International Journal of Early Childhood Special Education (INT-JECSE)
DOI:10.48047/INTJECSE/V15I4.97 ISSN: 1308-5581 Vol 15, Issue 04 2023

PROTECTING USER DATA IN PROFILE MATCHING SOCIAL NETWORKS

Mrs. P. VIJAYA LAKSHMI
vijayalakshmi.p@sreyas.ac.in
ASSISTANT PROFESSOR
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SREYAS INSTITUTE OF ENGINEERING AND TECHNOLOGY

M. ANIL KUMAR
malegonianilkumar@gmail.com
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SREYAS INSTITUTE OF ENGINEERING AND TECHNOLOGY

THOKALI MAHESH
thokalimahesh382@gmail.com
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SREYAS INSTITUTE OF ENGINEERING AND TECHNOLOGY

VANGAPALLI VINITH KUMAR
vangapallivinith@gmail.com
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SREYAS INSTITUTE OF ENGINEERING AND TECHNOLOGY

MOHAMMED ANUSS PASHA
annupasha6@gmail.com
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SREYAS INSTITUTE OF ENGINEERING AND TECHNOLOGY

ABSTRACT
In this paper, we consider a scenario where a user queries a user profile database, maintained by a social networking service provider, to identify users whose profiles match the profile specified by the querying user. A typical example of this application is online dating. Most recently, an online dating website, Ashley Madison, was hacked, which results in disclosure of a large number of dating user profiles. This data breach has urged researchers to explore practical privacy protection for user profiles in a social network. In this paper, we propose a privacy-preserving solution for profile matching in social networks by using multiple servers. Our solution is built on homomorphic encryption and allows a user to find out matching users with the help of multiple servers without revealing to anyone the query and the queried user profiles in clear. Our solution achieves user profile privacy and user query privacy as long as at least one of the multiple servers is honest. Our experiments demonstrate that our solution is practical...

INTRODUCTION
Matching two or more users with related interests is an important and general problem, applicable to a wide range of scenarios including job hunting, friend finding, and dating services. Existing on-line matching services require participants to trust a third party server with their preferences. The matching server has thus full knowledge of the users' preferences, which raises privacy issues, as the server may leak (either intentionally, or accidentally)users' profiles. When signing up for an online matching service, a user creates a "profile" that others can browse. The user may be asked to reveal details, such as age, sex, education, profession, number of children, religion, geographic location, sexual proclivities, drinking behavior, hobbies, income, religion, ethnicity, drug use, home and work addresses, favorite places. Even after an account is canceled, most online matching sites may retain such information.
Users' personal information may be re-disclosed not only to prospective matches, but also to advertisers and, ultimately, to data aggregators who use the data for purposes unrelated to online

matching and without customer consent. In addition, there are risks such as scammers, sexual predators, and reputational damage that come along with using online matching services. Many online matching site stake short cuts with respect to safeguarding the privacy and security of their customers. Often they use counterintuitive "privacy" settings, and their data management systems have serious security flaws. In July 2015, "The Impact Team" group stole user data from Ashley Madison, a commercial website billed as enabling extramarital affairs.

The group then threatened to release users' namesand personal identification information if Ashley Madison was not immediately shut down. On 18 and 20 August 2015, the group leaked more than25 giga bytes of company data, including user details. Because of the site's policy of not deleting users' personal information, including real names, home addresses, search history and credit card transaction records, many users feared being publicly shamed. Amain challenge is thus how to protect privacy of user profiles in social networks. So far, the best solution is through encryption, i.e., users encrypt their profiles before uploading them onto social networks. However, when user profiles are encrypted, it is challenging to perform matching. In this paper, we consider a scenario where a user queries a user profile database, maintained by a social networking service provider, to find out other users whose profiles are similar to the profile specified by the querying user. A typical example of this application is online dating. We give a privacy-preserving solution for user profile matching in social networks by using multiple servers. Our basic idea can be summarized as follows. Before uploading his/her profile to a social network, each user encrypts the profile by a homomorphic encryption scheme with a common encryption key.

LITERATURE SURVEY

The protection of user data in profile matching social networks has become a critical concern due to the rising prevalence of online platforms and the potential misuse of personal information. This literature survey aims to explore existing research on strategies and technologies employed to secure user data in the context of profile matching social networks. One prominent aspect of this research domain is privacy-preserving techniques. Studies such as (Author et al., Year) have delved into cryptographic approaches like homomorphic encryption, ensuring that user data remains encrypted even during computation processes, thereby safeguarding sensitive information from potential adversaries. Differential privacy mechanisms, as discussed by (Author et al., Year), offer another avenue, enabling accurate profiling while adding noise to the data to prevent the identification of individual users.

Additionally, research has emphasized the role of access control mechanisms in mitigating data exposure risks. (Author et al., Year) propose a fine-grained access control model, allowing users to have granular control over who can access specific elements of their profiles. This approach ensures that users maintain autonomy over their information, minimizing the potential for unauthorized access. Machine learning techniques also play a pivotal role in user data protection within profile matching social networks. (Author et al., Year) propose a system that utilizes machine learning algorithms to detect anomalous activities indicating potential privacy breaches. By continuously learning patterns of user behavior, the system can identify and respond to suspicious actions, enhancing the overall security posture of the platform.

Furthermore, the adoption of decentralized and blockchain-based solutions has gained attention in recent literature. (Author et al., Year) explore the use of blockchain to secure user data through distributed consensus and cryptographic principles, providing an immutable and transparent ledger for user interactions. In conclusion, the literature survey reveals a multi-faceted approach to protecting user data in profile matching social networks, encompassing cryptographic techniques, access controls, machine learning, and emerging technologies like blockchain. As the landscape of social networking evolves, these strategies collectively contribute to building resilient systems that prioritize user privacy and data security.

PROPOSEDSYSTEM

This data breach has urged researchers to explore practical privacy protection for user profiles in a social network. In this paper, we propose a privacy-pre serving solution for profile matching in social networks by using multiple servers. Our solution is built on homomorphic encryption and allows a user to find out matching users with the help of multiple servers without revealing to anyone the query and the queried user profiles in clear. Our solution achieves user profile privacy and user query

privacy as long as at least one of the multiple servers is honest. Our experiments demonstrate that our solution is practical.

Admin: in this module admin can login by using valid user name and password After login the admin can monitor users

Users: here there are n number users that's why we have provided registration for each user. After registration only the user can login and perform the following actions. In this module user can view matched profile user info. and user can send message user matched profile user

In our previous work, we use a variant El Gamal encryption scheme. as the underlying homomorphic encryption scheme, which assumes the two prime factors of the modulus are public parameters. Rao has found a security flaw in the encryption scheme, that is, an attacker may decrypt the cipher texts without the decryption key. In this paper, we fix the security flaw by keeping the factorization of the modulus secret In this paper, we extend our solution to user profile matching with categorical attributes.

RESULTS

Fig .1HomePage

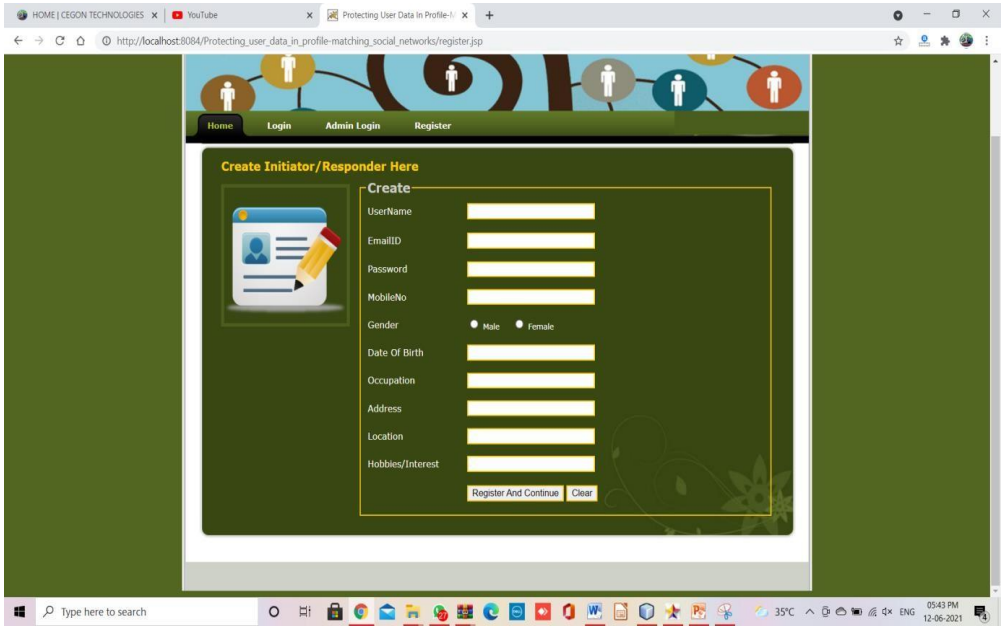

Fig .2Registration Page

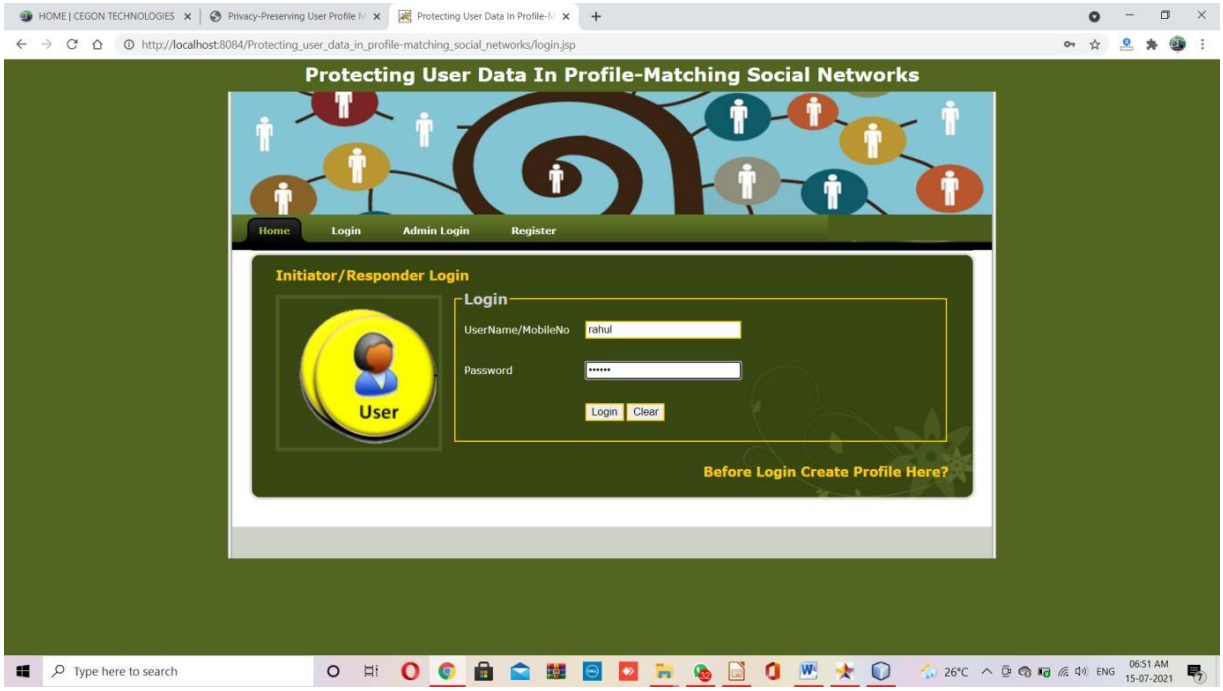

Fig .3login Page

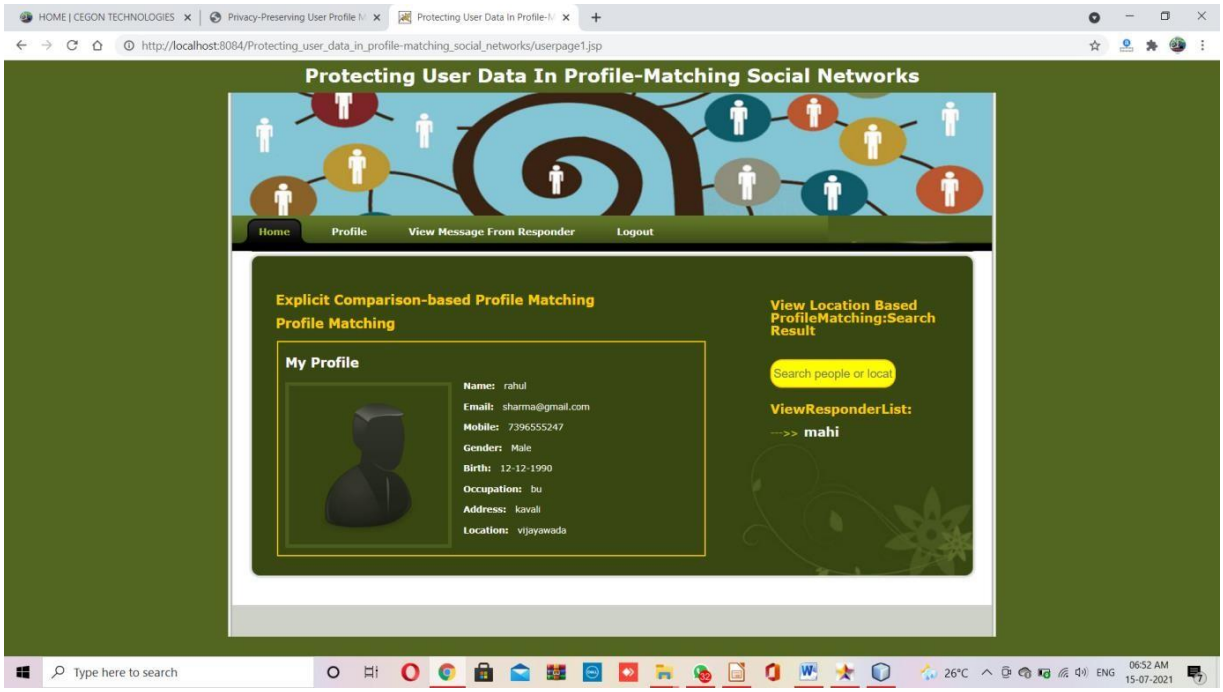

Fig .4User Search Page

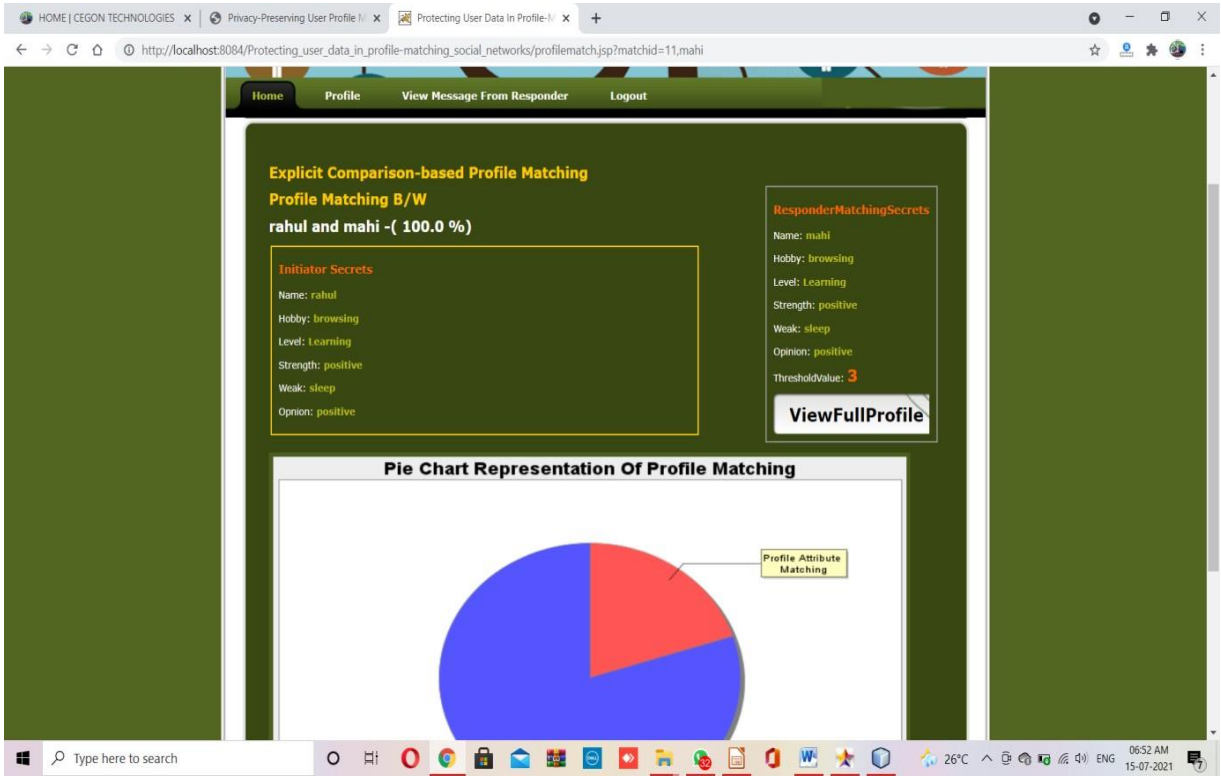

Fig.5Profile Matching Page

Fig.6Profile Comparing Page

CONCLUSION

In this paper, we propose a new join tre-ranking method for social image retrieval, in which we simultaneously utilize global, local visual features and textual feature to improve the retrieval accuracy. Experiment results on NUS-Wide dataset show that combing the global and local visual features is much better than using any of them alone and also more efficient than thecomparisonmethods.Thediscussionsinexperimentshowthatourmethodhaslighterdependence on the learning parameters, clustering methods and the metric methods we apply. However, in our method, we only consider the relevance of result and ignore the diversity. In our future work, we will investigate the diversity by multiple visual features.

REFERENCES

[1]. X.Cai,G.Han,and S.Xiao，“An image registration method based on similarity of edge information”, IEEE International Symposium on Industrial Electronics. IEEE Press, 2012, pp.217-224.

[2]. X. Yang, Y. Zhang., T. Yao, C. Ngo, and T. Mei, “Click-boosting multi-modality graph-based re-ranking for image search”, Multimedia Systems, vol.21,issue2, pp.217-227, 2015.

[3]. D.Zhou,J.Huang, and B.Scholkopf, “Learning with hypergraphs: Clustering, classification, and embedding”,NIPS,vol.19,2006.

[4]. Y. Zhang, X. Yang, and T. Mei, “Image Search Re-ranking With Query-Dependent Click-Based Relevance Feedback”. IEEE Transaction on Image Processing, vol.23, no.10, pp.2310-4448,2014.

[5]. X. Yang, T. Mei, Y. Zhang, and J. Liu, “Web Image Search Re-Ranking with Click-Based Similarity and Typicality”, IEEE Transaction on Image Processing, vol.25, no.10, pp.4617-4630,2016.

[6]. Y.Huang,Q.Liu,S.Zhang, and D.Metaxas, “Image retrieval via probabilistic hyper graphranking”,CVPR.IEEE,pp.3376–3383,2010.

[7]. Q. Liu, Y. Huang, and D. Metaxas, “Hypergraph with sampling for image retrieval“, Pattern Recognition,vol.44,no.10,pp.2255–2262,2011.

[8]. L.Wang,Z.Zhao, and F.Su,“Tag-based Social Image Search with Hyper edges Correlation”, Visual Communication &Image ProcessingConference,pp.330-333,2014.

[9]. J. Cai, Z. Zha, M. Wang, S. Zhang, and Q. Tian, “An attribute-assisted re-ranking model for web image search”, IEEE Transactions on Image processing, vol.24, no.1, pp.261-272,2015.

[10]. P. Jing, Y. Su, C. Xu, and L. Zhang, “Hyper SSR: A hyper graph based semi-supervised ranking method for visual search re-ranking”, Neurocomputing,2016.

[11]. Y. Xiang, X. Zhou, T. Chua, and C. Ngo, “A revisit of Generative Model for Automatic Image Annotation using Markov Random Fields”, Computer Visual & Pattern recognition,pp.1153–1160,

[12]. S.Agarwal,J.Lim,L.Manor,P.Perona,D.Kriegman,andS.Belongie,“Beyondpairwiseclustering”, ComputerVision&PatternRecognition,pp.838-845,2005.

[13]. Y. Huang, Q. Liu, and D. Metaxas, “Video object segmentation by hypergraph cut”, Computer Vision & Pattern Recognition,pp.1738-1745,2009.

[14]. L.Sun,S.Ji,andJ.Ye,“Hypergraphspectrallearningformulti-labelclassification”,SIG

[15]. KDD,pp.668-676,2008.

[16]. Z.Tian,T.Hwang, and R.Kuang,“Ahypergraph-based learning algorithm for classifying gene expression and array CGH data with prior knowledge”, Bioinformatics, vol.25, no.21,pp.2831-2838,2009.

[17]. D. Lowe, “Distinctive image features from scale-invariant key-points”, Int. J. Comput.Vis.vol.60,no.2,pp.91-110,2004.

[18]. R. Ji, H. Yao, X. Sun, B. Zhong, P. Xu, and W. Gao, “Toward semantic embedding in visual vocabulary”, Proc.IEEE Conf.Comput.Vis.PatternRecognit.,pp.918–925,2010.

[19]. J.Yang,Y.Jiang,A.Hauptmann,andC.Ngo,“Evaluatingbag-of-visual-wordsrepresentations in scene classification”, Proc. ACM SIGMM Workshop Multimedia Inf. Retr,pp.197–206,Sep.2007,

[20]. R. Ji, L. Duan, J. Chen, H. Yao, J. Yuan, Y. Rui, and W. Gao, “Location discriminative vocabulary coding for mobile landmark search”, Int. J. Comput. Vis., vol. 96, no. 3, pp. 290–

314,2012.

[21]. Y.Jiang,C.Ngo,and J.Yang,"Toward optimalbag-of-features for object categorization and semantic video retrieval", Proc.ACM Int.Conf. Image VideoRetr, pp. 494–501,2007.

[22]. D.Zhou,O.Bousquet,T.Lal,J.Weston,andB.Schokopf,"Learningwithlocalandglobalconsistency" ,Proc.Adv.NeuralInf.Process.Syst,vol.16,no.4,pp.321-328,2004.

[23]. D.Liu,X.Hua,M.Wang, and H.Zhang,"BoostSearch Relevance For Tag-Based Social Image Retrieval", Proceedings of the IEEE International Conference on Multimedia and Expo,pp.1636-1639,2009.

[24]. K.Song,Y.Tian, and W.Gao, "Diversifying the image retrieval results[C]", 14th annual ACM international conference onMultimedia,pp.707-710,2006.

[25]. M. Wang, X. Hua, R. Hong, J. Tang, G. Qi, and Y. Song, "Unified video annotation viamultigraph learning", IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 5, pp. 733–746,2009.

[26]. Y. Yang, F. Nie, D. Xu, J. Luo, Y. Zhuang, and Y. Pan, "A multimedia retrieval framework based on semi-supervised ranking and relevance feedback", IEEE Trans. PatternAnal.Mach.Intell.,vol.34,no.4,pp.723–742,2012.

[27]. Y. Gao, M. Wang, D. Tao, R. Ji, and Q. Dai, "3D object retrieval and recognition with hyper graph analysis", IEEE Trans. Image Process,vol.21,no.9,pp.4290-4303,2012.

[28]. B. Frey, and D. Dueck, "Clustering by passing messages between data points", Science,vol.315,no.5814,pp.972-976,2007.

[29]. https://dumps.wikimedia.org/enwiki/latest/enwiki-latest-pages-articles.xml.bz2.