SOCIAL MEDIA PROTECTION FRAMEWORK AGAINST THE VARIOUS ATTACKS USING DATA MINING

[1]Ms. P.S. Khorgade, [2]Dr.Mrs. S. S. Sherekar, [3]Dr.V.M.Thakare

[1]Student ME, [2]Professor, Professor

[1] PG Department of Computer Science and Engineering,
[1]SGBAU, Amravati, India

Abstract: This paper has proposed a novel framework, named NetSpam, which utilizes spam features for modeling review data sets as heterogeneous information networks to map spam detection procedure into a classification problem in such networks. Using the importance of spam features helps us to obtain better results in terms of different metrics experimented on real-world review data sets from Yelp and Amazon Web Sites it impinges on a large proportion of the population and affects government service policies and people's life quality. Typical welfare countries, such as Australia and Canada, have accumulated a huge amount of social security and social welfare data. Social networks have attracted billions of users and supported a wide range of interests and practices. Users of social networks can be connected with each other by different communities according to professions, living locations, and personal interests. Social media has gripped live in a dramatic way. Privacy protection of user data lying with the service provider need to be preserved when published for the purpose as the research as the release of sensitive personal information of an individual may pose security threats. Proposed approach has been validated using the data of real time social network twitter.

Index Terms: **Social media, Social network, Spam review, Security, Privacy protection, inference attacks, sanitization techniques.**

I. INTRODUCTION

The Online Social Media portals play an influential role in information propagation which is considered as an important source for producers in their advertising campaigns as well as for customers in selecting products and services. These reviews thus have become an important factor in success of a business while positive reviews can bring benefits for a company, negative reviews can potentially impact credibility and cause economic losses [1]. Social security data mining (SSDM) seeks to discover interesting patterns and exceptions in social security and social welfare data. From the data mining goal perspective, it aims to handle different business objectives, such as debt prevention. From the data mining task perspective, it involves both traditional data mining methods, such as classification, as well as the need to invent advanced techniques, e.g. Complex sequence analysis communities are increasingly interested in "what do social security data show" and recognize the value of data-driven analysis and decisions to enhance public service objectives, payment accuracy, and compliance. Within them Arraign of machine learning and data mining with public sectors, an emerging data mining area is the analysis of social security/welfare data [2]. The online applications and cloud computing, allow their users to host large amounts of personal data on their platforms, important concerns regarding the security and privacy of user-related information arise. How to protect users' personal information, and encourage users to participate the privacy protection to improve the information security of the entire social network, have become one of critical problems for social network managers [3]. The gain sudden popularity is ranked by Twitter as a list of trends. Twitter and Google trends have become an important tool for journalists. Twitter in particular is used to develop stories, track breaking news, and assess how public opinion is evolving in the breaking story. Taking election campaigns as an example, journalists, campaigns, and pundits have tracked trends in Twitter traffic to determine candidates' popularity and predict likely election outcomes [4].
The rapidly growing numbers of mobile device as well as social multimedia application and services demand for direct connectivity means between users to of load the infrastructure of a network operator, which is possible over a range of wireless technology [5].

This paper proposed a system that implements a novel watermarking scheme for numeric database attributes which provide efficient in defeating a range of attacks, which may be used to remove or destroy the mark. This proposed method can improve the watermarked database and can support normal user modifications by simply applying the encoding algorithm.

II. BACKGROUND

Author use unigram, bigram and their composition. Other studies use other features like pair wise features (features between two reviews; e.g. content similarity), percentage of CAPITAL words in a review for circumstances is equal to $O(e^2m)$ where is number of edges in created network or reviews number. It need to check if there is a metapath between a certain node (review) with other nodes which is $O(e^2)$ and this checking must be repeated for very feature. So, time complexity for offline mode in which give the Main dataset to framework and calculate spam city of whole reviews, is $O(e^2m)$ where m is number of features [1].

Some methods use temporal and location features of users to find unusual behaviour of spammers. Li *et al.* in use some basic features and then run aHNC to find final labels on Damping's dataset. Almost engages behavioural features like rate deviation, extremity and etc. Xie*et al.* in also use a temporal pattern to find singleton reviews (reviews written just once) on Amazon. Luca and Zervas in use behavioural features to show increasing competition between companies' leads to very large expansion of spam reviews on products [2].

A game theoretic framework in proposed model interaction and influence when users choose strategies that make use of the privacy protection or not. The framework reveals that the protection of the users' privacy information depends not only on the users' own strategies, but also strategies of other users. In other words, the framework can analyse the information protection through users' interactions and decision making [3].

Author provides a comprehensive example of a possible SCA along the lines of extracting sensitive information from a Smartphone by utilizing off-the-shelf, inexpensive equipment available to anybody. In doing so, it focus on decentralized MSNs due to their more dynamic behaviour from the connectivity perspective, scenario of interest is when a group of users belonging to a particular MSN exploit social relationships to share data over the proximity-based links[4].

Methods can poses security challenges due to repetitive connection establishments, which in turn requires higher levels of security. Finally, deliver an overview of possible enhanced attacks that are reviewed in conjunction with solutions that may be useful to avoid losing personal and sensitive information, which is kept within the smart phones and other personal user devices [5].

III. PREVIOUS WORK DONE

Saeedreza *et al*. (2017) [1], has proposed Supervised learning can be used to detect review spam by looking at it as the classification problem of separating reviews into two classes: spam and non-spam reviews. To the best of our knowledge, the first researchers to have studied deceptive opinion spam using supervised learning were Jindal et al discuss the evolution of opinion mining, which had primarily focused on extracting or summarizing the opinions from text by using Natural Language Processing (NLP).

Longbing cao et.al.(2012) [2] the importance of social security and social welfare, business has been increase single organised in more and more contries,it large proportion of the population and affects government service policies and people's life quality. Typical welfare countries, such as Australia and Canada, have accumulated a huge amount of social security and social welfare data. Emerging business issues such as fraudulent outlays, and customer service and performance improvement challenge existing policies, well as techniques and systems including data matching and business intelligence reporting systems.

un Du*al. (*2018) [3], has proposed Social networks have attracted billions of users and supported a wide range of interests and practices. Users of social networks can be connected with each other by different communities according to professions, living locations, and personal interests. With the development of diverse social network applications, academic researchers, and practicing engineers pay increasing attention to the related technology. As each user on the social network platforms typically stores and shares a large amount of personal data, the privacy of such user-related information raises serious concerns.

Yubao Zhang *al. (*2017) [4] presents research on privacy protection relies on specific information security techniques such as anonymization or access control. However, the protection of privacy depends heavily on the incentive mechanisms of social networks, like users' psychological decisions on security execution and socio-economic considerations.

Roman Mostovoy*et.al.*(2017) [5],has proposed trend taxonomy trend detection and real events extraction from Twitter trends However, researchers have paid little attention to Twitter trend manipulation. It is reported that attackers manipulate Google trends by simply employing large group of people to visit Google and search for a specific keyword phrase. Also, Just et al inspected Twitter manipulation in an election campaign. As reported in The Wall Street Journal, robots have been used to undermine the "trending topics" on Twitter. Thus, the focus of this work is on Twitter trend manipulation.

IV. EXISTING METHODOLOGIES

A great number of research studies focused the problem of spotting spammers and spam reviews. However, since the problem is non-trivial and challenging, it remains far from fully solved. The effect of social networks could be captured by the influence model while the manipulation of a meme can be regarded as the effort to drive the meme to trend beyond the effect of the network. Manually check if the hash tag has been covered by any news media.

a. Linguistic-Based Methods

This approach extracts linguistic-based features to find spam reviews. Feng *et al.* [1] use unigram, bigram and their composition. Other studies use other features like pair wise features, percentage of CAPITAL words in a reviews for circumstances is equal to $O(e^2m)$ where is number of edges in created network or reviews number. It need to check if there is a met path between a certain node with other nodes which is $O(e^2)$ and this checking must be repeated for very feature. So, time complexity for offline mode in which we give the Main dataset to framework and calculate spam city of whole reviews, is $O(e^2m)$ where *m* is number of features.

The probability of unlabelled review *u* being spam, the following equations:

$$Pr_{u,v} = 1 - \Pi_{i=1}^{L} 1 - mp_{u,v}^{p_i} \times W_{p_i}$$
$$Pr_u = avg(Pr_{u,1}, Pr_{u,2}, \ldots, Pr_{u,n})$$

B. Behavior-Based Methods

The focuses on distribution of spammers rating on different products and traces them. Extract 36 behavioural features and use a supervised method to find spammers on Amazon an] indicates behavioural features show spammers' identity better than linguistic ones.

Xue*et al.* use rate deviation of a specific user and use a trust-aware model to find the relationship between users for calculating final spam city score. Munich *et al.* in use temporal and location features of users to find unusual behaviour of spammers.

To compute the weight of met path pi, for I = 1, L where L is the number of met paths, they propose following equation:

$$W_{p_i} = \frac{\sum_{r=1}^{n} \sum_{s=1}^{n} mp_{r,s}^{p_i} \times y_r \times y_s}{\sum_{r=1}^{n} \sum_{s=1}^{n} mp_{r,s}^{p_i}}$$

C. Selecting Hash tags in Twitter

A number of hash tags always flourish in Twitter[3]. Some of them do not correspond to external events. Call these endogenous hash tags memes throughout this paper. Most of the memes are combinations of words or acronyms, which are used to express an emotion or raise a question. Since the memes are not associated with any external events, the spread of the memes can be only due to the effect of social networks and manipulation. The effect of social networks could be captured by the influence mode while the manipulation of a meme can be regarded as the effort to drive the meme to trend beyond the effect of the network. To determine whether a hash tag is a meme, manually check if the hash tag has been covered by any news media.

***D.* other Attacks:**

Acoustic Cryptanalysis: The main difference with the power analysis attack is that the acoustic emissions [4] can be obtained from the user input, such as e.g., keyboards There are no reliable ways to avoid this type of the SCA.

E* .Thermal Imaging*: This SCA is similar to the acoustic type, with the main difference that the analysis[5] of a thermograph from the CPU instead of the acoustic data is exploited. A possible countermeasure is to utilize additional shield on the device. This, however, may bring along the overheating issues.

Visual Attack*:* One of the most direct attacks is ``spying'i.e., capturing the light emissions from a display, led, or other device. Any signaling or sensitive information should thus be removed from the visual representation.

V. ANALYSIS AND DISCUSSION

The propose Net Spam framework that is a novel network-based approach which models review networks as heterogeneous information networks. A new weighting method for spam features is proposed to determine the relative importance of each feature and shows how effective each of features are in identifying spasm from normal reviews [1].

The summarize several SSDM case studies from our real-life projects with Centreline to address some of the SSDM challenges. Rather than presenting each case in detail, summarize the cases by highlighting the main business objectives, research issues, and solutions. Where applicable, they refer to relevant documents and papers for detailed techniques and experimental results to enable the presentation of more cases and references to provide readers with comprehensive references and the means to drill down to specific design [2].

A game theoretic framework is established to model users' interactions that influence users' decisions as to whether to undertake privacy protection or not. To model the relationship of user communities, community-structured evolutionary dynamics are introduced, in which interactions of users can only happen among those users who have at least one community in common. Then the dynamics of the users' strategies to take a specific privacy protection or not is analysed based on the proposed community structured evolutionary game theoretic framework [3].

The detailed Twitter trending algorithm remains unknown. Meanwhile, due to the limitations of the dataset, we study only the simple factors of Twitter trending (i.e., tweet number). using the evidence of manipulation, we demonstrated before, they believe the algorithm of Twitter trending can be strengthened by considering more complicated factors Although spammers could produce cliques, it will no doubt increase their risk of being detected [4].

Mobile social networks (MSNs) are the networks of individuals with similar interests connected to each other through their mobile devices. Recently, MSNs are proliferating fast supported by emerging wireless technologies that allows achieve more efficient communication and better networking performance across the key parameters, such as lower delay, higher data rate, and better coverage [5].

TABLE 1: Comparison between existing methodologies.

Social media protection	Advantages	Disadvantages
NetSpem: A Network-Base Spam Detection Framework for Review in Online Social Media	1. To identify spam and spammers as well as different type of analysis on the topic. 2. To display only trusted review to the users.	1. There is no information filtering concept in the online social network. 2. Less complexity.
Social Security and Social Welfare Data Mining: An Overview	1.Better customer service, quicker response 2.Support economic development	1.Data integrity and protection 2.Fraud detection
Community-Structured Evolutionary Game for Privacy Protection in Social Networks	1. Worldwide connectivity. 2. Real time information sharing: many social networking site incorporate and instant messaging features, which late people exchange information in real time via a chat.	1. Cyber bullying and crime against children. 2. Risks and fraud or identity theft. 3. Corporate invasion of privacy: social networking invite major corporation to invite your privacy and sell your personal information.
Twitter Trends Manipulation: A First Look Inside the Security of Twitter Trending	1.Massive audience potential 2.widely accessible 3.Customer service and advertisement	1.Balancing post frequency 2.Full time management 3.Limited message size
Mobile Social Networking Under Side-Channel Attacks: Practical Security Challenges	1. Ability to connect to other people all over the world. 2. Easy and instant communication.	1. Information overwhelm. 2. Social peer pressure and cyber bullying. .

VI. PROPOSED METHODOLOGY

A new preventing private information inference attacks in social networks. An inference attack is the attack used to obtain private and sensitive information from the known data. This technique is used for sensitive information is not directly disclosed, it is possible to match the known information with other data sources available and successfully complete inference attacks. This can be prevented by proposing new sanitization techniques. They proposed a framework that has provision for making inference attacks and also prevention mechanisms in the form of sanitization techniques. The Sanitization techniques are very useful are used to combat such attacks in social networks. The more Generalized information loss and structured information loss are the metrics used to make use of sanitization techniques. In Proposed System implemented a proof-of-concept Face book application for the collaborative management of shared data, called Controller. The prototype application enables multiple associated users to specify their authorization policies and privacy preferences to co-control a shared data item.

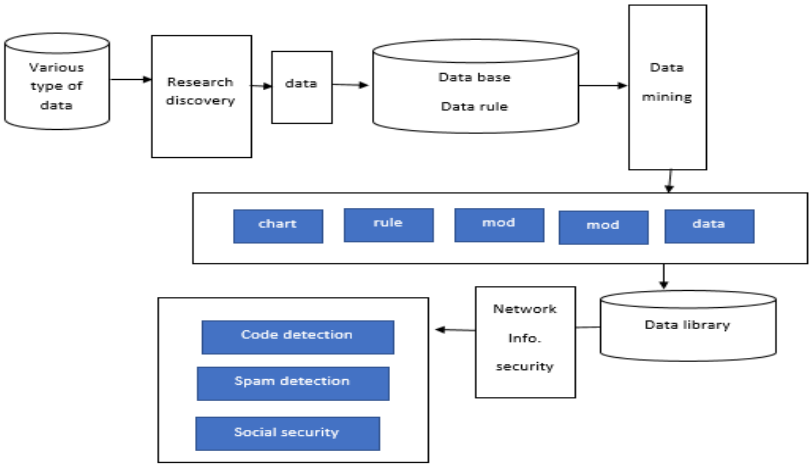

Fig 1: Social media protection framework against the various attacks.

VII. OUTCOMES AND POSSIBLE RESULT

An experimental result of the proposed method can indicate that a critical cost performance is an important parameter that helps the social network managers to make appropriate security service level and payment mechanism to encourage their users to accept the security service, and then promote the spreading of this secure behaviour. An inference attack is the attack used to obtain private and sensitive information from the known data.

VIII. CONCLUSION

Here a novel spam detection framework based on graph method to label reviews relying on a rank-based labelling approach is inbicated.The need for protecting private information in social networks. Especially, this paper focused on the private inference attacks on social networks. Sensitive information disclosure attacks are launched by hackers in which they infer unknown information from the known information. Information inference attacks can disclose the weakness of security mechanism in social networking systems. The privacy protection behaviours of social network users by a community structured evolutionary game theoretic framework. The players, strategies, payoff matrix and the topology structure of users are defined in this framework.

IX. FUTURE SCOPE

From Observation, the scope to be studied in future work, the information diffusion and content sharing in multilayer networks is still a young research. Addressing the problem of spam detection in such networks can be considered as a new research line in this field.The proposed scheme also requires enhancing the performance under strong deletion attack conditions and also to improve the computation speed.

REFERENCES

[1] SaeedrezaShehnepoor, Mostafa Salehi, Reza Farahbakhsh, and Noel Crespi, “Netspam: Anetwork based spam detection framework for review in online social media”, IEEE transactions on information forensics and securityVol. 12, No. 7, Pg. No., 1585-1595 july 2017.

[2] Longbing Cao, Senior Member, “Social Security and Social Welfare Data Mining: An Overview”, IEEE transactions onVol. 21, No. 6, Pg. No. 2991-3003, June 2012.

[3] Jun Du, Student Member, IEEE, Chunxiao Jiang, Senior Member, IEEE, Kwang-Cheng Chen,” Community-Structured Evolutionary Game for Privacy Protection in Social Networks”, IEEE transactions on information forensics and securityVol, Issue 13 No. 03, Page No.: 574-589 Year: March 2017.

[4]Yubao Zhang, Student Member, IEEE, Xin Ruan,Student Member, IEEE, Haining Wang, Senior Member, IEEE, Hui Wang, and Su He,” Twitter Trends Manipulation: A First Look Inside the Security of Twitter Trending”, IEEE Transactions On Information Forensics and Security,Vol, Issue 12 No. 01, Page No.: 144-156 Year: JANUARY 2017

[5]Aleksandr ometov1, alla levina2, pavel borisenko2, roman mostovoy2,antonino orsino1, and sergey andreev1,”Mobile Social Networking Under Side-Channel Attacks: Practical Security Challenges”,Special Section On Socially Enabled Networking and Computing Vol, Issue: 5 Page No.: 2591-2599 Year: January 23, 2017. .