INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 3)
Available online at: www.ijariit.com

Secure multi-receiver data exchange for OSNs using predicate encryption

Pavithra A
pavithraa.ise@gmail.com
Bangalore Institute of Technology, Bengaluru, Karnataka

Hema Jagadish
hema.shravu@gmail.com
Bangalore Institute of Technology, Bengaluru, Karnataka

ABSTRACT

Online Social Network is an extremely prevalent administration among utilizations of the web and distributed computing. Security assurance has turned into a noteworthy issue in light of the fact that a considerable measure of individual data is put away on the OSN stage. To make proceeded with tasks OSN stages require promotion income. Assume if clients encode their messages for security reason, the OSN suppliers can't produce an exact notice to the clients who are associated with that system. It was exceptionally Intricate to all the while accomplish both securities safeguarding client's information and also an exact advertisement to the clients. Thus a secure multi receiver data exchange scheme using predicate encryption plot is proposed for OSN systems which ensures clients security and furthermore accomplishes modified commercial too. Also, users are allowed to view data only for the specified amount of time allows no more data stealers can access data. Contrasted and other predicate encryptions that are conveyed for OSN stages proposed to conspire increases substantially shorter ciphertext.

Keywords: *Secure Multireceiver, Predicate Encryption, Advertisements, and Online Social Network.*

1. INTRODUCTION

Internet and Cloud computing are growing vigorously over the world for recent years. Online Social Networks (OSNs) is one of the most popular and diverse services. Famous OSNs are Google, Facebook, Google, Dropbox, and Twitter and so on. A huge amount of information is stored into OSN platforms, hence the security of OSNs platform should be guaranteed. OSN providers is a part of OSN platform makes a profit from advertisement revenue to enable continued operations. Fig1 shows the architecture of Online Social Network. To easily share information with each other, possibly selected, users for professional, or personal purposes, every OSN user has to create his or her own OSN profile and make use of available OSN application for data exchange. For exchanging and sharing more personal information like contact data, photographs, and videos OSN with a more private and leisure-oriented background are most widely used.

1.1LiteratureSurvey

Web and distributed computing are flourishing over the entirety world lately. A standout amongst the most well known and various. Administrations is online informal communities (OSNs, for example, Facebook, Google, Dropbox, Twitter, et cetera. A considerable measure of individual data will be put away into OSN stages, with the goal that the security of OSN stages ought to be ensured. Numerous chips away at the protection safeguarding of OSNs have been proposed. In the engineering of an OSN stage, OSN suppliers make benefits from ad income to empower proceeded with activities. In any case, securing client protection and delivering precise promotion all the while may be a logical inconsistency in OSN stages because of the accompanying reasons.

1) OSN suppliers separate the catchphrases from clients' information and messages for sponsors. Be that as it may, this needs clients' information to be in non-encoded structures and in this way uncovered the protection of clients.

2) If clients scramble the information before posting for security safeguarding, at that point OSN suppliers can't remove the watchwords from the ciphertext.

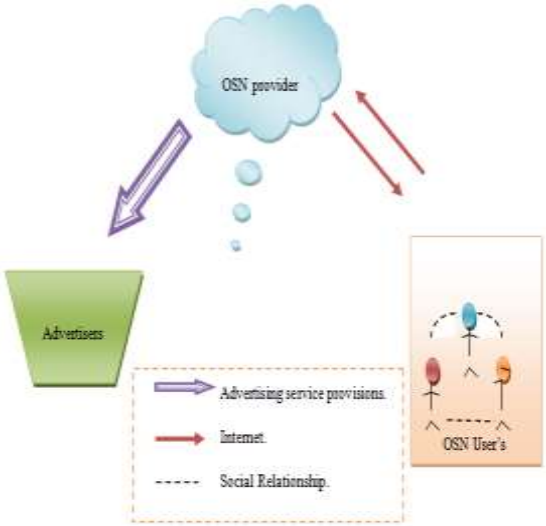

Fig. 1: Model of Online Social Network Architecture

2. METHODOLOGY

Users can securely share the data. To do so, first, users have to register into OSN, using login credentials the users can share the data into OSN. Before uploading data into OSN, users have to encrypt the data. Fig 2 shows Construction of SMDE Platform.

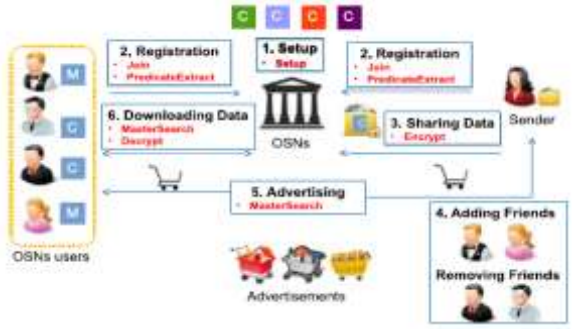

Fig 2: Proposed SMDE Architecture

At to start with, the OSN supplier runs Setup where it creates its master key and the general population parameters for the stage. A client runs the Registering calculation to join the OSN stage. At the point when a client joins this stage and picks his own particular key combine, the OSN supplier can deliver predicate tokens for the client to locate the coordinated information effectively. By utilizing the Sharing Data calculation, a sender encrypts his information and sends them to the recipients when he wants to share them with the beneficiaries in the OSN stage. In the event that a sender might want to include or expel companions, he can play out the Adding/Removing Friends calculation. The OSN supplier executes the Advertising calculation to check if some predefined business watchwords exist in the scrambled information of clients, and the promoters can issue modified commercial to those clients whose encoded information contain the watchwords. At long last, a client plays out the Downloading Data calculation to discover intrigued information and unscramble them productively. The stream of the proposed development is additionally delineated in Fig. 2.

Setup

The OSN supplier executes Setup(1^n) to create the framework parameters and the master secret key. The OSN supplier distributes param and keeps msk mystery.

Registering in the OSN platform

When a client i joins the framework, he performs Join(i) to create his own key combine (PKi, SKi).. At that point, client i sends the list i to the OSN supplier for enlistment and keeps SKi as mystery. a

User i can pick and send predicate vectors to the OSN supplier to ask for predicate tokens. After getting a predicate vector $\vec{v}$, the OSN supplier calls Predicate Extract$(param, \overrightarrow{v})$ to figure a predicate token SK $\vec{v}$ for client i which is related with $\vec{v}$ and can give client i to an undecryptable hunt.

Sharing Data

Let f_w= {i |user i is a companion of user w} be the list set of the companions of client w in the OSN stage. On the off chance that client w might want to impart to his companions in the information M associated with a key word vector $\vec{x}$, he can perform

Encrypt$\{PKi\}_{i \in fw}$
$(param, M, \vec{x})$to get the ciphertext
$C = (\{C'_i\}_{i \in fw}, C_0, \{C_{1,j}, C_{2,j}\}^{n}_{j=1})$.

At that point, he sends the ciphertext C to his companions by means of the OSN stage**.**

Adding Friends/ Removing Friends

If client w might want to include another companion, say client i, at that point he should refresh his companion set

$f_w = f_w + \{i\}$ in the OSN stage.

User w can refresh his companion set $f_w = f_w - \{j\}$ in the OSN stage on the off chance that he needs to expel client j from his companion list.

Advertising

At the point when the OSN supplier might want to check if a ciphertext C coordinates a predicate $\vec{v}$, it can figure $SK\vec{v}$=$\boldsymbol{PredicateExtract}$ $(param, \vec{v})$and execute **MasterSearch** $(param, C, SK\vec{v})$.The OSN provider can just search matched ciphertexts but it cannot decrypt them. If the output is 1, the advertiser can send the advertisement corresponding to $\overrightarrow{v}$ to those users who can decrypt C.Otherwise (i.e., the output is $\perp$), C does not match $\vec{v}$.

Downloading Data

If user *i* would like to find the ciphertexts matching $\vec{v}$ in his received ciphertexts, *Cij* 's, he can get
$SK\vec{v}$, = $\boldsymbol{PredicateExtract}$ $(param, \vec{v})$and run **MasterSearch** $(param, C\ SK\vec{v})$.for each *Cij* . Then, he downloads*Ci_v = {Cij*| **MasterSearch** (*param,Cij , SK*)= 1*}* and executes**Decrypt** (*param,Cij , SK*$\vec{v}$, *SKi*)for each *Cij* in *Ci_v* by using his secret key *SKi*. Onthe other hand, the unselected receivers of a ciphertext are unable to decrypt the ciphertext uploaded by the sender.

3. SECURE MULTI RECEIVER DATA EXCHANGE (SMDE) USING PREDICATE ENCRYPTION

SMDE Scheme comprises six calculations, **Setup**, **Join**, **PredicateExtract**, **Encrypt**, **MasterSearch**, and **Decrypt**.

Step-1 $\boldsymbol{Setup}$ is a calculation that takes input as a security parameter (l^n). It restores master key msk and system parameters $param$.

Step-2 $\boldsymbol{Join}$ is a calculation that takes i as input which is an index of user i.It res tores a keypair (PKi, SKi). Composing this as $\boldsymbol{Join}(\boldsymbol{i}) \rightarrow (PKi, SKi)$.

Step-3 $\boldsymbol{PredicateExtract}$ is a calculation that takes predicate vector $\vec{v}$. It restores a predicate token SKv. Composing this as $\boldsymbol{PredicateExtract}$ $(param, v)$.

Step-4 $\boldsymbol{Encrypt}$ is a calculation that takes input as $param$, a message M, keyword vector x and a set $\{PK1, PK2, \ldots . PKt\}$ containing the public keys of t receivers. It restores a ciphertext C. Composing this as $\boldsymbol{Encrypt}\{PKi\}^{t}_{i=1}(param, M, X) \rightarrow C$.

Step-5 $\boldsymbol{MasterSearch}$ is an algorithm that takes $param$ as input, a ciphertext C, and a predicate token vector v. It returns 1 or distinguished symbol $\perp$. Composing $\boldsymbol{MasterSearch}(param, C, SK, \vec{v}) \rightarrow 1/\perp$.

Step-6 Decrypt is an algorithm that takes a $param$ as input, a ciphertext C, a predicate token $SK\vec{v}$ of predicate vector $\vec{v}$, and secret key SK_i. It returns a message M. Composing this as $\boldsymbol{Decrypt}(param, C, SK\vec{v}, SK_i) \rightarrow M$.

4. CONCLUSION

Secure MultiReceiver Data Exchange (SMDE) Tool solves the most important issue in protecting user's privacy and generating accurate advertisement simultaneously. Sending accurate advertisement to the data users may help the client who has to tie-up with certain brand companies. It also helps a client of the application to get the benefit of preserving user's data. Since the most important data are available only for authorized users, the data is securely transmitted over the internet with better predicate encryption techniques. Multiple authorized users can have access to the precious data which are generated by the team experts in an organization.

5. REFERENCES

[1] Chun-I Fan, Member, IEEE, Yi-Fan Tseng, Jheng-Jia Huang, Shih-Fen Chen, and Hiroaki Kikuch , Member, IEEE," Multireceiver Predicate Encryption for Online Social Networks", IEEE Transactions On Signal And Information Processing Over Networks, Vol. 3, No. 2, June 2017

[2] I. Fan and S. Y. Huang, "Controllable privacy-preserving search based on symmetric predicate encryption in cloud storage," Future Gener. Comput.Syst., vol. 29, no. 7, pp. 1716–1724, 2013.

[3] H. Tran, H. L. Nguyen, W. Zha, and W. K. Ng, "Towards security insharing data on cloud-based social networks," in Proc. 8th Int. Conf. Inf.Commun. Signal Process., 2011, pp. 1–5.

[4] Y. H. Lin, C. Y. Wang, and W. T. Chen, "A content privacy-preserving protocol for energy efficient access to commercial online social networks," in Proc. IEEE Int. Conf. Commun., 2014, pp. 325–341.

