ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Human Effects to Enhance Clustering Techniques That Assists User in Grouping the Friends

S. Srigowthem[1], K.G.S Venkatesan[2], Sourav Kumar Nag[3], Suraj Raj[4]

Assistant Professor, Dept. of C.S.E., Bharath University, Chennai, Tamil Nadu, India[1].

Associate Professor, Dept. of C.S.E., Bharath University, Chennai, Tamil Nadu, India[2].

Dept. of C.S.E., Bharath University, Chennai, Tamil Nadu, India[3].

Dept. of C.S.E., Bharath University, Chennai, Tamil Nadu, India[4].

ABSTRACT: We enhance existing and introduce new social network privacy management models and that we live their human effects. First, we tend to introduce a mechanism exploitation tried cluster techniques that assists users in grouping their friends for ancient group- based mostly policy management approaches. we tend to found measurable agreement between clusters and user-defined relationship teams. Second, we tend to introduce a replacement privacy management model that leverages users' memory and opinion of their friends (called example friends) to line policies for different similar friends. Finally, we tend to explore completely different techniques that aid users in choosing example friends. we tend to found that by associating policy temples with example friends (versus cluster labels), users author policies a lot of expeditiously and have improved perceptions over ancient group-based policy management approaches. additionally, our results show that privacy management models may be additional increased by utilizing user privacy sentiment for mass customization. By police work user privacy sentiment (i.e., AN unconcerned user, a pragmatist or a fundamentalist), privacy management models may be mechanically tailored specific to the privacy sentiment and desires of the user.

KEYWORDS: Policy, human factors, privacy, access control, social network, Clasuet Newman Moore (CNM) Model.

I. INTRODUCTION

Social networks is additionally an incredible quantity of user profile knowledge and content on-line. .Nobody is virtually forced to hitch an internet social network, and most networks we all know regarding encourage, however don't force users to reveal - for example - their dates of birth, their cellular phone numbers, or wherever they presently live [2]. And yet, one cannot facilitate however marvel at the character, amount, and detail of the non-public data some users offer, and chew over however knowing this data sharing is. dynamical cultural trends, familiarity and confidence in digital technologies, lack of exposure or memory of conspicuous misuses of non-public knowledge by others could all play a job during this new development of knowledge revelation [5]. Yet, on-line social networks' security and access controls area unit weak by choice - to leverage their price as network product and enhance their growth by creating registration, access, and sharing of knowledge uncomplicated. At constant time, the prices of mining and storing knowledge still decline. Combined, the 2 options imply that data provided even on on the face of it non-public social networks is, effectively, public knowledge, that might exist for as long as Associate in Nursing body has an incentive to take care. Given the widespread adoption of SNSs, the increasing public scrutiny of on-line behavior, and also the policy implications encompassing privacy on the web a lot of usually, it's stunning that few empirical knowledge are collected on the privacy practices of today's SNS users [1]. Moreover, the selection of a privacy level will itself be seen as Associate in Nursing act of intrinsic interest, expressing a private style. Here, we tend to analyze the privacy preferences.

After providing background on the protection choices accessible on Facebook, we tend to posit 2 forms of mechanisms by that a private could adopt a ‘‘private’’ profile and develop four hypotheses to assess these mechanisms [3]. In our initial section of results, we tend to check these hypotheses by analyzing behavioural, demographic, and cultural knowledge from a brand new social network dataset [6]. In our second section of results, we tend to expand upon these findings with a close exploration of the particular cultural preferences that tend to be related to ‘‘the style for privacy”. we tend to conclude by indicating the relevancy of this paper for the longer term study of privacy and on-line behaviour [4].

For example, on Facebook, there area unit over thirty billion items of content shared every month. New content is being further each day; a mean Facebook user generates over ninety items of content every month. this massive quantity of content as well as the many range of users on-line makes maintaining acceptable levels of privacy terribly difficult. variety of conclusions will be drawn from these studies. First, there area unit varied levels of privacy controls, counting on the web web site [10]. For instance, some sites create on the market user profile information to the web with no ability to limit access. Where as different sites limit user profile viewing to merely trustworthy friends. different studies introduce the notion of the privacy contradiction in terms, the link between individual privacy intentions to disclose their personal info and their actual behaviour [12]. Individuals voice considerations over the dearth of adequate controls around their privacy info where as freely providing their personal information. different analysis concludes that people lack acceptable info to form up on privacy selections [15] . Moreover, once there's adequate info, short advantages area unit typically opted over semi permanent privacy. However, contrary to common belief, individuals area unit involved regarding privacy . however managing ones privacy will be difficult [9]. This may be attributed to several things, for instance, the dearth of privacy controls on the market to the user, the complexness of exploitation the controls, and also the burden related to managing these controls for giant sets of users [20].

II. LITERATURE SURVEY

R. McMillan, proposed that “Google Buzz Criticized for Disclosing Gmail Contacts. This paper considers routing to parallel queues in which each queue has its own single server, and service times are exponential with non-identical parameters [19]. We give conditions on the cost function such that the optimal policy assigns customers to a faster queue when that server has a shorter queue. The queues may have nite buyers, and the arrival process can be controlled and can depend on the state and routing policy. Hence our results on the structure of the optimal policy are also true when the assigning control is in the "last" node of a network of service centers. Using dynamic programming we show that our optimality results are true in distribution [17].

Acquistic and R. Gross, proposed that “Imagined Communities: Awareness, Information Sharing and Privacy on the Facebook [25]. The prevalence of dynamic-content web services, exemplified by *search* and *online social networking*, has motivated an increasingly wide web-facing front end. Horizontal scaling in the Cloud is favored for its elasticity, and distributed design of load balancers is highly desirable [28].

J. Bonneau and S. Preibusch, proposed that “The Privacy Jungle: On the Market for Data Protection in Social Networks [24]. The most critical property exhibited by a heavy-tailed workload distribution(found in many WWW workloads) is that a very small fraction of tasks make up a large fraction of the workload, making the load very difficult to distribute in a distributed system [30]. Load balancing and load sharing are the two predominant load distribution strategies used in such systems. Load sharing generally has better re- sponse time than load balancing because the latter can exhibit excessive overheads in selecting servers and partitioning tasks.

H. Krasnova, O. Gu¨ nther, S. Spiekermann, and K. Koroleva, proposed that “Privacy Concerns and Identity in Online Social Networks [32], ”We carry out a longitudinal study of evolution of small-time scaling behavior of Internet traffic on the MAWI dataset spanning years. MAWI dataset contains a number of anomalies which interfere with the correct identification of scaling behavior, and hence to mitigate these effects, we use a sketch-based procedure for robust estimation of scaling exponent [34]. We first show the importance of robust estimation procedure while studying small-time scaling behavior of Internet traffic. With affordable infrastructure provided by the Cloud, an increasing variety of dynamic-content web services, including search, social networking and e-commerce, are offered via the cyber space. For all service-oriented applications, short response time is crucial for a quality user experience [36].

C. Dwyer, S.R. Hiltz, and K. Passerini, we proposed that Users' mental models of privacy and visibility in social networks often involve natural subgroups, or communities, within their local networks of friends [35]. Such groupings are not always explicit, and existing policy comprehension tools, such as Facebook's Audience View, which allows the user to view her profile as it appears to each of her friends, are not naturally aligned with this mental model.

R. Dhamija and A. Perrig, we proposed that In this paper, we introduce PViz, an interface and system which corresponds more directly with the way users model groups and privacy policies applied to their networks [21]. PViz allows the user to understand the visibility of her profile according to natural sub-groupings of friends, and at different levels of granularity. We conducted an extensive user study comparing Despite requiring users to adapt to new ways of exploring their social spaces, our study revealed that PViz was comparable to Audience View for simple tasks, and provided a significant improvement for more complex, group based tasks [26].

J. Bonneau and S. Preibusch, we proposed that In this paper, we compare the impact of two different privacy policy representations – Audience View and Expandable Grids – on users modifying privacy policies for a social network site. Despite the very different interfaces, were very few differences in user performance. However, users had clear, and different, preferences and acknowledged the tradeoffs between the two representations [29]. Our results imply that while either interface would be a usable option for policy settings, a combination may appeal to a wider audience and offer the best of both worlds.

Bonneau and S. Preibusch we proposed that The rapid growth of contemporary social network sites (SNSs) has coincided with an increasing concern over personal privacy. College students and adolescents routinely provide personal information on profiles that can be viewed by large numbers of unknown people and potentially used in harmful ways. SNSs like Facebook and MySpace allow users to control the privacy level of their profile, thus limiting access [27].

Acquisti and J. Grossklags, we proposed that In this paper, we take the preference for privacy itself as our unit of analysis, and analyze the factors that are predictive of a student having a private versus public profile [48]. Drawing upon a new social network dataset based on Facebook, we argue that privacy behavior is an upshot of both social influences and personal incentives. Students are more likely to have a private profile if their friends and roommates have them; women are more likely to have private profiles than are men; and having a private profile is associated with a higher level of online activity. Finally, students who have private versus public profiles are characterized by a unique set of cultural preferences—of which the ''taste for privacy'' may be only a small but integral part [33].

R. McMillan, we proposed that Over the last few years, social networking has evolved from a service initially only open to American university alumni into a mass, consumer-oriented service [31]. Today, social networking is one of the most-used services on the Internet. Facebook, the flagship of social network services, now has more than 955 million users around the world1 and is the second most popular website in the world, according to Alexa2. The importance of LinkedIn, a professional social networking service, in enhancing the way people connect professionally, maintain business relationships, and attract new hires is growing significantly. Twitter, the micro-blogging service, is considered one of the key media channels that brands and companies should be addressing. Social networking websites play a growing role as communication platforms and, for some digital natives, Facebook and others have replaced traditional email or even instant messaging services for daily casual information exchange [51].

III. EXISTINNG SYSTEM

Many current social networking platforms offer a simple policy management approach. Security aware users are able to specify policies for their profile objects. For example, my work colleague is restricted from seeing my photos. But my trusted best friend from school may access all my information. Facebook provides an optional mechanism that allows users to create custom lists to organize friends and set privacy restrictions [43]. Similarly, Google+ allows users to create Circles of friends, such as family, acquaintances, and so on, where the user can apply policies based on these Circles. Facebook also has smart lists that automatically group friends who live nearby or attend the same school. However, managing access for hundreds of friends is still a very difficult and burdensome task security unaware users typically follow an open and permissive default policy. Large amount of content coupled with the significant number of users online makes maintaining appropriate levels of privacy very challenging. Lack of privacy controls and the security of content are very less. Measuring human efforts is very difficult. All groups are mingled the users not to give the any privacy levels.

IV. PROPOSED SYSTEM

We introduce three new improvements to privacy management models:
1. Assisted Friend Grouping—an incremental improvement to traditional group-based policy management.
2. Same-As Policy Management—a new paradigm improvement over traditional group-based policy management.
3. Example Friend Selection—an incremental improvement to Same-As Policy Management.
i)Assisted Friend Grouping leverages proven clustering techniques to aid users in grouping their friends more effectively and efficiently. We found measurable agreement between clusters and user-defined relationship groups.
ii)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 [47]. Users are thinking of people, not groups. Using a visual policy editor that takes advantage of friend recognition and minimal task interruptions

iii)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.
Our model leverages a user's memory and opinion of their friends to set policies for other similar friends. Studies have shown that users perform more efficiently using recognition-based approaches that have minimal task interruptions . Measuring their human effects [44]. User simply leverages their memory and opinion of a friend to set policies for other similar friends. Traditional group-based policy management, which assists users in grouping their friends more efficiently. Large amount of content to easily maintained I in many group levels. Security is very high, each group to give privacy levels

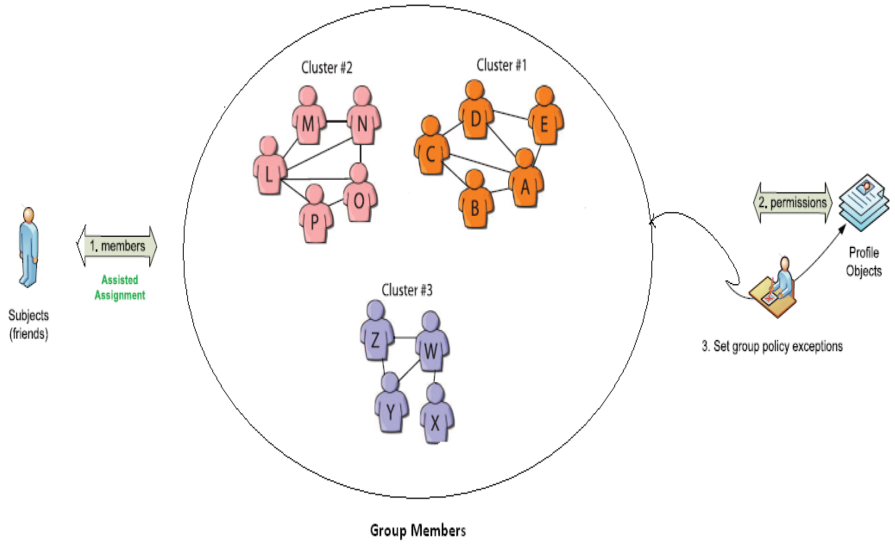

Fig 1: Architecture diagram of Group Members, self group policy exception.

V. MODULES

A. Group-Based Policy Management :

We introduce a user-assisted friend grouping mechanism that enhances traditional group-based policy management approaches. In Figure 1, the Assisted Friend Grouping leverages proven clustering techniques to aid users in grouping their friends more effectively and efficiently [41]. We found measurable agreement between clusters and user-defined relationship groups. In addition, user perceptions of our improvements are encouraging. We introduce 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. We found measurable agreement between clusters and user-defined relationship groups. In addition, user perceptions of our improvement are encouraging [38].

B. Assign Group permission :

We introduce a new privacy management model that is an improvement over traditional group based policy management approaches [37]. Our 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 [39]. This allows users to be more selective and careful in assigning permissions. Users are thinking of people, not groups. Using a visual policy editor 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. In group-based policy management, the user must first group their friends. After which, they must select group permissions (setting the group policy). Finally, friend-level exceptions to the group policy are set [40]. A user's attention (mental model) is focused in multiple areas. Whereas in Same-As Policy Management, the user's attention is focused on a specific friend. Users leverage their memory and opinion of a friend to set policies for other like friends. In essence, we use a friend recognition approach, with minimal task interruptions, to aid the user in setting policies. A representative friend is selected (same-as example friend), profile object permissions are assigned to this example friend and other similar friends (same-as friends) are associated with the same set of object permissions [42].

C. Example Friend Selection :

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 [45]. We detect user privacy sentiment that can be leveraged to further enhance privacy management models. For example, Unconcerned Users who author more open policies may leverage a less flexible coarse-grained privacy management approach. Whereas a Fundamental list, who authors more conservative policies, will find a fine-grained approach better suited for meeting their privacy needs. Privacy management models can be further refined and enhanced by detecting and leveraging user privacy sentiment [46].

D. Visual policy :

The visual policy uses three approaches for assisting users in selecting their same-as example friend: Random, CNM Order, and Sample CNM Order. Random presents friends to the user in random order. Both the CNM Order and Sample CNM Order approaches leverage the CNM network clustering algorithm. Our prototype clusters the user's social network graph creating CNM clusters of friends [49].

CNM Order, we present the user's friends in CNM cluster order, i.e., all the friends in Cluster #1 are presented to the user followed by all the friends in Cluster#2, and so on. The first friend presented for each cluster is the friend with the highest degree (friend with the highest number of friend connections) in that cluster [50]. This friend is the same-as example friend for that cluster. The premise is the highly connected friends are potentially more well known and thus easier to remember making them good candidates for same as example friends. Sample CNM Order, we present all of the friends with the highest degree within their cluster first. These friends are highly connected and are potentially more well known and, thus, easier to remember making them good candidates for Same-As Example Friends [53].

VI. CONCLUSION AND FUTURE WORK

In this paper, we tend to enhance existing and introduce new privacy management models, additionally to mensuration their human effects. First, we tend to gift AN improvement to ancient group-based policy management, that assists users in grouping their friends a lot of expeditiously [52]. With assisted Friend Grouping, we tend to found measurable agreement between clusters and user-defined relationship teams. Second, we tend to introduce Same-As Policy Management, that leverages users' memory and opinion of their example friends to line policies for alternative similar friends. Finally, we tend to introduce 2 techniques for aiding users in choosing their example friends. By associating policy templates with friends versus cluster labels, Same-As Policy Management allowed users to author policies a lot of expeditiously and was a lot of absolutely perceived over ancient cluster based mostly policy management.

Our future work plans embrace running further studies and comparison the 2 CNM-based policy management model enhancements (Assisted Friend Grouping and Example Friend Selection) in terms of policy definition, openness, and their human effects. additionally, we have a tendency to arrange to more investigate patterns in alignment of clusters and user-defined relationship teams. we have a tendency to conjointly arrange to develop a epitome that leverages user privacy sentiment for the mass customization of a privacy management model..

VII. ACKNOWLEDGEMENT

The author would like to thank the Vice Chancellor, Dean-Engineering, Director, Secretary, Correspondent, HOD of Computer Science & Engineering, Dr. K.P. Kaliyamurthie, Bharath University, Chennai for their motivation and constant encouragement. The author would like to specially thank **Dr. A. Kumaravel** for his guidance and for critical review of this manuscript and for his valuable input and fruitful discussions in completing the work and the Faculty Members of Department of Computer Science &Engineering. Also, he takes privilege in extending gratitude to his parents and family members who rendered their support throughout this Research work.

REFERENCES

1. A. Acquisti and R. Gross, "Imagined Communities: Awareness, Information Sharing and Privacy on the Facebook," Proc. Sixth Int'l Conf. Privacy Enhancing Technologies (PET '06), 2006.
2. A. Acquisti and J. Grossklags, "Privacy and Rationality in Individual Decision Making," IEEE Security & Privacy, Vol. 3, No. 1, PP. 26-33, Jan./Feb. 2005.
3. A. Besmer, J. Watson, and H.R. Lipford, "The Impact of Social Navigation on Privacy Policy Configuration," Proc. Symp. Usable Privacy and Security, 2010.
4. J. Bonneau and S. Preibusch, "The Privacy Jungle: On the Market for Data Protection in Social Networks," Proc. Workshop the Economics of Information Security (WEIS '09), 2009.
5. B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham, "A Semantic Web Based Framework for Social Network Access Control," Proc. Symp. Access Control Models and Technologies, 2009.
6. B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, and B.M. Thuraisingham, "Semantic Web-Based Social Network Access Control," computers & Security, vol. 30, pp. 108-115, 2011.
7. K.G.S. Venkatesan. Dr. V.Khanna, Dr. A.Chandrasekar, "Autonomous system for mesh network by using packet transmission & failure detection", Inter. Journal of Innovative Research in computer & comm. Engineering, Vol. 2, Issue 12, PP. 7289 – 7296, December - 2014.
8. Teerawat Issariyakul, Ekram Hoss, "Introduction to Network Simulator".
9. K.G.S. Venkatesan and M. Elamurugaselvam, "Design based object oriented Metrics to measure coupling & cohesion", International journal of Advanced & Innovative Research, Vol. 2, Issue 5, pp. 778 – 785, 2013.
10. S. Sathish Raja and K.G.S. Venkatesan, "Email spam zombies scrutinizer in email sending network Infrastructures", International Journal of Scientific & Engineering Research, Vol. 4, Issue 4, PP. 366 – 373, April 2013.
11. G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," IEEE J. Sel. Areas Commun., Vol. 18, No. 3, pp. 535–547, March - 2000.
12. K.G.S. Venkatesan, "Comparison of CDMA & GSM Mobile Technology", Middle-East Journal of Scientific Research, 13 (12), PP. 1590 – 1594, 2013.
13. P. Indira Priya, K.G.S.Venkatesan, "Finding the K-Edge connectivity in MANET using DLTRT, International Journal of Applied Engineering Research, Vol. 9, Issue 22, PP. 5898 – 5904, 2014.

14. Y. Cheng, J. Park, and R.S. Sandhu, "A User-to-User Relationship- Based Access Control Model for Online Social Networks," Proc. 26th Ann. IFIP WG 11.3 Conf. Data and Applications Security and Privacy, 2012.

15. A. Clauset, M. Newman, and C. Moore, "Finding Community Structure in Very Large Networks," Physical Rev. E, vol. 70, p. 066111, 2004.

16. E. Cutrell, M. Czerwinski, and E. Horvitz, "Notification, Disruption, and Memory: Effects of Messaging Interruptions on Memory and Performance," Proc. Conf. Human Computer Interaction, 2001.

17. K.G.S. Venkatesan and M. Elamurugaselvam, "Using the conceptual cohesion of classes for fault prediction in object-oriented system", International journal of Advanced & Innovative Research, Vol. 2, Issue 4, PP. 75 – 80, April 2013.

18. Ms. J.Praveena, K.G.S. Venkatesan, "Advanced Auto Adaptive edge-detection algorithm for flame monitoring & fire image processing", International Journal of Applied Engineering Research, Vol. 9, Issue 22, PP. 5797 – 5802, 2014.

19. K.G.S. Venkatesan. Dr. V.Khanna, "Inclusion of flow management for Automatic & dynamic route discovery system by ARS", International Journal of Advanced Research in computer science & software Engg., Vol.2, Issue 12, PP. 1 – 9, December – 2012.

20. Needhu. C, K.G.S. Venkatesan, "A System for Retrieving Information directly from online social network user Link ", International Journal of Applied Engineering Research, Vol. 9, Issue 22, PP. 6023 – 6028, 2014.

21. K.G.S. Venkatesan, R. Resmi, R. Remya, "Anonymizimg Geographic routing for preserving location privacy using unlinkability and unobservability", International Journal of Advanced Research in computer science & software Engineering, Vol. 4, Issue 3, PP. 523 – 528, March – 2014.

22. R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," Proc. USENIX Security Symp., 2000.

23. P. Dunphy, A.P. Heiner, and N. Asokan, "A Closer Look at Recognition-Based Graphical Passwords on Mobile Devices," Proc. Symp. Usable Privacy and Security, 2010.

24. C. Dwyer, S.R. Hiltz, and K. Passerini, "Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and MySpace," Proc. Am. Conf. Information Systems (AMCIS '07), 2007.

25. L. Fang and K. LeFevre, "Privacy Wizards for Social Networking Sites," Proc. Conf. World Wide Web, 2010.

26. Selvakumari. P, K.G.S. Venkatesan, "Vehicular communication using Fvmr Technique", International Journal of Applied Engineering Research, Vol. 9, Issue 22, PP. 6133 – 6139, 2014.

27. K.G.S. Venkatesan, G. Julin Leeya, G. Dayalin Leena, "Efficient colour image watermarking using factor Entrenching method", International Journal of Advanced Research in computer science & software Engg., Vol. 4, Issue 3, PP. 529 – 538, March – 2014.

28. B. Liu, M. Hu, and J. Cheng, "Opinion observer: analyzing and comparing opinions on the web," in Proc. 14th Int'l Conf. on World Wide Web, PP. 342–351, 2008.

29. C. Lin and Y. He, "Joint sentiment/topic model for sentiment analysis," in Proc. 18th ACM Conf. on Information and Knowledge Management, PP. 375–384, 2009.

30. R.Baeze-yates, C.Hurtado, and M.Mendoza, "Query Recommendation exploitation question Logs in Search Engines", *Proc.Int'l Workshop Current Trends in information Technology*, PP. 588-596, 2004.

31. K.G.S. Venkatesan. Kausik Mondal, Abhishek Kumar, "Enhancement of social network security by Third party application", International Journal of Advanced Research in computer science & software Engineering, Vol. 3, Issue 3, PP. 230 – 237, March – 2013.

32. G. Ateniese, S. Kamara, and J. Katz, "Proofs of Storage from Homomorphic Identification Protocols," Proc. 15th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT), PP.. 319-333, 2009.

33. F. Sebe, J. Domingo-Ferrer, A. Martı´nez-Balleste, Y. Deswarte, and J.-J. Quisquater, "Efficient Remote Data Possession Checking in Critical Information Infrastructures", IEEE Trans. Knowledge and Data Eng., Vol. 20,No. 8, PP. 1034-1038, August - 2008.

34. K.G.S. Venkatesan and M. Elamurugaselvam, "Design based object oriented Metrics to measure coupling & cohesion", International journal of Advanced & Innovative Research, Vol. 2, Issue 5, PP. 778 – 785, 2013.

35. Annapurna Vemparala, Venkatesan.K.G., "Routing Misbehavior detection in MANET'S using an ACK based scheme", International Journal of Advanced & Innovative Research, Vol. 2, Issue 5, PP. 261 – 268, 2013.

36. K.G.S. Venkatesan. Kishore, Mukthar Hussain, "SAT : A Security Architecture in wireless mesh networks", International Journal of Advanced Research in computer science & software Engineering, Vol. 3, Issue 3, PP. 325 – 331, April – 2013.

37. Annapurna Vemparala, Venkatesan.K.G., "A Reputation based scheme for routing misbehavior detection in MANET"S ", International Journal of computer science & Management Research, Vol. 2, Issue 6, June - 2013.

38. K.G.S. Venkatesan, "Planning in FARS by dynamic multipath reconfiguration system failure recovery in wireless mesh network", International Journal of Innovative Research in computer & comm. Engineering, Vol. 2, Issue 8, August - 2014.

39. D. Ferraiolo and R. Kuhn, "Role-Based Access Control," Proc. Nat'l Computer Security Conf., 1992.

40. P.W. Fong, "Relationship-Based Access Control: Protection Model and Policy Language," Proc. Conf. Data and Application Security and Privacy, 2011.

41. P.W.L. Fong and I. Siahaan., "Relationship-Based Access Control Policies and Their Policy Languages," Proc. symp. Access Control Models and Technologies, 2011.

42. T. Joachims, "Optimizing Search Engines exploitation Clickthroygh information", *Proc. ACM SIGKDD*, 2002.

43. K.G.S. Venkatesan, "Comparison of CDMA & GSM Mobile Technology", Middle-East Journal of Scientific Research, 13 (12), PP. 1590 – 1594, 2013.

44. Y.Xu,K. Wang, B.Zhang, and Z.Chen, "Privacy-Enhancing personalised net search", *Proc. World Wide Web(WWW) Conf.*, 2007.

45. K.G.S. Venkatesan and M. Elamurugaselvam, "Using the conceptual cohesion of classes for fault prediction in object-oriented system", International journal of Advanced & Innovative Research, Vol. 2, Issue 4, PP. 75 – 80, April - 2013.

46. C. Mohan and H. Pirahesh, "ARIES-RRH: Restricted Repeating of History in the ARIES Transaction Recovery Method", In *ICDE*, PP. 718–727, 1991.

47. K.G.S Venkatesan, D. Priya, "Secret-Key generation of Mosaic Image", Indian Journal of Applied Research, Vol. 3, Issue 6, PP. 164-166, June - 2013.

48. R. Karthikeyan, K.G.S. Venkatesan, M.L. Ambikha, S. Asha, "Assist Autism spectrum, Data Acquisition method using Spatio-temporal Model", International Journal of Innovative Research in computer & comm. Engineering, Vol. 3, Issue 2, PP. 871 – 877,

February - 2015.

49. K.G.S. Venkatesan and M. Elamurugaselvam, "Design based object oriented Metrics to measure coupling & cohesion", International journal of Advanced & Innovative Research, Vol. 2, Issue 5, PP. 778 – 785, 2013.

50. G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. Int'l Conf. Security and Privacy in Comm. Networks (SecureComm '08), PP. 1-10, 2008.

51. K.G.S. Venkatesan, AR. Arunachalam, S. Vijayalakshmi, V. Vinotha, "Implementation of optimized cost, Load & service monitoring for grid computing", International Journal of Innovative Research in computer & comm. Engineering, Vol. 3, Issue 2, PP. 864 – 870, February – 2015.

52. L. Hubert and P. Arabie, "Comparing Partitions," J. Classification, vol. 2, pp. 193-218, 1985.

53. S.T. Iqbal and B.P. Bailey, "Investigating the Effectiveness of Mental Workload As a Predictor of Opportune Moments for Interruption," Proc. Computer Human Interaction Extended Abstracts on Human Factors in Computing Systems (CHI '05), 2005.