Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 4 – No.9, April 2016 – www.caeaccess.org

Social Network with Dynamic Identity-based Broadcast Encryption using Security Tree

Ali Meligy
Minufiya University,
Minufiya, Egypt

Ayman Alazab
Minufiya University,
Minufiya, Egypt

ABSTRACT
In this paper, we suggest the security tree scheme using dynamic identity-based broadcast encryption, using this scheme, it is possible to parted a message to many linked nodes and represent these nodes as security tree and give every receiver permission to read special linked nodes from security tree.

General Terms
Online Social Website is stretched over worldwide such as Facebook, Linked In; and then there are many security threats by attackers. In addition because sensitive data is concentrated on the central server, privacy can by expose to SNS provider as well as malicious users. To overcome this problem, many previous researches suggest data may not be stored in central server. When a user transmits a message, then server does not interfere with the process. Thus, the user who transmits a message needs way to message thee key that are used to message the key that are used for message encryption scheme.

Keywords
Social Network Service, Decentralized, DIBBE, Security Tree.

1. INTRODUCTION
Online Social website is stretched over worldwide such as Facebook, Linked In; Social Network Service market is stretched over worldwide. According to e-markets survey, the number of SNS users seems to surpass the 10 million users worldwide [1]. According as many users use SNS, Privacy exposure has become a problem. To overcome this problem, each service provides different solutions. Nevertheless, privacy exposure is still a problem, becomes sensitive data generated by users stores in central server. To overcome this problem, many previous researches suggest decentralized system SNS [3], [4], [5]. Unlike the centralized system, the systems have the concept of peer to peer network. Thus communication between the users is carried without the central provider because the decentralized systems do not have the central provider; the users in the systems should have the security systems without the central provider. When we need to send a message that contain more than one part, and we need to allocate for each receiver a special part. Above all, the system need to the encryption scheme for transmitting the user's information and linked nodes that determined parts for each receiver. In this paper, we suggest the security tree for encryption in decentralized systems. In the system does not have the central server, each user have a key and list of linked nodes in security tree that determined special nodes to decrypt from your message? To obtain the efficient security tree in encryption message in decentralized system. We will use the concept the dynamic identity-based broadcast encryption scheme proposed by Jiang [7]. This paper organized as follow section II reviews identity-based broadcast encryption scheme. Section III explains the methods that used to modify Jiang, H's DIBBE scheme. Section IV explains the results that obtain by modify Jiang scheme. Section V discuss of roll scheme. Section VI concludes.

2. RELATED WORK
Identity-Based Encryption [8] is type of public key encryption. The encryption is suggested by Shamir 1984. In this cryptosystem, the public and identifiable information such e-mail, phone number is used as public key and private generator generates the corresponding private key. The sender's uses and IBE do not need to look up the public keys and corresponding certificates of the receivers, because the identities (e.g. emails or IP addresses) together with common public parameters are sufficient for encryption.

The concept of identity-based broadcast encryption scheme [6], the authority generates user's private key using master secret key and each user identity, and transmits an encrypted message through a broadcast channel. Then valid receiver can decryption the message using has private key.

Identity-Based Broadcast Encryption has some problem. First, the maximum number of users should be predetermined. Second, each receiver must know all of the receivers. However, it is natural that each receiver knows only his own information. To solve these problems, the concept of Dynamic Identity-Based Broadcast Encryption was introduced by Jiang [7]. This scheme consists of four algorithms: Setup, Extract, Encrypt and Decrypt.

3. METHODS
In this paper, we will parted a message to many parts, this parts represent as linked nodes, node that represent container of data. These linked nodes represent as binary tree that refer to security tree. In Jiang H's DIBBE Scheme [7], we need to modified Encrypt and Decrypt algorithm to parted the message and apply Security Tree.

3.1 Security Tree
In this paper, we will define a security tree as a binary tree that contains a finite set of one or more data items (or nodes) such that: 1-There is a special node called the root of tree. 2-Removing nodes (or data item) are partitioned into number of mutually exclusive (i.e., disjoined) subsets each of which is itself a tree are called sub tree. Now we discuss a two ways of representing binary tree T in memory: 1-Sequential representation using arrays 2-Linked List representation.

Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 4 – No.9, April 2016 – www.caeaccess.org

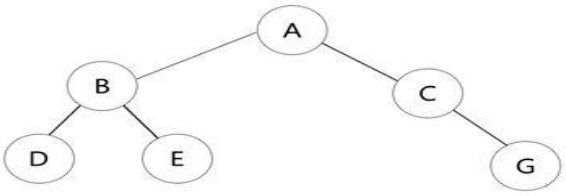

Figure 1. Binary Tree

An array can be used to store the nodes of a binary tree; the nodes in an array of memory can be accessed sequentially.

Figure 2. Array Representation of Binary Tree

The most popular and practical way of representing a binary tree is using linked list (or pointers). In linked list, every element is represented as nodes. A node consists of three fields such as: 1- Left child (L Child). 2- Information of the Node (Info). 3- Right child (R Child). The L child links to the left child node of the parent node. Info holds the information of every node and R child holds the address of right child node of the parent node (see Figure 3).

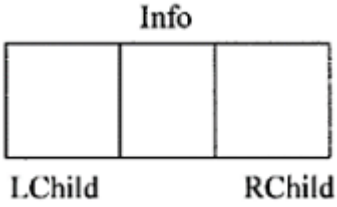

Figure 3. The Structure of a Binary Tree Node

Following figure (Figure 4) shows the linked list representation of the binary tree in Figure 1.

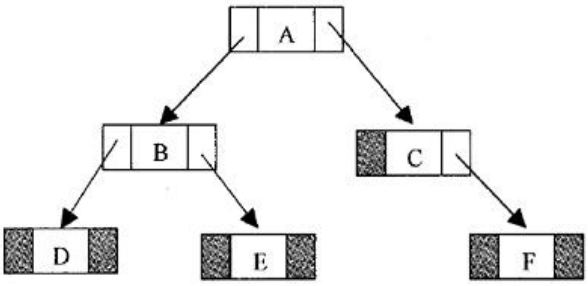

Figure 4. Linked List Representation of Binary Tree

The basic operations that are commonly performed a binary tree is listed below: Create an empty binary tree, traversing a binary tree, inserting a new node, deleting a node, searching for a node.

Tree traversal is one of the most common operations performed on tree data structures. It is a way in which each node in the tree is visited exactly once in a systematic manner. There are three ways of traversing a binary tree. They are: pre Order Traversal (Node-left-right), in Order Traversal (Left-node-right), post Order Traversal (Left-right-node).

A binary search tree is a binary tree, which is either empty or satisfies the following properties: every node has a value and no two nodes have the same value (i.e., all the values are unique), if there exists a left child or left sub tree then its value is less than the value of the root and the value(s) in the right child or right sub tree is larger than the value of the node. All the nodes or sub trees of the left and right children follows above rules.

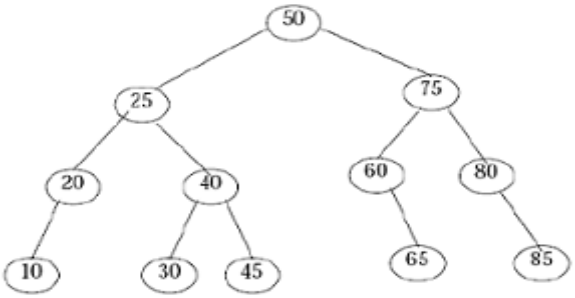

Figure 5. Typical Binary Search Tree

The operations performed on binary tree can also be applied to binary search tree (BST) inserting a node, searching a node and deleting a node. Another most commonly performed operation on BST is traversal. The tree traversal algorithms (pre-order, post-order and in-order) are the stander way of traversing a binary search tree.

A BST is constructed by the repeated insertion of new nodes to the tree structure. Inserting a node in to a tree is achieved by performing two operations: The tree must be searched to determine where the node is to be inserted and then the node is inserted into the tree.

Searching a node was part of the operation performed during insertion. When searcher searches about node we will compare root value if large than root direct right else direct left until reach a node that we want.

This section gives an operation to delete a DATA of information from a binary tree. First search and locate the node to be deleted. Then any one of the following conditions arises: The node to be deleted has no children, the node has exactly one child (or sub trees, left or right sub tree) and the node has two children (or two sub trees, left and right sub tree).

3.2 Setup (λ)

Given the security parameter λ a bilinear map group system $B = (P, G_1, G_2, G_T, e(.,.))$ is constructed such that |P|=λ. Also, two generators $g \in G_1$ and $h \in G_2$ are randomly selected as well as a secret value $\gamma \in Z_p^*$. Choose a cryptographic hash function: $H: \{0,1\}^* \rightarrow Z_p^*$. B and H constitute system public parameters. The master secret key is defined as $MSK = (g, \gamma)$. The public key $PK = (v, h)$ is where $v = e(g, h)$.

3.3 Extract (MSK, ID)

Given $MSK = (g, \gamma)$ and the identity ID, it outputs: $SK = \frac{1}{g^{\gamma}.h(ID)^*}$.

Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 4 – No.9, April 2016 – www.caeaccess.org

3.4 Encrypt (S, MSK, PK)

Assume for notational simplicity that $S = \{ID\}_{j=1}^{s}$. Given $PK = (v, h)$, the broadcaster randomly picks $k, r \leftarrow Z_p^*$ and computes $Hdr = (T_1, T_2, C_1, C_2)$ and K where $T_1 = r.\gamma^s \bmod p$, $T_2 = \Pi_{i=1}^{s}\left(H(ID_i)\right) \bmod p$, $C_1 = g^{-k/r}$, $C_2 = h^{k.\gamma.T_1.T_2/r}$, $K = v^{\frac{k}{r}}$ .Encrypt outputs (Hdr, K). (Then K is used to encrypt the message) [7].

In this paper, we assume a group of Linked Nodes the present as tree that refer to $ST = \{LN\}_{i=1}^{*}$, ST is refer to Security Tree, LN is refer to Linked Node, and a group of linked nodes that present $LN = \{P\}_{i=1}^{*}$ and P is refer to part of message and every receiver take list of linked nodes that determined by sender $RLN = \{R, \{P\}_{i=1}^{*}\}_{i=1}^{*}$ and we to add to header of message ST, RLN to become: Hdr = (T1, T2, C1,C2,ST,RLN) Encrypt output (Hdr, k) k is used to encrypt the message.

3.5 Decrypt (S, ID_i, sk_{ID_i}, Hdr , PK)

In order to retrieve the message encryption key K encapsulated in the header $Hdr = (T1, T2, C1, C2)$,, user with identity ID_i and the corresponding private key $sk_{ID_i} = \frac{1}{g^{\gamma.h(ID_i)}}$ computes. $K = \left(e\left(C_1, h^{p_{i,s}(\gamma)}\right).e(sk_{ID_i}, C_2)\right)^{\frac{H(ID_i)}{T_2}}$ with $p_{i,s}(\gamma) = \frac{(T_1-1).T_2}{H(ID_i)} \bmod p$ When receiver decrypt a message, first determined a list of linked nodes correspond to ID second decrypt the nodes (Message parts).

4. RESULTS

4.1 Security Requirement for P2P Social Network with DIBBE using Security Tree

We need some security requirements for communicating securely. We explain security requirements for SNS in Table 1 [1] [2] [9] [10].

Table1. Security Requirements for SNS

Security Requirement	Explanation
Access Control	SNS should prevent leakage of personal information and unintended spread of information. Thus, SNS should support success control about user's contents.
Confidentiality	SNS should provide encryption in order to maintain the confidentiality of the content transmitted between users. Also, SNS shall ensure the confidentiality transmitted that is stored on a server to cope with intentional information leakage of internal managers.
Availability	**The user who wants to communicate with other users can access from every device.**
Integrity	**SNS should provide the integrity of the information generated by authorized users.**
Privacy	**SNS should protected users privacy from any others both internal and external malicious users.**
Forward Secrecy	**The user who wants to transmit message to other users add them to receiver group. If involved users in group are removed, then they cannot read the message the transmitted by the user.**
Backward Secrecy	If the user adds some users to receiver group at some point, involved users in the group cannot read message written by the user in the past.

In this paper, we need to define new security requirement, Security Tree Secrecy, If user adds some users to receiver group and specify some of linked nodes from security tree in the message, involved users in the group cannot read other linked nodes that don't specify for this user that written by the user.

4.2 Security Tree Scheme Using DIBBE

The users, who want to receiver a message, sent by Sender, should send his own ID and public key to Sender S. Using these values; Sender can first specify Linked Nodes for every receiver, second send a message to the users who sends the values (see Figure 6).

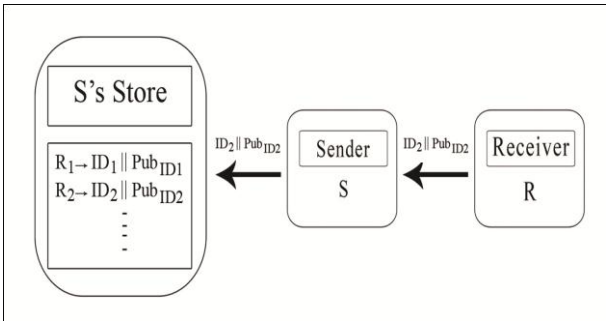

Figure 6: Add to Receiver Group

4.2.1 Setup

For sending a message, Sender receive a public key IDs from receivers, Determined the linked nodes in security tree from a message for every receiver.

4.2.2 Extract

Sender who wants to send a message is provided receiver identity, public key from own storage. Using master secret key and receivers identity, Sender generate receivers private key SK_{ID} and he transmits the private key that is encrypted using receivers public key, respectively. Using Security Tree, he determined Linked Nodes for every receiver.

4.2.3 Encrypt

Sender generates K and r randomly, and he calculates Hdr and K using k, r and receiver's identity, and the sender broadcasts Hdr and PK (see Figure 7).

4.2.4 Decrypt

Receiver 1 who is including receiver group can calculates the key K and linked nodes that determined for Receiver 1 that can decrypt the messages transmitted by sender. But Receiver 2 who is not included in receiver group each receiver can read linked nodes that determined by sender and cannot read other this.

Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 4 – No.9, April 2016 – www.caeaccess.org

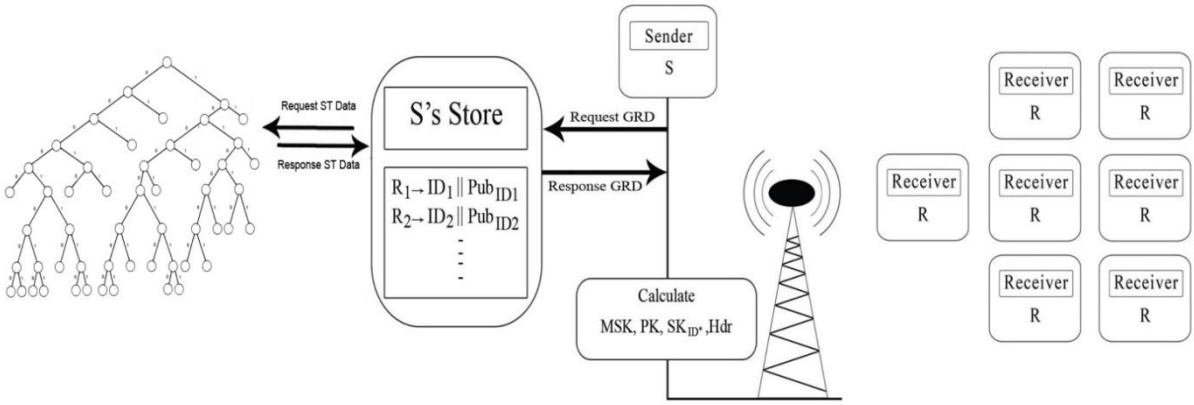

Figure 7: Setup & Extract & Encrypt Steps

5. DISCUSSION

The suggest Security Tree scheme is to manage message contents that read by receiver for encryption message in decentralized systems for SNS. In these systems, there are no SNS providers, because of this; the systems are safe from internal attackers. In these systems, there are linked nodes for every receiver in group of receivers, because of this; the system is safe from internal attackers in a group of receivers. Despite this advantage, the user in the systems should have the security systems without the central provider. In this paper, we provide the security systems using DIBBE. The user who wants to send a message broadcast the message to all users. If the user receivers the message is included in receiver group, then the user can read linked nodes contents that specified for him, otherwise the user cannot read the message. If the who transmits the message wants to add new receiver or to remove a receiver. There the user can simply modify the receiver group and system of linked nodes of message. Although the decentralized systems do not have the SNS provider, the systems can have the security systems using DIBBE suggested by Jiang. Using this scheme, the user who wants to transmit the message securely by every user in receiver group has a list of linked nodes in security tree from a message that can read.

Security Requirement	Explanation
Access control	The user who transmits message chooses identity of users who receiver the message from users storage. Because the user encrypts the message using the key made of receivers identity stored in the users storage, users who receiver the messages can decrypt the encrypted message using their own private key. Users who can decrypt the encrypted messages are regarded that the users have accessible permission.
Confidentiality	Every message transmitted by users is encrypted using a proper key. The key used to encrypt is the key made of receiver's identity. Thus, to encrypt the encrypted message, receiver should use the private key corresponded to their identity.
Availability	The user who wants transmit a message can always encrypt the message using receivers identity stored in the user's storage. Also, receivers can always decrypt the encrypted message because the message is encrypted using the key made of their identity.
Integrity	In this scheme, every encrypted message should be attached with secure systems that apply of cryptographically secure hash function. The identity of message transmitted by users can be checked by validating the secure systems.
Privacy	A user who transmits a message should encrypt the message using receiver's identity. Receiver can decrypt the encrypted the message using his own private key. This, users who are not included in receiver group cannot read the encrypted message.
Forward Secrecy and Backward Secrecy	Using DIBBE, the user who wants to transmit a message encrypts the message using receiver's identity. These, In the process of encryption, users who will receive the message are determined. If the user who sends a message wants to add new users private key in extract step, then the user sends the key to new user and the user encrypts a message using new users identity, this, new receiver can read the encrypted message. However, the receiver cannot read the message that was encrypted previously. Therefore, our scheme supports backward secrecy. If the user don't wants to share his information with a receiver any more, he will not use

	the receiver cannot read the message that is encrypted subsequently, Therefor, Our scheme supports forward secrecy.
Security Tree Secrecy	In this paper, we support Security Tree in one message if user who transmits a message adds user to some of linked nodes this linked nodes permissions to read some of message contents, receiver not read other linked nodes. Therefor this scheme is more security.

6. CONCLUSION

According as many users use SNS, various security threats have occurred, for this reason, SNS provides various solutions, but, the SNS provided by SNS providers does not solve the problem of privacy exposure by SNS providers. To overcome this problem, many previous researches suggest decentralized systems for efficient Security Tree Scheme we used the concept of Dynamic Identity-Based Broadcast Encryption Scheme proposed by Jiang. Using this method, the user who transmits a message may not store sensitive information in central server. By security tree scheme we can put a huge message of data in small parts and organized these parts as linked nodes in security tree. Every receiver in sender store has permission to decrypt some linked nodes that determined by sender, other linked nodes not allow for decrypted.

7. REFERENCES

[1] Jeong, H., Won, D.: Access-control-based Efficient Privacy Protection Method for Social Networking Services. Journal of The Korea Institute of Information Security & Cryptology 1(23), 81–88 (2013).

[2] Youngman Jung, Yoonho Nam, Jiye Kim, Woongryul Jeon, Hanwook Lee, and Dongho Won.: Key Management Scheme Using Dynamic Identity-Based Broadcast Encryption for Social Network Services College of Information and Communication Engineering, Sungkyunkwan University, 300 Cheoncheon-dong, Jangan-gu, Suwon-si, Gyeonggi-do, 440-746, Korea

[3] Yeung, C.A., Licaardi, L., Lu, K., Seneviratne, O., Lee, T.B.: Decentralization: The future of online social networking. In: Proc. Int. Joint Conf. W3C Workshop (2009).

[4] Datta, A., Buchegger, S., Vu, L.H., Strufe, T., Rzadca, K.: Decentralized online social networks. In: Handbook of Social Network Technologies and Applications, pp. 349–378 (2010).

[5] Cutillo, L.A., Molva, R., Strufe, T.: Privacy preserving social networking through decentralization. Wireless On-Demand Network Systems and Services, 145–152 (2009).

[6] Zhang. : Identity-Based Broadcast Encryption with Recipient Privacy. In 978-1-4244-5539- 3/10/$26.00 ©2010 IEEE (2010).

[7] Jiang, H., Xu, Q., Shang, J.: An efficient dynamic identity-based broadcast encryption scheme. In: 2010 Second International Symposium on Data, Privacy and E-Commerce (ISDPE), pp. 27–32 (2010).

[8] Boldyreva. : Identity-based Encryption with Efficient Revocation. In Proceedings of the 14th ACM Conference on Computer and Communications Security, CCS 2008, ACM Press, 2008.

[9] Ajami, R., Ramadan, N., Mohamed, N., Al-Jaroodi, J.: Security Challenges and Approaches in Online Social Networks: A Survey. International Journal of Computer Science and Network Security 11(8) (August 2011).

[10] Zilpelwar, R.A., Bedi, R.K., Wadhai, V.M.: An Overview of Privacy and Security in SNS. International Journal of P2P Network Trends and Technology 2(1) (2012)\