International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue V, Mar 2019- Available at www.ijraset.com

Efficient and Secure Mechanism for Privacy Preserving and Data Sharing in Online Social Networks

Aravind Kalyan[1], Tarun Reddy[2], Jothi Kumar[3]
[1, 2]*B.Tech Student, CSE, SRM University, Kanchipuram, Chennai*
[3]*Asst. Prof, CSE, SVS SRM University, Kanchipuram, Chennai*

Abstract: ***The main aim of our research topic is privacy protection in online social network in particular when a user's confidential data is exposed in contents posted by another's, such as pics, with individuals being tagged. Day to day life people are mostly linked with the online social networking. By using this platform every user can share their data to other user. Online social networking plays an important role for individual. Along with their is a huge risk of sharing their own data with end users. Because there is a link between one users. Multiple users every user has their own opinion on the data share. There is a huge risk in online networking platform. so keeping in view about the upper problem they brought on mechanism it; In this research paper we implement an novel secure mechanism called trust based collaborative privacy management in this mechanism if the user wont to share any data to other user that can be kept only to the said user according to the privacy of the individual with this mechanism securely can be maintained and that would result to the encouragement of an individual for using online networking platform and can make Indian as a digital Indian Be free and live safe.***
Keywords: privacy management, social networks, privacy policy

I. INTRODCUCTION

Online social networks such as Face book, twitter, Google etc.. Have now become the important platform for every user to share their data to the other users Millions of people are sharing their data from of photos, texts, videos on online social networking such data consists sensitive information of users. If that data is used by unauthorised entities users privacy must be compromised. Privacy plays an important role in OSNs to protect such privacy users must take measures to prevent data breach Even though by changing the privacy selling an individual can protect but sure more messages should also be taken. The protection of privacy is major issue in online social networks. To secure users' privacy, on one hand, the service suppliers of OSNs have to take measures to stop information breach. On the opposite hand, users themselves will control the access to their information by utilizing the privacy setting function proposed in OSNs. An access control policy, additionally referred to as the privacy policy, defines that users are allowed to access a user's information. Current OSNs usually utilize user relationship to differentiate between legitimate users and unauthorized users. as an example, Face book users will specify if their information can be accessed by friends, specific teams or everybody. To require conditions for Social network users who want access another user's information in online social network we implement secure control mechanism for protect data in OSN networks. While there's no strict restriction on users who post information. A consequence of this one-side restriction is that the user who posts information may accidentally violate different users' privacy. Small the subsequent example. Suppose that a user A posts a photograph of him/her fiddling with a friend B, and user A specifies that the pic is accessed by his/her colleagues. If user B considers this pic to be sensitive and user B isn't familiar with user A's colleagues, then user B's privacy are violated. Within the above case, the pic is truly co owned by the 2 users. Hence, the privacy policy specified by user A have to be compatible with user B's privacy policy, otherwise, user B can suffer a loss in privacy. Information which is co-owned by multiple users is quite common in OSNs. Privacy management of such information needs a collaboration of all concerned users. Issue of collaborative privacy management in OSNs has attracted much attention in recent years. Most studies deal with this drawback by 1st detecting the conflicts among completely different users' privacy policies, so generating an aggregated policy that may resolve the conflicts to the most important extent. Given an information item, a user's privacy policy is mostly represented by a group of users with whom the user needs to share the info. Usually there's a negotiator who collects users' policies and makes a bunch call via some aggregation theme. In most cases, the conflicts among users' privacy policies can't be completely eliminated, which suggests the aggregated policy may still cause a privacy loss to a number of the users. The way to create a trade-off between information sharing and privacy preserving is a crucial question for the planning of the conflict resolution methodology.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue V, Mar 2019- Available at www.ijraset.com

II. RELATED WORKS

L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren describe the information about the growing popularity and development of online networking brings a serious threat to the privacy of individual's information. Important emerging topic in data mining is called as privacy preserving data mining (PPDM) has studied extensively in recent year. Basic idea of CPDM Is to protect the sensitive information of an individual. Current PPDM deals with how to reduce privacy loss due to data mining operation , infect unwanted disclosure may also happened due to data collection data publication etc. In this paper we come across the privacy issue related to data mining and investigate approaches that make the individual information reveals.M. Qiu, K. Gai, and Z. Xiong of describes the information regarding Wireless data transmission have enable the dramatically such as social networks and big data applications. Multichannel wireless communication is one of the approaches for transforming information when the user is connected to wireless networking environment. Fixed communication scan hardly meets the requirement of higher privacy protections because of conflict cost by for performance and security demand. J. M. Such and N. Criado of describes the information about Data shared to social media may effect more than one user privacy **example** photos, that depict multi user, in comments many users may mention, events that are invited etc. Lack of privacy management in current privacy system users are enable to control to whom those items are actually shared or not computation mechanism can make to control the multiple policy into single policy for an item , then that problem may be solved. In this paper we propose the first computation mechanism to solve conflict for multiple party privacy management in social media. With these users can reach the solution of conflict.

III. OVERVIEW OF THE SYSTEM

In the proposed trust based privacy management mechanism, we introduce a setting based in how to protect the user's data as their final decisions with this setting a user can link the privacy to only one user as he wished other users can also see .he can share his data on the basis of privacy. The setting to be done I.e. upper confidence bound (UIB) policy to solve the problem with the UIB an individual can be safe. The trust values between users all. Associated with the user's privacy loss. The proposed policy can protect the data of an individual from recessing their data to billions of users.

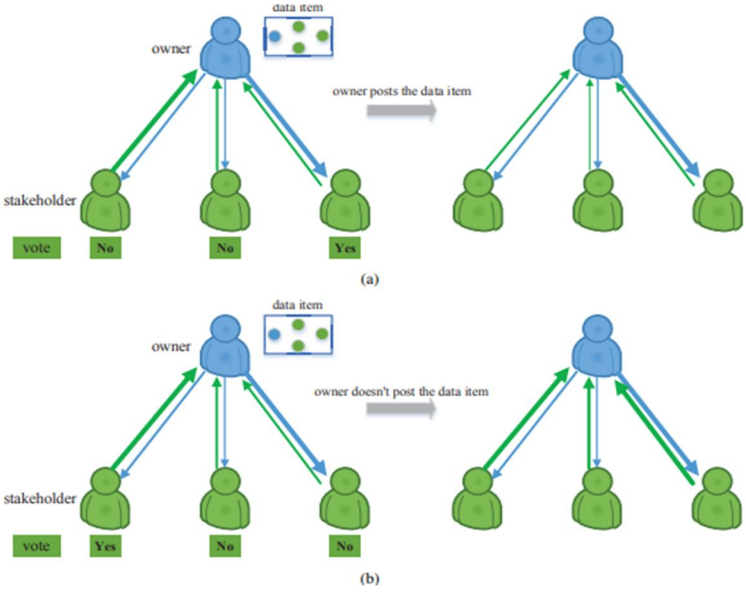


Fig 1: System Architecture

IV. TRUST RELATION SHIP

This phase is used between users to secure data of online social users or to find whether user is authenticated or not. The proposed secure mechanism will evaluate trust values between various users based on their interactions. In this investigate phase we center of attention on how to make use of trust to support the users to be more considerate of others' confidentiality. In Rathore and Tripathy describes the information about the a trust-based access control technique which uses the trust values to describe access conditions. That is, a user can specify the least trust level that is required for a different user to access his/her privacy information. In Sun et al. Describes the information about a trust-weighted voting system to aggregate various users' confidentiality policies. In our research article, we also utilize trust values to signify how much influence a user's view will have on the aggregated choice.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue V, Mar 2019- Available at www.ijraset.com

V. MULTIPARTY ACCESS CONTROL

The main feature of online social network is this acts as a interface between users its build a platform for users to share their information in online social network. This multiparty access control model consists of a multi policy specification mechanism and evolution of the policy. Suppose the owner of data item is let d in space m of one user U_1 in online social network. So here U_1 is owner of the item d.So U_1 is called as provider of d.We mainly analyze some scenarios like user profile sharing, content data sharing also relationships. Here the owner and communicator will specify access policies to control the sharing of user profile attributes. In this provider let d be a data item posted by user U_1 to somebody space in online social networks. That posted content may also have multiple tagged users. The work of stakeholder in social network is here T be the set of various tagged users associated with data item d.In this authorization concept from both data owner and stakeholder be reflected. In proposed scheme MPAC applied for who want to access the shred data.

VI. SECURITY MECHANISM

The trust-based mechanism implemented within the on top of section, we can draw the following easy conclusion: if the user never posts knowledge which will disclose alternative users' privacy, then the user will maintain a high name. and therefore the user's privacy is well preserved by alternative users, since his/heropinions ar extremely valued by others. However, considering that the core performs of OSNs is data sharing, it's unreasonable to suppress the sharing of co-owned information. a way to accomplish a balance between information sharing and privacy conserving is a vital issue within the study of information privacy during this section, we discuss a way to utilize the edge bth introduced within the trust-based mechanism to create a trade-off between privacy conserving and data sharing..

VII. DATA FLOW DIAGRAM FOR SYSTEM

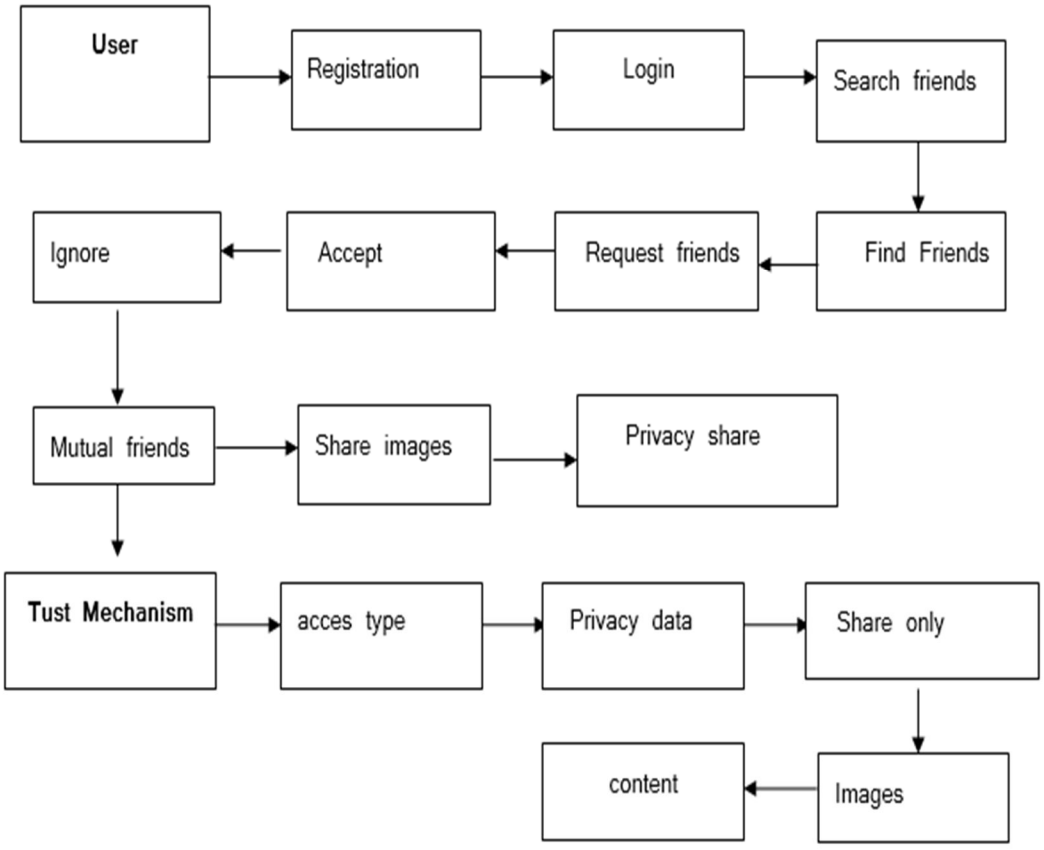


Fig 2: DFD for implemented system

VIII. SEQUENCE DIAGRAM

This diagram shows interactions and process of the system the below figure describes the information about system operations

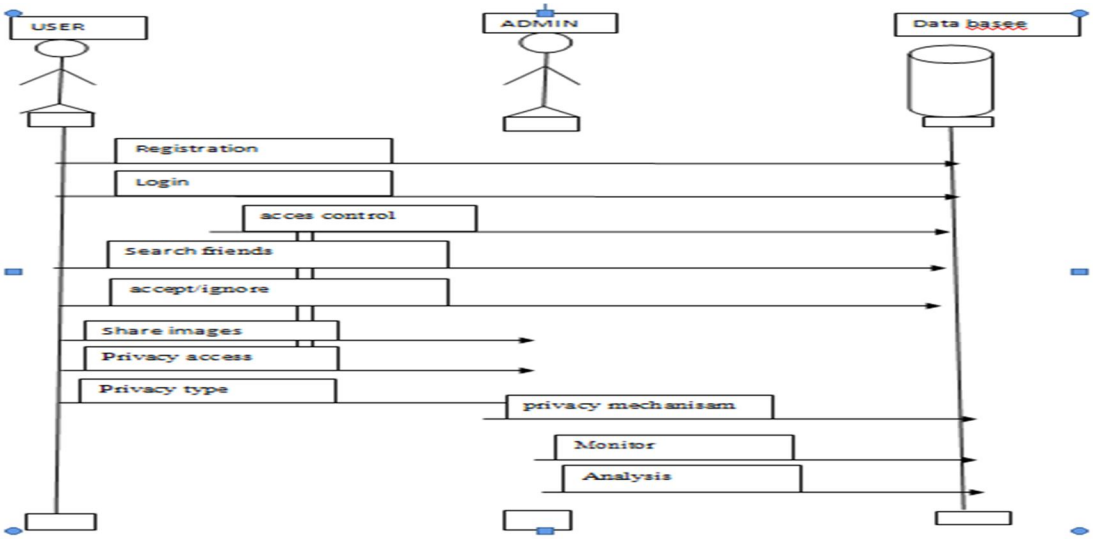
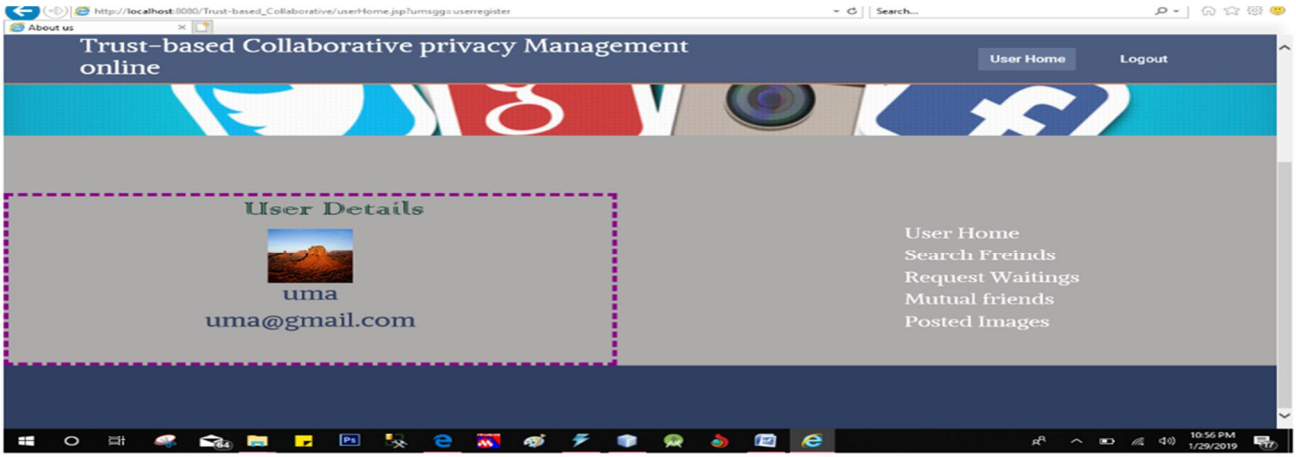


Fig 3: Sequence Diagram

IX. RESULTS



Admin Login

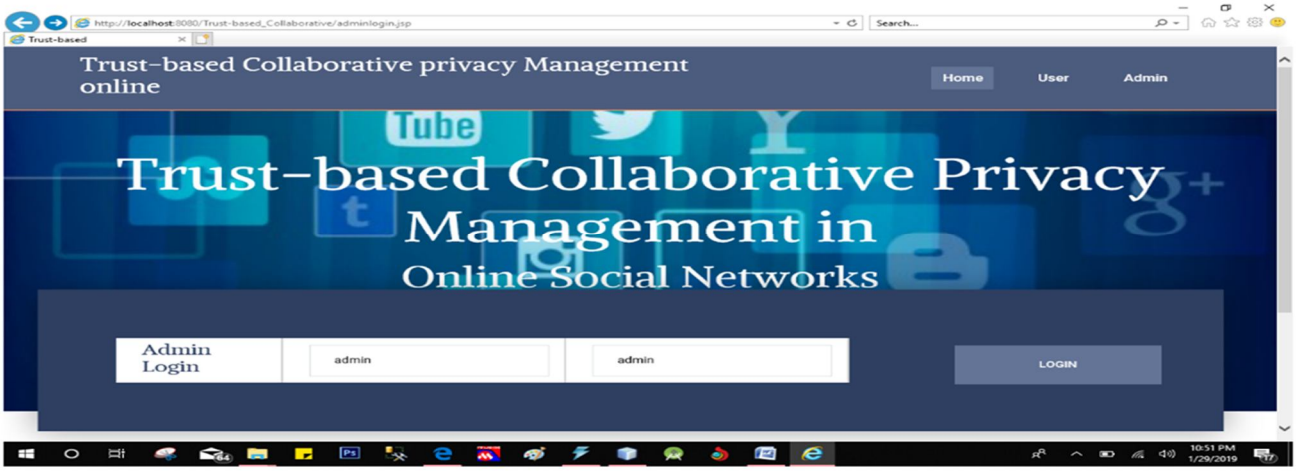
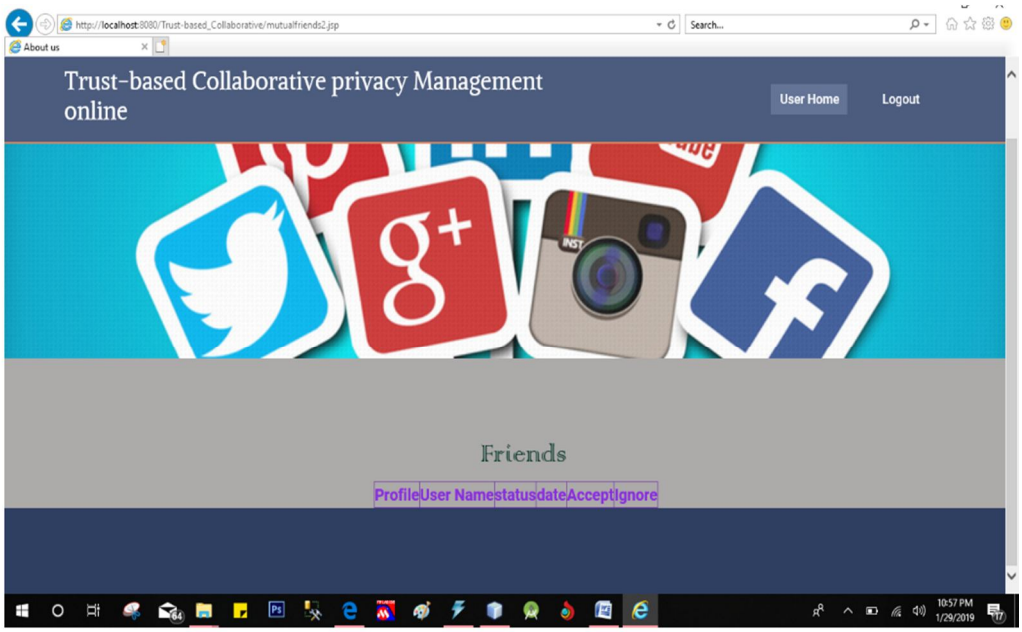


Fig 4.Admin Login



Post Image

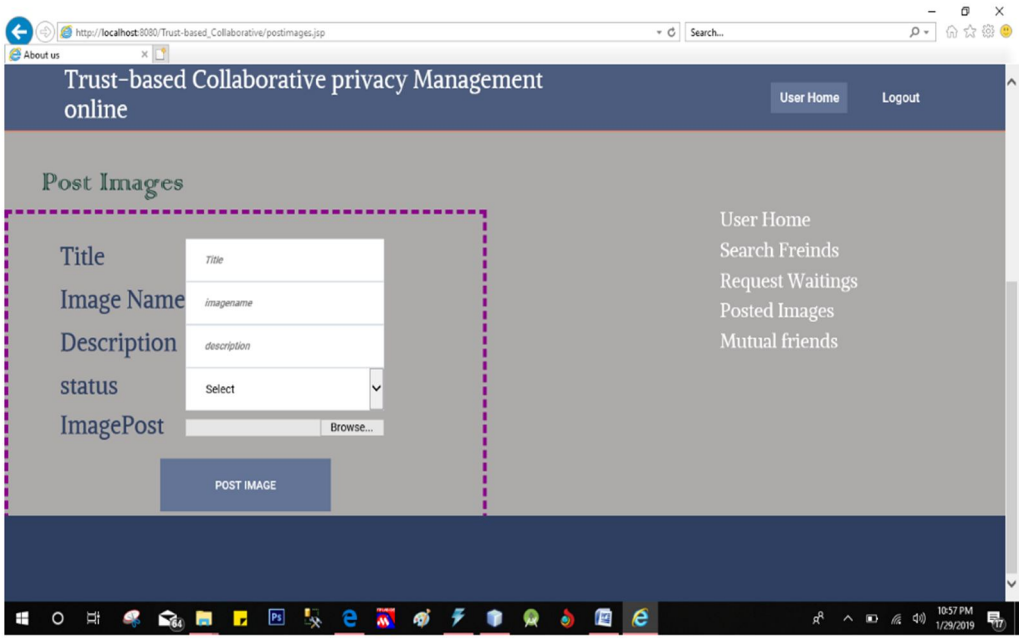


Fig 5: Post Image

X. CONCLUSION

In this article as per we analyze and focus on problem of privacy and data security in Online social networks. To solve the issue we implement secure mechanism called as propose a trust-based mechanism. Before post data item data owner need to ask stakeholders' opinions on data sharing, and then after user will take the final decision by evaluating the aggregated opinion with a pre-specified threshold. In this Mostly user will trust stakeholder. In the proposed trust based privacy management mechanism, we introduce a setting based in how to protect the user's data as their final decisions with this setting a user can link the privacy to only one user as he wished other users can also see .he can share his data on the basis of privacy. The setting to be done I.e. upper confidence bound (UIB) policy to solve the problem with the UIB an individual can be safe. The trust values between users all. Associated with the user's privacy loss. The proposed policy can protect the data of an individual from recessing their data to billions of users.

REFERENCES

[1] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for online social networks: challenges and opportunities," IEEE Network, vol. 24, no. 4, pp. 13–18, July 2010.
[2] L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, "Information security in big data: Privacy and data mining," IEEE Access, vol. 2, pp. 1149–1176, 2014.
[3] L. Xu, C. Jiang, Y. Chen, J. Wang, and Y. Ren, "A framework for categorizing and applying privacy-preservation techniques in big data mining," Computer, vol. 49, no. 2, pp. 54–62, Feb 2016.
[4] M. Qiu, K. Gai, and Z. Xiong, "Privacy-preserving wireless communications using bipartite matching in social big data," Future Generation Computer Systems, 2017.[Online].Available: http://www.sciencedirect.com/science/article/pii/S0167739X17301449
[5] C. Fiesler, M. Dye, J. L. Feuston, C. Hiruncharoenvate, C. Hutto, S. Morrison, P. Khanipour Roshan, U. Pavalanathan, A. S. Bruckman, M. De Choudhury, and E. Gilbert, "What (or who) is public?: Privacy settings and social media content sharing," in Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing, March 2017, pp. 567–580.
[6] A. C. Squicciarini, M. Shehab, and F. Paci, "Collective privacy management in social networks," in Proceedings of the 18th ACM International Conference on World Wide Web, April 2009, pp. 521–530.
[7] H. Hu, G.-J. Ahn, and J. Jorgensen, "Detecting and resolving privacy conflicts for collaborative data sharing in online social networks," in Proceedings of the 27th ACM Annual Computer Security Applications Conference, December 2011, pp. 103–112.
[8] J. M. Such and N. Criado, "Resolving multi-party privacy conflicts in social media," IEEE Transactions on Knowledge and Data Engineering, vol. 28, no. 7, pp. 1851–1863, July 2016.
[9] P. Auer, N. Cesa-Bianchi, and P. Fischer, "Finite-time analysis of the multiarmed bandit problem," Machine learning, vol. 47, no. 2-3, pp. 235–256, 2002.
[10] H. Hu, G.-J. Ahn, Z. Zhao, and D. Yang, "Game theoretic analysis of multiparty access control in online social networks," in Proceedings of the 19th ACM Symposium on Access Control Models and Technologies, New York, NY, June 2014, pp. 93–102.
[11] H. Hu, G. J. Ahn, and J. Jorgensen, "Multiparty access control for online social networks: Model and mechanisms," IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 7, pp. 1614–1627, July 2013.
[12] N. Vishwamitra, Y. Li, K. Wang, H. Hu, K. Caine, and G.-J. Ahn, "Towards pii-based multiparty access control for photo sharing in online social networks," in Proceedings of the 22Nd ACM on Symposium on Access Control Models and Technologies, June 2017, pp. 155–166.
[13] P. Mehregan and P. W. Fong, "Policy negotiation for co-owned resources in relationship-based access control," in Proceedings of the 21st ACM on Symposium on Access Control Models and Technologies, June 2016, pp. 125–136.
[14] J. Golbeck, "Trust on the world wide web: A survey," Foundations and Trends in Web Science, vol. 1, no. 2, pp. 131–197, 2008.
[15] S. Zakhary, M. Radenkovic, and A. Benslimane, "Efficient location privacy-aware forwarding in opportunistic mobile networks," IEEE Transactions on Vehicular Technology, vol. 63, no. 2,