Trust Aware System for Social Networks: A Comprehensive Survey

Manasa S. M.
Department of Computer Science and Engineering
University Visvesvaraya College of Engineering,
Bangalore University
Bangalore 560001

Manjula S. H.
Department of Computer Science and Engineering
University Visvesvaraya College of Engineering,
Bangalore University
Bangalore 560001

Venugopal K. R.
Department of Computer Science and Engineering
University Visvesvaraya College of Engineering,
Bangalore University
Bangalore 560001

ABSTRACT
Social networks are the platform for the users to get connected with other social network users based on their interest and life styles. Existing social networks have millions of users and the data generated by them are huge and it is difficult to differentiate the real users and the fake users. Hence a trust worthy system is recommended for differentiating the real and fake users. Social networking enables users to send friend requests, upload photos and tag their friends and even suggest them the web links based on the interest of the users. The friends recommended, the photos tagged and web links suggested may be a malware or an untrusted activity. Users on social networks are authorised by providing the personal data. This personal raw data is available to all other users online and there is no protection or methods to secure this data from unknown users. Hence to provide a trustworthy system and to enable real users activities a review on different methods to achieve trustworthy social networking systems are examined in this paper.

Keywords
Social Networking, Sybil Attack, Geo-tag,

1. INTRODUCTION
A social networking site is a social structure consisting of performing artists and an arrangement of the dyadic ties between these onscreen characters. The interpersonal organization point of view reviews the arrangement of techniques that are breaking down the entire structure users and in addition an assortment of hypotheses clarifies this statement. Analysis of social networks is difficult as it is a study of interpersonal relationships. Jacob Moreno built the main sociograms in 1930s to allow interpersonal communications. These methodologies were scientifically formalized in 1950's and also the speculations and methods for casual organizations need to be pervasive within the social and activity sciences by the Eighties. Informal community analysis is currently one of the significant ideal models in contemporary humanism, and is additionally utilized in many other social and formal sciences.

Typically users on social networks make friends with other who work with them or who live close to them as neighbours or colleagues. Friends made through this type of technique are called geographic location based friends. Now users on social networks can become friends based on there life style activities, interest, hobbies, profession, location and based on mutual friends. Friends on social networks are suggested based on the social graphs, mutual friends and similarity of interest. And these methods of friend suggestions on social networks are not appropriate methods because the users on social networks can be a real user or a fake user.

Online social networks (OSNs) are the platform for intercommunication and interaction. User interacts with the internet are made easily available with the help of OSNs. Facebook, Twitter, Lnkedin, google+ are major social networking platforms that seeks personalizing the web experience by providing users to get the information pertaining the profile visitors and known friends on their account through many platforms such as OpenGraph. Social behaviour of a user and the design of application in social platform can be provided by deeply understanding the user interactions with the social networks.

Challenges with the existing social networking services is to determine the suggested friends, web links, location shared and data collected are trustworthy or untrustworthy service. Most of the social networking sites rely on the traditional methods of suggesting this services based on mutual friend relationship. For example, Facebook and Twitter rely on link analysis that shares a common link to find the mutual friends and suggest common friends as an optimal friends. This method is not appropriate to suggest trustworthy friends.

The main social networking services are: 1) Trustworthy Large Scale Social Networks Evaluation 2) Data Privacy Preserving 3) Friend Recommendation 4) Vote Trust In social Networking 5) Trust Based web recommendations

A. Motivation:
The number of users on social networks is increasing rapidly in recent years. Social networking users provide their personal user information online that is displayed on user's profile. Data provided by online social networking users are available to other online users. Users on social networking site may be a known user or an unknown user. Strangers on social networking sites can use the available user data for any kind of cybercrimes or for anti-social activities. This may lead to cyber bullying by which the user has to face emotional trauma. Social networking sites are occasionally used for social emotional harassments by posting their private photos or by posting statements that emotionally affect the user. It is very important to provide protection for the online social networking users and for the personal data provided by them with the help of trustworthy mechanisms.

B. Organisation
Section 2 describes about Trust Worthy Large Scale Social Networks Evaluation. Section 3 describes Data privacy in Social Networks.Section 4 evaluates Trustworthy Web Recommendations on Social Networks.Section 5 describes

Friend Recommendations and its trustworthy computation. Section 6 describes about the authentication mechanisms used to access social networks and its advantages. Section 7 describes about Trust based Web Recommendations and link analysis.

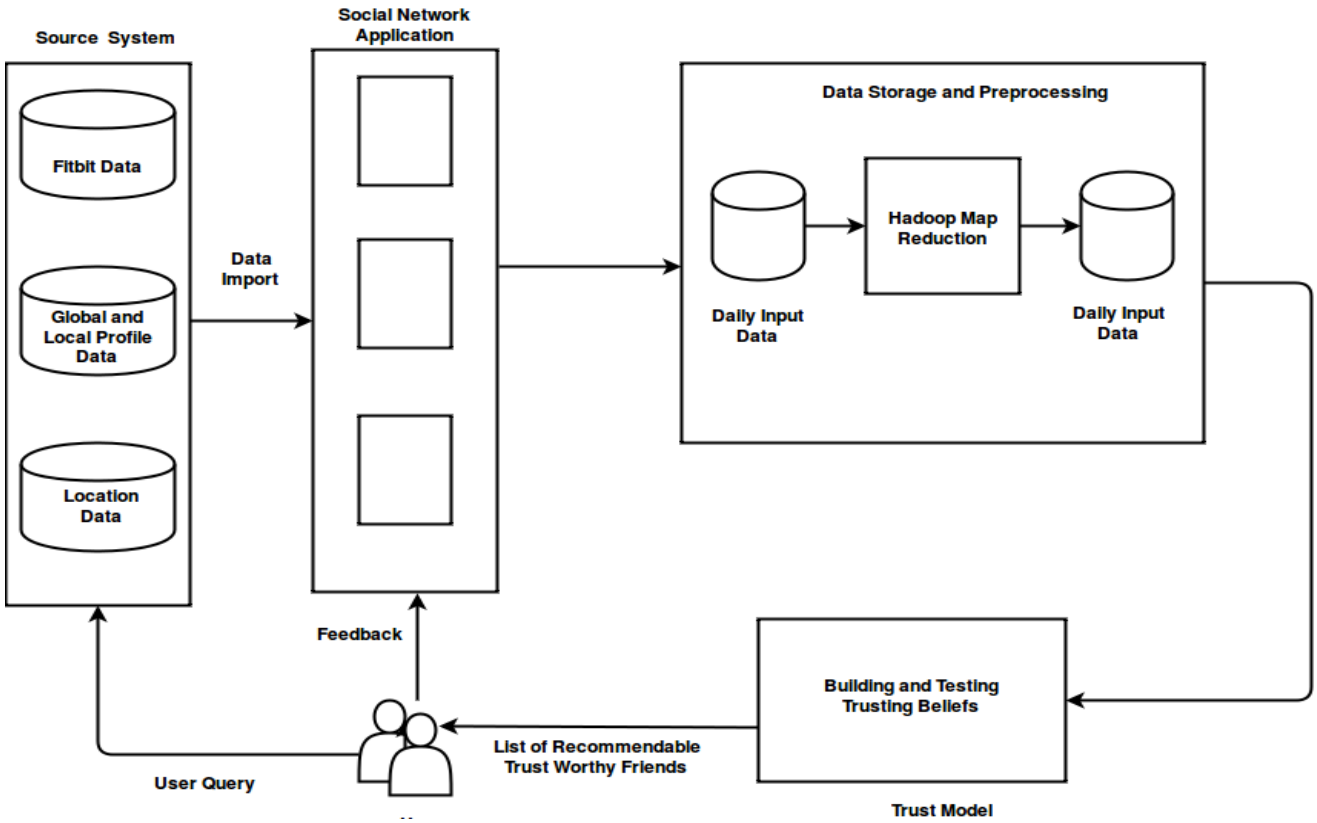

Fig. 1. System Architecture of Social Networks

2. TRUSTWORTHY LARGE SCALE SOCIAL NETWORKS EVALUATION

Iglesia et al., [1] proposed computational dynamic trust model for authorising the user, this model distinguishes between integrity and competence trust of the user. Integrity and competence trust are related to different context and functions. Cross context information is used to build, enable and test the trust models. This allows automatic trust management that computes the trusting behaviour of the user. Trust environments show that the integrity trust model predicts accurate user behaviour than other trust models.

Liang et al., [2] describe a quantitative measure of group compactness that considers both similarity and trustworthiness among the users present in the group. User to Group (U2G) matching algorithm is used to optimize the compactness with agent networks. It allows the software agents associated with online social networks to dynamically determine, manage and detect most suitable groups to join for the user. It improves the internal compactness of the groups on social networks. It does not improve intra group compactness.

Li et al., [3] demonstrate a Preference and Honesty Aware Trust Model (PHAT) for evaluating the user preferences and false ratings while choosing a service from the pool of service providers. The model automatically mine user preferences from their requirements and compute the weights QoS attributes when integrating trust into multi-dimensional QoS attributes. Process of trust evaluation determines trust of each Qos attribute and helps the users to access the trust of prioritised services based on interactions with services. Process of global trustworthiness evaluation evaluates the honesty of customers requesting for the service. The hybrid honesty assessment model differentiates between honesty user and cheating user based on connections and consistency present between the two users.

PHAT model depends entirely on the interactions and hence computes the trust quotient of a newly published web services are not recommended Eirinaki et al., [4] [5] introduced a model for trust management in online social networks with respect to its reputation mechanism that considers explicit and implicit connections then provides personalised user recommendations to the network members. It measures the trust and its connections that are determined in social networks and indexes personalised ratings of the trust value of the user. Personalised ratings of the social network members generate personalised trustworthy and non-trustworthy user, which helps in forming trust and untrust connections. Explicit user-to-item connections are not computed.

Ivanov et al., [6] design a method of automatic geotag propagation in online social network images based on its content and context. Well known landmarks and geotags associated with them can be incorrect or a spit tag that damages the integrity and reliability of the propagation system. A Coincident-Based model is used to tackle the spamming activities in social tagging system and a higher rank of bookmark shows geotag tagged correctly by the trusted users. An Authority model determines the goodness of the tag propagated with respect to the content. This measures the trust and reliability of the users in geotagging mechanism. Propagation of tags based on trust modelling depends on user behaviour and tags can propagate with the same accuracy.

Multimedia content tagging and tag propagation is not considered.

Caton et al., [7] recommend a social compute cloud in which infrastructure of cloud is provided by friend vector. In social cloud resources and services sharing occurs through the relationship developed between the network users. Matching algorithm invokes the matching services and matches the consumer and provider for sharing resources. Resource allocation is quick compared to allocation algorithms. User preferences cannot be detected automatically.

Hao et al., [8] propose a MobiFuzzy Trust for hypothesizing the trust connections between mobile users which are not connected by graphs on mobile social networks. Fuzzy linguistic approach shows the trust metrics present between mobile users. It achieves high value of trust transitivity for the higher weights of basic trust users. These techniques enhance the human's understanding of trust and describe values to express trust between users. Determining the mobifuzzy trust values dynamically in mobile social networks is a challenge because the trust values between the new users keep changing.

Liu et al., [9] design a novel social network structure with trust, social relationship and recommended roles to express the quality of trust. Multiple Foreseen Path-Based Heuristic algorithm for Optimal Social Trust Path Selection (MFPB-HOSTP) identifies the social trust path. It identifies the trust path with better quality than Heuristic algorithm for Optimal Social Trust Path Selection (HOSTP). Trust oriented services based on social networks database has to be maintained in order to identify the most trustworthy user and service provider.

Gong et al., [10] [11] explain the novel framework of attacks in social authentications. Model of forest fire attacks iteratively harm users by compromising on trustee based social authentications. It decreases the number of compromised users with average recovery probability of attacks. Defence strategies ensures that user chooses to be trustee minimum number of users and minimises the number of untrusted users.

Gjoka et al., [12] demonstrate a semantic web based system for friend recommendation in social networks. Friend recommendations are based on life style activities on users instead of social graphs. Computing user impact ranking and friend recommendation algorithms return friendbook users a list of people with similar life style. This recommendations accurately show the preferences of choosable friends. It fails in recommending trustworthy friends.

Laranjeiro et al., [13] discuss a technique to automatically fix the robustness issues in web services. A method to improve the robustness includes a procedure of gathering information, generating a workload, executing a set robustness tests and fixing disclosed robustness problems. The implemented approach results in improving the robustness of web service code. This can be used in web service developments and to improve the robustness of already deployed web services. It does not address workloads environment.

Jia et al., [14] analyse the throughput and delay in wireless cognitive social networks, integrating a social relation into cognitive radio networks. Source node selects a destination node based on rank based network model. The primary and secondary networks achieves the common scaling law as being stand alone networks

Chuet al.,[15]describe a spatial social union, a method to measure user similarity and integrate connections between user, item and locations. Modified Fast-Floyd algorithm is used to compute the multi-dimensional matrix and vector. It takes less time in travelling from user's location to item's location consuming less energy. Trust and distrust recommendations based on user perspective has to addressed.

Deng et al., [16] [17] design a trust based methodology to recommend in social networks. TrustCliques algorithms implemented to achieve trustworthy recommendation in social networks. Deep learning matrix factorisation approach is compared with different state of art methods to get best performance when processed with different data sets. It is used to detect trust aware groups on social networks. Time sensitivity factor has to be considered while making trustworthy recommendations in social networks.

Wang et al., [18] define an expression to evaluate value-added services and its composition. Graphical Search-based Web Service Composition(WSC) algorithm is used to define the feasible composite solutions that can service the users query. Same-Intension and Different-Extension achieves the performance of the system.

Chen et al., [19] describe a novel approach to connect the isolated service islands to a global social service network and enhance the services sociability on a global scale. Social link recommendation algorithm is used to develop the quality of social relationships. It is observed that success rate decreases with increase in the number of services, the rate of success still guarantees the quality of service discovery. Limitations of this approach is that the users feedback such as is not involved to ensure the quality of social link.

3. DATA PRIVACY PRESERVING

Lianggui et al., [20] describe Pathe Integral Monte Carlo Quantum Annealing(PIMCQA) based selection algorithm for complex service oriented online social networking sites to overcome the NP- Complete problem and to improve the efficiency of searching ability of online social networking sites. It returns the high-quality search time at tolerable cost. This tool is used for solving the Optimal Social Trust Path(OSTP) in large complex online social networking sites. The quality selection of solution of OSTP selection should be improved quantitatively avail a database to keep track of participants and relationship represents of different Quality of Trust (QoT) attributes.

Jiang et al., [21] propose a trust evaluation scheme named Generalized Network Flow Trust(GFTrust) to overcome path dependencies with the advantage of network flow and model trust decay pertaining to each node. GFTrust solves path dependencies and trust decay issues, and then predicts a trust value that is closer to the truth value. And it improves the trust prediction accuracy and bears sybil tolerance. Node leakage functions are dynamic as per the node assumptions which is not a efficient way of predicting the leakage value hence the node leakage value should be fixed to achieve effective trust evaluation scheme.

Iftikhar et al., [22] [23] [24]prove user's ownership rights of data in social networking site and provides mechanism for data recovery with the help of reversible watermarking technique. In social networks, user's trust has a important role in achieving reliable recommendations; this recommendations purely depends on initialization of user and latent feature vectors.

Deng et al., [25] describe an approach for recommendations in social networks to overcome this disadvantage of dependencies. This approach utilizes deep learning for initialization and to synthesis users interest with their trusted friends interest for online recommendations. A matrix factorisation method called Deep Learning Based matrix Factorisation(DLMF) is used to setup the initial values of the parameters and a Social Trust Ensemble model is used to consider only the trusted friend's recommendations. The DLMF achieves better recommendation accuracy than any other state of art methods. It should have a time sensitivity parameter to achieve trust aware recommendations as recommendations depend on the friends rating which change dynamically.

Mobile Social Networks (MSN) are important platforms to disseminate information. Spreading rumours in MSN's is the current massive threat. To address this issue Zaobo et al., [26][27][28] [29] have introduced a heterogeneous network based epidemic model to define rumour spreading in MSN's. This model incorporates cost efficient strategies to control rumour spreading.

Nergiz et al., [30] [31] [32] design an approach, for secure multiparty protocols which gains distributed k-anonymity that allows users to achieve utility advantage from the protocol is within an acceptable range before initiating the protocol. Secure Look Ahead Protocol for Optimal Distributed k-anonymity, Secure Look Ahead Protocol for Descendant Preserving Distributed k-Anonymization are designed to achieve distributed k-anonymity. The look a-head computations performed are highly localised and acurate.

Todays world of web services such as Gmail, Facebook and online banking dependent on user authentication, but this results in issues like the user may forget the passwords, the password might be changed by the hackers or attackers which deny the user accessing accounts. Li et al., [33] develops a secure method in which web servers provide the backup for user authentication mechanism. It helps the user to regain the access to their accounts. But, all this mechanisms are either insecure or unreliable.

4. FRIEND RECOMMENDATION

Guo et al., [34] [35] propose a trust-based privacy-preserving friend recommendation scheme for Online Social Networks(OSN), where OSN users find matched friends with the help of user attributes, and develop a secure social contact with unknown users through a trusted multi-hop chain. Trust-Based Privacy-Preserving Friend Recommendation algorithm provides user privacy and identity for social coordinates. This scheme is used to derive the objective trust level to compute the average trust level without revealing OSN user trust level.

Qiao et al., [36] propose an Encounter method of probability to calculate the similarities in user behaviours in the real world based on their check-in data. As a solution to this challenge of check-in data, a Kernel Density Estimation (KDE)-based user check-in probability estimation method is implemented. This method returns the accurate users with similar check-in details.

Doost et al., [37] describe a temporal-topic model to determine user behaviours and predict their potential friends in micro blogging. LDA model is used to find the temporal topics of each document that helps in determining the user behaviour. The implemented method gives the accurate list of recommendable friends based on their behaviour.

Existing social networking sites allow users to add other users as friends but the problem is that a large amount of raw data is generated about friends. To overcome the challenge, Das et al., [38] recommend a method using physical and social context to add new friends. First, it computes friendship scores with physical context and then it calculates friendship score with the help of social context. and then combines all the scores depending on the friendship score and recommend friends. Physical context like current location and time of the user, social context includes social networking site of the user that enhances the search methods by using top-k algorithm and expands the user search dynamically. This method after computing friendship scores sorts the friends in ascending order depending on the friendship scores.

Users online can predict the unknown ratings on social networking sites with the help of trusted friends and their recommendations. Existing system considers the current rating of the user but ratings are dynamic in nature will not give accurate opinion on rating. To address this, Jiang et al., [39] propose a multiple prediction scheme. This scheme uses fluid rating mechanism that reveals time evolving human opinions. These opinions, obtained at each stage of fluid mechanism ratings, are combined to rate accurately. This method is feasible and effective in new rating mechanisms online.

In social recommender system, it is very important to analyse the benefits of individuals in using social networking sites and maximising the efficiency of network in transmitting the information on a large scale. To analyse this, Flex et al., [40] design a stochastic recommendation model for social networks and suggest a set of parameters for computing user experience and network efficiency. Experiments result show that the users are able to identify good connections they receive and improvement is statistically significant.

Many social networking web sites recommend friends to individuals based on similarity, popularity or friends of friend that considers only a few characteristics. To investigate the social network structure Kwon et al., [41] develop an algorithm for network correlation based recommendation. Network correlation based social friend recommendation selects important features of related networks and they are maximally preserved before and after network alignments are done. The proposed algorithm recommends friends precisely on flicker network. This method is used in accurate recommendation to be made on social networking sites. Trust metrics are not evaluated with respect to provide privacy of the user data.

Network based recommendation approach deals with the problem of cold start users on social networks. Trust information of user is used in obtaining reliable recommendations online. To address this challenge Farrahi et al., [42] propose a novel trust based approach for recommendation online. This is a two phase recommendation approach that uses trust cliques algorithm to initialise and synthesise the users and their trusted friends interests for recommendations. It is observed that the recommendation process has accurate results and used in trust worthy item recommendations online. As the trust values keep changing with time, time sensitivity for trust aware recommendations are still challenging.

Profile matching is widely used in mobile social networks. Social networks recommend friends based on their personal data. However, making this data publicity on cloud is vulnerable to any kind of privacy issues. To overcome this

issue, Li et al.,[43] describe a Scalable and Privacy preserving Friend Matching protocol(SPFM). This method recommends scalable friends without revealing users personal data and prevents honest but curios mobile cloud from retrieving original data and recommend friends. Experimental analysis shows a secure and accurate friend matching and friend recommendations. This method can be used for the application which generates a large set of raw user data. Protecting private data of users online in friend recommendation systems still remains as a challenge.

Bian et al., [44] propose the idea of friendship based recommender system where computations are made based on inputs from overall user population. Prediction algorithms are used to find the bi-directional friendship online. This method is used to select strangers to avoid compromising of data from the similarity with different privacy approaches. Working on unbiased real world data sets are difficult.

Table 1. Comparative Study on Friend Recommendations

Author	Algorithms	Performance	Advantage	Disadvantage
Zhibo Wang et al., 2015 [45].	(1) Latent Dirichlet Allocation (2) Friend Recommendation.	Friendbook achieves satisfactory results on energy performance.	Due to its privacy concerns id of users are re-vealed instead of their real names.	user request is accepted only if the registered id is known.
Tang et al., 2016 [46].	(1) User matching algorithm.	Users with similar person-ality are recommended as friends.	Progressive improvement on personality matching.	No information on actual personality.
Deng et al., 2016 [47].	(1) Latent Dirichlet Allocation Al-gorithm	Number of duplications is more with increasing number of locations.	Activity bags are used and bags are flexible to find routines.	System does not provide mechanism to protect user data.
Huang et al., 2016 [48].	(1) K-anonymization algorithm (2) top-K Algorithm.	Friend sorting is done in ascending order.	Friend sorting.	Efficient friend recommendations are not possible.

5. VOTE TRUST IN SOCIAL NETWORKING

Number of users who relay on online social networks are increasing by day and hence, providing the trustworthy information to these users are necessary. Online social networking sites suggest untrustworthy online payment links. These links are treated as spam, manipulate the rating of online, or exploit the knowledge extraction from the network. To capture the diverse behaviour of fake and real OSNs profile, Cao et al., [49] developed a new tool Sybil Rank. It deals with Tuenti, the largest online in Spain, operations to detect fake accounts in a period of time.

Table 2. Comparative Study On Vote Trust In Social Networks

Author	Algorithms	Performance	Advantage	Disadvantage
Asl et al., 2015 [57].	(1) Misloves Algorithm (2) Com-munity Detection (CD) algorithm.	Sybil ranks's support multiple seeds to improve its performance.	It enables users to directly target the counter measures.	SybilRank maintains ac-curate values for each of the seed placement strate-gies.
Chen et al., 2015 [58].	(1) Shelf Community Detection Al-gorithm	Vote accuracy is high with the better performance.	Ranking Sybil Defence	It is unclear about the sybil defence on social networks consuming more resource.
Jiang et al., 2016 [59].	(1) PostSimilarity Graph Cluster-ing	Best possible threshold are determined and com-bined to work efficiently.	Wall messages differenti-ate between malware and facebook messages.	Online communication and collaboration tools are executing spams and malware.
Zheng et al., 2015 [60].	(1) Spam-to- Spam detection.	provides results five of the largest spam campaigns	Soliciting spam, spam-as-a-service	Large scale spam mainte-nance is tedious.

All the traditional networks depend on trusted identifiers certification authority. Unlike to the traditional solutions, Vishwanath et al., [50] propose schemes that do not require a central trusted identifier and relies on the trust between users. Due to Sybil defence schemes on social networks attacker will not be ale to develop a social connections to non-Sybil nodes which are then connected to the network. Community detection algorithm is implemented that attempts to find cluster nodes used for Sybil defence. Existing sybil schemes demonstrate that the various algorithms that rank the nodes based on their connectivity to trusted nodes. Nodes poses good connectivity with the trustworthy nodes, are placed on the highest rank and are assumed to be more trusted on local communities this scheme works effectively for Sybil defence.

In recent past, social networking spam has been gaining attention from the researchers, involving in the tool development to detect spam. All this methods use URL blacklist social networking spam trap to generate dataset of Twitter spam. Thomas et al., [51] characterizes the activities of the Twitter accounts controlled by spammers and their

tools and techniques are evaluated. It completely analyse five of the largest spam campaigns targeting Twitter, which reveals a diverse set of strategies for reaching audience and sustaining campaigns in Twitters hostile environment. It highlights the necessity of better spam control.

To overcome the weakness of the Sybil guard and Sybilimit, Danezis et al., [52] propose a defence mechanism for centralised Sybil Sybil Defender. Sybil identification algorithm identifies the Sybil nodes and detects its community which is surrounding the Sybil node. It has minimum number of Sybil edges in OSNs. It has advantage in effectively detecting the Sybil communities which is surrounded by Sybil nodes with different size and structures.

Single point of failure in central authority leads to denial-of-service attack, and results in bottle neck performance. Challenges in decentralized approaches are hard to prevent the Sybil attacks in decentralised authority. Yu et al., [53] present SybliGuard, a novel decentralised protocol which limits the compromise influence of Sybil and its attacks. The design is based on specific insights regarding social network, where the indexes are the nodes of the graph while the human-established trust relation are edges, which provide the malicious edges. This protocol determines the numbers of attack edges are being independent Sybil identities.

If the number of nodes in the system is Sybil nodes, then a malicious user can out vote the honest user which has overcome by the SybilGuard protocol. But the protocol suffers from two major limitations. To address this issue, Yu et al., [54] propose a new protocol which provides the same insight as Sybil Guard but offers a improved and near-optimal guarantees, here the protocol is SybilLimit as it limits the number of attacked edges to be accepted and it is near-optimal. The improvement is desired from the multiple techniques and are combined and this fast mixing property is validated and confirmed on the real-world Social networks.

Online social network has attracted many people, as it allows the user to interact with each other share information, ideas, plans, events, and their interest within their individual networks. In OSNs, evaluation of users social influence for various applications is very essential. Yanbinetal.,[55]propose a fine grained feature based social influence (FBI) evaluation model, which constructs a initial social influence and then designs a social influence adjustment model which is based on the PageRank algorithm. The FBI model performs well with less duplication, by identifying all users social influences Yang et al., [56] propose small talk which is a social lubricant that helps to connect people especially strangers, and initiates the conversation and enables them to be friends with each other in physical proximity. But due to the slow identification of the topics of common interest, small talks in the real world are superficial. The effectiveness of the small talks can be improved by the mobile phones due to their popularity. Here E-SmallTalker, is a distributed mobile communication system which allows networking in physical proximity and automatically discovers the common interest in the conversation. A Bluetooth Service Discovery Protocol (SDP) is built to exchange the topics.

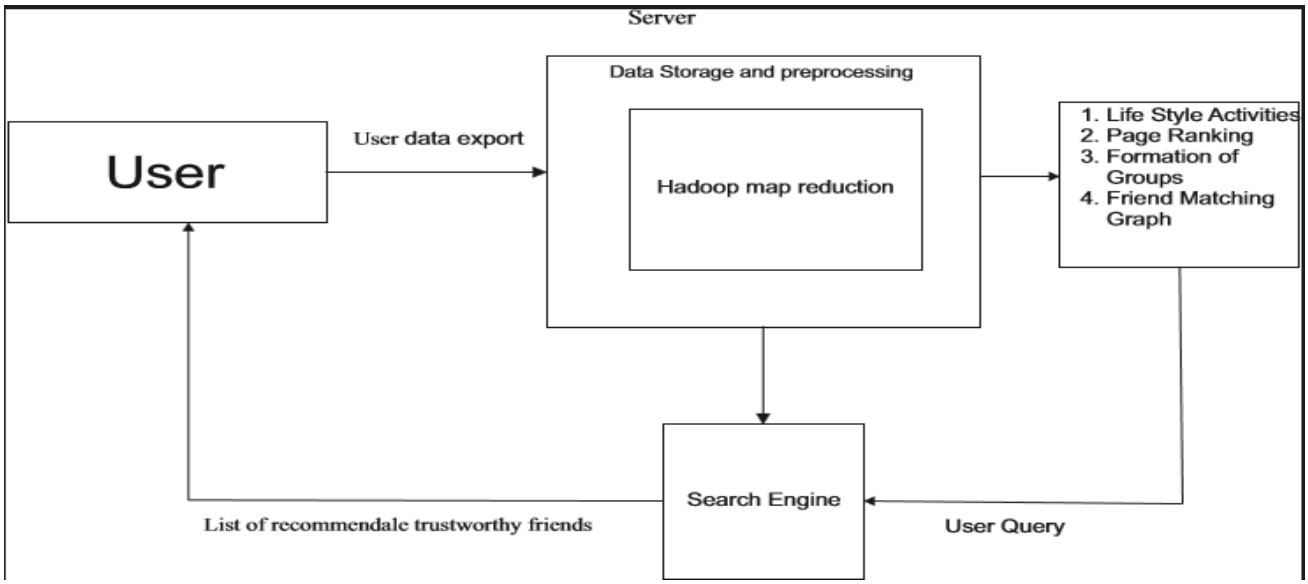

Fig. 2. System Architecture for Vote Trust in Social Networks

6. TRUST BASED WEB RECOMMENDATIONS

Trust plays a very important role in social interactions, it depend on many factors structure, context, individual actors attributes etc.. it is often measured quantitatively according to degrees of trust. Parra et al., [61] [62] propose a trust modelling for statistical relational learning (SRL). It is shown that the probabilistic soft logic (PSL) is particularly well-suited for capturing the relational aspects of trust modelling and PSL provides a framework, while various strengths of trust are easily accommodated by its soft truth. Many sociological theories of trust in PSL are modelled. The resulting PSL programs are compared with the existing trust prediction methods.

Due to the wide deployment and the advancement of the wireless communication technology, most of the car manufacturers have quipped vehicles that enable vehicles to communicate with each other. Shim et al., [63] propose a conditional privacy preserving authentication scheme called CPAS, works on pseudo identity- based signatures for secure infrastructure communication of the vehicles in the vehicular ad hoc networks. CPAS is the fastest conditional privacy preserving authentication scheme for secure V-to-I communications.

Miluzzo et al., [64] [65] [66] [67] developed an application called CeneMe. CeneMe is a personal sensing system using which user can share his data on social networking by confirming the safer presence of their friends. Sensing presence accounts activity such as sitting, walking and meeting friends also in terms of disposition like happy, sad etc. Human activity inferring algorithm is used to predict the users behaviour. Classifierss performance CeneMe services depend upon the capability of analysing the components running on the mobile devices as well as the servers. It is helpful in finding the exposure of the humans to the harmful ultra violet radiations of the sun. Using this classifier it is possible to find out whether the person is outside the building, but not inside the vehicle.

Madgule et al., [68][69][70][71] propose a Global Relationship Model (GRM) to analyse the strength of relationship between users who possess secure connection in heterogeneous SNSs. Framework designed enables user to develope their social connections over cyberspace and create more social and economic opportunities for the users and also evaluates the global relationship strengths between two users with more precision i.e., when a peer node has more friends, the desired social path can effectively be established. This system lack privacy to user's data.

Wen et al., [72] [73] [74] [75] [76][77] propose a series of empirical and theoretical analysis on the basis of mathematical model conducting two types of analysis in this work. These models work on Restraining the spread of rumors in online social networks (OSN). The degree measure has better short-term performance in the early stage. The overhead is that truth clarification method mainly has a long-term performance. Zhang et al., [78][79][34] formulate a set of novel group immunization problems for multiple natural settings to study the problem of controlling propagation at group scale unlike individual scale. Hence this approach addresses the problems of controlling epidemics by means of interventions that can be implemented at a group level. SDP and Group greedy walk algorithm work for edge deletion. Developing provable approximation algorithms for node deletion by leveraging SDP and Group greedy walk is needed.

7. CONCLUSIONS

A comprehensive review on trust aware system for social networks is presented briefly in this paper. Trust analysis has received less attention in social networks. Thus trust models and trust computation in social networks are to be considered to provide trustworthy social networking systems. Trust and trust metrics are evaluated through the different trust models and methods. The review studies on the disadvantages and challenges faced in achieving trust in social net- works. In recommending friends online trustworthy recommendations are very important to consider the recommended friend online. Trust worthy web recommendations are lagging online because the links suggested can be a malware which has the caability to encrypt the system data and cause the user threat. Hence a trustworthy web recommendations made by trustworthy friends has to be suggested and accepted. User authentication itself has become a treat in currecnt social networking sites because untrusted sybils on social networks has access to user data and try to pretend as innocents and make changes original user data. We have different aspects of social networks in which trust plays a major role in preventing the data loss and providing security for the user data. Analysing the human behaviour on social networks provides the data of how trust can be proccessed using principles of human sciences.

8. REFERENCES

[1] D. L. Iglesias, J.-M. Marques, G. Cabrera, H. Rifa-Pous, and A. Mon- tane, "Hornet: Microblogging for a Contributory Social Network," IEEE Internet Computing, vol. 16, no. 3, pp. 37–45, 2012.

[2] X. Liang, K. Zhang, X. Shen, and X. Lin, "Security and Privacy in Mobile Social Networks: Challenges and Solutions," IEEE Wireless Communications, vol. 21, no. 1, pp. 33–41, 2014.

[3] B. Li, L. Liao, H. Leung, and R. Song, "PHAT: A Preference and Honesty Aware Trust Model for Web Services," IEEE Transactions on Network and Service Management, vol. 11, no. 3, pp. 363–375, 2014.

[4] M. Eirinaki, M. D. Louta, and I. Varlamis, "A Trust-Aware System for Personalized User Recommendations in Social Networks," IEEE Transactions on Systems, Man, and Cybernetics, vol. 44, no. 4, pp. 409– 421, 2014.

[5]G.Vasanthakumar,P.D.Shenoya,andK.R.Venugopal,"PTIB: Profiling Top Influential Blogger in Online Social Networks,"

[6] I. Ivanov, P. Vajda, P. Korshunov, and T. Ebrahimi, "Comparative Study of Trust Modeling for Automatic Landmark Tagging," IEEE Transactions on Information Forensics and Security, vol. 8, no. 6, pp. 911–923, 2013.

[7] S. Caton, C. Haas, K. Chard, K. Bubendorfer, and O. F. Rana, "A Social Compute Cloud: Allocating and Sharing Infrastructure Resources via Social Networks," IEEE Transactions on Services Computing, vol. 7, no. 3, pp. 359–372, 2014.

[8] L. Yang, F. Hao, S. Li, G. Min, H. Kim, and S. Yau, "An Efficient Approach to Generating Location-Sensitive Recommendations in Ad- hoc Social Network Environments," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 11, pp. 2944–2955, 2014.

[9] G. Liu, Y. Wang, M. A. Orgun, and E.-P. Lim, "Finding the Optimal Social Trust Path for the Selection of Trustworthy Service Providers in Complex Social Networks," IEEE Transactions on Services Computing, vol. 6, no. 2, pp. 152–167, 2013.

[10] N. Z. Gong and D. Wang, "On the Security of Trustee-Based Social Authentications," IEEE Transactions on Information Forensics and Se- curity, vol. 9, no. 8, pp. 1251–1263, 2014.

[11] K. R. Venugopal, K. Srinivasa, and L. M. Patnaik, Soft Computing for Data Mining Applications. Springer, 2009.

[12] M. Gjoka, C. T. Butts, M. Kurant, and A. Markopoulou, "Multigraph Sampling of Online Social Networks," IEEE Journal on Selected Areas in Communications, vol. 29, no. 9, pp. 1893–1905, 2011.

[13] N. Laranjeiro, M. Vieira, and H. Madeira, "A Technique for Deploying Robust Web Services," IEEE Transactions on Services Computing, vol. 7, no. 1, pp. 68–81, 2014.

[14] R. Jia, K. Zheng, J. Zhang, L. Fu, P. Du, X. Wang, and J. Xu, "Asymptotic Analysis on Throughput and Delay in Cognitive Social Networks," IEEE Transactions on Communications, vol. 62, no. 8, pp. 2721–2732, 2014.

[15] H. C. Chu, D. J. Deng, and J. H. Park, "Live Data Mining Concerning Social Networking Forensics based on a Facebook Session through Aggregation of Social Data," IEEE Journal on Selected Areas in Communications, vol. 29, no. 7, pp. 1368–1376, 2011.

[16] S. Deng, L. Huang, G. Xu, X. Wu, and Z. Wu, "On Deep Learning for Trust-Aware Recommendations in Social Networks," IEEE Transactions on Neural Networks and Learning Systems, 2016.

[17] P. D. Shenoy, K. Srinivasa, K. R. Venugopal, and L. M. Patnaik, "Dynamic Association Rule Mining using Genetic Algorithms," Intelligent Data Analysis, vol. 9, no. 5, pp. 439–453, 2005.

[18] P. Wang, Z. Ding, C. Jiang, and M. Zhou, "Constraint-Aware Approach to Web Service Composition," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 44, no. 6, pp. 770–784, 2014.

[19] W. Chen, I. Paik, and P. C. Hung, "Constructing a Global Social Service Network for Better Quality of Web Service Discovery," IEEE Transactions on Services Computing, vol. 8, no. 2, pp. 284–298, 2015.

[20] L. Liu and H. Jia, "Trust Evaluation via Large-Scale Complex Service- Oriented Online Social Networks," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 45, no. 11, pp. 1402–1412, 2015.

[21] W. Jiang, J. Wu, F. Li, G. Wang, and H. Zheng, "Trust Evaluation in Online Social Networks Using Generalized Network Flow," IEEE Transactions on Computers, vol. 65, no. 3, pp. 952–963, 2016.

[22] S. Iftikhar, M. Kamran, E. U. Munir, and S. U. Khan, "A Reversible Watermarking Technique for Social Network Data Sets for Enabling Data Trust in Cyber, Physical, and Social Computing," IEEE Systems, pp. 1–10, 2015.

[23] G. Vasanthakumar, A. K. Upadhyay, P. F. Kalmath, S. Dinakar, P. D. Shenoy, and K. R. Venugopal, "Up3: User Profiling from Profile Picture in Multi-Social Networking," in 2015 Annual IEEE India Conference (INDICON), pp. 1–6, IEEE, 2015.

[24] R. Schlegel, C.Y. Chow, Q. Huang, and D. Wong, "Privacy-Preserving Location Sharing Services for Social Networks," IEEE Transactions on Sevices Computing, pp. 1–14, 2015.

[25] S. Deng, L. Huang, G. Xu, X. Wu, and Z. Wu, "On Deep Learning for Trust-Aware Recommendations in Social Networks," IEEE Transactions on Neural Networks and Learning Systems, pp. 1–13, 2016.

[26] Z. He, Z. Cai, J. Yu, X. Wang, Y. Sun, and Y. Li, "Cost-Efficient Strategies for Restraining Rumor Spreading in Mobile Social Networks," IEEE Transactions on Vehicular Technology, pp. 1–12, 2016.

[27] F. Hao, S. Li, G. Min, H.C. Kim, S. S. Yau, and L. T. Yang, "An Efficient Approach to Generating Location-Sensitive Recommendations in ad-hoc Social Network Environments," IEEE Transactions on Services Computing, vol. 8, no. 3, pp. 520–533, 2015.

[28] T. Wang, H. Krim, and Y. Viniotis, "A Generalized Markov Graph Model: Application to Social Network Analysis," IEEE Journal of Selected Topics in Signal Processing, vol. 7, no. 2, pp. 318–332, 2013.

[29] S. Joshi, V. Simha, D. Shenoy, K. R. Venugopal, and L. Patnaik, "Classification and Treatment of different Stages of Alzheimers Disease using Various Machine Learning Methods," International Journal of Bioinformatics Research, vol. 2, no. 1, pp. 44–52, 2010.

[30] M. E. Nergiz, E. Cicek, T. Pedersen, and Y. Saygin, "A Look-Ahead Approach to Secure Multi-party Protocols," IEEE Transactions on Knowledge an d Data Engineering, vol. 24, no. 7, pp. 1170–1185, 2012.

[31] V. M. Prabhakaran and M. M. Prabhakaran, "Assisted Common In- formation with an Application to Secure Two-Party Sampling," IEEE Transactions on Information Theory, vol. 60, no. 6, pp. 3413–3434, 2014.

[32] N. Laranjeiro, M. Vieira, and H. Madeira, "A Technique for Deploying Robust Web Services," IEEE Transactions on Services Computing, vol. 7, no. 1, pp. 68–81, 2014.

[33] Z. Li, C. Wang, S. Yang, C. Jiang, and X. Li, "Lass: Local-Activity and Social-Similarity Based Data Forwarding in Mobile Social Networks," IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 1, pp. 174–184, 2015.

[34] H.-P. Yueh, W. Lin, Y.-L. Liu, T. Shoji, and M. Minoh, "The Devel- opment of an Interaction Support System for International Distance Education," IEEE Transactions on Learning Technologies, vol. 7, no. 2, pp. 191–196, 2014.

[35] L. Guo, C. Zhang, and Y. Fang, "A Trust-Based Privacy-Preserving Friend Recommendation Scheme for Online Social Networks," IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 4, pp. 413–427, 2015.

[36] X. Qiao, W. Yu, J. Zhang, W. Tan, J. Su, W. Xu, and J. Chen, "Recommending Nearby Strangers Instantly Based on Similar Check-In Behaviors," IEEE Transactions on Automation Science and Engineering, vol. 12, no. 3, pp. 1114–1124, 2015.

[37] M. Doost mohammadian and U. A. Khan, "Graph-Theoretic Distributed Inference in Social Networks," IEEE Journal of Selected Topics in Signal Processing, vol. 8, no. 4, pp. 613–623, 2014.

[38] A. Das and M. M. Islam, "SecuredTrust: A Dynamic Trust Computation Model for Secured Communication in Multiagent Systems," IEEE Trans- actions on Dependable and Secure Computing, vol. 9, no. 2, pp. 261– 274, 2012.

[39] J. Jiang, C. Wilson, X. Wang, W. Sha, P. Huang, Y. Dai, and B. Y. Zhao, "Understanding Latent Interactions in Online Social Networks," ACM Transactions on the Web (TWEB), vol. 7, no. 4, pp. 1–18, 2013.

[40] F. M. F. Wong, Z. Liu, and M. Chiang, "On the Efficiency of Social Recommender Networks," in 2015 IEEE Conference on Computer Communications (INFOCOM), pp. 2317–2325, IEEE, 2015.

[41] J. Kwon and S. Kim, "Friend Recommendation Method using Physical and Social Context," International Journal of Computer Science and Network Security, vol. 10, no. 11, pp. 116–120, 2010.

[42] K. Farrahi and D. Gatica-Perez, "Discovering Routines from Large-Scale Human Locations using Probabilistic

Topic Models," ACM Transactions on Intelligent Systems and Technology (TIST), vol. 2, no. 1, pp. 3–6, 2011.

[43] M. Li, R. Na, Q. Qian, H. Zhu, X. Liang, and L. Yu, "SPFM: Scalable and Privacy-Preserving Friend Matching in Mobile Cloud," IEEE Internet of Things Journal, 2012.

[44] L. Bian and H. Holtzman, "Online Friend Recommendation through Personality Matching and Collaborative Filtering," Proc. of UBICOMM, pp. 230–235, 2011.

[45] Z. Wang, J. Liao, Q. Cao, H. Qi, and Z. Wang, "Friendbook: a Semantic- Based Friend Recommendation System for Social Networks," IEEE Transactions on Mobile Computing, vol. 14, no. 3, pp. 538–551, 2015.

[46] Q. Tang and J. Wang, "Privacy-Preserving Friendship-based Recom- mender Systems,"

[47] S. Deng, L. Huang, G. Xu, X. Wu, and Z. Wu, "On Deep Learning for Trust-Aware Recommendations in Social Networks," 2016.

[48] S. Huang, J. Zhang, L. Wang, and X.-S. Hua, "Social Friend Recommendation Based on Multiple Network Correlation," IEEE Transactions on Multimedia, vol. 18, no. 2, pp. 287–299, 2016.

[49] Q. Cao, M. Sirivianos, X. Yang, and T. Pregueiro, "Aiding the Detection of Fake Accounts in Large Scale Social Online Services," in Presented as part of the 9th USENIX Symposium on Networked Systems Design and Implementation (NSDI 12), pp. 197–210, 2012.

[50] B. Viswanath, A. Post, K. P. Gummadi, and A. Mislove, "An Analysis of Social Network-based Sybil Defenses," ACM SIGCOMM Computer Communication Review, vol. 40, no. 4, pp. 363–374, 2010.

[51] K. Thomas, C. Grier, D. Song, and V. Paxson, "Suspended Accounts in Retrospect: An Analysis of Twitter Spam," in Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference, pp. 243–258, ACM, 2011.

[52] G.DanezisandP.Mittal,"Sybilinfer: Detecting SybilNodes using Social Networks.," in NDSS, San Diego, CA, 2009.

[53] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "Sybilguard: De- fending Against Sybil Attacks via Social Networks," in ACM SIGCOMM Computer Communication Review, vol. 36, pp. 267–278, ACM, 2006.

[54] H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao, "Sybillimit: A Near- Optimal Social Network Defense against Sybil Attacks," in 2008 IEEE Symposium on Security and Privacy (sp 2008), pp. 3–17, IEEE, 2008.

[55] Z. Yanbin, "Detecting and Characterizing Social Spam Campaigns in Online Social Networks," 2010.

[56] Z. Yang, C. Wilson, X. Wang, T. Gao, B. Y. Zhao, and Y. Dai, "Uncovering Social Network Sybils in the Wild," ACM Transactions on Knowledge Discovery from Data (TKDD), vol. 8, no. 1, pp. 2–8, 2014.

[57] E. K. Asl, J. Bentahar, H. Otrok, and R. Mizouni, "Efficient Community Formation for Web Services," IEEE Transactions on Services Comput- ing, vol. 8, no. 4, pp. 586–600, 2015.

[58] X. Chen, B. Proulx, X. Gong, and J. Zhang, "Exploiting Social Ties for Cooperative D2D Communications: A Mobile Social Networking Case," IEEE/ACM Transactions on Networking, vol. 23, no. 5, pp. 1471–1484, 2015.

[59] W. Jiang, J. Wu, G. Wang, and H. Zheng, "Forming Opinions via Trusted Friends: Time-Evolving Rating Prediction using Fluid Dynamics," IEEE Transactions on Computers, vol. 65, no. 4, pp. 1211–1224, 2016.

[60] N. Zheng, S. Song, and H. Bao, "A Temporal-Topic Model for Friend Recommendations in Chinese Microblogging Systems," IEEE Trans- actions on Systems, Man, and Cybernetics: Systems, vol. 45, no. 9, pp. 1245–1253, 2015.

[61] J. Parra-Arnau, A. Perego, E. Ferrari, J. Forne, and D. Rebollo- Monedero, "Privacy-Preserving Enhanced Collaborative Tagging," IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 1, pp. 180–193, 2014.

[62] G. Vasanthakumar, P. D. Shenoy, and K. R. Venugopal, "Pfu: Profiling Forum Users in Online Social Networks, a Knowledge Driven Data Mining Approach," in 2015 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE), pp. 57–60, IEEE, 2015.

[63] K.A. Shim, "An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks," IEEE Transactions on Vehicular Technology, vol. 61, no. 4, pp. 1874–1883, 2012.

[64] E. Miluzzo, N. D. Lane, S. B. Eisenman, and A. T. Campbell, "Cenceme–Injecting Sensing Presence into Social Networking Applications," in European Conference on Smart Sensing and Context, pp. 1–28, Springer, 2007.

[65] Y. Altshuler, E. Shmueli, G. Zyskind, O. Lederman, N. Oliver, and A. Pentland, "Campaign Optimization through Behavioral Modeling and Mobile Network Analysis," IEEE Transactions on Computational Social Systems, vol. 1, no. 2, pp. 121–134, 2014.

[66] S. Wen, M. S. Haghighi, C. Chen, Y. Xiang, W. Zhou, and W. Jia, "A Sword with Two Edges: Propagation Studies on both Positive and Negative Information in Online Social Networks," IEEE Transactions on Computers, vol. 64, no. 3, pp. 640–653, 2015.

[67] B. Carminati, E. Ferrari, and A. Perego, "Enforcing Access Control in Web-Based Social Networks," ACM Transactions on Information and System Security (TISSEC), vol. 13, no. 1, pp. 1–6, 2009.

[68] P. Lin, P.-C. Chung, and Y. Fang, "P2P-isn: A Peer-to-Peer Architecture for Heterogeneous Social Networks," IEEE Transactions on Network, vol. 28, no. 1, pp. 56–64, 2014.

[69] R.Schlegel, C.Y. Chow, Q. Huang, and D. Wong, "Privacy-Preserving Location Sharing Services for Social Networks," IEEE Transactions on Services Computing, vol. 99, no. 1, pp. 1–11, 2016.

[70] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order Preserving En- cryption for Numeric Data," in Proceedings of the 2004 ACM SIGMOD International Conference on Management of Data, pp. 563–574, ACM, 2004.

[71] L. Barkhuus, B. Brown, M. Bell, S. Sherwood, M. Hall, and M. Chalmers, "From Awareness to Repartee: Sharing Location within Social Groups," in proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 497–506, ACM, 2008.

[72] M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking," in Proceedings of the 1st International Conference on Mobile Systems, Applications and Services, pp. 31–42, ACM, 2003.

[73] L. Siksnys, J. R. Thomsen, S. Saltenis, and M. L. Yiu, "Private and Flexible Proximity Detection in Mobile Social Networks," in 2010 Eleventh International Conference on Mobile Data Management, pp.75– 84, IEEE, 2010.

[74] E. Toch, J. Cranshaw, P. H. Drielsma, J. Y. Tsai, P. G. Kelley, J. Spring- field, L. Cranor, J. Hong, and N. Sadeh, "Empirical Models of Privacy in Location Sharing," in Proceedings of the 12th ACM International Conference on Ubiquitous Computing, pp. 129–138, ACM, 2010.

[75] S. Wen, M. S. Haghighi, C. Chen, Y. Xiang, W. Zhou, and W. Jia, "A Sword with Two Edges: Propagation Studies on both Positive and Negative Information in Online Social Networks," IEEE Transactions on Computers, vol. 64, no. 3, pp. 640–653, 2015.

[76] Y. Liu, S. Xu, and G. Tourassi, "Detecting Rumors Through Modeling Information Propagation Networks in a Social Media Environment," in International Conference on Social Computing, Behavioral-Cultural Modeling, and Prediction, pp. 121–130, Springer, 2015.

[77] S. Wen, J. Jiang, Y. Xiang, S. Yu, W. Zhou, and W. Jia, "To Shut Them Up or to Clarify: Restraining the Spread of Rumors in Online Social Networks," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 12, pp. 3306–3316, 2014.

[78] Y. Zhang, A. Adiga, S. Saha, A. Vullikanti, and B. A. Prakash, "Near- Optimal Algorithms for Controlling Propagation at Group Scale on Networks," IEEE Transactions on Knowledge and Data Engineering, no. 12, pp. 3339–3352, 2016.

[79] X. Chen, M. Vorvoreanu, and K. Madhavan, "Mining Social Media Data for Understanding Students Learning Experiences," IEEE Transactions on Learning Technologies, vol. 7, no. 3, pp. 246–259, 2014.