PROTECTING USER DATA IN SOCIAL NETWORK PROFILE MATCHING

VELICHALA SAGARIKA, H.no: 22S41D5813,Mtech (CSE), Department of Computer Science, VAAGESWARI COLLEGE OF ENGINEERING Thimmapur,Karimnagar, Telangana, INDIA, Email-id: chatlausharani1@gmail.com.

DR. E. SRIKANTH REDDY,Professor, Department of Computer Science, VAAGESWARI COLLEGE OF ENGINEERING Thimmapur,Karimnagar, Telangana, INDIA.

ABSTRACT

In this article, we explore what happens when a person queries a social media provider's user profile database to identify others with similar profiles. Online dating is a notable example of this application. The recent breach of the Ashley Madison dating platform, which exposed millions of user profiles, has highlighted the urgent need for stronger privacy safeguards in social media systems.To address this issue, we present a privacy-preserving mechanism for profile matching in social networks using multiple servers. Our approach leverages homomorphic encryption, enabling users to find matching profiles without revealing their queries or searched profiles in plaintext. The proposed method guarantees the confidentiality of user data and queries, provided that at least one of the servers operates honestly. Experimental results confirm that our solution is both practical and effective.

Index Terms:- Privacy-preserving profile matching, homomorphic encryption, social networks, multi-server architecture, secure query processing, data confidentiality.

1.INTRODUCTION

A significant and common issue in many settings, including job searches, social media, and dating services, is how to bring people together who have similar interests. For current online matching systems to work, consumers must trust a third-party server with their preferences. There are legitimate privacy issues about the potential accidental or intentional disclosure of user profiles due to the extensive interest data stored by the matching server. When someone signs up for a dating site online, they create a public "profile" that other users may see. User details such as age, gender, education level, employment position, number of children, religion, location, income, ethnicity, sexual orientation, alcohol consumption, hobbies, favorite places, and drug use may be requested. Even after deleting an account, data from many online matching services may remain. In addition to users' possible matches, marketers and data aggregators may see their personal information. The latter two groups may use the former's data for purposes unrelated to online matching, and the former may do so without the users' knowledge or consent. Furthermore, there are risks associated with utilizing online matching services, such as fraud, sexual predators, and significant damage to one's reputation. Users' privacy and security are compromised by many online dating services. Their data management systems have serious security flaws, and they often utilize "privacy" settings that aren't consistent. Ashley Madison was a commercial website that aimed to facilitate extramarital romances. In July 2015, a group called "The Impact Team" hacked user data from the site. Unless Ashley Madison was removed from the situation immediately, the gang threatened to reveal the names and personal details of users. Around 25 gigabytes of corporate data, including user information, was distributed by the corporation between August 18 and 20, 2015. A number of users have voiced their worries about the site's tendency to save personally identifiable information (such as names, addresses, search histories, and credit card numbers) and the public shame that may result from it. Two unconfirmed suicides were linked to the data breach, according to Toronto police on August 24, 2015. Users are now even more wary about giving out personal information due to this data breach. To prevent identity theft, users of these services should exercise caution. Protecting the anonymity of social media accounts is a critical concern. Encryption, in which users protect their accounts before sharing them on social media, has proven to be the most effective option so far. But encrypted user profiles make matching impossible. This article takes a look at what happens when a user asks a social media company's database for users with similar profiles to the one they've already provided. One of the best examples of this use is internet dating. We provide a method for social network profile matching that uses several servers while protecting user privacy. What follows is a concise summary of the essential idea. Everyone uses a homomorphic encryption method with a common encryption key to secure their profile before sharing it on social media. As a result, the encrypted data would be accessible to the hacker even if the user profile database was breached. The user encrypts the target person's profile and includes a dissimilarity threshold while sending the query to the social networking service provider in order to find them in the network. According to the research, a large number of servers secretly exchange the decryption key by comparing the chosen user profile with every record in the database. Users get the matching person's contact details if the degree of dissimilarity is less than a certain threshold.

OBJECTIVES:

Our key contributions can be summarized as follows:

- we clearly define the user profile matching technique, user profile confidentiality, and user query confidentiality.
- we introduce a privacy-preserving user profile matching technique based on a single dissimilarity threshold and extend it to support multiple dissimilarity criteria.
- we evaluate the security of our protocols and demonstrate that, provided at least one of the participating servers is reliable, the confidentiality of user profiles and queries is preserved.
- we perform extensive evaluations on a real dataset under varying parameter settings. The results confirm that our proposed approaches are both practical and efficient.

2.LITERATURE SURVEY

M. von Arb, M. Bader, M. Kuhn, and R. Wattenhofer proposed that mobile social software has recently become an active area of research and development. Over the past years, numerous systems have been introduced in an attempt to replicate the success of their Internet-based counterparts. Many mobile solutions aim to enhance existing platforms with location-awareness. However, the price of mobility is often the lack of popular friendship exploration features or the costs associated with accessing a central server required for this functionality. In their work, the authors address this issue by introducing a decentralized method capable of exploring a user's social neighborhood through the detection of friends-of-friends. Unlike approaches that rely solely on system users, their method leverages real-world friendships while adequately addressing related privacy concerns. Furthermore, they present **VENETA**, a mobile social networking platform that implements, among other features, their novel friend-of-friend detection algorithm.

E. D. Cristofaro and G. Tsudik described that the increasing dependence on anytime-anywhere data availability, along with growing concerns about privacy loss, motivates the need for privacy-preserving techniques. A particularly interesting and common challenge arises when two parties must privately compute the intersection of their respective datasets. In such cases, one or both parties may need to obtain the intersection, but neither should learn any additional information about the other's data. Although prior research has produced several effective and elegant Private Set Intersection (PSI) techniques, efficiency remains an ongoing challenge. This paper investigates variations of PSI and introduces a set of secure protocols that are significantly more efficient than the state-of-the-art.

D. Dachman-Soled, T. Malkin, M. Raykova, and M. Yung explained that computing set intersection privately and efficiently between two mutually mistrusting parties is a fundamental task in private data mining. Ensuring robustness—specifically, the ability to handle arbitrarily misbehaving (i.e., malicious) parties—while maintaining protocol efficiency (without resorting to costly generic techniques) has been an open problem. In their work, the authors present the first solution to this challenge.

T. ElGamal proposed a new signature scheme, along with an implementation of the Diffie–Hellman key distribution protocol that achieves a public-key cryptosystem. The security of both systems relies on the computational hardness of the discrete logarithm problem over finite fields.

M. Freedman, K. Nissim, and B. Pinkas examined the problem of computing the intersection of private datasets belonging to two parties, where the datasets consist of elements drawn from a large domain. This problem has wide applications in online collaboration. The authors present protocols that rely on homomorphic encryption and balanced hashing, designed for both semi-honest and malicious settings. For lists of length *k*, their solution achieves **O(k)** communication overhead and **O(k log log k)** computation. The semi-honest protocol is secure in the standard model, while the malicious protocol is secure in the random oracle model. Additionally, they address the problem of approximating the size of the intersection, proving a linear lower bound on the communication overhead for this task, and offering a suitable secure protocol. The study also explores other matching problem variants, including extending the protocol to the multi-party setting and considering approximate matching.

3.PROBLEM STATEMENT:

A user's profile becomes public when they sign up for an online dating service. Such profiles may include information about the user's age, gender, education, occupation, religion, sexual orientation, income, ethnicity, drug use, preferred locations, and drinking habits, among other details. Even after an account is deactivated, many online matching services may retain some of this information.Without the user's knowledge or consent, personal data can also be shared with third parties, including advertisers, data aggregators, and even prospective matches. These third parties may then use the information for purposes unrelated to online matching.The use of online matching services carries a high risk of fraud, exploitation by sexual predators, and reputational harm. Moreover, many platforms place customers' personal information at risk due to poorly designed data management systems. They often suffer from critical security vulnerabilities and employ inconsistent or incompatible "privacy" settings, further undermining user safety.

DISADVANTAGES:

- User data is at risk, raising serious privacy concerns.
- In the face of sophisticated cyberattacks, existing privacy protection measures may prove insufficient.

4.PROPOSED MODEL:

This article examines the scenario in which a user queries a social media company's database to identify other profiles similar to a given one. Online dating provides a prime example of this application. To address the associated privacy risks, we propose a privacy-preserving method for social network profile matching using a cluster of servers.The core principle of our approach is as follows: each user encrypts their profile with a homomorphic encryption scheme and a shared encryption key before uploading it to the social network. As a result, even if an attacker gains access to the database, only encrypted information would be exposed.When a user wishes to search for similar profiles, both the target profile and a dissimilarity threshold are encrypted and submitted as a query to the social network provider. Multiple servers, each holding a portion of the decryption key, collaboratively compare the encrypted query against all database entries without revealing sensitive data. If the dissimilarity between profiles falls below the defined threshold, the requesting user receives the contact details of the matched individual.

ADVANTAGES:

- By relying on at least one honest server, the system safeguards both user profiles and queries.
- It is efficient, practical, and well-suited for real-world applications.

5.SYSTEM MODEL:

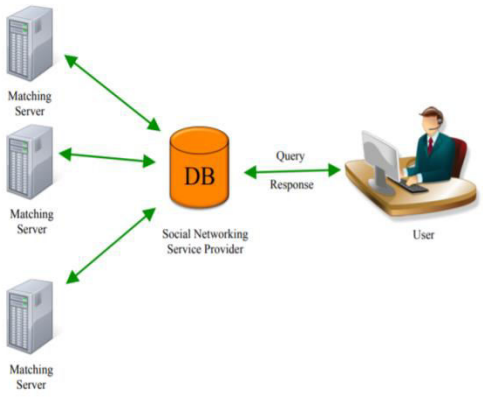


Fig.1 Privacy-Preserving User Profile Matching Model

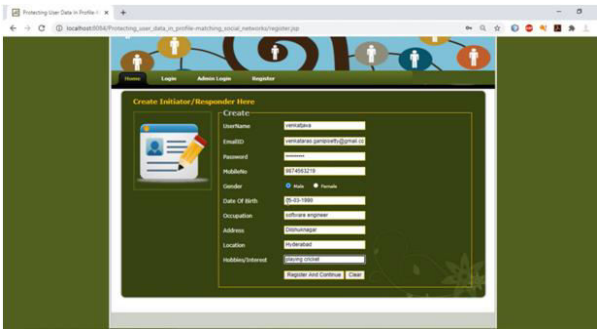
6.MODULES DESCRIPTIONS

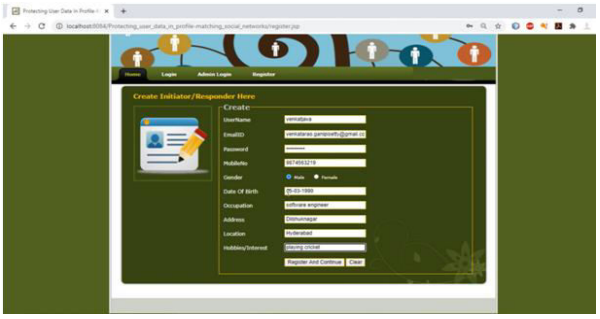
1. Admin Module

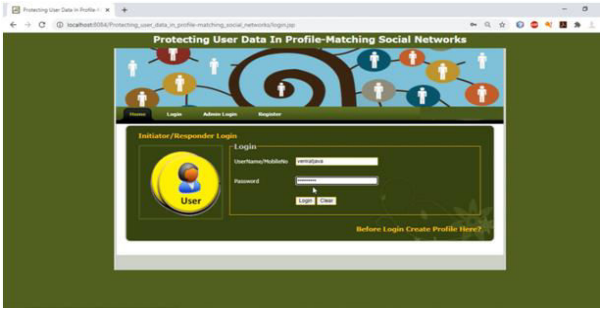
In this module, the admin accesses the system using a valid username and password. The admin is responsible for managing user details and has the ability to terminate application sessions when required.

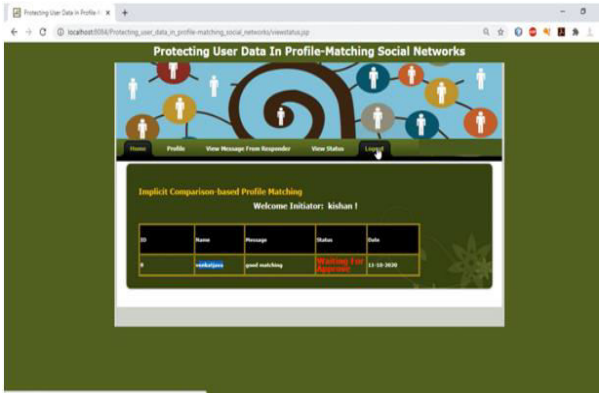
2. Initiator and Responder Module In this module, both the Initiator and the Responder register with the application. Once enrolled, they can log in to the system. The Initiator initiates a search for user profiles, while the Responder participates in the matching process. Both parties are able to identify and compare profiles within the same category to find suitable matches.

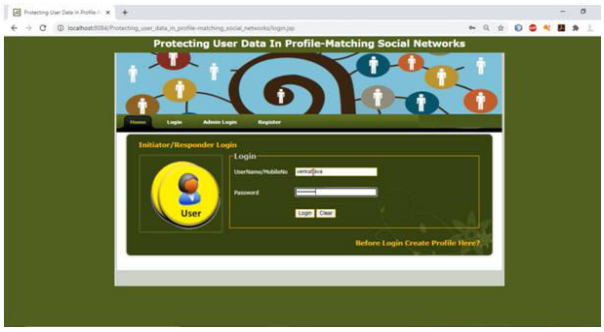
7.SCREENSHOTS











8.CONCLUSION

In this paper, we proposed a novel solution for privacy-preserving user profile matching using homomorphic encryption and multiple servers. The proposed approach enables users to identify matching profiles with the assistance of multiple servers, while ensuring that neither the queries nor the user profiles are revealed. Security analysis has demonstrated that the protocol effectively preserves both user profile privacy and query privacy. Furthermore, experimental results confirm that the protocol is both practical and feasible for real-world applications.

9.FUTURE ENHANCEMENT

As part of future work, we aim to further enhance the system's performance by optimizing the computation of conditional gates through parallel processing techniques. This improvement is expected to reduce computational overhead and increase the scalability of the protocol.

10.REFERENCES

[1]R. Agrawal, A. Evfimievski, and R. Srikant, "Information sharing across private databases," in Proc. 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 Proc. IEEE WIMOB, 2008, pp. 184–189.

[3]B. H. Bloom, “Space/time trade-offs in hash coding with allowable errors,” Communications of the ACM, vol. 13, no. 7, pp. 422–426, 1970.

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

[5]D. Chaum, “Blind signatures for untraceable payments,” in Advances in Cryptology — 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 Proc. ACNS, 2009, pp. 125–142.

[8]T. ElGamal, “A public-key cryptosystem and a signature scheme based on discrete logarithms,” IEEE Trans. Inf. Theory, vol. 31, no. 4, pp. 469–472, 1985.

[9]M. Freedman, K. Nissim, and B. Pinkas, “Efficient private matching and set intersection,” in Proc. EUROCRYPT, 2004, pp. 1–19.

[10]C. Gentry, “Fully homomorphic encryption using ideal lattices,” in Proc. STOC, 2009, pp. 169–178.

[11]S. Goldwasser and S. Micali, “Probabilistic encryption and how to play mental poker keeping secret all partial information,” in Proc. 14th ACM Symposium on Theory of Computing (STOC), 1982, pp. 365–377.

[12]D. Harris, D. M. Harris, and S. L. Harris, Digital Design and Computer Architecture. San Francisco, CA: Morgan Kaufmann, 2007.

[13]C. Hazay and Y. Lindell, “Efficient protocols for set intersection and pattern matching with security against malicious and covert adversaries,” in Proc. TCC, 2008, pp. 155–175.

[14]C. Hazay, G. L. Mikkelsen, T. Rabin, T. Toft, and A. A. Nicolosi, “Efficient RSA key generation and threshold Paillier in the two-party setting,” in Proc. CT-RSA, 2012, pp. 313–331.

[15]Y. Huang, L. Malka, D. Evans, and J. Katz, “Efficient privacy-preserving biometric identification,” in Proc. NDSS, 2011.

[16]S. Jarecki and X. Liu, “Efficient oblivious pseudorandom function with applications to adaptive OT and secure computation of set intersection,” in Proc. TCC, 2009, pp. 577–594.

[17]R. Li and C. Wu, “An unconditionally secure protocol for multi-party set intersection,” in Proc. ACNS, 2007, pp. 226–236.

[18]M. Li, N. Cao, S. Yu, and W. Lou, “FindU: Privacy-preserving personal profile matching in mobile social networks,” in Proc. IEEE INFOCOM, 2010, pp. 1–9.

[19]L. Kissner and D. Song, “Privacy-preserving set operations,” in Proc. CRYPTO, 2005, pp. 241–257.

[20]G. S. Narayanan, T. Aishwarya, A. Agrawal, A. Patra, A. Choudhary, and C. P. Rangan, “Multi-party distributed private matching, set disjointness and cardinality of

set intersection with information-theoretic security," in Proc. CANS, 2009, pp. 21–40.