ESBA BASED PRIVACY PROTECTION IN OSCS

Sajin R Nair[1], Ajeesh S[2], Smita C Thomas[3]

[1]PG Scholar, Dept. of Computer Science& Engineering, Mount Zion College of Engineering, Pathanamthitta, Kerala, India
[2]Asst. Prof., Dept. of Computer Science & Engineering, Mount Zion College of Engineering, Pathanamthitta, Kerala, India
[3]Research Scholar, Vels University, India

Abstract - *Online social communication system (OSCS) depicts system and coupling between them. The systems are often connected separately and by personal information exchange brought much advantages to clients. The personal privacy leaks are major obstacle in OSCS. The security and privacy protection in OSCS are main focus point on now a days. In this paper, we proposed to solve problems in OSCS s such as security and privacy protection by encryption scheme based on attributes. Then hierarchy genetic algorithm and radial based administration are implemented. Tolerate vector machine is used to preprocess information of the OSCS. Finally a bit host inflation algorithm is used.*

Key Words: Online social communication system (OSCS), Novel method in OSN, Encryption scheme based on attributes (ESBA), hierarchy genetic algorithm (HGA), radial based administration (RBA), Tolerate vector machine(TVM), and bit host inflation algorithm

1. INTRODUCTION

Online social communication system (OSCS) analysis can be implemented to examine the working of data flow patterns in communities, and emergent behavior of physical and biological systems. Online social communication system is an interconnection network that provides various communication. Online social communication have created large amount of information within the communication system. Such information contains many relevant and delicate data about persons [2]. In general, OSCSs have a distinctive form, which is a type of virtual communication system for information exchange. Social networking becomes increasingly important due to the recent surge in online interaction [4].Correlated with a traditional communication system, special access characteristics of OSNs are:

•Strong Relationship for User Information: As data sharing is the most crucial role of an OSCS, individual client can attack the data of other client as a guest and can be inspect by other client at the corresponding time.

•High Confidentiality for User Information: Client data should be more relevant, must be highly intimate. To secure the information about the users, it is essential to increase OSCS security. Personal information accumulated on OSCSs are necessary to encrypt and provide the security to the personal information about the clients.

Mainly used OSCS privacy protection methods are:

1.1 SEMISUPERVISED LEARNING METHOD

On the basis of different node weights of client to increase the durability of communications between clients. Large scale applications this technique is not suitable.

1.2. DIGITAL COPYRIGHT

Integration of client management technique can be used for security and privacy protection. Good performance in multiple platforms and not suitable for single platform.

1.3. MATRIX FACTORIZATION MODEL

Seeker–source based technique can be used method. Here different data can be integrated and used. Long processing time can be required to process the data for feature extraction is the main drawback of this method.

Information exchange through online social communication system contain many relevant information about the client and that information has more important to hold secure [2].Local information about each client in social communication system may attack adversely by others [1]. Old techniques may use as a graph to obtain the security of the online social communication system [3]. The durability of this interaction is acute for secure information handling. More recent works based on information management balancing of security and services provided by the online social communication system [4].

In this paper, we proposed to solve problems in OSCS s such as security and privacy protection by encryption scheme based on attributes. Then hierarchy genetic algorithm and radial based administration function are implemented. Tolerate vector machine is used to preprocess information of the OSCS. Finally a bit host inflation algorithm is used.

2. LITERATURE SURVEY

Prateek Joshi and C. C. Jay Kuo [1] proposed a survey on privacy protection in online social network. The survey results shows that the information loss in online social networks is higher. This survey focuses on the possible attack strategies and solutions for solving these attacks.

The work in [2] elaborates on the idea of computational resources performance in online social network. For this method the attackers can easily interfere and demonstrate the social network for user. This paper also focuses that the information attack for user attributes and what are the issues on the data after the attack. The Binary Coded Grouping-based Inspection (BCGI) algorithm group's users in the NAN based on the binary sequences of identification numbers BCGI groups the users in the NAN. BCGI locate malicious users by only one inspection step works there is a unique malicious user in the NAN. Each inspection box includes inspectors and sub-inspectors. An inspector box which contains a head inspector and several sub inspectors. The head inspector is responsible for finding the presence of dirty users; the sub-inspectors take charges of acquiring the malicious [2] meters exactly.

3. ONLINE SOCIAL NETWORK

An online social communication system (OSCS) is a social communication structure made of clients or enterprise. And the connection may create interdependency between the clients instead among nodes [5]. In fact, a communication system may contain the bounds such as nodes and links. The node is a point in a network that define the flow of relationships. The link is the type of exchange information.

3.1. OSCS INFORMATION DRIPPING

Information can be dripped through offline social communication such as meetings, conferences. The drip of information through communication system is basically different from offline complement part [4]. The important communication criteria such as friends' requests, uploads varieties of photos and videos, updates status, sharing links of third party applications are other way of venues of information dripping.

3.2. SECURITY PROBLEMS IN OSCS

Without knowing complete consequences users share personal data on online communication systems (social networks). It is a trade-mark between allow security to clients and releasing the same data to the purpose of broadcasting companies. While the data are meant for the broadcasters, attackers can easy to take the data. It will decreases the confidentiality of the information [4].An example of information attack in clients is given in Fig. 1.

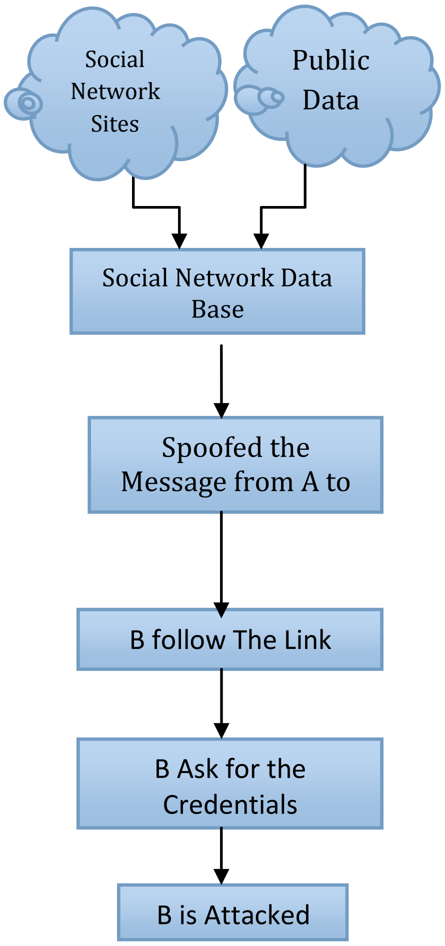

Fig -1. Information Attack in clients Online Communication

4. NOVEL METHOD IN OSN PROTECTION

Hierarchy genetic algorithm and radial based administration (HGA-RBA) can used determine the framework of the neural network. At the time of learning process the this type of algorithm has slow speed of conjunction Proposed method the generate a novel security prediction model, hierarchy genetic algorithm (HGA) is borrowed.

4.1 INITIALIZATION OF OSCS INFORMATION SECURITY

Primary stage of OSCS security information initialized when the of OSCS security information encoding is finished. Initially, the population size P is determined. In this paper, the value range of population size P is between 10 and 150.

4.2. GENERATION FOR FITNESS

To improve the consistency of OSCS also need to decrease its complexity and increase its accuracy.

Initially, accuracy for the object administration of OSCS is conferred as

$$F_1 = ESS = \sum_{k=1}^{N} \quad (x_k - y_k)^2 \qquad (1)$$

where F1 means the object administration of OSCS accuracy, error for sum of squares (ESS) is the quadratic sum of error between OSCS output and the predicted of output, N is the number of training samples, xk denote OSCS output and yk is predicted output.

The object function of OSCS complexity can be described by the number of nodes in hidden layers can be presented as,

$$F_2 = \quad L \qquad (2)$$

where L means the number of nodes in OSCS hidden layer. We blend (1) and (2) to get (3), which is the function for fitness of complexity and accuracy for object administration.

$$f = [N * log[\frac{1}{N}\sum_{k=1}^{N} \quad (y_k - y_k{}')^2]+4F_2] + F_1 \qquad (3)$$

the fitness function is f, output of the training for RBA value is yk. When yk is lower, f is higher also L is lower.

4.3 OSCS INFORMATION PRETREATMENT

To apply Tolerate vector machine (TVM) tools to pre-treat previous OSCS information to assure that the information is suitable for input.

$$f(x) = \sum_{i=1}^{N} \omega_i k(x,x_i) + b \qquad (4)$$

4.4 ENCRYPTION ALGORITHM FOR OSN SECURITY

Our encryption algorithm ESBA is chosen as our encryption algorithm. ESBA applies specific attributes for encryption,

Our ESBA method based on a ciphertext format consists of the processes such as, initialization, encryption, secret key generation, decryption, and secret key transmission.

Lagrange coefficient OSCS data set can be initially determined, in which S means OSCS data set, and i and j mean different OSCS data. The process is:

$$\Delta_{i,s}(x) = \prod_{J\varepsilon S, j\neq i} \frac{x-i}{i-j} \qquad (5)$$

The public parameters PK and plaintext MK can be computed in

$$PK = (G_0, g, h = g^{\beta}) \qquad (6)$$

where α means the number of OSCS client requests, successful OSCS client requests β, and g means the OSN information attribute.

$$MK(\beta, g^{\alpha}) \qquad (7)$$

We perform the encryption process after the initialization process. The encryption process PK to transform the information from plaintext MK into ciphertext CT.

$$CT = T, x, k_x, d_x, C = R^s \qquad (8)$$

Where T means the access function, x means the OSCS data, kx means the threshold of OSCS data, dx is the number of polynomial generated, R means the OSCS data at access function of T, and S is the OSCS data set. The next step is to decrypt the information by using the encrypted value and the primary secret key.

$$SK = \left(D = g^{\frac{\alpha+\beta}{\beta}}, \forall \epsilon S | D_j = g^r * H(j)^r\right) \qquad (9)$$

The secret key is finally transmitted to the information to compute the iteration function

$$F_x = \prod_{z\epsilon S_x} F_z{}^{\Delta_{i,S'_x}(0)} \qquad (10)$$

Here the above mentioned complete process as shown a flow chart in Fig.2.The complete encryption process can be represented as the form flow chart.

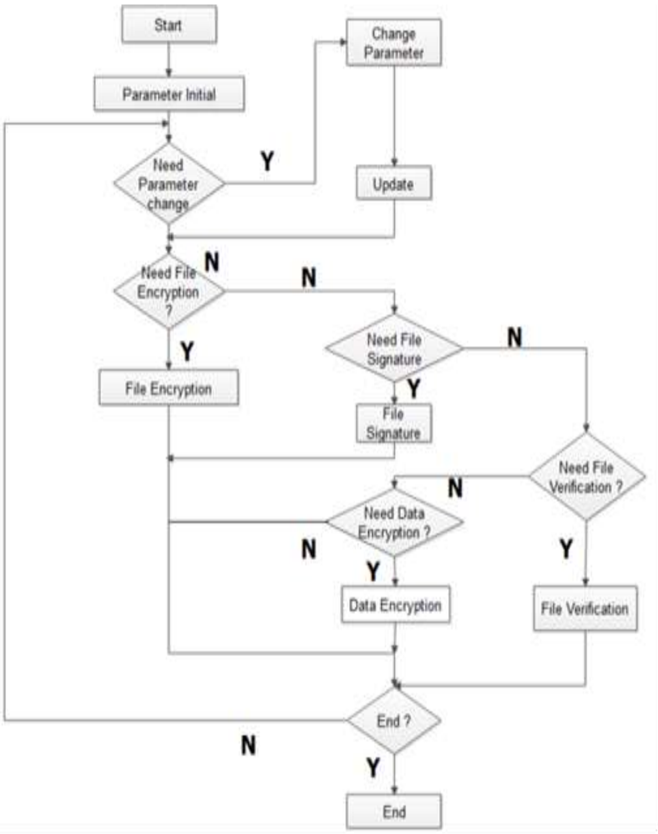

Fig-2. Encryption flowchart

ESBA based encryption method is shown in Fig.3.

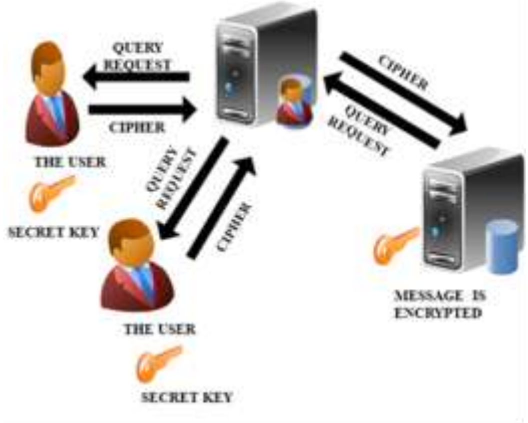

Fig.-3. ESBA based encryption method for access data.

Here in this process the client may contain set of attributes. Data stored on the server in the form of cipher text format after the encryption. A client can admittance a request, the client needs to send credentials. The attribute access can be done by the controller. Admittance control withdraw and transmit the cipher text with related attributes in the form of credentials. Client needed information of private key to decrypt the cipher text. The cipher text format is does not match user attributes it cannot be decrypted and the operation is failed.

5. PRACTICAL ANALYSIS

Practically implemented and analyze the result based on the security and privacy protection of the proposed method. The comprehensive practical measure is as follows.

5.1 PRACTICAL PLATFORM OF OSCS SECURITY

The experiment was performed on a personal computer having following features.

Table -1: Practical Platform

NAME	PARAMETER
CPU	Intel Dual Core Processor i3-2350 M2.4GHZ
OPERATING SYSTEM	WINDOWS XP
MEMORY	5G
NETWORKTOOLS	ECLIPSE 3.4
IDK VERSION	1.6.0-26

During the secret key generation, different secret keys are generated for different properties. The result can be shown in Table 2.

Table -2: Generation Time for Secret Key

Number of Attributes	**10**	**20**	**30**	**40**	**50**	**60**
Number of Secret Key						
1	0.14	0.36	0.60	0.72	0.86	0.96
2	0.14	0.37	0.58	0.73	0.84	0.95
3	0.14	0.36	0.53	0.75	0.82	0.94
0	0.14	0.32	0.58	0.71	0.86	0.98
5	0.14	0.35	0.59	0.73	0.84	0.98

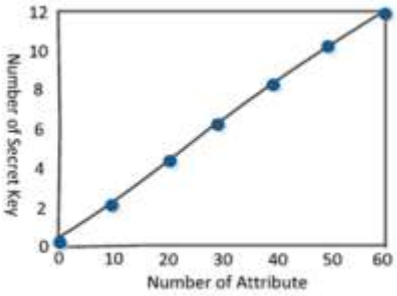

Chart1: Relationship between the number of secret keys and its properties.

Chart1, shows the relationship between the number of secret keys and its properties, which are linearly dependent. As the number of secret keys increases, the number of attributes also increases.

5.2 PRACTICAL RESULTS ANALYSIS OF OSCS SECURITY

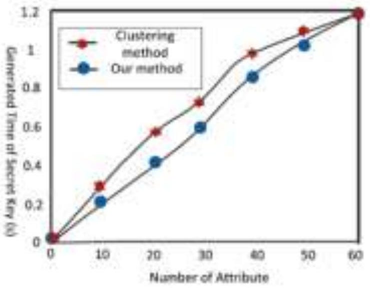

Chart2: Secret key generation Time

Chart2, shows the relationship between secret key generation time and its properties. By using the proposed method the secret key can be generated in 0.4 s. While in the clustering method it takes 0.6 s.

In the comparison between the proposed method and the clustering method, accuracy of the encryption is 94.2% than in clustering method ie; it shows an increase of 41% of accuracy.

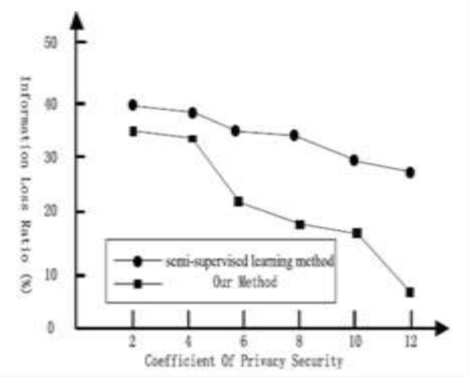

Chart3: Data loss in semisupervised learning method and our method.

Chart 3, shows the comparison of the data loss in semisupervised learning method and our methods. The data loss in semisupervised method is 33.6% and in proposed method is 17.59%. So the result shows that the proposed method is more secure than the existing one.

5. CONCLUSIONS

The proposed system implements an OSCS technique for security against personal privacy leaks. In order to solve the privacy and security issues, the proposed system combines ESBA and radial based administration (RBA), Tolerate vector machine (TVM), and bit host inflation algorithm.

For security prediction in OSCS, hierarchy genetic algorithm is used. Then, pre-processing is done by using Tolerate vector machine(TVM). Then the preprocessed information can be encrypted by ESBA encryption.

Our next work aims to the following improvements such as

1) Provide EABS based protection to cloud computing.

2) EABS encryption technique is used for the protection against attack in OSCS

REFERENCES

1) Prateek Joshi and C. –C. Jay Kuo. "Security and Privacy In Online Social Networks: 2011 Second International Conference on Online Social Networks: A SurveyIEEE, 2016.

2) Theodore Georgiou, Amr El Abbadi and Xifeng Yan Computer Science Department University of California "Privacy Cyborg: Towards Protecting the Privacy of Social Media Users" IEEE 33rd International Conference on Data Engineering.E.

3) Yingying Tao and Quan Bai. " Detecting Abnormal Attention in Online Social Networks from Local Views." International Conference on IEEE International Conference on Agents (ICA), 2017.S.

4) XI Chen and Katina Michael. "Privacy Issues and Solutions in Social Network Sites."DigitalObjectIdentifier10.1109/MTS.2012.2225674 Date of publication: 19 December (2012):pp 43-53.

5) Ruggero G. Pensa and Gianpiero Di Blasi" A Centrality-based Measure of User Privacy in Online Social Networks." IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM) 2016:pp1438-1439.K.

6) Nurul Nuha Abdul Molok. "Information Leakage through Online Social Networking: Opening the Doorway for Advanced Persistence Threats." 8th Australian Information Security Management Conference (2010):pp70-80.

7) J. E. Park, B. Bold, and Y. H. Park, "Efficient scheme for generating file shares in combinatorial-based file sharing with distributed cloud storage," in Proc. ICGHIT, Hangzhou, pp.79–80, Feb. 2017.

8) Donghui Hu, Fan Chen, Xintao Wu and Zhongqiu Zhao" A Framework of Privacy Decision Recommendation for Image Sharing in Online Social Networks." First International Conference on Data Science in Cyberspace (2016): pp244-251.