Journal of Engineering Science and Technology
Vol. 15, No. 6 (2020) 4107 - 4122

A NOVEL METHOD FOR MULTI-DIMENSIONAL CLUSTER TO IDENTIFY THE MALICIOUS USERS ON ONLINE SOCIAL NETWORKS

KEERTHANA N.[1,*], VIJI VINOD[2], SUDHAKAR SENGAN[3]

[1]Department of Computer Science, Dr.M.G.R Educational and Research Institute, Tamil Nadu, India
[2]Department of Computer Applications, Dr.M.G.R Educational and Research Institute, Tamil Nadu, India
[3]Department of Computer Science and Engineering, Sree Sakthi Engineering College, Coimbatore-641104, Tamil Nadu, India
*Corresponding Author: keerthana.mca@drmgrdu.ac.in

Abstract

The initiation of Online Social Networks (OSN) has distorted a shared passive reader into an information provider. The Social Networks (SN) utilization of media in long-range interpersonal communication in our community is progressively getting to be well known. A victim of a winning attack is in which data including user names, email addresses, session tokens, and encoded/salted secret phrase of users undermined in a Twitter. It helps the users to share knowledge and to exchange viewpoints, and also to represent themselves in interactive online communities and to connect other users with common interests. OSN has transformed users' social domain into commercial space. It generates a problem around privacy and protection for OSN users. The OSN service providers store their consumers' private and confidential data securely, and sometimes it may be misused by data administrators, third parties, or unauthorized users. In this article, the trend of social networking websites aims to review and analyse these types of cyber threats of SN and develop measures to shield the identity in cyberspace, i.e., the security of non-public data and identity in social networks is studied. Specific protection and privacy concerns are clarified along with the guidelines for OSN users to defend themselves against these problems while utilizing SN. And this paper proposed a new method over the design of the multi-Dimensional Clustering (*m*-DC) method for FB-Friends, which characterize the weight esteems which utilize the assessments of inactive and dynamic user attacks. The better percentages of using m-DC for Face book users are achieved 45.64% in the precision, recall, and F1 score as 51.15%, 45.8 %, 59.19 %.

Keywords: Attacks, Cluster, Face book, Intrusion detection, Malicious user, Social Network Security.

1. Introduction

Social media is a means of contact for electronic interactions between the data owner (data generator) and users (end users) who build virtual communities through OSN. A social network is a social graph reflecting a link between people, organizations, and social activities. Online social networks are a better approach for correspondence and data sharing pulled in enormous users. An OSN is an online portal that end-users utilize to build social networks or partnerships with people that have standard views, preferences, experiences, and real-life interactions. The massive quantity of users' private information retained by the interpersonal Facebook Groups suppliers makes them an exciting objective for cyber-attacks [1]. These instances are identified as new dangers with users' protection.

The following have been some of the standard characteristics of social networking sites: (i) All modern online social networking platforms are web-based, have an Internet connection; (ii) The OSN profile information is mainly used for logging into the social networking platform for the authentication process; (iii) Commonly the social networking systems promote the establishment of social connections between members. The primary goal of OSNs' is to exchange information with the maximum consumers. Here, the users use OSNs for posting their daily operations, such as Facebook, Twitter, and LinkedIn. OSN participants also exchange information with colleagues and friends about themselves and their lives. Nevertheless, any of the exposed material through the OSN remains private in such reported results, which would, therefore, not be released at all. Users usually post certain aspects of their everyday life routine through status updates or photo sharing and video sharing.

OSN service companies are gathering a variety of data from their customers to deliver customized offerings, but they may use for commercial purposes. Additionally, data consumers can often be given to third parties for contributing to privacy leakages. This knowledge will exploit malicious users and violate a person's privacy. Data protection preserves knowledge against unwanted and harmful exposure by revealing, altering, abusing, or deleting electronically recorded or sharing data. A victim of a winning attack is in which data including usernames, email addresses, session tokens, and encoded/salted secret phrase of users undermined in a Twitter. With the growth of social networking and the increasing prevalence of electronic contact utilizing OSNs [2], increasingly more sensitive personal data is accessible. While most of the data exchanged by OSNs is not confidential, confident consumers are posting their data. Therefore, the use of publicly accessible confidential data will contribute to consumer privacy disclosure. Users' privacy is at higher risk because publicly accessible data can be tracked, and their actions can be connected to such data for processing and collecting secret knowledge from them. To safeguard the theoretical quality of electronic digital data [3], the inherent meaning of the data shall be secured.

The article’s principal emphasis is to find out the OSN-related problems of safety and protection and teach people every day how to defend themselves from these security and privacy concerns. Privacy is someone's freedom to retain knowledge to themselves, or at least share it with specific persons only. Conditions for privacy and security used to hold sensitive details free from unnecessary applications.

The word *'privacy protection'* is used in the circumstances where private data passed on to any other entity, an OSN in this instance, and the OSN wishes to

disclose and share this data for analysis or commercial reasons to some other entity. Therefore, at the same time, the OSN needs to protect the anonymity of its customers. In this situation, anonymization methods are implemented by the OSN to protect consumer privacy.

The second term is *'privacy protection,'* which used where the end-user does not even wish to share their data with the OSN server. Protection strategies are employed, in this situation, to preserve users' data. Our emphasis is on privacy, but at the same time, over the protection methods used to safeguard user data, thus the words of security and privacy are used in the complete article.

Also, propose another design of the multi-Dimensional Clustering (*m*-DC) method [4, 5] for FB-Friends, which characterize weight esteems utilizing the assessments examined previously. Using information from the FB, it results in the grouping of data is performed, and the closeness between the outcomes was discriminated [6]. The objective is to guarantee that the *m*-DC algorithm clusters a FB-U's as correspondingly as conceivable to how the client would group their friends. This paper addresses the problems that can affect OSN users, as well as providing them advice about how to safeguard their privacy when using OSNs [7, 8].

2. Literature Review

Numerous OSNs [9] have countless enrolled clients nowadays. Over a billion dynamic users, Facebook is presently the biggest and most famous OSN in the world. OSNs are Google+, with more than 235 million dynamic users; Twitter, with more than 200 million dynamic users; and LinkedIn, with more than 160 million active users. While a few specialists demand that OSNs are a passing design and will inevitably be supplanted by another Internet craze, current user measurements agree that OSNs are setting down deep roots. An ongoing review by the Pew Research Center's Internet and American Life Project uncovered that 72% of online American grown-ups utilize interpersonal interaction locales, an emotional increment from the 2005 Pew overview, which found that only 8% of online American grown-ups utilized long range informal communication destinations. Besides, the review uncovered that 89% of online American grown-ups are between the ages of 18 to 29 utilize informal community locales, while in 2005 , just 9% of the overview members in this age group utilized this kind of webpage.

Moreover, Facebook and Google+ portable applications are the second and fourth most of the time utilized by cell phone applications. It should be noticed that the utilization of OSNs on cell phones was not just advanced a considerably "closer relationship" to informal organizations yet additionally can represent other protection concerns, particularly in regards to the gathering of area information and the open door for promoters to distinguish specific kinds of users. Other than being mainstream among grown-ups, OSNs have turned out with very well-known with little youngsters and adolescents.

OSN suppliers have to put unique assets in opposing attacks, and in sanitizing the social charts and user-created substance facilitated on their foundation. Those endeavors have included improving to more readily secure user qualifications, utilizing CAPTCHA [10] difficulties in delaying forceful attacks, using photograph-based social verification to check user accounts when they are seen as strange, building cross-organization associations to stifle Internet dangers cooperatively and so forth. To encourage the augmentation of the protection line,

OSN suppliers will, in general, include more framework support for an assortment of directed AI-based ways to deal with catch malicious activities.

The SCAN algorithm [11] is another clustering algorithm, which considers the fundamental contrasts of a system outline to perform clustering and characterizes two different jobs: which interfaces at least two clusters that are profoundly related. An anomaly, which has a generally lower level of relationship with different individuals in the Group Recommendation System (GRS) [12] gives a computation technique and proposes that the clients connect school clubs like their very own qualities is the role of a hub. The GRS utilizes 15 highlights that are standardized to values somewhere in the range of 0 and 1 as the bases for computing the separation between individuals, including time zone, age, and so on.

Clustering calculations is partitioned into a few sorts, for example, various levelled, divided, thickness based, network-based, fuzzy-based clustering. Traditional hierarchical algorithms control permit making a full tree of the covering groups. Non-hierarchical approaches depend on the enhancement of some goal work, which characterizes parting items set. In this gathering, there is a specific arrangement of bunching calculations k-means that utilization the total of squares of the weighted deviations of items facilitates from the focuses of required groups as the physical capacity. Groups are searched in a circular/ellipsoidal shape [13].

A few kinds of Clustering algorithms subdivided into hierarchical, partitioned, thickness based, grid-based, fluffy clustering. Classical hierarchical algorithms permit to make the full tree of covering clusters. Non-hierarchical algorithms depend on the streamlining of some target work, which characterizes parting objects set. In this gathering, there is the different arrangement of clustering algorithms k-implies which utilize the aggregate of squares of the weighted deviations of objects coordinates from the focuses of required clusters as the target function. The round/ellipsoidal shape [14, 15] investigated by Clusters.

In Table 1, we show the merits and the demerits of different privacy studies that were carried out to understand the privacy perception of OSN users [16-19]. The studies reveal that mostly it is the unawareness of privacy and its importance that results in a privacy breach. People find managing privacy settings as a time consuming and confusing task. Therefore, there is a direct need for efficient tools and mechanisms to ensure privacy. Many researchers have come up with privacy-preserving tools and efficient mechanisms to resolve the problems stated above.

The article [20-23] describes the actions and perceptions of social network consumers by completing and evaluating different human ecology teams, but such activities map to limitations found in social networking applications. In the article [24], the scientific highlights the industrial and social edges of safe and well wise use of social networking internet sites.

In the article [24-27], discourses security problems, security, and network managers, which regularly address network policy management services like firewall, intrusion, intromission system, antivirus and knowledge lost. It reports security, the framework to safeguard corporate info against the threats associated with social networking internet sites.

Table 1. A Comparison showing the pros and cons of different privacy studies in the field of OSNs [24-29]

Researcher	Investigation Analysis	Techniques
Liu et al. [241	Measured the disparity between actual and the desired privacy settings	No mention of tool/ method made
Stutzman and Kramer-Duffield [25]	Studied relationship between network structure, assumption violation and informal privacy activities that only profile friends	Self-reported data, Limited accuracy, and recall, Nonresponse bias
Wang et al. [26] and	Investigated the regrets associated with users' posts	No solutions provided
Johnson et al. [27]	Analysis of privacy issues of consumers, their network configurations, and awareness of the privacy-preserving approaches posted information.	The sample used was biased toward users who were unconcerned with privacy
Sleeper et al. [28]	Studied the sharing behaviour	Small sample size, Difficult to generalize, Diary study resulted in biased data
Braunstein et al. [29]	An indirect technique for measuring content privacy concerns	The use of privacy language made extensively; respondents might have adjusted their responses, thus making the data biased.

3. Proposed Methods FB-U IDS with SNA

These FB-U IDS with Social Networking Agent (SNA) proposed work (Fig. 1.) present dual investigations, which include the utilization of SNA in this segment. The first calculation is viewed as information mining for FB, though the subsequent calculation viewed as arriving at explicit users in focused associations. Most SNs expect users to make accounts to set up associations with other network users. A user's record may incorporate individual information in many cases, for example, photos, birthday, principal residence, ethnicity, and personal interests. In most undirected SNs, users' interface with each other by transmitting companion demands. The beneficiary must acknowledge the companion demand to set up a companion interface with the initiator of the request. At the point when this procedure has finished, the two gatherings secure the benefit of getting one another's profile subtleties voluntarily .

Consequently, we chose to characterize an acknowledged companion demand as an invasion of the informal community of the user. Our calculations depend on the foundation of SNA on SN. The thought was that, when users acknowledge these SNA companion demands, these SNA additions expanded access to users' profiles and may assemble extra data about users and, now and again, data about the user's FB-F.

3.1. Objective of Intrusion Detection of FB-Users

Figure 1 represents the ID of FB Users

- A malicious user can naturally approve his FB addresses grade (e.g., discover which locations are most likely genuine and dynamic) by questioning an SN and send a spam message to FB-U.
- Social phishing can join with the past attack, i.e., the malicious user, the profile of a user, and this data utilizations is used to send focused phishing messages (if the client has an open profile and open friend list).
- FB-profiles can bring a malicious user of the FB-U of an FBG and utilize this data during the examination stage preceding the genuine viciousness.

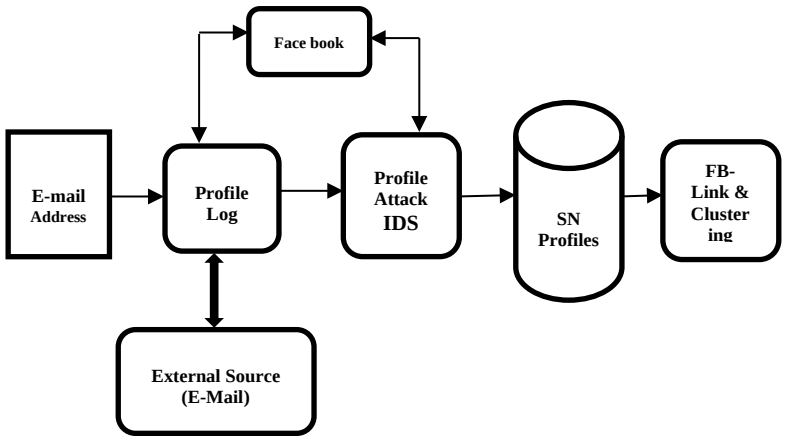

Fig. 1. Proposed overview of intrusion detection of FB-Users.

3.2. A Novel Algorithm for Intrusion Detection in OSN

The suggested algorithm included multiple actions: First, as described in *Algorithms I and II*, we had to crawl targeted organizations and collect public details regarding workers who had generated user-profiles and claimed that in the past, they had been employed or worked in the targeted organizations. The crawling process focused on OSN's Facebook and a passive socialbot account that we developed, P. In the actions, the crawler was identical to the one added. As an entry, the crawler provided many user IDs who were workers of the targeted organization. It crawled their friend's list and was able to collect users in the targeted company who were employees.

3.2.1. Algorithm I: SNA based FBG-U Intrusion Detection (ID)

Input: FB-U ID, Inactive SNA, Dynamic SNA, FBG

Output: FBG–FB Profile and Links

Begin

FBG Public Chart = FBG and Malicious User

Create I- SNA and Profile

n=0

While (I-SNA<=100 (Maximum Users))

Send FB-F request to I- SNA users

End While

While (I-SNA<=20 (Threshold Value of Users Groups)
Send FB-F request to FBG of I-SNA users
End While
While (FBG of I-SNA users <= Maximum of FBG)
Send FB-F request to FBG of I-SNA users
End While
Return FB logs
End

3.2.3. Algorithm II: SNA specific FB-U Intrusion Detection (ID)

Input: FB-U ID, Inactive/Dynamic SNA, FBG, FBG-U, FBG Public Chart
Output: FBG–FB Profile and Links
Begin
FBG Public Chart = FBG Malicious Users
Create I-SNA and Profile
N=0
While (N<100 (Maximum Users)) **Do**
FBG = Randomize FBG
N=N+1
End While
While (N<25 (Threshold Value of Users Groups) **Do**
Send FB-F Request to Randomize FBG
End While
For
FBG-F= FBG
End For
For (F=FBG-F)
Send FB-F request to lower order
End For
For (FB-U=FBG-U)
Send FB-F request to FBG-U
End For
End

3.3. Finding the Success of Particular Users in FBGs

Step 1: In Algorithm 1, focused on malicious associations and accumulated public data about representatives who built up FB-U accounts and expressed that they were functioning and focused on associations before. The malicious procedure depended on the FB and a detached SNA account, X that made. The malicious user got, as info, a list of FB-U IDs who were FB-U in the focused association. It

malicious their FB-Fs list and had the option to accumulate users who were representatives in the focused association.

Step 2: It preceding the invasion of a focused association, planned a FB-U profile for SNA. It was significant that it appeared to be a solid profile of a genuine user. (E.g., photographs, posts).

Step 3: Before the finish of the malicious procedure, increased adequate data about FB-U who were working or had worked in the focused-on associations and their associations. As it were, assembled insight while concentrate on associations' representatives, which used to arbitrarily choose ten users to fill and focused towards the arriving at the process.

Step 4: For each selected user, it distinguished their FB-Fs inside an association, and our SNA sent FB-F requests towards them.

Step 5: After the fulfillment of the way toward sending FB-F requests to focused the users' shared FB-Fs, sent FB-F requests to the ten focused users. A short time later, refer to the number of them who acknowledged our SNA's FB-F requests.

4. Performance Evaluation of *m*-DC

To evaluate the presentation of the proposed strategy, we have utilized three techniques: precision, review, and F1 score. The expression *"accuracy"* speaks to the precision rate of clustered friends who are clustered into the right gatherings, whereas the expression *"review"* states to the exactness rate of all friends clustered into the proper groups. The F1 score is utilized to estimate the blend of exactness and review for keeping away from predispositions in either analysis or accuracy. To start with, we utilized the ideas of accuracy and study to analyse the subjects' clustering utilizing SCAN and *m*-DC utilizing Eqs. (1) And (2), here FCS speaks to the number of friends characterized by subject, FCA speaks to the number of friends ordered by algorithm, and $F_{CS} \cap F_{CA}$ speaks to the number of friends in a similar gathering in FCS and FCA. At that point, we use Eq. (3) to process the F1 scores (Fig. 2).

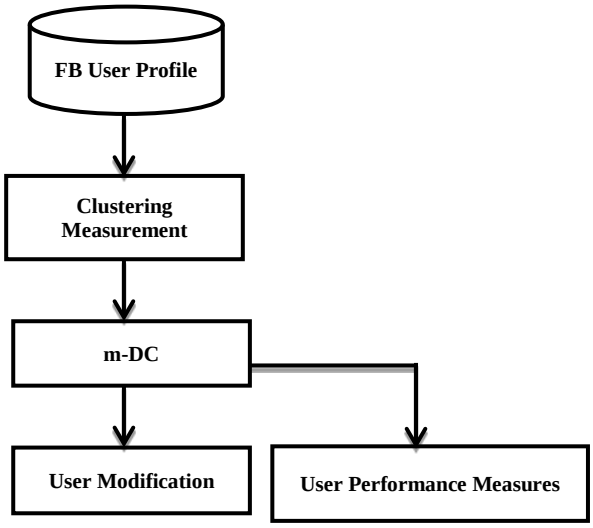

Fig. 2. The proposed *m*-DC flow of FB-U classification.

$$\Pr ecision = \frac{F_{CS} \cap F_{CA}}{F_{CA}} \tag{1}$$

$$\mathrm{Re}call = \frac{F_{CS} \cap F_{CA}}{F_{CS}} \tag{2}$$

$$F_1 = \frac{2X \Pr ecisionX \mathrm{Re}call}{\Pr ecision + \mathrm{Re}call} \tag{3}$$

5. Result and Discussions

Presently, FB is the most broadly utilized long-range social networking service. More than one billion individuals use it consistently; in this manner, we picked FB as our test information source. FB launches graph API. So, we utilized the FB Graph API to gather individual data from FB-users' assent. We recovered distinctive data dependent on a lot of estimations, which appeared in Table 2. As appeared in Table 2, there was an aggregate of 10 subjects utilized in this trial. The absolute number of their FB friends went from 350 to 1000. Overall, the issues in this investigation have 350 FB-friends; hence, most are hesitant to physically cluster their friends, then consider errand of clustering troublesome once we demand them to do the card-sorting. Figures 3, 4, and 5 show Precision; Recall and F1 score estimations of *m*-DC and SCAN various techniques.

Table 2. Resultant dimensions of objects retrieved by the Facebook graph.

Measurement	Features
Social Groups	Familiar friends and Object ID in FB-UG
Counties	Location of FB User
Societies	Workplace and Edification
Connection Strength	Photos, Name, Location

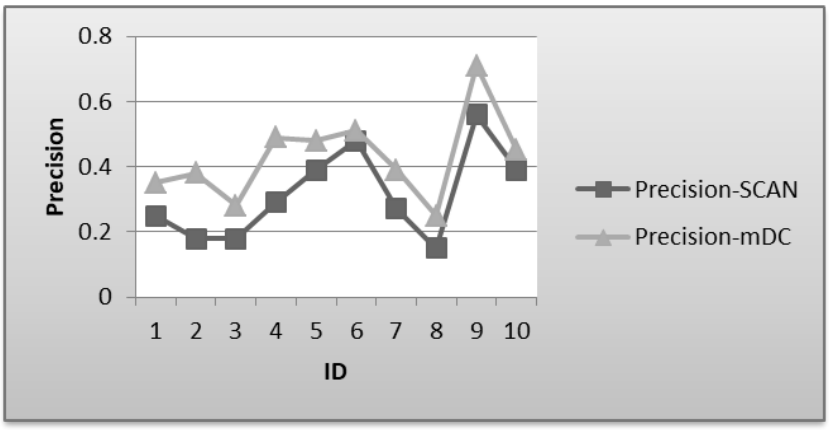

Fig. 3. Performance analysis of the Precision of the *m*-DC vs. SCAN.

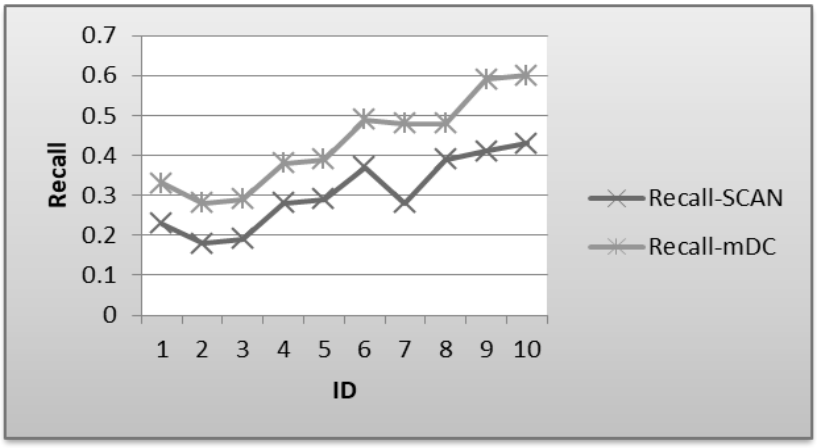

Fig. 4. Performance analysis of Recalls of the *m*-DC vs. SCAN.

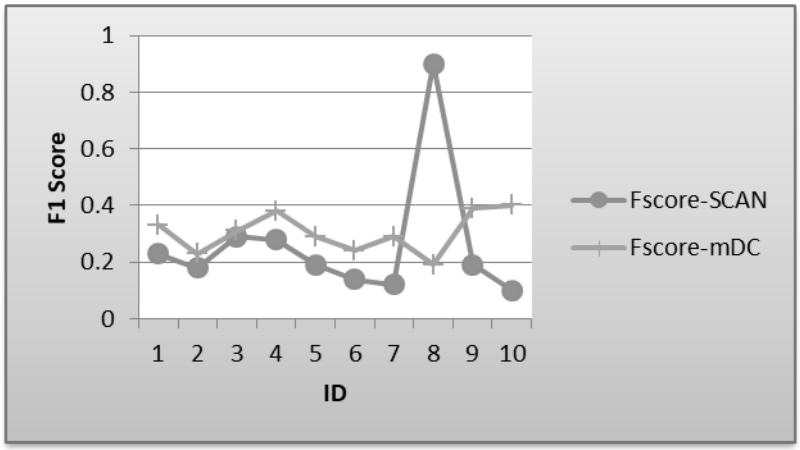

Fig. 5. Performance analysis of F1 Scores of *m*-DC vs. SCAN.

As presented in Table 3, SCAN and *m*-DC approaches associated by computing the typical Precision, Recall, *F*1 score, and Similarity. The enhanced percentages between *m*-DC and SCAN are 45.64% in the precision of 51.15%, in the recall of 45.8 %, and 59.19 % in the *F*1 score.

Table 3. Comparison of Precision, Recall, and F1 Scores of the *m*-DCV vs. SCAN.

Methods	Precision	Recall	F1-Score
SCAN	19.19%	25.98%	21.19%
Proposed m-DC	45.64%	51.15%	59.19%

5.1. The extraction of information of data of an FBG

Two analyses directed in this test. One test tried Algorithm I, while the subsequent test tried Algorithm II. The accompanying outcomes introduced in the accompanying two areas. Three-D-SNA on FB utilized for mining data from three

unique associations. To begin with, the SNA named SNA_1, SNA_2, SNA_3, SNA_4, and SNA_5 for coming to the FBG_1, FBG_2, FBG_3, FBG_4, FBG_5 association. Additionally, we worked as a detached SNA account is as I-SNA. I-SNA was an open FB-U account without companions. And utilized I-SNA just for malicious as a stay point. I-SNA had no FB-Fs, so malicious with I-SNA had the option to give openly accessible information. After completed the malicious procedure utilizing I-SNA, we used the SNA_1, SNA_2, and SNA_3 dynamic SNA for coming to the FBG_1, FBG_2, and FBG_3 associations, separately, utilizing the systems portrayed in Algorithm I. The interruption procedure by our SNA was finished expertly when vindictive again on the focused-on associations, however this time with SNA_1, SNA_2, and SNA_3 rather than I-SNA.

As referred in Table 3, the SNA_1 to SNA_5. SNA increased 182 shared FB-Fs of the focused-on users in the focused-on associations, so they had the option to reveal progressively concealed associations and users in the focused-on associations. In the first process, SNA_1 to SNA_2 was able to gain 71 FB-Us who declared in their profile that they were currently FBG_1 users /past FBG_1 users. Overall, SNA_1: SNA_2 sent 126 FB-F requests to 126 different FBG_1: FBG_2 users, and the rate of acceptance was 45.12%. SNA_2 increased 60 FBG_1: FBG_2 FB-U, while SNA_2 sent 156 FB-F requests to FBG_3: FBG_4 representatives, which demonstrates abound of acknowledgment of 59.10%. Rather than SNA_3 and SNA_4, SNA_5 accomplished 45 FBG_5 representatives that turned into its FB-Fs. SNA_5 sent 56 FB-F requests to 59 distinctive FBG_3 FB-U and performed a pace of acknowledgment of 54.16%.

Next, the malicious with SNA_1 on the FBG_1 association to reveal new representatives and new associations that didn't discover when vindictive with I-SNA. At long last, distinguished 2198 casual associations of 465 FB-Us who, as per their FB-Ps, worked at the FBG_1 association. It implies that SNA_1 found 6.91%more representatives and 19.20% extra hidden associations. By malicious with SNA_2, had the option to distinguish 2781 personal associations of the 590 FBG_2 representatives. This work demonstrates that SNA_2 the possibility to reveal 12.10% more FB-U and 9.19% progressively concealed connections. Additionally, by malicious with SNA_3, recognized 4918 personal associations of the 780 FBG_3 FB-U. It means that SNA_3 detected 10.91% more users, and 23.71% more hidden links. Additionally, by malicious with SNA_4, recognized 8512 personal associations of the 870 FBG_3 FB-U. It means that SNA_3 detected 15.87% more users, and 28.91% more hidden links. Additionally, by malicious with SNA_5, recognized 13918 unofficial associations of the 980 FBG_3 FB-U. It means that SNA3 detected 14.19% more users, and 10.92% more hidden links.

Also, the *m*-DC calculation utilization, SNA_1, was ready to find 43 groups with an average size of 8.12 FB-U and maximal size of 92 FB-U. SNA_2 had the option to find 48 groups with a standard size of 21.3 FB-U and maximal size of 198 FB-U. SNA_3 had the option to find 97 groups with an average size of 9.19 FB-U and maximal size of 289 FB-U. SNA_4 had the option to find 180 groups with a standard size of 18.10 FB-U and maximal size of 410 FB-U. SNA_5 had the option to find 210 groups with a standard size of 29.12 FB-U and a maximal size of 559 FB-U. The following Fig. 6 accomplish user acceptance.

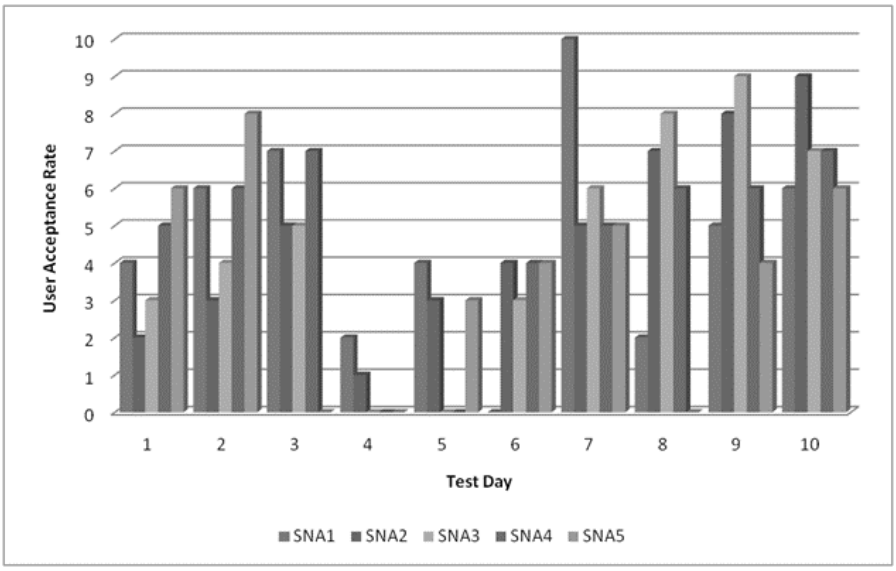

Fig. 6. User acceptance rate in difference social groups.

5.2. The success of exact FB-Users

In this area, resent the after-effects of Algorithm II dependent on the usage of our proposed calculations. The SNs order the accompanying outcomes utilized by the active SNA. It will be ideal if you see that acknowledged users characterized as frequent companions of focused users who accepted an SNA's FB-F request while dismissed users characterized as shared FB-Fs of the focused-on users who dismissed an SNA 's FB-F requests.

We have utilized four active SNA on FB to invade focused on users in four distinct associations. Our SNA sent FB-F requests to focused users' common FB-Fs to pick up; however, many shared FB-Fs as could be expected under the circumstances to encourage acknowledgment by the focused-on users. It presents the outcomes obtained from the SNA_4, SNA_5, and SNA_6, SNA_7 that endeavoured to invade explicit representatives in the focused-on associations, FBG_6, FBG_7, and FBG_8 separately.

In the first place, randomly picked ten users who expressed on their FB-Ps that they work or had worked in FBG_6 association. At that point, we gathered the FB-Fs of the ten, which is focused on users who worked in the FBG_6 association and sent them FB-F requests. Next, SNA_6 sent FB-F requests to the ten focused on users FB-U_1 to FB-U_{10}. Altogether, SNA_6 sent 127 FB-F requests and was effective in interfacing with 48 unique users. While the focus on users, SNA_6 had the option to progress toward becoming FB-Fs with five, which is focused on users FB-U_1, FB-U_5, FB-U_6, FB-U_8, and FB-U_{10}, making towards half the success rate. Besides, SNA_6 had the option to progress toward becoming FB-Fs, with 37.10% of all users who got its FB-F requests.

SNA_7 sent 123 FB-F requests to 145 users in the FBG_7 association, including the ten focused on users. Among them, 38 users acknowledged, and 76 users dismissed SNA_7's requests. Concerning focused on users, SNA_7 had the option to

progress toward becoming FB-Fs with seven focused on FB-Users of FB-U_1, FB-U_2, FB-U_3, FB-U_5, FB-U_7, FB-U_9, and FB-U_{10}, with a triumph pace of 69.19%. Also, SNA_7 had the option to turn into a FB-F of 43.13% of the considerable number of users who got FB-F requests. By tolerating the SNA's FB-F requests, we had the option to uncover more data, for example, hidden users, associations among users, and gatherings, in correlation with the open data accumulated with the detached I-SNA.

As to concealed FB-U, SNA_1 found 465 users contrasted and I-SNA, which found 450 users; SNA_2 found 590 users distinguished and I-SNA, which found 550 users, and SNA_3 found 780 FB-U compared and I-SNA which found 650 FB-U. Concerning associations, SNA_1 discovered 870 links contrasted and I-SNA, which created 750 connections, SNA_2 discovered 980 links contrasted and I-SNA, which discovered 850 links, and SNA_3 created 13918 links contrasted and I-SNA which found 10235 links.

In the first place, to appear to be a genuine user, SNA_8 sent 78 FB-F requests to irregular users with more than a thousand FB-Fs. Among them, 43 users acknowledged its FB-F requests, and 29 users asked SNA_8 to be their FB-F.

6. Conclusion and Future work

This paper discusses numerous privacy and protection concerns relating to OSN customers, including data from OSN service providers, as well as data collections by third parties. The main aim was to teach OSN consumers about how to defend themselves from such problems while they are using social media. The primary contribution is to identify four dimensions used in SN cluster mates. Friends that have defined positions are only for manual clustering, which reduces the algorithm's risk of misjudgement. SCAN and *m*-DC methods are related by calculating average precision, recall, F1 score, and resemblance. The improved ratios among m-DC and SCAN are 45.64% in the precision of 51.15%, the recall of 45.8%, and 59.19% of the F1 score. In this work, it showed attacks by SNA. This examination has a few future research efforts. One conceivable effort is progressively exhaustive testing to finish discovered for the social contrasts among users and FBG association of SNA when characterizing their personality.

Additionally, the heading is to utilize the calculation for arriving at explicit users to explore whether our outcomes are predictable after some time and to survey whether any changes are there in users' mindfulness and reactions to security problems. And also, it utilizes the calculation on different SNs and lookout the contrasts between them. Besides, it could separate among female and male profiles when arriving at SN clients to research any gender contrasts that exist.

Nomenclatures

F_{CS}	Precision
F_{CA}	Recall
F1	Score

Greek Symbols

N	No. of Facebook Users
ID	Intrusion Detection

Abbreviations

D-SNA	Dynamic SNA
FB	Facebook
FBG	Facebook Group
FB-U	FB User
GRS	Group Recommendation System
ID	Intrusion Detection
I-SNA	Inactive SNA
m-DC	multi-Dimensional Clustering
OSN	Online Social Network
SN	Social Network
SNA	Social Networking Agent

References

1. Lee, K.; Caverlee, J.; and Webb, S. (2010). Uncovering social spammers: social honeypots+ machine learning, in *Proceeding of 33rd international ACM SIGIR Conference. Research and. Development in. Information Retrieval*, 435-442.
2. Stringhini, G.; Kruegel, C.; and Vigna, G. (2010). Detecting spammers on social networks. *Proceeding 26th Annual Computer Security Application. Conference*, Texas, USA, 1-9.
3. Wang, A. (2010). Don't follow me: Spam detection in twitter. (2010). *International Conference on Security and Cryptography (SECRYPT)*, Athens, Greece, 1-10.
4. Danezis, G; and Mittal, P. (2009). Sybilinfer: Detecting Sybil nodes using social networks. *Proceeding of Network and Distributed System Security Symposium*, California, USA.
5. Fire, M.; Kagan, D.; Elyashar, A.; and Elovici, Y. (2012). Social privacy protector protecting users' privacy in social networks. *Proceeding 2nd International Conference on Social Eco-Informatics (SOTICS)*, Venice, Italy, 46-50.
6. Fire, M.; Kagan, D.L.; Elyashar, A; and Elovici, Y. (2013). Friend or foe? Fake profile identification in online social networks. *Social Network Analysis and Mining*, 4,194(2014).
7. Fire, M; Katz, G.; and Elovici, Y. (2012). Strangers intrusion detection-detecting spammers and fake profiles in social networks based on topology anomalies. *ASE Human Journal*, 1(1), 26-39.
8. Tran, D.N.; Min, B.; Li, J.; and Subramanian, L. (2009). Sybil-resilient online content voting. *Proceeding of the 6TH UNISEX Symposium on Networked System Design and Implementation*, 9, 15-28.
9. Wang, G.; Konolige, T.; Wilson, C.; Wang, X.; Zheng, H.; and Zhao, B.Y. (2013). You are how you click: Clickstream analysis for sybil detection. *Proceeding 22nd USENIX Conference on Security*, 241-256.
10. Wang, G.; Mohanlal, M.; Wilson, C.; Wang, X.; Metzger, M.J.; Zheng, H.; and Zhao, B.Y. (2012). Social Turing tests: Crowdsourcing Sybil detection. *arXiv preprint arXiv:1205.3856*.

11. Motoyama, M; McCoy, D.; Levchenko, K.; Voelker, G.M.; and Savage, S. (2010). Dirty jobs: The Role of freelance labor web service abuse. *Proceedings of the USENIX Security Symposium*, 14.
12. Nazir, A; Raza, S.; Chuah, S.N.; and Schipper, B. (2010). Ghostbusting Facebook: Detecting and characterizing phantom profiles in online social gaming applications. *Proceeding of 3rd Conference on Online Social Networks*, 1.
13. Eslami, M.; Aleyasen, A.; Moghaddam, R.Z.; and Karahalios, K. (2014). Friend grouping algorithms for online social networks: preference, bias, and implications. In: Aiello LM, McFarland D (eds). *Social informatics, Springer, Berlin*, 34-49.
14. Gao, B.; Berendt, B.; Clarke, D.; De Wolf, R.; Peetz, T.; Pierson, J.; and Sayaf, R. (2012). Interactive grouping of friends in OSN: towards online context management. In: Paper presented at the data mining workshops (ICDMW), *IEEE 12thInternational Conference, Brussels*, 555-562.
15. Hossmann, T.; Nomikos, G.; Spyropoulos, T.; and Legendre, F. (2012). Collection and analysis of multi-dimensional network data for opportunistic networking research. *Computer Communication*, 35(13), 1613-1625
16. Kelley, P.G.; Brewer, R.; Mayer, Y.; Cranor, L.F.; and Sadeh, N. (2011). An investigation into Facebook friend grouping. *In: Human-computer interaction-INTERACT 2011, Springer, Berlin*, 216-233.
17. Speicher, T; Ali, M.; Venkatadri, G.; Ribeiro, F.N.; Ar-vanitakis, G.; Benevenuto, F.L.; Gummadi, K.P.; Loiseau, P.; and Mislove, A. (2018). On the potential for discrimination in online targeted advertising. *Proceeding of Machine Learning Research*, 81(1-15).
18. Murtagh, F. (1983). A survey of recent advances in hierarchical clustering algorithms. *The Computer Journal*, 26(4), 354-359.
19. PhanBinh, E.; and FjeldstadØystein, D. (2013). Considering clustering measures: third ties, means, and triplets. *Social Networks*, 35(3), 300-308.
20. Venkatadri, G.; Liu, Y.; Andreou. A.; Goga, O.; Loiseau, P.; Mislove, A.; and Gummadi, K.P. (2018). Privacy risks with facebook's pii-based targeting: auditing a data broker's advertising interface. *2018 IEEE Symposium on Security and Privacy*, San Francisco, USA, 89-107.
21. Baykara, M.; and Gurel, Z.Z. (2018). Detection of phishing attacks. *2018 6th International Symposium on Digital Forensic and Security*, Antalya, Turkey, 1-5.
22. Amir Roknifard. (2014) Admin-Hacking Social Media. Threats & Vulnerabilities- ' Threats & Anti-Threats Strategies for Social Networking Websites'.‖ *Hakin9*.
23. Hope, Bradley,; Warren, P.; Strobeland Dustin Volz. (2019)High-Level Cyber Intrusions Hit Bahrain Amid Tensions With Iran. *The Wall Street Journal*. Dow Jones & Company
24. Liu, Y.; Gummadi, K.P.; Krishnamurthy, B.; and Mislove, A. (2011) Analyzing Facebook privacy settings: User expectations vs. reality. *Proceedings of the ACM SIGCOMM conference on Internet Measurement Conference*, 61-70.

25. Stutzman, F; and Kramer-Duffield, J. (2018). Friends only: examining a privacy-enhancing behavior in Facebook. *Proceedings of the 28th International Conference on Human Factors in Computing Systems*, Georgia, USA, 1553-1562.
26. Wang, Y.; Norcie, G.; Komanduri, S.; Acquisti, A.; Leon, P.G.; and Lorrie Cranor, L.F. (2011). I regretted the minute I pressed share: A qualitative study of regrets on Facebook. *Proceedings of the Seventh Symposium on Usable Privacy and Security*, 10, 1-16.
27. Johnson, M.; Egelman, S.; and Bellovin, S.M. (2012). Facebook and privacy: It's complicated. *Proceedings of the Eighth Symposium on Usable Privacy and Security*, 9, 1-15.
28. Sleeper, M.; Balebako, R.; Das, S.; McConahy, A.L.; Wiese, J.; and Lorrie Cranor, L.F. (2103). The post that wasn't: exploring self-censorship on Facebook. *Proceedings of the 2013 conference on Computer Supported Cooperative Work*, 793-802.
29. Braunstein, A.; Granka, L.; and Staddon, J. (2011) Indirect content privacy surveys: measuring privacy without asking about it. *Proceedings of the Seventh Symposium on Usable Privacy and Security*, 15.