International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.03, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Enhancing Security of Encrypted Data Sharing on Social Network

Kiran Dhainje[1] , Aditya Shignote[2] , Sakhu Ayare[3] ,

Sonal Mahadik[3],Prof. Kamna Sahu[5]

[1234]Student, Dept of Computer, GSMCOE, Balewadi, Pune, Maharashtra, (India)

[5]Professor, Dept of Computer, GSMCOE, Balewadi, Pune, Maharashtra, (India)

ABSTRACT

In our Proposed system the recognition of the need for a finer grain and more personalized privacy in data publication of social networks. We will propose a privacy protection scheme that not only prevents the disclosure of identity of users but also the disclosure of Selected features in users' profiles. An individual user can select which features of her profile she wishes to conceal. We want to group nodes with as similar neighborhood information as possible so that we can change as few labels as possible and add as few noisy nodes as possible. In this application, we will use hybrid cryptography for providing security while sharing the information. The encryption helps for cryptographic purpose and it also provides attribute base encryption this involves over many people that decrypts the cipher text. It involves the different users and allow to decrypt it based on their policies.

Keywords: Online Social Network, Global Acceptance Ratio, Facebook Worms, Twitter Worms, OSN, Privacy, social networks, Hybrid Cryptography.

I.INTRODUCTION

The real growth of networking, people can store and share their data through online. By sharing the photos, chatting with friends and colleges or by sharing personal records for verification. As people use these technologies, they only anxiety about security. People would like to share its own data with the authorized user. The encryption helps for cryptographic purpose and it also provides attribute base encryption this involves over many people that decrypts the cipher text. It involves the different users and allows to decrypt it based on their policies. Thus, every user can decrypt their own data with security. By applying a new technique like generating the keys that can be only private keys of users.

Social networks are attracting significant interest from researchers in different domains, especially with the advent of social networking systems which enable large-scale collection of network information. However, as much as analysis of such social networks can benefit researchers, it raises serious privacy concerns for the people involved in them. To address such privacy concerns, several techniques, such as kanonymity- based

approaches, have been proposed in the literature to provide user anonymity in published social networks. Sensitive data about users of the online social networks should be protected. In this application, we will use hybrid cryptography for providing more security of information. A hybrid cryptosystem can be constructed using any two separate cryptosystem Symmetric and non-symmetric. But, for creating this application we will use only symmetric cryptography because it is faster than asymmetric cryptography. Our scheme presents a multiparty access control model, which enables the disseminator to update the access policy of cipher text if their attribute satisfy the existing access policy. In this, we will propose a secure data sharing scheme in OSNs based on cipher text-policy attribute-based re-encryption and secret sharing.

1.1.HARDWARE REQUIREMENT

- **Processor** **:** PentiumIV 2.6 ghz
- **RAM** **:** 512 mbdd ram
- **Monitor** **:** 15" color
- **Hard Disk** **:** 20 GB
- **Key Board** **:** Standard Windows Keyboard

For developing this system we will required and Netbeans IDE and implementation language will be Java. Above mention software source are easily available on internet.

II.SOFTWARE REQUIREMENT

- **Operating System** **:** Windows XP/7
- **Programming Language** **:** Java
- **Database** **:** MySQL
- **Tool** **:** Netbeans
- **PROBLEM STATEMENT**

Currently OSNs have come under Sybil attacks. Less secure, data misuse for that we provide the unique solution using the our proposed system

- **LITERATURE SERVEY**

In the previous papers there was best method for sharing the data in [1] secure way that is attribute base system though it works fine it has drawback called third party problem. To overcome this problem we will introduce new algorithm. It will generate user secret key to perform a two way communication. A [2] new generalization approach for sensitive labels, which can afford utility without compromising privacy. In previous papers, author proposed the sensitive label privacy disclosure problem in weighted graph, develop a label anonymous approach. A model for [3] attaining privacy while publishing the data in social networks, in which node labels

are both part of adversaries' background knowledge and sensitive label information that has to be protected. Used [4] k-neighbourhood anonmity for anonymizing social networks based on different privacy protection levels. They showed that the algorithm performs well in terms of protection it provides and also proposed an [5] effective privacy preserve algorithm which resists reidentify attacks successfully with little information loss. Based on message passing, an approach of privacy preserve in social networks proposed in previous papers.

III.SYSTEM ARCHITECTURE

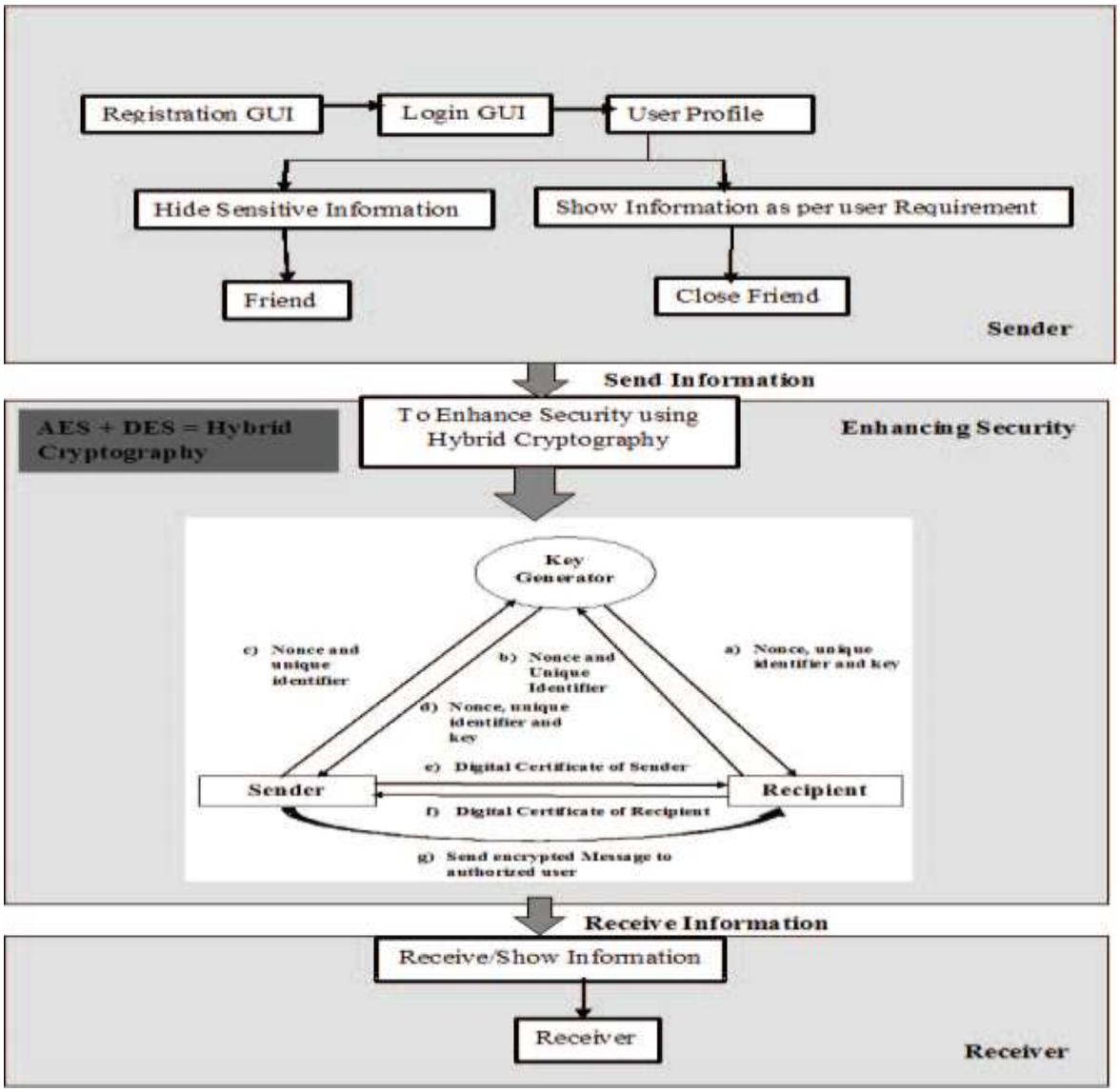

Fig.1 System Architecture.

We also useining the graphical password as sequrity , mail verifications , OTP for authentications .

IV. MATHEMATICAL MODEL

SYSTEM DESCRIPTION:

1. V= V1, V2, V3,……..VN

1. A = A1, A2, A3……..An

1. G = V, E

– System models the friend invitation interactions among users as a directed, signed

– Consider a set V, A set of users registering with our system. This set can be represented as follows :

– These users can perform social activities such as chatting, profile update, add remove friends, search friends etc. Now consider a set a which is a set of social activities, user can perform. This sent can be represented as,

– The main aim of System is to takes as input the friend invitation graph G, and outputs the classification of any node or user u as real, Sybil or unknown.

– The friend invitation graph G is represented as follows:

– Where V Set of nodes or users.

– E represented the set of links.

V.FUTURE SCOPE

Future scope of this technique is that , as it provides more security than the others existed systems more secure login of users is possible .so this technique is not just limited for PDA i.e. personal digital Assistant but also it is very useful for providing protection against Hacking, Dictionary attacks ,etc. In future it will be used for Banking Applications, Mobile phones applications where the security is more important. It also use with the 3D password technique for providing more and more security.

VI.CONCLUSION

This paper deals with the sensitive information of users on social network. In this paper the third party issues about information can be solved using hybrid cryptography. That is more secure than the previous way it is very helpful for between the client and server. Therefore this method attain security and privacy so this method is more climbed to manages the data while sharing in the network work.

REFERENCES

[1] Chen, Ke, et al. "Protecting Sensitive Labels in Weighted Social Networks."Web Information System and Application Conference (WISA), 2013 10th. IEEE, 2013.

[2] Anjaiah, N., and C. H. Ravi. "Protecting the Sensitive Information on Online Social Networks." International Journal of Research 1.9 (2014): 1163-1168.

[3] Lan, Lihui, Hua Jin, and Yang Lu. "Personalized anonymity in social networks data publication." Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference on. Vol. 1. IEEE, 2011.

[4] Zhang, Lijie, and Weining Zhang. "Edge anonymity in social network graphs." Computational Science and Engineering, 2009. CSE'09. International Conference on. Vol. 4. IEEE, 2009.

[5] Xiang, Kelin, et al. "Message Passing Based Privacy Preserve in Social Networks." Multimedia Information Networking and Security (MINES), 2012 Fourth International Conference on. IEEE, 2012.

[6] M Chase, .S.S.M chow, "improving privacy and security in multi authority attribute based encryption" proc .ACM conference on computer and communication security pp.134- 130, 2012.

[7] Attrapadung H. Imai, "conjunctive broadcast and attribute based encryption," proc paring 2012.

[8] S.Rafaeli, D.Hutchison," A survey of key management for secure group communication", ACM computing surveys.

[9] Li Y, Shen H. Anonymizing graphs against weight-based attacks[C]//Data Mining Workshops (ICDMW), 2010 IEEE International Conference on. IEEE, 2010: 491-498.

[10] Backstrom L, Dwork C, Kleinberg J. Wherefore art thour3579x?: anonymized social networks, hidden patterns, and structural steganography[C]//Proceedings of the 16th international conference on World Wide Web. ACM, 2007: 181-190.

[11] Das S, Egecioglu O, El Abbadi A. Anonymizing weighted social network graphs[C]//Data Engineering (ICDE), 2010 IEEE 26th International Conference on. IEEE, 2010: 904-907.

[12] D.Boneh ,M.K Franklin ,"identify based encryption from the weli paring " proc CRYPTO 2010,LNCS Vol,2139,pp.243.