ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 6, Issue 2, pp: (194-197), Month: April - June 2018, Available at: www.researchpublish.com

Multi receiver Predicate Encryption on Online Social Networks

[1]Suresh, [2]Binod, [3]Anjan, [4]Sumit, [5]Kavya K

Abstract: **Here we are describe about online social network based data storage and retrieving process on networking server. Then OSN as online social network server is very popular and most common users to be used. if the users encrypt the messages, then OSN providers cannot generate accurate advertisement to users and different types of social networks using data will be transferred from source to destination between communications as possible. Unfortunately, none of the works on OSNs can achieve both privacy preserving and accurate advertisement simultaneously. We propose the first multireceiver predicate encryption scheme for OSN platforms. Not only does the proposed scheme protect the users' privacy but it achieves customized advertisement as well. In this section with giving input data as video to be encrypted with send the data for destination. Finally another user is receiving given data with using data decryption.**

Keywords: **online social network, OSN platforms, predicate encryption.**

1. INTRODUCTION

INTERNET and cloud computing are thriving over the whole world in recent years. One of the most popular and diverse services is online social networks (OSNs), such as Facebook, Google, Dropbox, Twitter, and so on. A lot of personal information will be stored into OSN platforms, so that the security of OSN platforms should be guaranteed. Many works on t heprivacy preservation of OSNs have been proposed. I n t he architecture of an OSN platform, OSN providers make profits from advertisement revenue to enable continued operations. However, protecting user privacy and producing accurate advertisement simultaneously might be a contradiction in OSN platforms due to the following reasons. OSN providers extract the keywords from users' data and messages for advertisers. However, this needs users' data to be in non-encrypted forms and thus exposes the privacy of users. If users encrypt the data before posting f or privacy pre-serving, then OSN providers cannot extract the keywords from the cipher text. A straight forward solution t o t his problem would be predicate encryption (PE), which was first introduced by Katz et al. in 2008. Such encryption mechanisms provide an evaluation for encrypted messages with predicate tokens, which makes it feasible to search in cipher text space. There are two types in PE: asymmetric predicate encryption (ASPE) and symmetric predicate encryption (SPE). The main difference between these two types is the identity of the searcher. SPE is appropriate for the systems where t he searcher is the one who encrypts the data, such as personal cloud storages. I n an ASPE system, nevertheless, the searcher is not necessarily the encryptor of the data. Hence, ASPE is fitting f or secure e-mail systems or credit card payment gateways. It seems that ASPE might be more suitable in solving the contradictory scenario in OSN platforms. Further-more, the keywords of ASPE are associated with the cipher text, which is suitable f or OSN providers to produce customized advertisement efficiently. When ASPE is applied, however, the encryption procedure needs to use the parameters defined by the receiver to enable the search. This requirement will cause a great cost on communication. For instance, if a sender wants to share a file with an n-dimensional predicate vector to t receivers, then it will result in a ciphertext of O (n × t) length. In order to cope with the problems mentioned above for the OSN plat-form, we propose a multi-receiver predicate encryption (MRPE) scheme. The main difference between ASPE and MRPE is that, in an ASPE scheme, each user will generate his own public parameters. As we mentioned above, this would lead to the un-desirable expansion of ciphertexts, since a s ender should use different public parameters to execute the encryption algorithm for each receiver. In our MRPE scheme, the public parameters are defined by a third party, and the encryption process can be performed with inputting a set of receivers. Since the public parameters are independent of the receivers, the length of a cipher text can be compressed. This property cannot be achieved in ASPE because in an ASPE, a tuple of public parameters would correspond to a secret key.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 6, Issue 2, pp: (194-197), Month: April - June 2018, Available at: www.researchpublish.com

2. EXISTING SYSTEM

A straight forward solution to this problem would be predicate encryption (PE), which was first introduced in 2008. Such encryption mechanisms provide an evaluation for encrypted messages with predicate tokens, which makes it feasible to search in cipher text space. Here social networks are mainly used for data transferring for it seems that ASPE might be more suitable in solving the contradictory scenario in OSN platforms. Further-more, the keywords of ASPE are associated with the cipher text, which is suitable for OSN providers to produce customized advertisement efficiently. When ASPE is applied, however, the encryption procedure needs to use the parameters defined by the receiver to enable the search. Social networks with different Medias using data will be transferred but here multiple users using this website and easily hacking some secret informations and there is no scheme that can solve the problems mentioned in Section I of the OSN platforms. In order to cope with the problems, we have proposed a multi-receiver predicate encryption scheme, Decreases Face-to-Face Communication Skills on social networks with one of main problem and easily cheating with others. So here social networking based what are those problems we are described in this section to be list of below.

Demerits of Social Networks:

- Lacks Emotional Connection
- Decreases Face-to-Face Communication Skills
- Conveys Inauthentic Expression of Feelings
- Causes Face-to-Face Interactions to Feel Disconnected
- Facilitates Laziness

Existing Architecture:

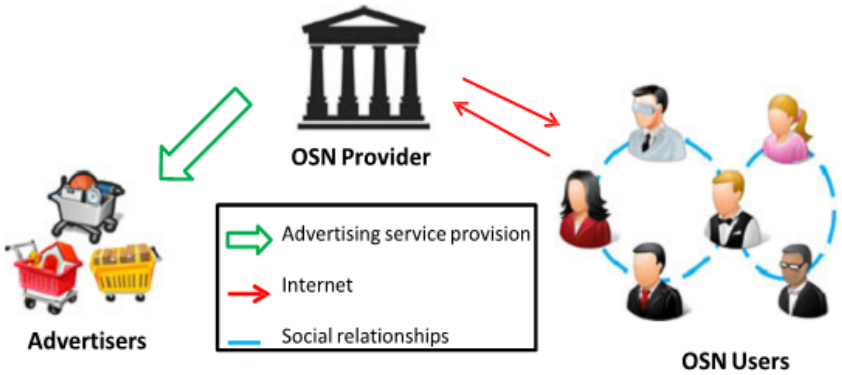

Fig. 1. The model of online social networks.

3. PROPOSED SYSTEM

Online social network (OSN) is a very popular service. Since a lot of personal information is stored on the OSN platform, privacy protection on such an application has become a critical issue. If the users encrypt their messages, then OSN providers cannot generate accurate advertisement to users.Wepropose the first multi receiver predicate encryption scheme for OSN platforms. Not only does the proposed scheme protects the users' privacy but it achieves customized advertisement as well. One of the most popular and diverse services is online social networks (OSNs), such as Facebook,Google, Dropbox, Twitter, and so on.OSN providers extract the keywords from users' data andmessages for advertisers.If users encrypt the data before posting f or privacy pre-serving, then OSN providers cannot extract the keywordsfrom the ciphertext.Thus, when the proposed MRPE scheme is applied to OSN, not only do the users protect their privacy but also t heycan search the interested ciphertext efficiently. For those users who upload information and keep in touch with their friends in online social networks, OSN providers offer the storage for t hem to store, upload, share,and view the data.

Merits:

- Easily communicate with other peoples on world.
- Data will be transferred or communicated with short times.
- Invaluable Promotional Tool & Helps to Catch and Convict Criminals.
- Information Spreads Incredibly Fast.

4. METHODOLOGY

Online Social Networks (OSNs) have become part of daily life for millions of users. Users building explicit networks that represent their social relationships and often share a wealth of personal information to their own benefit. The potential privacy risks of such behaviour are often underestimated or ignored. The problem is exacerbated by lacking experience and awareness in users, as well as poorly designed tools for privacy -management on the part of the OSN. Furthermore, the centralized nature of OSNs makes users dependent and puts the Service Provider in a position of power. Because Service Providers are not by definition trusted or trustworthy, their practices need to be taken into account when considering privacy risks. This chapter aims to provide insight into privacy in OSNs. First, a classification of different types of OSNs based on their nature and purpose is made. Next, different types of data contained in OSNs are distinguished. The associated privacy risks in relation to both users and Service Providers are identified, and finally relevant research areas for privacy-protecting techniques are discussed. Clear mappings are made to reflect typical relations that exist between OSN type, data type, particular privacy risks and privacy-preserving solutions. Even though Social Networks have always been an important part of daily life, now that more and more people are connected to the Internet, their online counterparts are fulfilling an increasingly important role. OSNs have also become a hot topic in areas of research ranging from sociology to computer science and mathematics. Aside from allowing users to create a network to represent their social ties, many OSNs facilitate uploading of multimedia content, various ways of communication and sharing many aspects of daily life with friends. People can stay in touch with (physically remote) friends, easily share content and experiences and stay up to date in the comfort of their own home or when on the move. However, benefits aside, potential threats to user privacy are often underestimated. For example, due to the public nature of many OSNs and the Internet itself, Current social networks require users to place absolute faith in their operators, and the inability of operators to protect users from malicious agents has led to sensitive private information being made public. We propose an architecture for social networking that protects users' social information from both the operator and other network users. This architecture builds a social network out of smart clients and an untrusted central server in a way that removes the need for faith in network operators and gives users control of their privacy. Many may not think about it, but using a social network thought to be a sobering activity, as it requires the user to place absolute faith in the Social Network Operator (SNO). First, the social network user provides the SNO with a great deal of personal information which an attacker could use to answer personal knowledge questions and thus impersonate the user. Next, the user tells the SNO who their real-life friends are, which is highly valuable information to those conducting targeted phishing attacks. The user then posts comments and photographs of which some SNOs may claim ownership. Finally, even if it they are legal and appropriate in context, these comments and photographs could cause material harm to the user should they come to light in another context [19] and thus expose the user to the threat of blackmail . SNOs have databases with such information for millions of users, and their incentives—mostly pertaining to growth—may not be aligned with those of their users. Users wishing to protect their personal information must have alternatives which do not rely on the all-knowing SNO: no matter how incompetent or wicked a network operator is, users should be able to expect that their private information is only shared with others when they desire it.

5. CONCLUSION

Due to the thriving nature of internet and cloud computing, OSN platforms have become a popular application. The most important issue is protecting users' privacy and generating accurate advertisement simultaneously in OSN platforms. However, there is no scheme that can solve the problems mentioned in Section I of the OSN platforms. In order to cope with the problems, we have proposed a multi-receiver predicate encryption scheme, which can achieve both privacy pre-serving and customized advertisement. The proposed scheme is the first multi-receiver predicate encryption and our work supports a user to search for his interested data encrypted and shared by other users in the OSN platform.

Future Enhancements:

In this section with enhancements for networking with the proposed scheme greatly reduces the size of ciphertext. In the future works, we will further improve it to reach constant size of ciphertext and achieve CCA security in the standard model. Thus, we need to develop privacy – preserving framework that overcomes the worries in privacy security y and encourage users to adopt cloud storage services confidently.

REFERENCES

[1] J. Anderson, J. Diaz, C. Bonneau, and F. Stajano, "Privacy -enabling social networking over untrusted networks," in Proc. Workshop Online Social Netw., 2009, pp. 1–6.

[2] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin, "Persona: An Online Social Network with User-Defined Privacy.

[3] J. Katz and A. Yerukhimovich, "On black-box constructions of predicateencryption from trapdoor permutations," in Proc. 15th Int. Conf. TheoryAppl. C ryptol. I nf. S ecur., Adv. C ryptol. , Tokyo, Japan, Dec. 6–10, 2009, pp. 197.

[4] Y. Kawai and K. Takashima, "Predicate- and attribute-hiding inner productencryption in a public key setting," in Pairing-Based Cryptography— Pairing , vol. 8365, Berlin, Germany : Springer, 2013, pp. 113–130.

[5] N. Koblitz, A. Menezes, and S. Vanstone, "The state of elliptic curve cryptography," Des. Codes Cryptography, vol. 19, pp. 173–193, 2000.

[6] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B . Waters, "Fullysecure functional encryption: Attribute-based encryption and (hierarchical) innerproduct encryption," in Proc. Adv. Cryptology—EUROCRYPT2010 (LNCS), vol. 6110, Berlin, Germany: Springer, 2010, pp. 62–91.