now 1.55 billion monthly active users, 1.31 billion mobile users, and 1.01 billion daily users1 there are also a lot of security/privacy concerns. One of the main source of these concerns is that OSN users establish new relationships with unknown users with the result of exposure of a huge amount of personal data. Unfortunately, very often users are not aware of this exposure as well as the serious consequences this might have. Also, some users are less concerned about information privacy; therefore, they post more sensitive information on their profiles without specifying appropriate privacy settings and this can lead to security risks . As a result, today's social networks are exposed to many types of privacy and security attacks. These attacks exploit the OSN infrastructures to collect and expose personal information about their users, by, as an example, successfully convincing them to click on specific malicious links with the aim of propagating these links in the network. These attacks can either target users personal information as well as the personal information of their friends. Another widely used attack is the

ISSN: 0971-1260
Vol-22-Issue-2-April-June-2019

generation of fake profiles, which are generated with the only purpose of spreading malicious content. In addition, there is a growing underground market on OSNs for malicious activities in that, for just few cents, you can buy Face book likes, share, Twitter followers, and fake accounts. This can lead to misusing the account and using them to acquire fake government based identity proofs. Although many solutions, targeting one specific kind of attacks, have been recently proposed having a more general solution that can cope with the main privacy/security attacks that can be perpetrated using the social network graph is missing. In this paper, we make a step towards the definition of a unique tool that helps OSN providers as well as users to detect several types of attacks and also protect the user information controlling the mishaps of fake identities. We believe that linking each id with mobile numbers will serve the purpose. Big data integrates all the information and each time a new registration is made on the government based websites eg.PAN /AADHAR an OTP (One time password will be generated. Our goal in this paper is to provide maximum security to the information. The goal is to compare the behavioral patterns of users with other users in the network to find anomalous behaviors. Defining the normal behavior has two main issues. The first is the definition of a user behavioral profile able to catch those user's activities and interactions that are considered meaningful for risk assessment. The second issue regards how to model a 'normal behavior'. In doing this, we have to consider that OSN users are really heterogeneous in observed Behaviors.Based on this principle, we propose a two-phase risk assessment, where users are first grouped together according to some features meaningful for group identification. Then, for each identified group, we build one or more normal behavioral models. To reach this goal, the key contributions include determining various user features to model normal/anomalous behaviors, and integrating them with probabilistic-clustering approach (the Expectation Maximization algorithm). As it will be illustrated in the paper, we carried out experiments on a dataset to show that the proposed two-phase risk assessment outperforms a simplified behavioral-based risk assessment where behavioral models are built over the whole OSN population, without a group identification phase. Any fraudulent usage will be intimated as a Sybil attack and a notification will be sent t the user. Thereby, the user has an idea that his account is being misused.

PRESENT SYSTEMS:

Though the usage of Online Social Network (OSN) is prevalent, there is still a lot of security and privacy concerns. The well known applications like face book still face an issue of revealing the users information,thus failing to provide the necessary protection to the information.By this, it had the following disadvantages.Firstly,more number of user's profiles were compromised .Secondly,we can easily see the user information we share the profile.The main drawback was there is no encryption system for security.The existing Systems assess the risk using a score based on how she/he behaves in the OSN. The key idea was to find out how the user behavior diverges from the normal behavior.Therefore for meaningful risk assessment a normal user behavior should be well defined.The objective of the project is to compromising OSN account and to protect the user profile using OTP generation.The proposed system can be seen as two stages .In the first stage, a risk assessment is made on the user behaviour to determine how much it is deviant from the normal behaviour.secondly,Sybil attacks are being identified in social media as a result of this assessment.At the final

ISSN: 0971-1260
Vol-22-Issue-2-April-June-2019

stage, we deploy a centralised server for all kinds of Government Registrations where the user has to provide three different mobile numbers . In case of any new fake use of user details ,OTP will be generated to all the three numbers and automatic notification is communicated to the main user for authentication, only after permission, the requested user can view the mobile number.Thus it helps to avoid any misbehaviors related to user information.The advantages of the proposed system is as follows.The user profile is given maximum security ,the Sybil attacks are identified, the user profile is encrypted,the profile is protected using OTP.

RISK ASSESSMENT BASED ON USER BEHAVIORS:

A risk score with a user based on how he/she behaves in the OSN able to catch those user's activities and inter- actions that we consider meaningful for risk assessment. In an OSN, a variety of activities are possible, such as writing comments/posts, reading, or sharing items, as well as different types of interactions, like commenting on a users' post, viewing profile information, assigning likes, joining special groups or pages, sending invitations to others. In designing a behavioral profile we do not aim at monitoring all users' activities, but only those that might reveal risky conducts. As an example, writing a lot of comments/posts without receiving any like on them can be considered a warning that the corresponding user might be a victim of an attack. On the contrary, simply having a high number of friends, posts, comments and likes cannot be considered as a risky behavior. However, having a high number of friends, posts, comments and likes in a short period of time can be considered risky. In order to identify a set of *behavioral features*, meaningful for risk assessment.

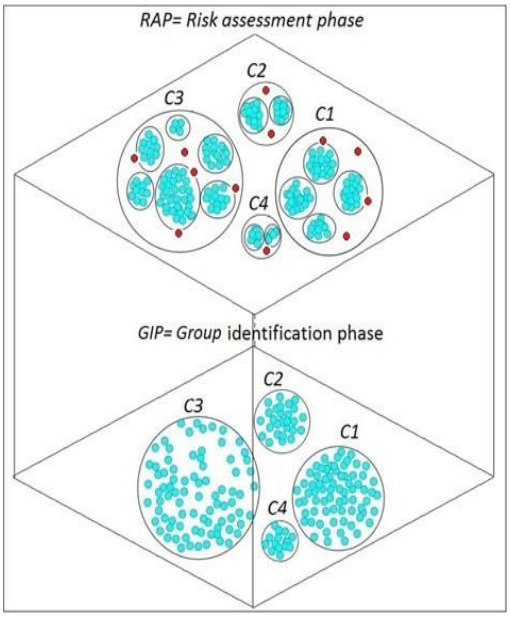


Fig. 1. Two phase risk assessment.

We have deeply reviewed the literature looking for well-known OSN attacks (see Section 2).The second issue to be addressed regards how to model a normal behavior that, according to the proposed approach, has to be used as baseline to measure how much users diverge from it and thus to compute the corresponding risk score., the proposed approach performs a first phase aiming at *identifying groups in the OSN*. This is achieved by exploiting clustering techniques over a set of user features meaningful for group identification, called, in what follows, *Group identification features*. It is easy to determine the users who do not fall in that group.

SYBIL ATTACKS:

Sybil attacks are one of the most prevalent and practical attacks in OSNs. To launch a Sybil attack, a malicious user has to create multiple fake identities , known as sybils, with the purpose to legitimate his/her identity , so as to unfairly increase his/her power and influence within a target community giving rise to spam and malware on Face book and Twitter. In

ISSN: 0971-1260
Vol-22-Issue-2-April-June-2019

general, we can classify Sybil attacks into two types. The first is sybils with *tight-knit community (dense friendship graph).* According to these attacks, adversaries create the Sybils shows to belong to another type, that is, those with *sparse community (sparse friendship graph).*

Identity clone attacks: In this type of attack, a malicious user creates similar or even identical profiles to impersonate victims in an OSN. The key goal is to obtain personal information about a victim's friends after successfully forging the victim, and to establish increased levels of trust with the victim's social circle for future deceptions. The cloned identity can also be used to propagate malicious messages to other users in the network

Compromised accounts attacks: Compromised accounts are accounts where legitimate users have lost complete or
partial control of their login credentials. Accounts can be com- promised in a number of ways, for example, by exploiting a

MODULES:

1. Design of social media like webpage
2. Host Monitoring and Storage
3. Inscribing the user data
4. Anomalous behavior
5. Triple OTP generation

MODULES DESCRIPTION:

DESIGN OF SOCIAL MEDIA LIKE WEB PAGE:

In this module the design of web application and database connectivity will describe. Using Java Servlet Page (JSP) we design the page like social media (face book, twitter, etc). In this part we will get all the user information and store it on MySQL. MySQL is our database to store all the details including user profile information, user post information, friends list and all other details related to the user.

HOST MONITORING AND STORAGE:

Centralized server will communicate with the user and corresponding server. It will get all the details about the user and their request from the web application and it will pass to the corresponding web form and return it to the client side. It is major part of our application to maintain all the details.

INSCRIBING THE USER DATA:

In this part we secure the user details by showing the user profile information to others in encrypted form. In our implementation we secure the user sensitive information like mobile number from other user. Because using mobile number, DOB and location any one can see one's personal government identity. So for that problem we secure the information.

ANOMALOUS BEHAVIOR:

In this we monitor user anomalous behavior. It means today user's social media account is compromised by some unauthorized people. we will identify the following anomalous behavior like Sybil attack, more number of friend request in short period of time, posting more number content in short time. Those types of attacks will be identified by our application.

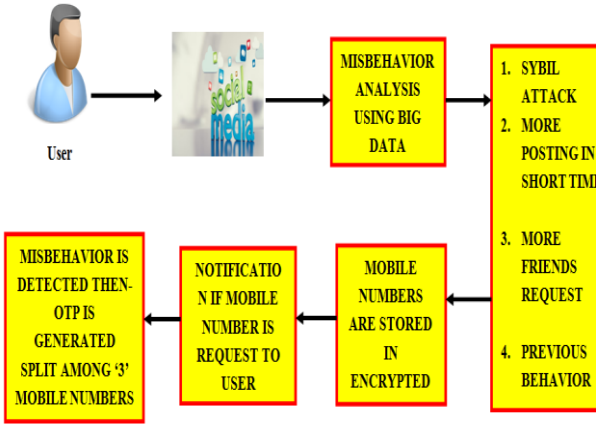
TRIPLE OTP GENERATION:

This module will describe about triple OTP security. In this we get three different mobile numbers for security. If users want

ISSN: 0971-1260
Vol-22-Issue-2-April-June-2019

to apply any application to get any authenticity they have to share these three random OTP on that place. After that verification, user can apply for any application.

FLOWCHART:



FURTHER WORKS:

Primarily our project can provide solution for a server at a primary level .Implementation of our project on a centralized server requires proper permissions from the governmental agencies and will be developed after 10-15 years for the whole database. In Future our application can be extended to many other social networks.

LIMITATIONS:

Our limitations in the project are we at least require data about a large number of users, their mobile numbers which have been registered in the sites, a large scale centralized server which can monitor the anomalous behaviors.

IMPLEMENTATION:

Online Social Networks can be made secure preserving the security using Big data, notifying the user through OTP. By this there is no compromise in the user information .Social media can thus be used without any risk and fear of user that his /her information will be lost.

CONCLUSION:

Thus the paper concludes that every user profile information is secured using big data. User's profile compromising is secured using OTP protection using three types of mobile numbers registration.And hardware designing are the core concepts in our project. It requires larger data and working to complete the project.

ISSN: 0971-1260
Vol-22-Issue-2-April-June-2019

REFERENCES:

- Naeimeh Laleh, Barbara Carminati, and Elena Ferrari, Fellow, "Risk Assessment in Social Networks Based on User Anomalous Behaviors" in IEEE transaction on dependable and secure computing, vol.15, no.2,march/april 2018.

- C. Gurcan Akcora, B. Carminati, and E. Ferrari, "Privacy in social networks how risky is your social graph?" in Proc. IEEE 28th Int. Conf. Data Eng., 2012, pp. 9–19.

- Christa S. C. Asterhan and T. Eisenmann, "Online and face-to-face discussions in the classroom: A study on the experiences of 'active' and 'silent' students," in Proc. 9th Int. Conf. Comput. Supported Collaborative Learn.-Vol. 1, 2009, pp. 132–136.

- L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, "All your contacts are belong to us automated identity theft attacks on social networks," in Proc. 18th Int. Conf. World Wide Web, 2009, pp. 551–560.

- Y. Boshmaf, K. Beznosov, and M. Ripeanu, "Graph-based Sybil detection in social and information systems," in Proc. IEEE/ACM Int. Conf. Adv. Social Netw. Anal.Mining, 2013, pp. 466–473.

- Y. Boshmaf, D. Logothetis, G. Siganos, J. Ler_ıa, J. Lorenzo, M. Ripeanu, and K. Beznosov, "Integro: Leveraging victim prediction for robust fake account detection in OSNs," in Proc. Netw. Distrib. Syst. Security Symp., 2015, pp. 8–11.

