ISSN: 2321-7782 (Online)
Volume 4, Issue 2, February 2016
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Review of Access Control in Decentralized Online Social Network

Neha Charjan[1]
M .E.CSE Department 2nd year & SGBAU university
Amravati - India

Prof. Sneha Bohra[2]
CSE Department & SGBAU university
Amravati - India

Abstract: ***Today, Online social networks (OSNs) suffer from various privacy and security concerns. Many users share their private and personal data on online social network. That is Users are not in the control of their own data and depends on Online Social Network (OSN) operator to enforce access control policies. To address these issues centralized online network replaced by decentralized online social network (DOSN). In DOSN, there is no single provider but the set of peers that take on share of the processor. DOSN removes the central provider and helps to achieve both privacy and security. This paper is about the survey of Decentralized online social Networks (DOSN).***

Keywords: Online Social Network (OSN), Decentralized Online Social Network (DOSN), Predicate Encryption (PE), Reverse Encryption algorithm (REA).

I. INTRODUCTION

For many users in this fully wired Net Generation, OSNs are not only the way to keep in touch but a way of life. It provides various services to the users such as to create public profile, interact over internet by email and instant messaging, sharing of ideas, events, interests and many more. There are numbers of OSN. All contains sensitive information and that why severely suffer from various security and privacy exposures.

Existing social networking services are centralized which provides services that have sole authority to control all the data of the users. Centralized online social network collect and store private information and results in privacy leak because of single provider. Thus, there is a need of more than one provider to recover from privacy leak problem. Thus the solution is decentralization of OSN.

A DOSN is an online social network implemented on a distributed information management platform, such as network of trusted servers or peer to peer systems. Thus, there is no single provider but set of peers that take on share of the task needed to run the system. This helps to remove privacy problem of centralized OSN. The number of DOSN are launched which are mentioned in the literature survey where each uses different techniques to address privacy and security concerns. [1]

II. LITERATURE SURVEY

Cutillo, Molva,Strufe [2] proposed Safebook, in this paper Online social network (OSN) architecture is described. OSN consists of three levels as Social Network (SN), Social Network Service (SNS) and Communication and transport (CT) services as shown in fig 1.

SN level includes corresponds to social interaction in real life like finding friends, commenting, likes etc. To implements these functions SN level relies on SNS level provider. SNS include web access, storage, retrieval, communication and are implemented in centralized or decentralized fashion. SNS level relies on transports and internetworking protocols and infrastructures implemented by CT level. In this architecture attacker may be a malicious member on SN level, a malicious service provider on SNS level or a party may misuse access to the infrastructure at CT level.

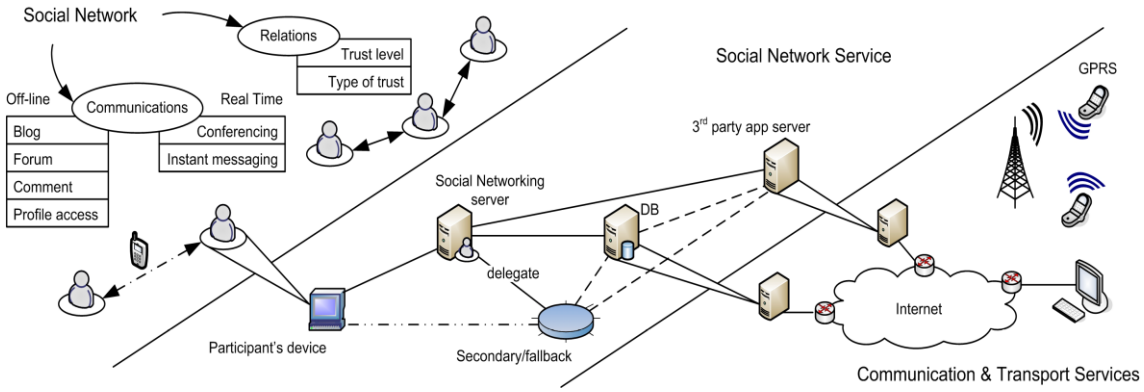

Fig. 1 OSN Architecture

Safebook is a decentralized online social network based on real life trust. It include operations like account creation, Data publication, retrieval of data, Contact request and acceptance, message management etc. It consists of three tier architecture with direct mapping of levels to OSN as shown in fig 2 bellow.

Each party in a safebook is represented by nodes. Nodes in safebook forms two types of overlays as matryoshkas and peer to peer substrate. Where matryoshkas are concentric structures in SN provides data storage and communication privacy created around each node and peer to peer substrate providing lookup services. Safebook also features a Trusted identification service assures that each user gets at most one identifier.

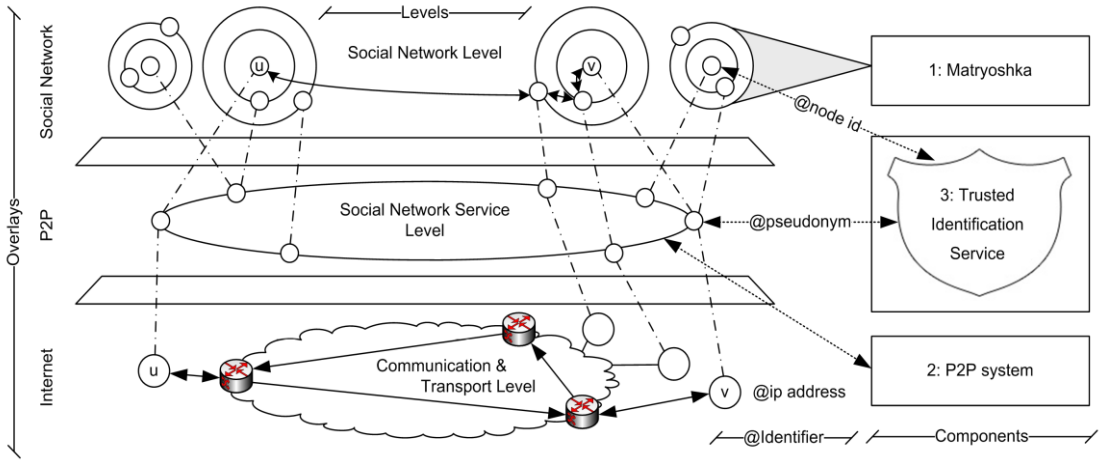

Fig.2 Safebook architecture

Badem, Baden, Spring, Starin [3] presented Persona. Persona provides access control by hiding user data by attribute based encryption. It allows users not to OSN to apply fine grained policy over access to private data. This is achieved by access control list (ACL). ACLs contain users' public keys and their access rights. Thus, Persona does not guarantee privacy and also storage is not trusted.

Nilizadeh, Jahid, Mittal, Kapadia [4] proposed cachet, an architecture that provides strong privacy and security guarantees while preserving the main functionality of OSN. In cachet combination of techniques are necessary for supporting complex functionality requirements of OSNs. It uses an object oriented design for flexible data management, attribute based cryptography for access control, hybrid combination of distributed hash tables and social contacts for information retrieval. Social contacts act as caches to stores the recent updates in social networks and reduces the cryptographic as well as communication overhead in the network. Thus, Cachet protects confidentiality, integrity, availability of user content and privacy of user relationships.

Guenther, Manulis, Strufe [5] presented a cryptographic approach for private profile management by building block for applications in which users maintains their profiles, publish and retrieve data, and authorizes other users to access different portion of data in their profiles. Confidentiality and unlinkability are the two main security and privacy goals for the data which

is kept in profiles and only authorized users are authorized to retrieve this data. It provides specification, analysis and the comparison of two private profile management schemes by different encryption based techniques. For profile management broadcast and symmetric encryption techniques are used.

Bodriagov, Kreitz, Buchegger [6] analyses predicate encryption and adapt it in DOSN context. Univariate polynomial construction is proposed for access policies in PE which drastically increases performance of the scheme but it leaks some part of the access policy to users with access rights. Bloom filter is utilized as a means for decreasing decryption time. PE is only suitable for encrypting for small sets or bounded set of groups of separate identities.

Mousa, Nigm, Faragallah [7] proposed REA (Reverse Encryption algorithm). This is simple, fast and provides maximum security. Also limits the added cost time required for encryption and decryption. The steps of encryption and decryption is shown below in fig.3 and fig.4.

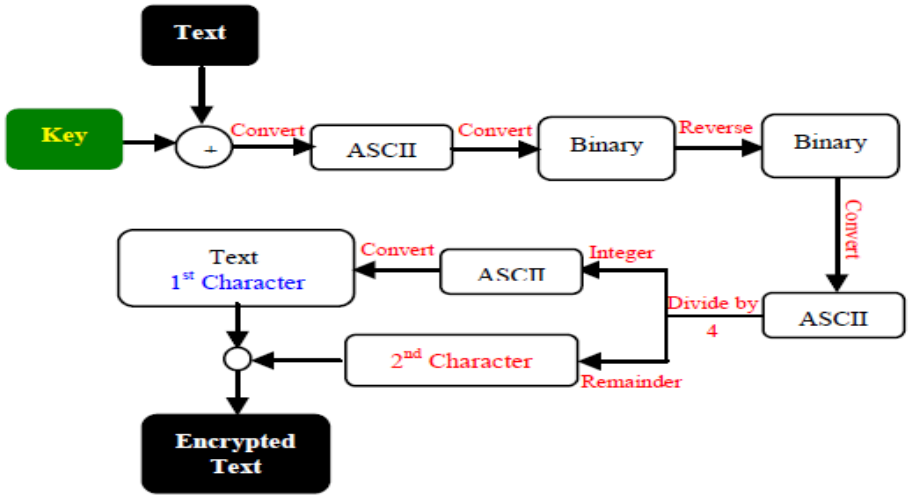

Fig.3 REA Encryption

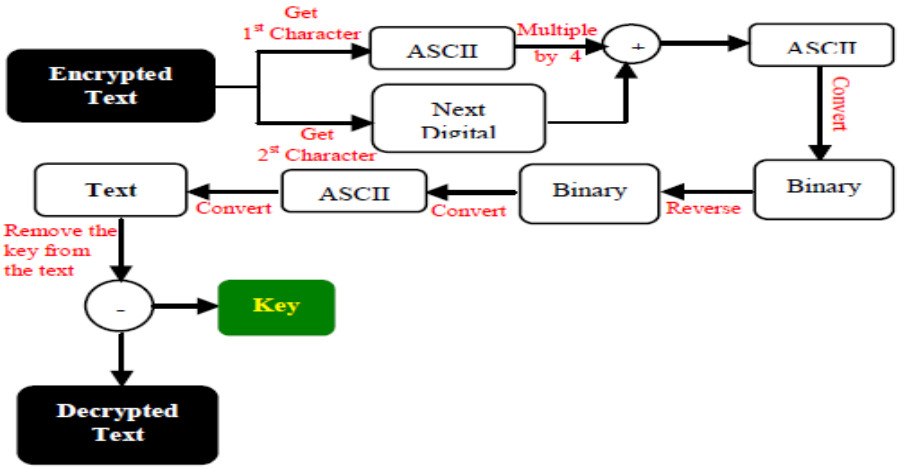

Fig.4 REA Decryption

In this work, security is implemented on user data. Security is achieved by encrypting user's personal data at the time of storage. The stored data on servers is in non readable form. For access control, extension of REA (Reverse Encryption Algorithm) as Bit Shift REA is used and performance is measured in terms of time required for query execution, encryption and decryption.

III. CONCLUSION

DOSN have the potential to provide better environment where users have more control over privacy, security and ownership of their data. This paper is the literature survey of DOSN for achieving more benefits in terms of privacy of data and high performance in the coming.

References

1. Ching-man Au Yeung1, Il aria Liccardi1, Kanghao Lu2, Oshani Seneviratne2, Tim Berners-Lee2," Decentralization: The Future of Online Social Networking", Massachusetts Institute of Technology, Cambridge, MA 02139, USA.
2. Leucio Cutillo, Reflk Molva, Thorsten Strufe, "Safebook: a Privacy Preserving Online Social Network Leveraging on Real-Life Trust", Communications Magazine, IEEE, vol. 47, no. 12, pp. 94 –101, dec. 2009.
3. Randy Badem, Adam Baden, Neil Spring, Bobby Bhattacharjee, and Daniel Starin, "Persona: an Online Social Network with User-Defined Privacy", SIGCOMM'09, August 17-21, 2009, Barcelona, Spain.
4. Shirin Nilizadeh, Sonia Jahid, Prateek Mittal, Nikita Borisov, and Apu Kapadia, "Cachet: a Decentralized Architecture for Privacy Preserving Social Networking with Caching", in CoNEXT. ACM, 2012, pp. 337–348.
5. Felix G¨unther, Mark Manulis, and Thorsten Strufe," Cryptographic Treatment of Private User Profiles", ser. LNCS, vool.7126. Berlin,Heidelberg:Springer-Verlag, 2012, pp.40-54.
6. Oleksandr Bodriagov, Gunnar Kreitz, and Sonja Buchegger, "Access Control in Decentralized Online Social Networks: Applying a Policy-Hiding Cryptographic Scheme and Evaluating Its Performance", KTH Royal Institute of Technology, School of Computer Science and Communication Stockholm, Sweden.
7. Ayman Mousa, Elsayed Nigm, Sayed El-Rabaie and Osama Faragallah," Query Processing Performance on Encrypted Databases by Using the REA Algorithm", International Journal of Network Security, Vol.14, No.5, PP.280-288, Sept. 2012.

