SAFEGUARDING USER INFORMATION IN CONTEXTUAL SOCIAL NETWORKS

1 Mrs. B. RAJASRI, 2 A. SINDHU, 3 B. SINDHU REDDY

4 A. PRASANNA, 5 A. ASHRITHA REDDY

1Assistant Professor, Department of CSE, Sri Indu College of Engineering and Technology-Hyderabad

2345Under Graduate, Department of CSE, Sri Indu College of Engineering and Technology-Hyderabad

ABSTRACT

Social media has become an important part of life. People across the world use social media for random purposes. They post their accomplishments, achievements, vacation photos and others onthe social media. However, they do not often realize that they are attracting very serious incidents that can occur due to their posts. Online privacy is one of the crucial points to safeguard our personal information. However, protecting privacy in online social networks (OSNs) is challenging as OSNs follow the strategy "Take it or Leave it." Users need to provide informationasked by the service providers in order to use the OSNs that may lead to compromise the users' data privacy. To provide privacy-aware OSNs it is important to know user's awareness about privacy. To achieve this, survey is conducted and from analysis of survey the user's awareness and requirements of privacy-aware mechanism is presented in this chapter. Survey analysis showsthat users of OSNs required to have trusted third party to manage their preferences and attributesto protect their privacy. Furthermore, user required new privacy law in Indian context and they need to hide their identity on OSNs.

In this paper, we consider a scenario where a user queries a user profile database, maintained bya social networking service provider, to identify users whose profiles match the profile specifiedby 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 numberof 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 multipleservers without revealing to anyone the query and the queried user profiles in clear. Our solutionachieves user profile privacy and user query privacy as long as at least one of the multiple serversis honest. Our experiments demonstrate that our solution is practical.

Keywords: Security, Data Privacy

INTRODUCTION

Online social networks (OSNs) such as Facebook, Google+, and Twitter are inherently designed to enable people to share personal and public information and make social connections with friends, coworkers, colleagues, family and even with strangers. In recent years, we have seen unprecedented growth in the application of OSNs. For example, Facebook, one of representative social network sites, claims that it has more than 800 million active users

and over 30 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) shared each month. To protect user data, access control has become a central feature of OSNs a typical OSN provides each user with a virtual space containing profile information, a list of the user's friends, and web pages, such as wall in Facebook, where users and friends can post content and leave messages. A user profile usually includes information with respect to the user's birthday, gender, interests, education and work history, and contact information. In addition, users can not only upload content into their own or others' spaces but also tag other users who appear in the content. Each tag is an explicit reference that links to a user's space. For the protection of user data, current OSNs indirectly require users to be system and policy administrators for regulating their data, where users can restrict data sharing to a specific set of trusted users. OSNs often use user relationship and group membership to distinguish between trusted and untrusted users. For example, in Facebook, users can allow friends, friends of friends, groups or public to access their data, depending on their personal authorization and privacy requirements. The existing work could model and analyze access control requirements with respect to collaborative authorization management of shared data in OSNs. The need of joint management for data sharing, especially photo sharing, in OSNs has been recognized by the recent work provided a solution for collective privacy management in OSNs. Their work considered access control policies of a content that is co-owned by multiple users in an OSN, such that each coowner may separately specify her/his own privacy preference for the shared content.

Contextual social networks (CSNs) have gained prominence in recent years as specialized platforms connecting individuals based on shared interests, activities, or contexts. Unlike traditional social networks, which cater to a wide range of interactions, CSNs provide niche communities where users can engage in meaningful conversations and share content relevant to their specific interests. As CSNs continue to grow in popularity, it becomes increasingly crucial to prioritize the safeguarding of user information and privacy within these platforms. This comprehensive guide will explore the key strategies and considerations for safeguarding user information in contextual social networks.

The rise of contextual social networks has provided users with specialized spaces to connect and interact with others who share similar passions, hobbies, or professional interests. These platforms offer a personalized and tailored user experience, enhancing engagement and fostering meaningful interactions. Nevertheless, in the pursuit of creating a personalized experience, CSNs collect, process, and store vast amounts of user data.

Protecting user information within CSNs is of paramount importance due to several reasons. Firstly, it upholds user trust and confidence, crucial for the success and sustainability of any social network. Users are more likely to actively participate and share content when they feel their personal information is handled securely. Secondly, privacy breaches can have severe consequences, including identity theft, financial fraud, or emotional distress, potentially tarnishing the reputation of the CSN and resulting in legal and regulatory challenges.

Safeguarding user information in contextual social networks is not only a legal requirement but also an ethical imperative. By prioritizing user privacy and implementing robust security measures, CSNs can foster a safe and trusted environment, encouraging users to engage actively and authentically within their chosen communities. In the subsequent sections of this

guide, we will delve deeper into each of these strategies, providing actionable insights and best practices to ensure the protection of user information in CSNs.

LITERATURE SURVEY

Increasing dependence on anytime-anywhere availability of data and the commensurately increasing fear of losing privacy motivate the need for privacy-preserving techniques. One interesting and common problem occurs when two parties need to privately compute an intersection of their respective sets of data. In doing so, one or both parties must obtain the intersection (if one exists), while neither should learn anything about other set.

Although prior work has yielded a number of effective and elegant Private Set Intersection (PSI) techniques, the quest for efficiency is still underway. This paper explores some PSI variations and constructs several secure protocols that are appreciably more efficient than the state-of-the- art.

Recently, mobile social software has become an active area of research and development. A multitude of systems have been proposed over the past years that try to follow the success of theirInternet bound equivalents. Many mobile solutions try to augment the functionality of existing platforms with location awareness. The price for mobility, however, is typically either the lack ofthe popular friendship exploration features or the costs involved to access a central server requiredfor this functionality. In this paper, we try to address this issue by introducing a decentralized method that is able to explore the social neighborhood of a user by detecting friends of friends. Rather than only exploiting information about the users of the system, the method relies on real friends, and adequately addresses the arising privacy issues. Moreover, we present VENETA, a mobile social networking platform which, among other features, implements our novel friend offriend detection algorithm.

We consider the problem of computing the intersection of private datasets of two parties, where the datasets contain lists of elements taken from a large domain. This problem has many applications for online collaboration. We present protocols, based on the use of homomorphic encryption and balanced hashing, for both semi-honest and malicious environments. For lists of length k, we obtain O(k) communication overhead and O(k ln ln k) computation. The protocol for the semi-honest environment is secure in the standard model, while the protocol for the malicious environment is secure in the random oracle model. We also consider the problem of approximating the size of the intersection, show a linear lower-bound for the communication overhead of solving this problem, and provide a suitable secure protocol. Lastly, we investigate other variants of the matching problem, including extending the protocol to the multi-party settingas well as considering the problem of approximate matching.

SYSTEM ANALYSIS

EXISTING 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.

DISADVANTAGES

•Privacy Concerns and Data Retention: Online matching services may collect a wide range of personal details from users' profiles, including sensitive information such as sexual preferences, drug use, and addresses. Even if users cancel their accounts, these sites might still retain their data, which could potentially be disclosed to advertisers and data aggregatorswithout the users' consent, raising significant privacy concerns.

•Security Vulnerabilities and Risks: Many online matching services might compromise user privacy and security. The paragraph points out that some platforms use counterintuitive privacy settings, and their data management systems have serious security flaws. This could leave users vulnerable to scammers, sexual predators, and reputational damage, highlightingthe potential risks associated with using these services.

PROPOSED SYSTEM

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. 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 user profile 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.

ADVANTAGES

•Enhanced Privacy Protection: The proposed solution focuses on preserving privacy while performing user profile matching in scenarios like online dating within social networks. By encrypting user profiles and queries using homomorphic encryption, the system ensures that even if the database is compromised, the sensitive information remains encrypted and unreadable by unauthorized parties.

•Efficient and Practical Solution: The approach uses multiple servers to efficiently compare user profiles while maintaining privacy. The experiments conducted on real datasets demonstrate that the proposed protocols are not only secure but also practical andefficient, providing users with a reliable method to find similar profiles without compromising their privacy.

IMPLEMENTATION

MODULE DESCRIPTION

- Admin
- Initiator
- Responder

ADMIN:

The role of an administrator (admin) in safeguarding user information in contextual social networks is crucial in maintaining the security, privacy, and trustworthiness of the platform. Admins play a pivotal role in implementing and overseeing various security measures and practices to protect users' personal data. Here are key responsibilities and actions admins should take to safeguard user information:

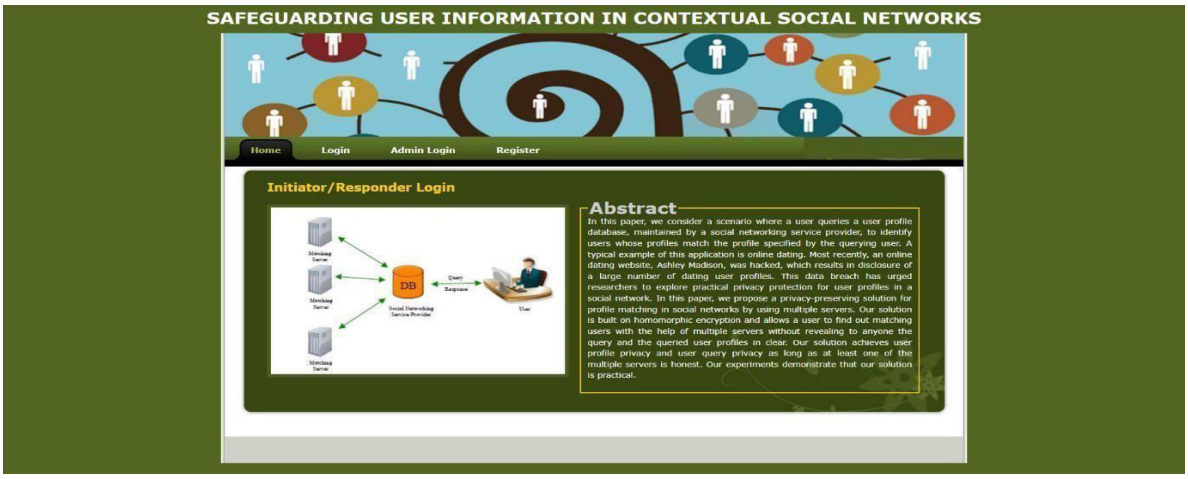
INITIATOR:

The initiator in the context of safeguarding user information in contextual social networks can refer to an individual, a team, or an entity responsible for initiating the development, implementation, and oversight of security measures and practices within the social network platform. This role is essential in ensuring that user information is protected, privacy is maintained, and security measures are effectively implemented. Here's an overview of the role of the initiator in safeguarding user information:

RESPONDER :

A responder in contextual social networks is someone who actively participates inConversations and interactions initiated by others. They engage with the content shared byinitiators, provide responses, contribute to discussions, and help keep the conversation going. Responders play a vital role in creating a dynamic and interactive community within the social network.Here's an overview of the role of a responder in safeguarding user information:

RESULTS



CONCLUSION

Safeguarding user information in contextual social networks involves implementing a comprehensive approach to ensure privacy, security, and responsible data handling within the unique context of these networks. Here's a conclusion summarizing the key aspects of safeguarding user information in contextual social networks.Implement strong encryption techniques to protect user data both in transit and at rest. Utilize robust access control mechanisms to limit access to sensitive information, ensuring that only authorized individuals can view or manipulate the data.Integrate privacy considerations into the design and development of the platform. This includesminimizing the collection of personal data, providing users with clear and transparent privacy policies, and obtaining explicit consent for data processing.

FUTURE SCOPE

Safeguarding user information in contextual social networks is crucial for ensuring user privacy and security. Contextual social networks, which revolve around sharing content within specific contexts or communities, present both unique challenges and opportunities in this regard.Future contextual social networks could offer more granular privacy controls, allowing users to define who can access their content based on contextual factors such as location, time, or social group. This could involve implementing features like time-limited content visibility or geofencing.: Implementing decentralized identity solutions, such as blockchain-based systems, can empower users to have more control over their personal information and how it's shared within contextual social networks.

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.

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

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

[10]C. Gentry, Fully homomorphic encryption using ideal lattices, in STOC 2009, pp 169-178.

[11]Zhe Liu, Le Yu, Wenbo He, "Privacy and Security in Online Social Networks: A Survey" Published in: IEEE Communications Surveys & Tutorials, 2015

[12]Joseph Bonneau, Sören Preibusch, "A Survey of Privacy in Online Social Networks"

Published in: ACM Computing Surveys, 2010

[13]S. Guha, Ravi Kumar, D. Rajan, Andrew Tomkins, "Preserving Privacy in Social Networks" Published in: ACM SIGMOD Record, 2008

[14]David Salomon, "User Data Privacy: Facebook, Cambridge Analytica, and the EU General Data Protection Regulation" Published in: IEEE Security & Privacy, 2018

[15]Mohamed Medhat Gaber, Ajith Abraham, "Data Privacy in Social Networks: A Survey" Published in: Data Mining and Knowledge Discovery, 2010

[16]Wenjia Li, Lingling Xu, et al. , "Privacy-Preserving Location-Based Services for Mobile Users in Cloud Computing" Published in: IEEE Transactions on Emerging Topics in Computing, 2015

[17]Petra M. Mäntylä, Tarmo Toikkanen, "Building Online Communities in Higher Education Institutions: Creating Collaborative Experience" Published in: Springer, 2018

[18]Shouling Ji, et al., "Securing the Privacy of Sensitive User Profile Attributes in Social Networks"