A User Data Protecting In Profile Matching Social Networks

[1] Adepu Mounika, [2] Dr.E.Srikanth Reddy

[12] Vaageswari College Of Engineering, Karimnagar, Telanganha, India

[1] manumouni428@gmail.com [2] srikanth574@gmail.com

ABSTRACT

In this paper, we focus on the situation when a user wants to find other users on a social networking service by searching a database of user profiles kept by that service. Online dating is a typical use case for this phenomenon. Recently, the hacking of the popular dating website Ashley Madison exposed the personal information of millions of its users. The recent data theft has prompted study into methods of effectively protecting social network user profiles from prying eyes. In this research, we present a distributed server system for social network profile matching that protects users' anonymity. To avoid disclosing the query and the searched user profiles in clear, we developed a system based on homomorphic encryption that enables a user to find matching users with the assistance of numerous servers. As long as one of the several servers is trustworthy, our method protects the confidentiality of both user profiles and user queries. The results of our experiments prove the viability of our approach. ElGamal encryption, Paillier encryption, homomorphic encryption, matching user profiles, protecting personal information

INDEX TERMS: social network profile, homomorphic encryption, Cloud Mobile Augmentation (CMA), Smart Card Web Services (SCWS), Attribute Based Encryption (ABE).

I. INTRODUCTION

As such, the problem of bringing together two or more people who share common interests is both crucial and universal, with applications in fields as diverse as employment search, social networking, and romantic encounters. In order to use preexisting online dating services, users must put their faith in an impartial server. As a result, the matching server is privy to sensitive information about its users' preferences, which can lead to privacy concerns if the server were to disclose that information (on purpose or by accident). Users of online dating services establish a public "profile" for potential matches to peruse. Information such as the user's age, gender, educational background, occupation, marital status, place of birth, religion, ethnicity, drug use, favourite hangouts, and favourite drinks may be requested. The majority of online dating services may keep such data even after an account is deactivated. Without the users' knowledge or approval, their personal information may be shared again with other parties such as marketers and data aggregators for uses unrelated to online matching. Using an online dating site is not without its dangers, such as falling victim to scammers or sexual predators, or having your reputation harmed as a result. Many online dating services don't take their users' right to privacy and security seriously. The "privacy" settings they deploy are often confusing, and their data management systems are prone to significant security breaches. Ashley Madison is a commercial website that promotes having extramarital affairs, however in July 2015, a gang calling themselves "The Impact Team" stole user data from the site. If Ashley Madison wasn't shut down immediately, the organisation threatened to publish users' identities and other personal details. More than 25 GB of firm data, including user identities, were leaked between August 18 and 20, 2015. Some people were afraid to use the site because of its policy of not removing their personal information, such as their names, addresses, search histories, and credit card purchases. Two unidentified deaths by suicide were reported by Toronto police on August 24, 2015, suggesting a connection to the data breach. Concerns about the risks of disclosing too much personal information have increased in the wake of this kind of data leak. Information theft is another risk that users of these services need to be aware of. Therefore, safeguarding the confidentiality of social media profiles is a pressing issue. The current best practise is for users to encrypt their profiles before uploading them to social networks, which protects them from prying eyes. But it's difficult to carry out matching when user profiles are encrypted. In this research, we focus on the case when a user queries a social networking service provider's user profile database in search of users who share similarities with the querying user's own profile. Online dating is a typical use case for this phenomenon. We provide a system that uses numerous servers to match users' profiles on social networks while protecting their anonymity. We can sum up our main concept as follows. Each user's profile is encrypted with a homomorphic encryption algorithm and a shared encryption key before being uploaded to a social network. So even if a hacker manages to get his hands on the user profile database, all they'll be able to decipher is encrypted information. A user's preferred user 1041-4347 (c) 2018 IEEE is encrypted whenever the user makes a social network connection request. Use for personal use is fine, but any further distribution or publication must have IEEE's approval. To learn more, visit http://www.ieee.org/publications standards/publications/rights/index.html. This article will appear in a forthcoming edition of this journal after further editing. Before it goes to print, the content may undergo revisions. Details about the citation: The inquiry includes the user's profile information and a dissimilarity threshold, and is submitted to the social network service provider. Multiple servers, which all have access to the decryption key thanks to the query, check each record against the selected user profile. If the degree of dissimilarity is below the threshold, the requesting user is given access to the contact details of the user whose profile was most closely matched. Among our primary contributions are 1) The user profile matching model, user profile privacy, and user query privacy are all formally defined. 2) We present a method for matching user profiles that respects their privacy, first for a single dissimilarity criterion and later for a set of criteria. Finally, we conduct security analysis on our protocols. When implemented on several servers, our protocols protect both user profiles and query histories if at least one of the servers is trustworthy. To assess the efficacy of our proposed processes across a range of configurations, 4) we do comprehensive experiments on a real dataset. Experiments validate the viability and efficacy of our approaches. In this publication, we build upon the following of our earlier research [32]. 1) We have previously worked with a homomorphic encryption system based on a variation of the ElGamal cypher [33], which operates under the assumption that the two prime factors of the modulus are known. Rao [22] discovered a vulnerability in the encryption technique, allowing ciphertexts to be decrypted without the proper decryption key. In this study, we address the issue by concealing the modulus's factorization. 2) In our earlier work, all matching servers used the same user profile data, hence they all needed to have their own user profile database. In this study, we solely save user profiles at the social service provider's end, eliminating the requirement for individual matching servers to store such information. In our prior work, 3) a query user is limited to choosing a single dissimilarity criterion for user matching. In this work, we introduce a system where the query user can choose from a variety of dissimilarity levels when matching with other users. 4) All of our prior work on user profile matching has relied solely on numerical characteristics. In this work, we further our approach to user profile matching by incorporating the usage of categorical criteria. 5) In this publication, we improve the privacy-preserving and speed-boosting techniques used in our earlier research. In addition, we present two brand new collaborative algorithms for secure data transmission and storage.

II. RELATED WORKS

2.1 N. Fernando, S. W. Loke, and W. Rahayu are the authors.

Despite widespread adoption, mobile computing still faces challenges in realising its full potential due to issues including resource constraint, frequent disconnections, and mobility. To solve these issues, mobile cloud computing moves application execution to remote servers. Here, we highlight the unique challenges of mobile cloud computing and present a comprehensive review of the research in this area. We classify the major problems plaguing this field and go over the various solutions that have been proposed. The report concludes with a critical evaluation of outstanding problems and suggestions for where future research should focus.

2.2 The advantages of cloud-based mobile augmentation, classification schemes, and unanswered questions

Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya are the authors.

Recently, CMA strategies have achieved significant traction in both the academic and business communities. When it comes to running resource-intensive mobile apps, the current gold standard is the Cloud Mobile Augmentation (CMA) approach, which makes use of resource-rich clouds to boost, improve, and optimise the computing capabilities of mobile devices. The goal of augmented mobile devices is to store large amounts of data and execute complex computations that are beyond the capabilities of traditional mobile devices, all while leaving as small a footprint as possible. Various cloud-based computing resources (such as far-flung clouds and close-by mobile nodes) are used by researchers to accommodate the wide range of computing needs experienced by mobile users. Although using cloud-based computing resources has many benefits, it is not a simple fix. One of the difficulties in making CMA flexible is understanding the essential aspects (such as the current status of mobile client and remote resources) that effect the augmentation process and making the best choice of cloud-based resource types. This research proposes a taxonomy of CMA methods after doing a thorough survey of the mobile augmentation sector. This research aims to address these questions by exploring the benefits and drawbacks of using a wide range of cloud-based resources for augmenting mobile devices, and by highlighting the impact of remote resources on the quality and dependability of augmentation procedures. Traditional and cloud-based augmentations are presented alongside their definitions, motivations, and a taxonomy of sorts. We provide a taxonomy after carefully examining the state-of-the-art CMA methods and dividing them into four categories: far-away fixed, close-by fixed, close-by mobile, and hybrid. An illustrative decision making flowchart for future CMA techniques is shown, along with an introduction to crucial decision making and performance restriction considerations that influence on the adoption of CMA approaches. Future research areas are provided, and the effects of CMA techniques on mobile computing are considered.

2.3 Thirdly, mobile cloud computing: the established method for safeguarding mobile cloud ecosystems
R. Kumar and S. Rajalakshmi are the authors.
Cloud computing's ideas mesh easily with mobile devices to provide convenient, always-available services. It is anticipated that the rise of mobile cloud computing would contribute to the development of new mobile ecosystems. There will undoubtedly be an increase in security concerns as a result of the increased prevalence of mobile devices in society. The vast expansion in Internet-enabled gadgets is another factor that will increase the importance of Internet security. One of the biggest difficulties for both customers and businesses is learning about the full capabilities of mobile cloud computing and figuring out how to address concerns about mobile cloud security, privacy, feasibility, and accessibility. Examining the current status of cloud security breaches, vulnerabilities of mobile cloud devices, and how to address those weaknesses in future work in the context of mobile device management and mobile data protection, this article examines the mobile cloud security difficulties and challenges. Mobile cloud computing security is also discussed, with an emphasis on SCWS (Smart Card Web Services) competition.

2.4 Fourthly, the combination of mobile cloud sensing, big data, and 5G networks creates a world that is both intelligent and smart.
WRITTEN BY: Q. Han, S. Liang, and H. Zhang
Cell phones have evolved over the years to become more sophisticated tools that can do more and better serve their users. These requirements can be as specific as a health care manager or as broad as an environmental watchdog. In essence, the introduction of mobile phones has improved the quality of our daily lives by making us more productive, resourceful, and comfortable. In this article, we first explain the concepts of mobile sensing and cloud computing independently, then combining them to establish the single notion of mobile cloud sensing. In addition, we will explain the components of mobile cloud sensing and provide an intuitive architectural explanation of the technique. Today, mobile cloud sensing has its limitations, but with the advent of 5G and the analysis of large data, we can solve these problems. With the development of mobile cloud sensing, 5G, and big data analysis, we anticipate further improvements in the standard of living.

2.5 Integrating Theory and Practice for Access Control in Distributed Systems.
Author(s): I. Stojmenovic

To protect sensitive information and resources, access controls allow only approved individuals to access them. In dispersed systems, where centralised activity coordination may be impractical or resource intensive, this issue becomes more difficult to solve. An emerging cryptographic basic, Attribute Based Encryption (ABE) is being put to use in the realm of access control. We discuss several recent issues with access control in distributed systems, including mobile ad hoc networks, vehicular networks, smart grids, and the cloud. There are various limitations and prerequisites associated with each of these uses. We demonstrate how ABE and its various versions can be adapted to meet the requirements of the aforementioned uses.

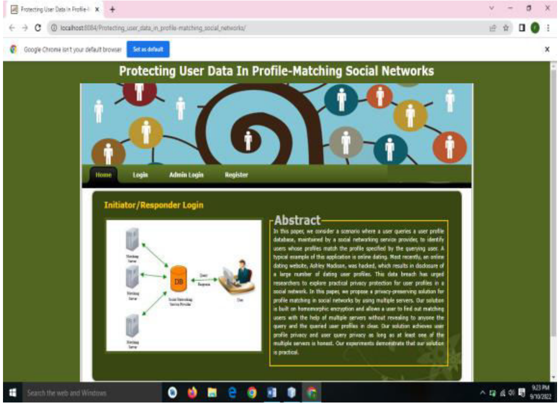
III. METHODOLOGY

Researchers are now looking towards realistic privacy protection for user accounts in social networks as a result of this data loss. In this research, we suggest a multi-server approach to profile matching in social networks that protects user privacy. Our solution, which is based on homomorphic encryption, enables a user to identify compatible users with the aid of multiple servers without disclosing the query or the user profiles being questioned to anyone. As long as at least one of the numerous servers is trustworthy, our solution achieves user query and profile privacy. Our experiments show the viability of our solution.

A.IMPLEMENTATION

- **Admin**:
  In this module admin can login by using valid user name and password After login the admin can monitor users
- **User**:
  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

IV. EXPERIMENT, RESULTS, AND ANALYSIS


Protecting User Data In Profile-Matching Social Networks
Home
Login
Admin Login
Register
Initiator/Responder Login
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.

FIg4.1.Home page

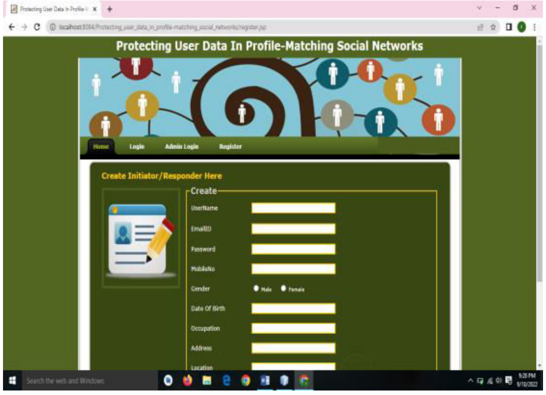


Fig4 .2 Register page

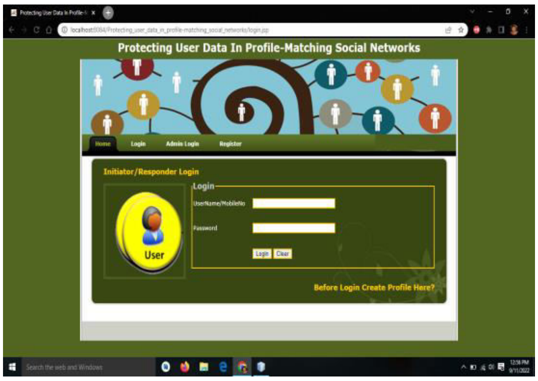

Protecting User Data In Profile-Matching Social Networks
Home
Login
Admin Login
Register
Initiator/Responder Login
Login
UserName/MobileNo
Password
Login
Clear
User
Before Login Create Profile Here?

Fig 4.3 Login page

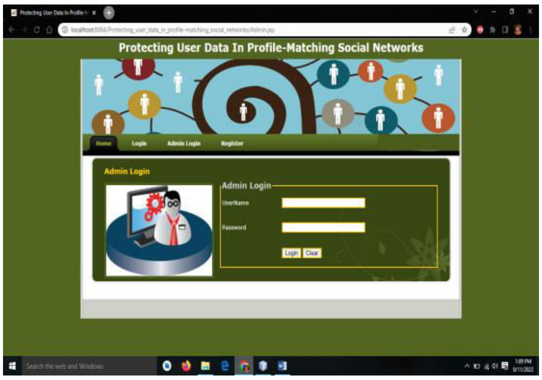


Fig4.4 Admin login page

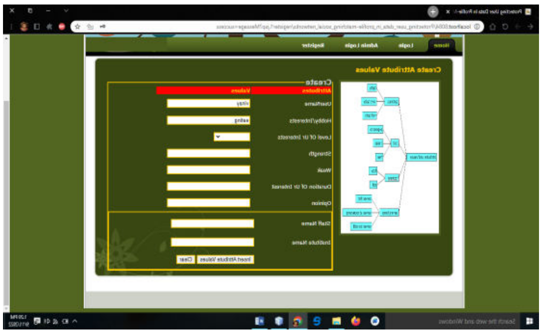


Fig.4.5.Create Attribute Values page

V. CONCLUSION AND FUTURE WORK

In order to increase the retrieval accuracy, we simultaneously employ global, local, and textual elements in our new joint re-ranking strategy for social picture retrieval. Results from experiments on the NUS-Wide dataset demonstrate that combining global and local visual features is both more effective than utilising any one of them alone and superior than comparison methods. Discussions during the experiment demonstrate that our method depends less on the learning parameters, clustering techniques, and metric methods we use. In contrast, our approach ignores diversity and only takes into account the relevance of the result. We will research the diversity by various visual features in our upcoming work..

REFERENCES

[1] R. Agrawal, A. Evfimievski, and R. Srikant, Information sharing across private databases, in SIGMOD 2003, pp. 86-97.

[2] M. von Arb, M. Bader, M. Kuhn, and R. Wattenhofer, Veneta: Serverless friend-of-friend detection in mobile social networking, in IEEE WIMOB 2008, pp. 184-189.

[3] B. H. Bloom, Space/time trade-offs in hash coding with allowable errors, Communications of the ACM 13 (7): 422-426, 1970.

[4] D. Boneh, E. J. Goh, K. Nissim, Evaluating 2-DNF formulas on ciphertexts, in TCC 2006, pp 325-341.

[5] D. Chaum, Blind signatures for untraceable payments, in Crypto 1982, pp. 199-203.

[6] E. D. Cristofaro and G. Tsudik, Practical private set intersection protocols with linear complexity, in Financial Cryptography and Data Security 2010.

[7] D. Dachman-Soled, T. Malkin, M. Raykova, and M. Yung, Efficient robust private set intersection, in ACNS 2009, pp. 125-142.