PROTECTING USER DATA IN PROFILE-MATCHING SOCIAL NETWORKS

GANASALA.V.S.S.SIRISHA[1], M.V.P.UMA MAHESWARA RAO[2]

[1]Student (MCA), NRI INSTITUTE OF TECHNOLOGY, A.P., India.

[2]Assistant Professor, Dept. of MCA, NRI INSTITUTE OF TECHNOLOGY, A.P., India.

Abstract —In this paper, 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

an online survey was used to collect information about users' behaviour on SNSs. The secondary method was a social experiment that tested SNSs users' reactions to profile access requests by a stranger. The research focused on four different social networks: Facebook, Twitter, Instagram, and Snapchat. The survey showed that there was a significant amount of disclosure of personal information; however, it differed from one social network to another. Facebook had the highest level of information disclosure, whereas Twitter had the lowest amount of information disclosure compared to the other networks. The research revealed that gender, age, and education had significant influences on information disclosure and users' privacy settings.

In general, males, young people between 16-24, and high school students showed reckless and very identifying behaviour on SNSs that might comprise their privacy and, in the worst cases, their safety, as they become more vulnerable to attacks from identity thieves and other malicious entities. The findings of the social experiment indicated that the majority of Facebook, Instagram, and Twitter users were likely to accept complete strangers into their personal private profiles. The study concludes by offering recommendations and guidelines that

may provide a safer browsing experience for social network users.

LITERATURE SURVEY

1. **Huang et al.** proposed a privacy-preserving solution for biometric matching, where the server holds a database{vi,pi}ni=1(vi denotes the biometric data corresponding to some identity profile pi), and the client who holds a biometric reading v′ wants to learn the identity pj for which vj is the closets match to v′ with respect to some metric (e.g., Euclidean distance), assuming this match is within some distance threshold δ. The idea is using Yao's garbled circuit technique [30] to perform the matching. Each gate of a circuit is associated with four cipher texts (a garbled table) by one party. The collection of garbled tables (the garbled circuit) is sent to another party, who uses information obtained by oblivious transfer to learn the output of the function on the parties' inputs. This work is most related to our work. The major difference is that we assume the database is encrypted while they assume the database to be in clear text.

2.Shahandashti et al. proposed a private fin-ger print matching protocol that compares two fingerprints. The protocol enables two parties, each holding a private finger print, to find out if their fingerprints belong to the same individual. The main building block of their construction is the aided computation. Consider a polynomial P(x) =∑akxk and a homomorphic encryption algorithm E for which Alice knows the decryption key. It is known that given{E(ak)}nk=1andx, the homomorphic property of E enables Bob to compute E(P(x)). Aided computation, on the other hand, enables Bob to compute E(P(x))given{ak}nk=1andE(x).A simplified description of their protocol is as follows. Let{pi}ni=1and{p′j}mj=1denote Alice's and Bob's finger print minutiae, respectively. They use the properties of homomorphic encryption schemes to privately calculate and compare the Euclidean distance and angular difference for each pair of minutiae(pi,p′j) to given thresholds. Their protocol enables Bob to calculate E(zij)for each pair(pi,p′j), such that zij is zero if the two minutiae match and non-zero otherwise. Then, using the aided computation idea, Bob calculates E(R(zij)), where R is a polynomial that maps zero to one and non-zero values to zero. Let σ=∑R(zij), where σ equals the total number of minutia matchings. Using the homomorphic property of the encryption scheme E(σ)can be calculated by Bob. Finally, the homomorphic property can be used to finalize the protocol and let Alice find out if σ is greater than or equal to a threshold or not. This work is also related to our work. The difference is that we assume the stored user data is encrypted while they assume two parties, each holding a private fingerprint in clear text.

PROPOSED SYSTEM

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 sites take shortcuts 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.

PROPOSED SYSTEM:

In this paper, 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. Therefore, even if the user profile database falls into the hand of a hacker, the hacker can only get the encrypted data. When a user wishes to find people in the social network, the user encrypts his/her preferred userprofile and a dissimilarity threshold and submits the query to the social networking service provider. Based on the query, multiple servers, which secretly share the decryption key, compare the preferred user profile with each record in the database. If the dissimilarity is less than the threshold, the matching user' contact information is returned to the querying user.

Our main contributions include

1) We formally define the user profile matching model, the user profile privacy and the user query privacy.

2) We give a solution for privacy-preserving user profile matching for a single dissimilarity threshold and then extend it for multiple dissimilarity thresholds.

3) We perform security analysis on our protocols. If at least one of multiple servers is honest, our protocols achieve user profile privacy and user query privacy.

4) We conduct extensive experiments on a real dataset to evaluate the performance of our

proposed protocols under different parameter settings. Experiments show that our solutions are practical and efficient.

IMPLEMENTATION

1. Security

Since the users may have different privacy requirements and it takes different amount of efforts to achieve them, we hereby (informally) define two levels of privacy where the higher level leaks less information to the adversaries.

2. Usability and Efficiency

For profile matching in MSN, it is desirable to involve as few human interactions as possible. In this paper, a human user only needs to explicitly participate in the end of the protocol run, e.g., decide whom to connect to based on the common interests. In addition, the system design should be *lightweight and practical*, i.e., being enough efficient in computation and communication to be used in MSN. Finally, different users (especially the candidates) shall have the option to flexibly *personalize their privacy levels*.

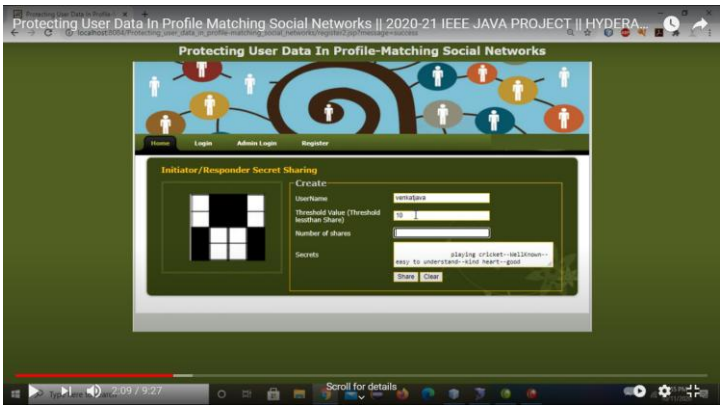
3.Shamir secret sharing scheme

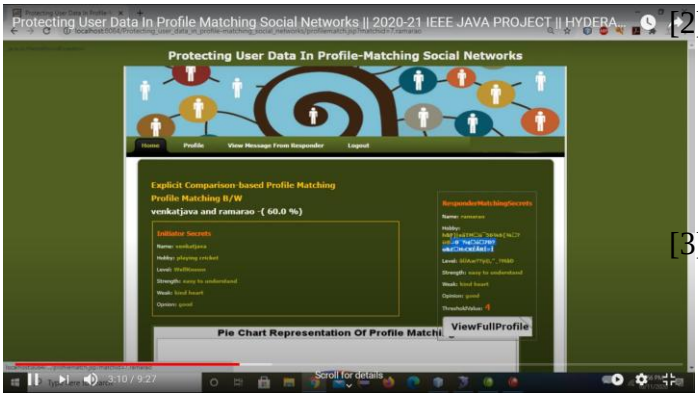
Secret sharing schemes are multi-party protocols related to key establishment. The original motivation for secret sharing was the following. To safeguard cryptographic keys from loss, it is desirable to create backup copies. The greater the number of copies made, the greater the risk of security exposure; the smaller the number, the greater the risk that all are lost. Secret sharing schemes address this issue by allowing enhanced reliability without increased risk.

4. Preventing Malicious Attacks.

Our protocols in this paper are only proven secure in the HBC model; it would be interesting to make it secure under the stronger malicious model, i.e., to prevent an adversary from arbitrarily deviating from a protocol run. we showed that with an additional commitment round before final reconstruction (which adds little additional overhead), a specific type of "set inflation attack" can be easily prevented where a malicious user influences the final output in her favorable way by changing her shares after seeing others'.

SAMPLE OUTPUT SCREENSHOTS





CONCLUSION

In this paper, proposed a new solution for privacy-preservinguser profile matching with homomorphic encryption techniqueand multiple servers. Our solution allows a user to find outthe matching users with the help of multiple servers withoutrevealing the query and the user profiles. Security analyseshave shown that the new protocol achieves user profile privacyand user query privacy. The experimental results have showedthat the new protocol is practical and feasible. Our future workis to improve the performance of computing conditional gatesby parallel computation.

Future Enhancement: Even if users with ulterior motives collude with one of the clouds, the personal data of other users will not be revealed. We can also develop an environment which is secure under the semihonest model through strict security analysis.

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 WIMOB2008, 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 onciphertexts, 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 protocolswith linear complexity, in Financial Cryptography and Data Security2010.

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

[8] T. ElGamal, A public-key cryptosystem and a signature scheme basedon discrete logarithms, IEEE Transactions on Information Theory 31(4): 469-472, 1985

[9] M. Freedman, K. Nissim, and B. Pinkas, Efficient private matching andset intersection, in EUROCRYPT 2004, pp. 1-19.

[10] C. Gentry, Fully homomorphic encryption using ideal lattices, in STOC2009, pp 169-178.

[11] S. Goldwasser and S. Micali, Probabilistic encryption and how toplay mental poker keeping secret all partial information, in Proc.

14thSymposium on Theory of Computing, 1982, pp. 365-377.

[12] D. Harris, D. M. Harris and S. L. Harris, Digital Design and ComputerArchitecture, Morgan Kaufmann Publishers, 2007.

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

[14]C. Hazay, G. L. Mikkelsen, T. Rabin, T. Toft, A. A. Nicolosi, EfficientRSA key generation and threshold paillier in the two-party setting, inCT-RSA 2012, pp. 313-331.