PROTECTING CHATTING LABELS ON SOCIAL NETWORKS

K.Hemalatha,
Department of information technology,
IFET College of Engineering,
Villupuram.

Senior Associate Prof. MS.J. Kalaivani,
Department of information technology,
IFET College of Engineering,
Villupuram.

ABSTRACT

In this business world, all information sharing delivering services are done through internet. There should be possibility for the vulnerabilities like brute force attack, cross site scripting, data breaching, SQL injection.Thus Privacy is one of the major concern. However, many solutions like black box testing tool, white box testing tool, web application security scanner etc are enforced, an attacker may still be able to infer one's private information. Proposed model uses sensitive labels based on private key to prevent the personal information from third persons so that the users can chat securely. Furthermore, a social network like chat application will be created and the private key based sensitive labels are applied to this chatting application to analyse the performance. Also the effectiveness of the proposed technique will be analysed.

Keywords-SecureChat,Emailauthentications,Protectattacker,Sensitivelabels,PrivateKey.

OBJECTIVE

The rapid growth of social networks, such as Face book and LinkedIn, more and more researchers found that it is a great opportunity to obtain useful information from these social network data, such as the user behaviour, community growth, disease spreading, etc. However, it is paramount that distributed social network data should not tell private information of individuals.

Thus, how to protect individual's secrecy and at the same time domain the efficacy of social network data becomes a challenging topic. In this paper, we consider a graph model where each apex in the chart is associated with a sensitive label. A graph. Recently, much work has

been done on anonym zing tabular micro data.

EXISTING SYSTEM

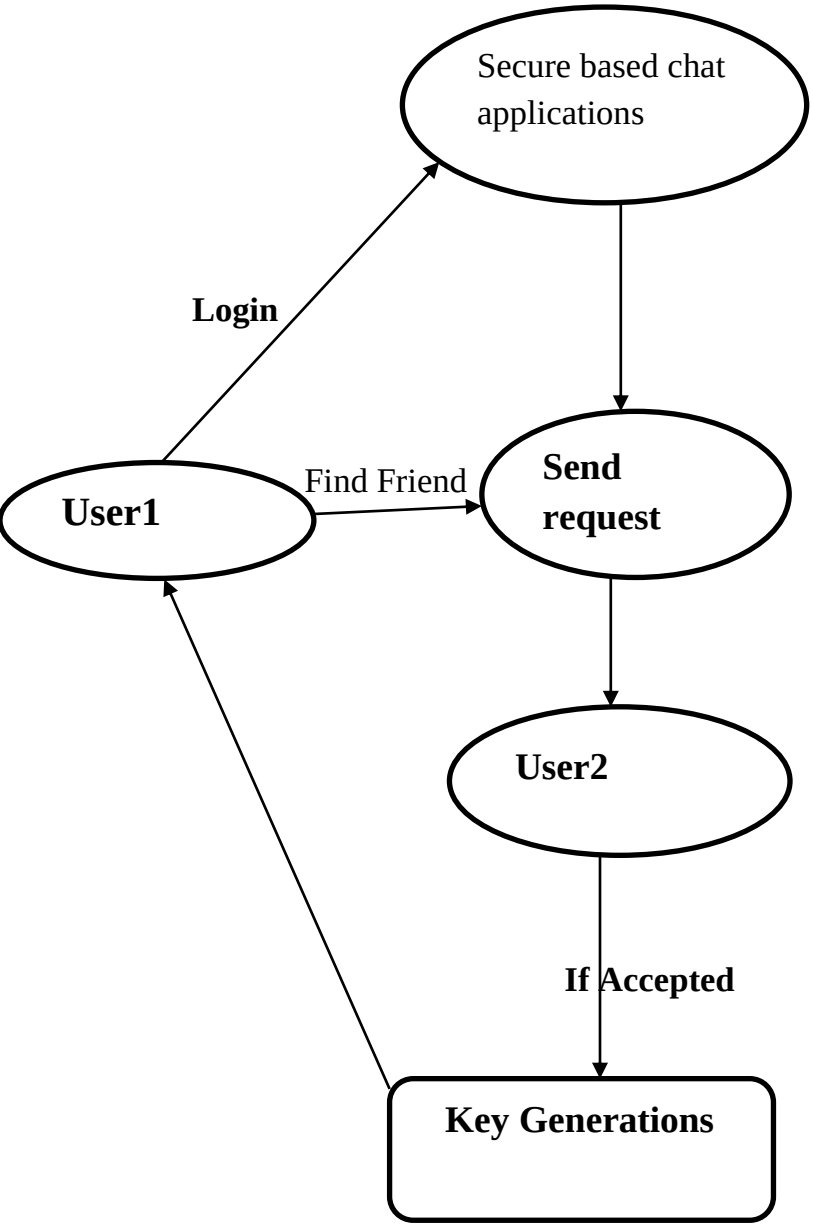
Even when these privacy models are compulsory, an attacker may still be able to assume one's private information if a group of nodes largely share the same sensitive labels. In other words, the label-node connection is not well protected by pure structure Anonymization methods. Furthermore, existing methods, which rely on edge editing or node clustering, may significantly alter key graph properties. In this paper, we define a diversity anonymity model that considers the protection of structural evidence as well as sensitive labels of persons. We further propose a novel Anonymization methodology based on adding noise nodes. We develop a new procedure by adding noise nodes into the original graph with the thought of announcing the least alteration to graph properties.

PROPOSED SYSTEM

A rigorous analysis of the theoretical bounds on the number of noise nodes added and their powers on an important graph property. Our extensive experimental results demonstrate that the noise node adding algorithms can achieve a better result than the earlier work using edge editing only. It is an interesting direction to study knowing algorithms which can decrease the number of noise nodes if the noise nodes contribute to both Anonymization and diversity. Another interesting way is to consider how to implement this safety model in a distributed environment, where different publishers publish their data individually and their data are corresponding.

The data published by each producer satisfy certain secrecy requirements,an attacker can still interruption user's secrecy by combining the data published by different publishers together. Proposed model sensitive labels based on private key generated are used to prevent the personal information from third persons. The users, can chat securely.

System Architecture



FEASIBILITY STUDY

The possibility of the project is examined in this part and business suggestion is put forth with a very general plan for the project and some cost approximations. During system investigation the feasibility study of the proposed system is to be accepted out. This is to confirm that the suggested system is not aimpediment to the company. For feasibility analysis, some accepting of the major requirements for the system is important.

Three key reflections involved in the feasibility enquiry are

- Economic feasibility
- Methodical feasibility
- Social feasibility

CONCLUSION

In a distributed situation, although the data published by each producer satisfy certain secrecy requirements, an invader can still break user's privacy by merging the data published by different originators together. Protocols should be planned to help these publishers publish aintegrated data together to security the privacy. In this paper, we propose a k-degree-l-diversity model for privacy stabilizing social network data publishing. We gadget both distinct l-diversity and recursive -diversity. In order to reach the condition of k-degree-

l-diversity, we design a noise node adding algorithm to idea a new graph from the new graph with the constraint of introducing fewer alterations to the new graph.

REFERENCES

[1] L. Backstrom, C. Dwork, and J.M. Kleinberg, "Wherefore Art Thou

r3579x?: Anonymized Social Networks, Hidden Patterns, and

Structural Steganography," Proc. Int'l Conf. World Wide Web

(WWW), pp. 181-190, 2007.

[2] A.-L. Baraba´si and R. Albert, "Emergence of Scaling in Random

Networks," Science, vol. 286, pp. 509-512, 1999.

[3] S. Bhagat, G. Cormode, B. Krishnamurthy, and D. Srivastava,

"Class-Based Graph Anonymization for Social Network Data,"

Proc. VLDB Endowment, vol. 2, pp. 766-777, 2009.

[4] A. Campan and T.M. Truta, "A Clustering Approach for Data and

Structural Anonymity in Social Networks," Proc. Second ACM

SIGKDD Int'l Workshop Privacy, Security, and Trust in KDD

(PinKDD '08), 2008.

[5] A. Campan, T.M. Truta, and N. Cooper, "P-Sensitive K-Anonymity

with Generalization Constraints," Trans. Data Privacy, vol. 2,

pp. 65-89, 2010.

[6] J. Cheng, A.W.-c. Fu, and J. Liu, "K-Isomorphism: Privacy

Preserving Network Publication against Structural Attacks," Proc.

Int'l Conf. Management of Data, pp. 459-470, 2010.

[7] G. Cormode, D. Srivastava, T. Yu, and Q. Zhang, "Anonymizing

Bipartite Graph Data Using Safe Groupings," Proc. VLDB

Endowment, vol. 1, pp. 833-844, 2008.

[8] S. Das, O. Egecioglu, and A.E. Abbadi, "Privacy Preserving in

Weighted Social Network," Proc. Int'l Conf. Data Eng. (ICDE '10),

pp. 904-907, 2010.

[9] W. Eberle and L. Holder, "Discovering Structural Anomalies in

Graph-Based Data," Proc. IEEE Seventh Int'l Conf. Data Mining

Workshops (ICDM '07), pp. 393-398, 2007.

[10] K.B. Frikken and P. Golle, "Private Social Network Analysis:

How to Assemble Pieces of a Graph Privately," Proc. Fifth

ACM Workshop Privacy in Electronic Soc. (WPES '06), pp. 89-98,

2006.

[11] S.R. Ganta, S. Kasiviswanathan, and A. Smith, “Composition

Attacks and Auxiliary Information in Data Privacy,” Proc. ACMSIGKDD Int’l Conf. Knowledge Discovery and Data Mining, pp. 265-

273, 2008