

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

Survey of Privacy Policy Based Friend-To-Friend Content Dissemination System

K. Sharmila Devi¹, D. Kalaiselvi², A. Gokilavani³

ME Scholar, Department of CSE, Jai Shriram Engineering College, Tirupur, Tamilnadu, India ¹

Professor, Department of CSE, Jai Shriram Engineering College, Tirupur, Tamilnadu, India²

Assistant Professor, Department of CSE, Jai Shriram Engineering College, Tirupur, Tamilnadu, India³

ABSTRACT: In this paper, new hybrid content storage and distribution system for user generated content (UGC). Despite the obviousness of developing the a hybrid scheme that exploits the advantages of opportunistic networks, offloading and decentralized storage and delivery, to date such a scheme has not yet been proposed again due to two primary reasons. First, the high communication and energy cost of decentralized content storage and distribution for mobile systems. Second, due to the address these two fundamental limitations by exploiting the possibility of content replication, considering initial encounter time and duration of users' encounters, and utilizing existing social networking services for opportunistic dissemination. Online social networks (OSNs) have experienced tremendous growth in recent years. These OSNs offer attractive means for digital social interactions and information sharing, but also raise a number of security and privacy issues. While OSNs allow users to restrict access to shared data, they currently do not provide any mechanism to enforce privacy concerns over data associated with multiple users. This paper enhances existing and introduces new social network privacy management models and measures their human effects. First, it introduces a mechanism using proven clustering techniques that assists users in grouping their friends for traditional group-based policy management approaches. It found measurable agreement between clusters and user-defined relationship groups. Second, it introduces a new privacy management model that leverages users' memory and opinion of their friends (called example friends) to set policies for other similar friends. Finally, it explores different techniques that aid users in selecting example friends. It is found that by associating policy templates with example friends (versus group labels), users author policies more efficiently and have improved perceptions over traditional group-based policy management approaches. In addition, the results show that privacy management models can be further enhanced by utilizing user privacy sentiment for mass customization. By detecting user privacy sentiment (i.e., an unconcerned user, a pragmatist or a fundamentalist), privacy management models can be automatically tailored specific to the privacy sentiment and needs of the user

KEYWORDS: Friend book, friend OSN, Content filtering, Language Model, Association Mining, Suppression Tag

I. INTRODUCTION

The papers leverages traditional group-based policy management as our baseline and progressively improve upon this privacy management model. With each new enhancement, we measure their human effects including cluster/user defined relationship group alignment, user privacy sentiment, efficiencies and user perceptions. The thesis introduces a user-assisted friend grouping mechanism that enhances traditional group-based policy management approaches.

Assisted Friend Grouping leverages proven clustering techniques to aid users in grouping their friends more effectively and efficiently. It introduces a new privacy management model that is an improvement over traditional group-based policy management approaches. The new paradigm leverages a user's memory and opinion of their friends to set policies for other similar friends, which we refer to as Same-As Policy Management. Users associate the policy with an example friend and in doing so have this friend in the forefront of their mind. This allows users to be more selective and careful in assigning permissions. Users are thinking of people, not groups. Using a visual policy editor

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

that takes advantage of friend recognition and minimal task interruptions, Same-As Policy Management demonstrated improved performance and user perceptions over traditional group-based policy management approaches.

It further enhances enhanced Same-As Policy Management by introducing Example Friend Selection—two techniques for aiding users in selecting their example friends that are used in developing policy templates. Both techniques reduced policy authoring times and were positively perceived by users. In addition, the thesis proposes an approach to enable the protection of shared data associated with multiple users in OSNs.

II. RELATED WORKS

Abdolreza Abhari & Mojgan Soraya [1] introduces a workload characterization study of the most popular short video sharing service of Web 2.0, YouTube. Based on a vast amount of data gathered in a five-month period, we analyzed characteristics of around 250,000 YouTube popular and regular videos. In particular, we collected lists of related videos for each video clip recursively and analyzed their statistical behavior. Understanding YouTube traffic and similar Web 2.0 video sharing sites is crucial to develop synthetic workload generators. Workload simulators are required for evaluating the methods addressing the problems of high bandwidth usage and scalability of Web 2.0 sites such as YouTube. The distribution models, in particular Zipf-like behavior of YouTube popular video files suggests proxy caching of YouTube popular videos can reduce network traffic and increase scalability of YouTube Web site. YouTube workload characteristics provided in this work enabled us to develop a workload generator to evaluate the effectiveness of this approach

Marco Valerio Barbera, Julinda Stefa [2] describe VIP delegation, a solution to this problem based solely on the inherent social aspects of user mobility. Our idea is to exploit a few, important subscribers that with their movements and interactions are able to communicate with all the rest of the network users on a regular basis. These VIP devices would act as a bridge between the network infrastructure and all the remaining of the network each time large amount of data has to be transferred. VIP delegation can help alleviate the network traffic in different scenarios. VIPs are defined according to well known social network attributes (betweenness, closeness, degree centrality and pagerank), and are selected according to two methods: global (network-based) and hood (community-based) selection. All methods rely on a short network observation period of 1 week, and select VIP sets that result small, efficient, and stable in time

Raul Gracia-Tinedo, Marc Sanchez-Artigas [3] describe Friend-to-Friend (F2F) storage systems are nowadays an interesting research topic and they constitute an alternative approach to leverage personal storage. The F2F paradigm is based on the synergy between social networks and storage systems: users store their data in a set of social friends. Thus, data is neither stored in a centralized server nor in unknown peers, enabling users to retain the control of their data. Moreover, the social component of F2F systems alleviates many undesirable problems present in large scale distributed systems e.g. security, trust, incentives. Essentially, the FriendBox Application State maintains up to date the data management information about users' files. This information expresses which friends store which files and the network address of each friend. This information is needed to perform friend-to-friend storage operations. The maintenance process of this information is carried out by FriendBox Storage Clients installed at participants.

Pan Hui, Jon Crowcroft, Eiko Yoneki [4] is focus on two specific aspects of society: community and centrality. Community is an important attribute of PSNs. Cooperation binds, but also divides human society into communities. Human society is structured. Within a community, some people are more popular, and interact with more people than others (i.e. have high centrality); we call them hubs. Popularity ranking is one aspect of the population. For an ecological community, the idea of correlated interaction means that an organism of a given type is more likely to interact with another organism of the same type than with a randomly chosen member of the population. This correlated interaction concept also applies to human, so we can exploit this kind of community information to select forwarding paths.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

Azeem J. Khan, V. Subbaraju & Archan Misra [5] explore the opportunities for addressing this emerging conflict by enabling more intelligent ad delivery to such mobile devices. One especially promising path is leveraging the increasing availability of heterogeneous wireless access technologies that offer less restrictive and more energy-efficient transport substrates for such data traffic.

However to understand the possibilities that exist, author first profile the advertisement traffic characteristics for some of the most popular advertisement-supported consumer applications, and then analyze the key features of mobile advertisement delivery. In proposed system then outline the principles of CAMEO, a middleware that uses predictive profiling of a user's {device, network and usage} context to anticipate the advertisements that need to be served, and then modulates their delivery mechanism to enable effective mobile advertising, but at considerably lower costs .

In this paper, they proposed a template for the design of a social networking privacy wizard. The intuition for the design comes from the observation that real users conceive their privacy preferences (which friends should be able to see which information) based on an implicit set of rules. Thus, with a limited amount of user input, it is usually possible to build a machine learning model that concisely describes a particular user's preferences, and then use this model to configure the user's privacy settings automatically.

III. SYSTEM ANALYSIS

The existing system introduces three new improvements to privacy management models:

- Assisted Friend Grouping an incremental improvement to traditional group-based policy management.
- Same-As Policy Management a new paradigm improvement over traditional group-based policy management.
- Example Friend Selection an incremental improvement to Same-As Policy Management.

A. Drawbacks Of Existing System

- If one person (A) specifies a policy to hide her friend list from the public and (B) one of the friends in that list specifies a weaker policy that permits his friend list visible to anyone, then relationship between A and B could be learnt
- Automatic configuration of privacy preferences is not included.
- Conflict resolution between privileges is not effective. For example, A uploads one photo which can be shared between friends list (F) and not visible to friends of friends, then B (one of the friends in F) can share it to friends list in F but not to all others.

B. Introduction To Tag Methodology

Tag

A tag is a user-contributed metadata, providing a mean of information or content item, created freely by users with personally salient keywords or labels, known as tags. The process of labeling is called tagging. Users can re-find the information later by means of those tags that they have created. Also, by tagging users can store resources for their future retrieval.

Collaborative tagging system

Collaborative tagging is a classification by the users and for the users. It isa social, decentralized and complex network where many annotations, generally provided by interrelated groups of individuals, are organized so to link resources and tags. Each resource item can be associated with many different tags, rather than with a single branch of a hierarchy. With tags chosen freely from common language and associated with web resources that are interesting for users (such as photographs, videos, web links and documents), collaborative tagging offers a sense of community in managing resources and results in a process of knowledge construction. Users can share their resources with others,

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

discover resources through the collaborative network, and contact people with similar interests. The benefit of collaborative tagging systems comes from the many views of the mass, rather than from a dominant opinion supplied by a few.

In fact, the form of tagging tends to stabilize over time because people usually choose to use the tags in three ways:

- Imitation, users are easily affected by the tags that were previously applied by others to the same page;
- Habit, users re-use tags that they have already used on other pages respect to their background and culture;
- Recommendation, users choose tags that are suggested by a given interface.

The social tagging system, based on multiple users and multiple words available for tagging, is in fact a semantic web application, which has the inherent vocabulary confusion problem leading to a series of limitations and weaknesses. Although author state have inferred that users could imitate the choices of tags applied by others, different tags used by different people for the same resource can still be present in the absence of a vocabulary control and without a standard to restrict user's tagging action. In fact, untrained people always use different form of words for their personal use, even one person himself also changes his own idea about tagging (and words available for tagging) over time. Therefore, tags have been noted to be inaccurate and leading to various ambiguities.

IV. METHODOLOGY

Several recommendation systems use a hybrid approach by combining collaborative and content-based methods, which helps to avoid certain limitations of content-based and collaborative systems. Different ways to combine collaborative and content-based methods into a hybrid recommender system can be classified as follows:

- Implementing collaborative and content-based methods separately and combining their predictions,
- Incorporating some content-based characteristics into a collaborative approach,
- Incorporating some collaborative characteristics into a content-based approach, and
- Constructing a general unifying model that incorporates both content-based and collaborative characteristics.

Adding Content-Based Characteristics to Collaborative Models Several hybrid recommender systems, including Fab and the "collaboration via content" approach, described in are based on traditional collaborative techniques but also maintain the content-based profiles for each user. These content-based profiles, and not the commonly rated items, are then used to calculate the similarity between two users. Recommender systems made significant progress over the last decade when numerous content-based, collaborative, and hybrid methods were proposed and several "industrial strength" systems have been developed. However, despite all of these advances, the current generation of recommender systems surveyed in this paper still requires further improvements to make recommendation methods more effective in a broader range of applications.

Collaborative tagging is currently an extremely popular online service. Although nowadays it is basically used to support resource search and browsing, its potential is still to be exploited. One of these potential applications is the provision of web access functionalities such as content filtering and discovery. For this to become a reality, however, it would be necessary to extend the architecture of current collaborative tagging services so as to include a policy layer that supports the enforcement of user preferences. On the other hand, as collaborative tagging has been gaining popularity, it has become more evident the need for privacy protection; not only because tags are sensitive information per se, but also because of the risk of cross referencing. In a nutshell, collaborative tagging would also benefit from a layer helping users protect their privacy.

A. Tagging And Taxonomy

Collaborative tagging describes the process by which many users add metadata in the form of keywords to shared content. Recently, collaborative tagging has grown in popularity on the web, on sites that allow users to tag bookmarks, photographs and other content. In this study analyze the structure of collaborative tagging systems as well as their dynamical aspects. Specifically, discovered regularities in user activity, tag frequencies, kinds of tags used, bursts of popularity in book marking and a remarkable stability in the relative proportions of tags within a given UR and present a dynamical model of collaborative tagging that predicts these stable patterns and relates them to imitation and shared knowledge.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

Collaborative tagging describes the process by which many users add metadata in the form of keywords to shared content. Proponents of collaborative tagging, typically in the web logging community, often contrast tagging-based systems from taxonomies. While the latter are hierarchical and exclusive, the former are non-hierarchical and inclusive. Familiar taxonomies include the Linnaean system of classifying living things, the Dewey decimal classification for libraries, and computer file systems for organizing electronic files. In such systems, each animal, book, file and so on, is in one unambiguous category which is in turn within a yet more general one.

The Tag desirable properties of a good tagging system, which include: (a) high coverage of multiple facets, (b) high popularity, and (c) least-effort. Faceted and generic tags can facilitate the aggregation of objects entered by different users. It makes discovery and recovery of tagged content easier. Tags used by a large number of people for a given object are less likely to be spam and more likely to be used by a new user for the same object. Least-effort has two meanings: The number of objects identified by the suggested tags should be small, and the number of tags for identifying an object should be minimized as well. This enables efficient recovery of the tagged objects.

Propose collaborative tagging techniques that suggest tags for an object based on what other users use to tag the object. This not only addresses the vocabulary divergence problem, but also relieves users the obnoxious task of having to come up with a good set of tags.

Propose a reputation score for each user based on the quality of the tags contributed by the user. By introducing the notion of “virtual” users, our tag suggestion algorithm incorporates not only user-generated tags but also other sources of tags. Adding semantics to the e-learning contents on the web can provide several benefits to the users:

- Provide a more accessible contents for the blind and visually impaired individuals, as the contents can be read by screen readers.
- Easier searching for technical and educational materials.
- The contents can be explained (e.g., using other students annotations or from relations between other contents).
 - Help people with learning disabilities in navigating the e-learning contents (e.g., providing information about a concept in the navigated e-learning as a tooltip).
 - According to (Bateman, 2007) collaborative tagging systems have potential to be a good fit with e-learning systems, because of the following:
- Learning managements systems currently lack sufficient support for self organization of learning content.
- Collaborative tagging has potential to further enrich peer interactions and peer awareness centered on learning content.
- Tagging, by its nature is a reflective practice, which can give students an opportunity to summarize new ideas, while receiving peer support (through viewing other learners' tags; tag suggestions).

The information provided by tags provides insight on learner's comprehension and activity, which is useful for both educators and administrators.

B. Tag Suppression

In our scenario of collaborative tagging, users tag resources on the web, for example, music, pictures, videos or bookmarks, according to their personal preferences. Users therefore contribute to describe and classify those resources, but this is inevitably at the expense of revealing their profile. To avoid being accurately profiled by tagging systems or in general by any attacker able to collect such information, users may adopt a privacy-enhancing technology based on data perturbation. The data-perturbative technology considered in this work is tag suppression, a technique that allows a user to refrain from tagging certain resources in such a manner that the profile resulting from this perturbation does not capture their interests so precisely.

Proposed system conceptually simple technique protects user privacy to a certain degree, but at the cost of the semantic loss incurred by suppressing tags. Other approaches based on data perturbation include the submission of false tags. For example, a user wishing to tag the webpage www.mentalhelp.net with “depression” could use the tag “sports” instead, to conceal their interest for this resource. In doing so, the user distorts their actual profile, although at the expense of a far greater impact on semantic functionality than suppression does resources are assigned tags that do not describe, in principle, the actual content of such resources.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

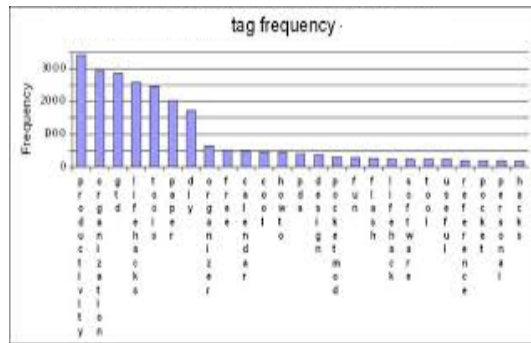


Fig 4.1 Histogram of relative frequencies of tags

A more intelligent form of tag perturbation consists in replacing (specific) user tags with (general) tag categories. In conceptual terms, and resorting to the example above, the user would use the tag “health” instead of “depression.” In this manner, the user would hide, to a certain extent, their genuine interest in that resource, but clearly at the cost of some vagueness or inaccuracy in the description of that webpage.

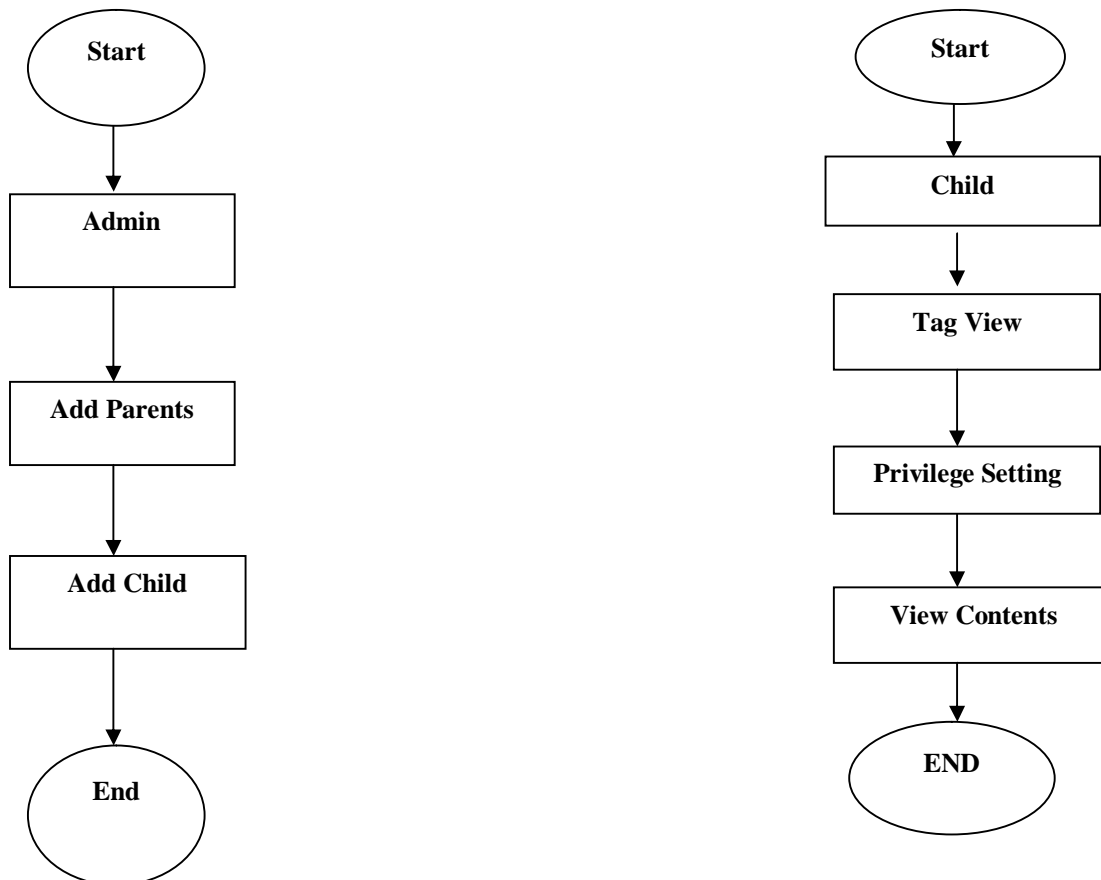


Fig 4.2 Histogram Tags

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

C. Advantage of Collaborative Methodology

In social network, users can allow friends to access their data, depending on their personal endorsement and privacy requirements. Although social network currently provide simple access control mechanisms allowing users to lead access to information contained in their profile, users unfortunately have no control over data. If a user posts a comment in a friend's space cannot specify which users can view the comment. In another case, when a user uploads a photo and tags friends who appear in the photo, the tagged friends cannot restrict who can see this photo, even though the tagged friends may have different privacy about the photo. The existing system introduces two strategies.

- Policies for resource recommendation
- Policies for parental control

Policies for resource recommendation: Suppose that Carol (C) is interested in literature, but not in resources concerning science-fiction. C realizes that the relevant tag categories are c1 ("books") and c2 ("literary criticism"), and she decides that the resources she is interested in are those associated with not less than 40 percent of the tags in either c1 or c2. In contrast, C finds out that the tag category that corresponds to the resources she is not interested in is c3 ("science-fiction, fantasy"), and she decides to discard all the resources associated with not less than 20 percent of the tags in c3. Consequently, C specifies the following policies:

- $pol1 = (\{(c1, \square, 0.4)\}, +)$,
- $pol2 = (\{(c2, \square, 0.4)\}, +)$,
- $pol3 = (\{(c3, \square, 0.2)\}, -)$

Suppose now that there exists a resource R1, which satisfies content constraints $(c1, \square, 0.4)$, $(c2, \geq, 0.4)$, and $(c3, \geq, 0.2)$. In such a case, there exists a conflict, since all policies pol1, pol2, and pol3 apply. According to the conflict resolution mechanism, policy pol3 prevails over policies pol1 and pol2, since the latter are positive policies. Consequently, resource R1 is marked as irrelevant to C.

Policies for parental control: Suppose that Alice (A) would like to enable a web filter for her son Bob (B) by granting him access only to contents specifically tailored for children. By checking the available tag categories, she realizes that the suitable one is c4: "entertainment for children." She then decides that resources suitable to children are those associated with not less than 60 percent of the tags from category c4. Moreover, just to be sure that no harmful content is accessed, she also would like to prevent access to "entertainment" resources that may include any content for adults. To achieve this, A specifies the following policies:

- $pol4 = (\{(c4, \geq, 0.6)\}, +)$,
- $pol5 = (\{(c5, \geq, 0.1)\}, -)$ where c5 is the tag category corresponding to "entertainment for adults."

Suppose now that B requests access to a resource R2 which satisfies both content constraints $(c4, \square, 0.6)$ and $(c5, \square, 0.1)$. In such a case, there exists a conflict, since both policies pol4 and pol5 apply. According to the conflict resolution mechanism, policy pol5 prevails over pol4 because pol5 is a negative policy. Consequently, Bob is denied access to resource R2.

- Full prototype is not developed for the experimented system.
- Tags are prepared for single language (English) only.
- Tags are generalized in single level. i.e., one common word for one tag. For example, to reduce the sensitivity of the work 'depression' the word 'health' is used.

IV. CONCLUSION AND FUTURE ENHANCEMENT

In this paper survey of Adaptive Privacy Policy Prediction (A3P) system that helps users automate the privacy policy settings for their uploaded images. The A3P system provides a comprehensive framework to infer privacy preferences based on the information available for a given user. In this project also effectively tackled the issue of cold-start, leveraging social context information. The experimental study proves that the A3P is a practical tool that offers significant improvements over current approaches to privacy. It helps the user to secure their account details and images they share. They have the options to set the persons who can see their information such as image and text they share.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

This paper future includes the option to set the file size limit. The user of the account can set the file size according to their needs. There is no need to make the configuration settings each time when the user logged into the account. Automatic configuration setting is included.

- One of these potential applications is the provision of web access functionalities such as content filtering and discovery.
- For this to become a reality, however, it would be necessary to extend the architecture of current collaborative tagging services so as to include a policy layer that supports the enforcement of user preferences.
- Collaborative tagging has been gaining popularity, it have been become more evident the need for privacy protection; not only because tags are sensitive information but also because of the risk of cross referencing

REFERENCES

- [1] A. Abhari and M. Soraya, "Workload generation for youtube," *Multimedia Tools and Applications*, vol. 46, no. 1, pp. 91–118, 2010.
- [2] M. Barbera, J. Stefa, A. Viana, M. de Amorim, and M. Boc, "Vip delegation: Enabling vips to offload data in wireless social mobile networks," in *DCOSS'11*. IEEE, 2011, pp. 1–8.
- [3] C. Boldrini, M. Conti, and A. Passarella, "Contentplace: socialaware data dissemination in opportunistic networks," in *Proceedings of the 11th international symposium on Modeling, analysis and simulation of wireless and mobile systems*. ACM, 2008, pp. 203–210.
- [4] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, and J. Scott, "Impact of human mobility on opportunistic forwarding algorithms," *Mobile Computing, IEEE Transactions on*, vol. 6, pp. 606–620, 2007.
- [5] G. Chen and F. Rahman, "Analyzing privacy designs of mobile social networking applications," in *IEEE/IFIP EUC'08*, vol. 2. IEEE, 2008, pp. 83–88.
- [6] T. Chen, M. A. Kaafar, and R. Boreli, "The where and when of finding new friends: Analysis of a location-based social discovery network." in *ICWSM*, 2013.
- [7] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," *Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09)*, pp. 199-212, 2009.
- [8] Y. Zhang, A. Juels, M.K.M. Reiter, and T. Ristenpart, "Cross-VM Side Channels and Their Use to Extract Private Keys," *Proc. ACM Conf. Computer and Comm. Security (CCS '12)*, pp. 305-316, 2012.
- [9] J. Somorovsky, M. Heiderich, M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, "All Your Clouds Are Belong to Us: Security Analysis of Cloud Management Interfaces," *Proc. Third ACM Workshop Cloud Computing Security Workshop (CCSW '11)*, pp. 3-14, 2011.
- [10] S. Bugiel, S. Nünberger, T. Pöppelmann, A.-R. Sadeghi, and T. Schneider, "AmazonIA: When Elasticity Snaps Back," *Proc. 18th ACM Conf. Computer and Comm. Security (CCS '11)*, pp. 389-400, 2011.
- [11] G. Danezis and B. Livshits, "Towards Ensuring Client-Side Computational Integrity (Position Paper)," *Proc. ACM Cloud Computing Security Workshop (CCSW '11)*, pp. 125-130, 2011.
- [12] S. Groß and A. Schill, "Towards User Centric Data Governance and Control in the Cloud," *Proc. IFIP WG 11.4 Int'l Conf. Open Problems in Network Security (iNetSec)*, pp. 132-144, 2011.
- [13] M. Burkhart, M. Strasser, D. Many, and X. Dimitropoulos, "SEPIA: Privacy-Preserving Aggregation of Multi-Domain Network Events and Statistics," *Proc. USENIX Security Symp.*, pp. 223-240, 2010.
- [14] D. Hubbard and M. Sutton, "Top Threats to Cloud Computing V1.0," *Cloud Security Alliance*, <http://www.cloudsecurityalliance.org/topthreats>, 2010.
- [15] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. A view of cloud computing. *Commun. ACM*, 53(4):50–58, 2010.
- [16] P. England and J. Manfredelli. Virtual machines for enterprise desktop security. *Information Security Technical Report*, 11(4):193 – 202, 2006.
- [17] T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum, and D. Boneh. Terra: a virtual machine-based platform for trusted computing. In *ACM Symposium on Operating Systems Principles*, pages 193–206. ACM, 2003.
- [18] O. Acii, cmez. Yet another microarchitectural attack: Exploiting I-cache. In *ACM Workshop on Computer Security Architecture*, pages 11–18, October 2007.
- [19] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage. Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds. In *16th ACM Conference on Computer and Communications Security*, pages 199–212, 2009.
- [20] J. Callas, L. Donnerhacke, H. Finney, and R. Thayer. Openpgp message format. Technical report, RFC 2440, November, 1998.
- [21] McIntosh, M., and Austel. P. XML Signature Element Wrapping attacks and Countermeasures. In *SWS '05: Proceedings of the 2005 workshop on Secure web services (New York, NY, USA, 2005)*, ACM Press, pp. 20-27.
- [22] Nadalin, A., Kaler, C., Monzillo, R., and Hallam-Baker, P. Web Services Security: SOAP Message Security 1.1 (WS-Security 2004). *OASIS Standard Specification (2006)*.