Safeguarding User Information In Contextual Social Networks

Syed Talib Razvi[1], Abdul Sami Khan[2], Mohd Fardeen Pasha[3], Mrs. B. Nagalakshmi[4]
[1,2,3]B.E. Students, Department of IT, Lords Institute of Engineering and Technology, Hyderabad [4]Assistant Professor, Department of IT, Lords Institute of Engineering and Technology, Hyderabad
nagalakshmi@lords.ac.in

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 on the 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 information asked 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.

Keywords: Social Networks, Privacy, Encryption, safeguard, personal information.

I.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[1].

The rise of contextual social networks[11] 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[3].

II.RELATED WORK

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 their internet bound equivalents. Many mobile solutions try to augment the functionality of existing platforms with location awareness[2].

Efficient Robust private set intersection:

Computing Set Intersection privately and efficiently between two mutually mistrusting parties is an important basic procedure in the area of private data mining. Assuring robustness, namely, coping with potentially arbitrarily misbehaving (i.e., malicious) parties, while retaining protocol efficiency (rather than employing costly generic techniques) is an open problem. In this work the first solution to this problem is presented.

Efficient private matching and set intersection:

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 setting as well as considering the problem of approximate matching.

Practical private set intersection protocols with linear complexity:

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.

Serverless friend-of-friend detection in mobile social networking:

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 their internet 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 of the popular friendship exploration features or the costs involved to access a central server required for 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 of friend detection algorithm.

III.RESEARCH METHEDOLOGY

Feasibility Study:

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Economical Feasibility:

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus, the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

Technical Feasibility:

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

Social Feasibility:

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

Feasibility Analysis:

Technical Feasibility:

Technology Stack:

The system's technical prerequisites can be readily fulfilled through the utilization of widely accessible technologies, such as data mining libraries, relational databases, and statistical tools. These foundational components collectively form a robust data in a structured manner, facilitating seamless retrieval and manipulation.

By leveraging these commonplace technologies, the system can harness the full potential of data mining, storage, and analysis, enabling it to operate efficiently and effectively. These readily available resources not only expedite development but also enhance the system's accessibility to a wider audience of developers and practitioners.

scalable and efficient data storage solutions. These databases empower the system to store and manage

Relational databases, exemplified by MySQL, offer

Incorporating HTML, CSS, and Java into the tech stack is essential for building modern, interactive, and visually appealing web application. Here's why these three technologies are integral to any web development project:

HTML(Hypertext Markup Language):

HTML serves as the structural foundation of web pages. It defines the layout and content structure of your application's user interface. With HTML, you can create various elements like forms, headings, paragraphs, and links. It is essential for presenting content to users in a structured and meaningful way.

CSS (Cascading Style Sheets):

CSS complements HTML by providing styling and design capabilities. It allows you to control the visual presentation of your web application, including aspects such as fonts, colors, layout, and responsiveness. By using CSS, you can ensure that your application is visually appealing, user-friendly, and responsive across different devices and screen sizes.

Social Feasibility:

The social feasibility of the "Anomalous User Behavior Detection System" is a critical aspect to consider, as it pertains to the system's acceptance and impact on individuals and society at large. Here, we examine the social feasibility of the system:

User Acceptance: Users may have concerns about the extent to which their behavior is monitored and whether their personal information is adequately protected. It is essential to transparently communicate the system's purpose and data handling practices to address these concerns. We have made sure to comply with all privacy policies suggested by our guides and advisors during the development of this project.

We have also ensured that users understand the system's purpose, how it works, and its benefits in terms of improved security. Providing training and support can enhance user and admin acceptance.

IV. 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 [4].

2.We give a solution for privacy-preserving user profile matching for a single dissimilarity threshold and then extend it for multiple dissimilarity thresholds [5].

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[6].

4.We conduct extensive experiments on areal dataset to evaluate the performance of our proposed protocols under different parameter settings. Experiments show that our solutions are practical and efficient [7].

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. Figure 1: Query-Response Architecture Between User, Service Provider, and Matching Servers in a Social Networking System [8].

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 and efficient, providing users with a reliable method to find similar profiles without compromising their privacy [9,10].

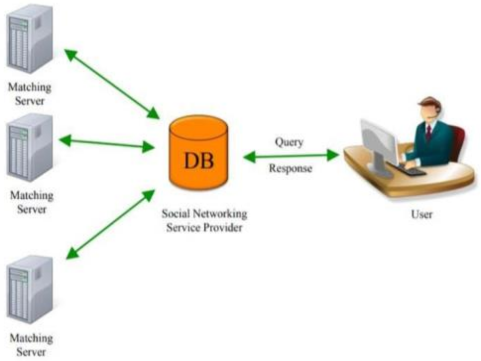


Fig.1: Query-Response Architecture Between User, Service Provider, and Matching Servers in a Social Networking System

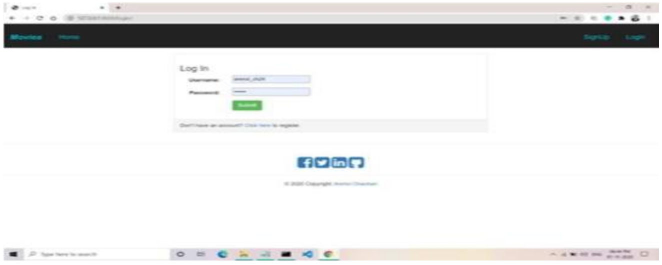
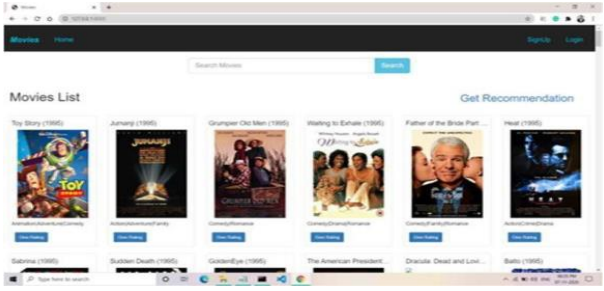


Fig.2 Effects of the operation on our System:



Our system working will suggest the user login system that have to collect the user's al the kinds of behavioral characteristics and that are stored in the database of the user in the mode of the login module of the user.

then after logging in to the system, the system will automatically give the suggestion to the user of the movie based on their recommendation [12],[13].

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.

Fig.3: User Interface of a Movie Recommendation System with Search and Genre Filters

V.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.

VI.REFERENCES

[1] R. Agrawal, A. Evfimievski, and R. Srikant, Information sharing across private databases, in SIGMOD2003, 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 ACM13 (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 EUROCRYPT2004, 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.