Secure Friend Recommendation System Based on Online User Activities

Ankita A.Bhujbal[1], Prajakta D.Pabale[2], Rani S.Dhone[3], Sandhya Gundre[4]
Department of Computer Engineering
[1, 2, 3, 4] DYPIEMR, Akurdi,

Abstract-*Social network sites (SNS's) have connected millions of users creating the social revolution. Users' social behavior influences them to connect with others with same mentality. Social networks are constituted because of its user or organizations common interest in some social emerging issues. The popular social networking sites are Facebook, Twitter, MySpace, Orkut, LinkedIn, Google plus etc. which are actually online social networking (OSN) sites. However, the large amount of online users and their diverse and dynamic interests possess great challenges to support recommendation of friends on SNS's for each of the users. In this paper, we proposed a novel friend recommendation framework (FRF) based on the behavior of users on particular SNS's. The proposed method is consisted of the following stages: measuring the frequency of the activities done by the users and updating the dataset according to the activities, applying FP-Growth algorithm to classify the user behavior with some criteria, then apply multilayer thresholding for friend recommendation. The proposed framework shows good accuracy for social graphs used as model dataset. Security and confidentiality plays an important role in the field of communication. Data Encryption Standard(DES) is a prominent symmetric cipher which provides confidentiality. DES uses a key length of 52 bits. In this advanced age, with huge resources and extreme computational power, DES algorithm is vulnerable to exhaustive search of the key.*

Keywords-Social Networking Sites (SNS's), Social Entities, Friend Recommendation Framework (FRF), FP-Growth Algorithm, Multilayer Thresholding.DES, encryption, key generation, permutation, cipher, crypt analysis, security.Cloud Computing, Public Cloud, Secret Sharing, Multiple clouds.

I. INTRODUCTION

The popularity of online social networking sites is getting higher day by day because of the friendliness introduced in the sites and technological advancement. Use of these sites has developed social traditions and behavior in its users [1]. Nowadays, recommendation system has gained its popularity to the researchers' because of its versatile notion of integrating different research areas. Researchers from psychology, human computer interaction, computer vision, data mining etc. are keeping their attention on this research area. A recommendation system generally interacts with its user in most possible friendly way and recommends doing something in its users favor. Recommendation systems for SNS's is a new scope of research as social peoples are more interested in online social networking (OSN) sites, likeFacebook [2], Twitter [3], Flickr [4], LinkedIn [5], MySpace [6], Google Plus [7] etc. In the social networking sites, a social entity or user makes connections with other known or unknown social entities, namely friends or partners, and share their news and views through the profound facilities of the sites. Friends could be offline or real-life friends, classmates, neighbors, colleagues, family members, relatives or anyone having a profile in the OSN sites. Recommending different aspects in SNS's is a new concept to make people socially sound. Community recommendation, connection or friendship recommendation, birthday reminder, event recommendation, restaurant or vacation spot recommender systems are common findings in the SNS's. Recommending people on social networking sites is worth studying because it is different from traditional recommendations of books, movies, restaurants, etc. due to the social implications of "friending".

Cloud computing has rapidly grown to be a platform of network-based computing. Public clouds have advantages in initial cost and availability. However, there are problems concerning confidentiality, such as improper use of data, because a third party's service provider manages data not only business user but also personal users [2].

Public cloud services are provided by a third party, and a user has to give data to the provider whose reliability is unknown. Therefore, if there are malicious operations inside the provider, a user's data can be abused. It has become common that documents which describe the way of management and operation are disclosed to a user as SLA; however, verification of the contents is not possible[3].

To mitigate the above threat to confidentiality, schemes using multiple public clouds have recently been proposed [6],[7].

We focus on a storage service, which is a major cloud service. We have proposed a concrete data management approach [5]. This approach uses secret sharing scheme [8], [9]. With our approach, confidential data) are distributed to multiple cloud services using secret sharing scheme. In this paper, the proposed approach is implemented by using an actual cloud service as a CSP, and the performance is evaluated.

The organization of the rest of this paper is as follows. The proposed approach for the evaluation is introduced in Section 2. Performance is experimentally evaluated in Section.

II.LITERATURE SURVEY

SNS's are an online phenomenon which provides social network based services to support easy message posting, information sharing and inter-friend communication. A social network is a set of people or groups of people with some pattern of contacts or interactions between them. The patterns of friendships between individuals, business relationships between companies, and intermarriages between families are all examples of networks that have been studied in the past. Social Networking sites (SNS's) provide users with opportunity to connect with their offline friends as well as making new friends with latent ties who otherwise would never have met them. They also supplement their relationships with close relations and help to maintain the social capital [8]. Understanding the behavior of a particular user in the context of SNS's is the main concern to determine the recommendation constraints. L. Jin et al [9] describe the wayto understand the users' behavior in OSN's. "Connectivity and interaction, traffic activity, malicious behavior, mobile social behaviors" are four issues needed for understanding user behavior in social network [9]. C. Wilson et al [10] mentioned that we can also use "photo comment and wall post as interaction to determine the behavior". Different researchers' have proposed different methods for recommending friend or connection such as clustering method [11-12], "categorizing users' interest" [13], cohesion based recommendation system [14], based on "user social relations and personal information profiles" [15], GeoLife – 2.0 location based recommendation system [11]. Yu Zheng et al [7] proposed a GPS-data-driven social networking service where people can share life experiences and connect to each other with their location histories. By mining people's location history that can measure the similarity between users and perform personalized friend recommendation for an individual. A friend recommendation system in biology field is also proposed in [11]. The previous approaches do consider user's interest, hence doesn't define the user behavior on a SNS. By identifying user's behavior on SNS's we can identify his/her interest in the SNS and using common and uncommon behaviors a friend recommendation system could be proposed.

In this paper, we does not only consider the familiar or persons having common interests to be recommended as friend, therefore persons having special or unique interests should be recommended as friends. We have proposed a novel friend recommendation framework (FRF) based on user's online behavior and the main contribution associates the definition of user's online behavior and algorithm to recommend a friend.

Later in this paper, section III defines the user's online behavior, section IV proposes the framework for friend recommendation, section V describes the experimental outcomes with some limitations and concludes with the section VI, having discussion about the future prospects of this framework.

III.EVALUATED SYSTEM ARCHITECTURE

In this section, we roughly introduce evaluated system architecture which is a degradation of the proposed data management approach for multiple clouds with a secret sharing scheme [5].

A. Basic Component Structure

Figure 1 illustrates the basic logical component structure. We use multiple public clouds without adding extra sharing storages within an organization guaranteeing data security because we assume also easy personal usage.

A client PC encrypts the secret data using a key. Users then transmit the encrypted data to the DDS (Data Distribution Server). The key is stored a client PC. The DDS applies the (k, L, n) secret sharing scheme to the encrypted data and transmits the generated share to each CSP. Furthermore, DDS generates a hash value to prevent falsification. Detailed processes are describes below.

B. Data Management Process

The encryption/ distribution and decryption/ restoration with the secret sharing scheme are described.

1) Encryption and Distribution

a) A client who wants to store secret data M encrypts M with a key K and generates the encrypted data S.Then, the client discards M.

b) The client transmits S to the DDS. A secure protocol like SSL is necessary if the network is not trustable.

c) The DDS creates n shares DSj from S using the (k, L, n) secret sharing scheme.

d) The DDS generates hash values HDj from each DSj.

e) The DDS send hash value information and the identification information of shares to a client's storage.

f) The DDS distributes generated shares to multiple CSPs' storages.

2) Decryption and Restoration

a) A client who uploaded S in the encryption and distribution procedure uploads HDj and identification information to the DDS.

b) The DDS selects arbitrary k cloud services out of n CSPs and requests the shares to each CSP, then, the DDS receives them.

c) The DDS verify the received shares by using the hash values HDi, which are uploaded in Step 1. If the received DSi fails verification, the DDS requests another share to another CSP.

d) The DDS restores S by applying the (k, L, n) secret sharing scheme.

e) A client receives S from the DDS.

f) The client decrypts S by using the key K and get original secret data M.

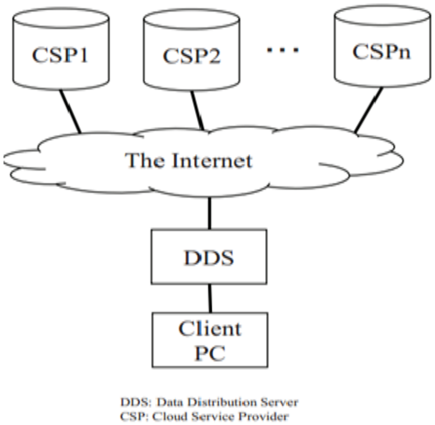

Fig. 1. Assumed Basic Logical Component Structure

IV. USER'S ONLINE BEHAVIOR

In SNS's a users are considered as social entity or connection. In Facebook, a user p can create a personal profile, add other Facebook friends, and join any community and many more [18]. Determining user's online behavior is a challenging work nowadays as the behavior fluctuates very often. User behavior is very important for this approach of friend recommendation system. In this section, we have defined what user's online behavior is formally.

A. Behavior Definition

Let's consider three set: users (U), activities (A) and related activities(R).

U = {u | users in SNS} = {u1, u2, u3, …… , un}

A = {a | activities of the users in SNS} = {a1, a2, a3, …, am}

R = {r | a subset of activities that any user may follow in a session or time duration in SNS}

R = P (A) (1)

So that,

R={{a1},{a2},{a3},.,{an},{a1,a2},{a1,a3},.,{a1,a2,a3,.,an}} (2)

The behavior of the user is completely related to the activities of the users. Users can do different activities. But the behavior will be those activities which are performed by the user in a particular time duration denoted as R. The equation for the behavior could be given as:

$$B: U \rightarrow R \quad (3)$$

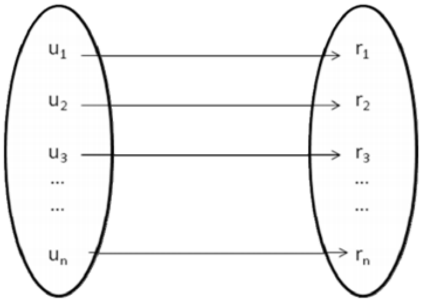

Fig. 2. User To Related Activity Relationship

Bi = behavior of the Ui at a particular moment. Therefore, R is a proper subset of A(R subset of A). Users behavior could be defined in several approaches like association rules in perspective of mining, complex graph activities, sequence mining etc. Suppose for two different users (u1 and u2) having activity set R in a specific timestamp are r1 and r2. The activities of different users could be different; again they could have some common activities.
Suppose,

r1 = {chat, mail, see event notifications}
r2 = {mail, see group activities}

The activities they have in common is, r1 U r2= {mail}.

The mining perspective of behavior could be effective in terms of finding common and uncommon behaviors from the activity sets. If the different activities are represented as sets then the association rules might be very effective to generate the common and uncommon activities from them. In this paper, we have introduced the association mining to identify the behaviors and retrieved the uncommon behaviors from the subset of activities.

The user behavior can be represented as a complex graph (Fig- 2) where activities will be the node and relation of the activities as edges of the graph G, then
B1 (U1, R1), B2 (U2, R2), B3 (U3, R3), B4 (U4, R4)
Where,
R1 = G1 = [{a1, a2}, {(a1, a2)}],
R2 = G2 = [{a1, a2, a3}, {(a1, a2), (a1, a3), (a2, a3)}],
R3 = G3 = [{a1,a2, a3, a4, a5}, {(a1, a3), (a3, a2), (a3, a4), (a4, a5)}],
R4 = G4 = [{a1, a3}, {(a1,3)}]

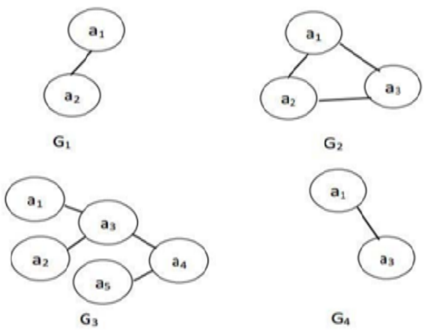

Fig. 3. Graph Representation Of Subset Of Activity Performed By User In Perticuler Time Duration

Again sequence of the activities can also be the behavior of the user. The sequences are the chronology of performing several activities related to SNS's and could be in any order.

S1 = a1→a2→ a3 →a5→ a6→ a3→a4 (4)
S2 = a1→a2→ a5→a7→ a8 (5)

These sequences (4) and (5) of the activities such as, S1, S2, …. Sn can be the behavior of the user u1.

Hence, B1 = {S1, S2, S3…. Sn}

Suppose we are considering a fixed amount of time. By this time users are doing different types of activities. Some of the users used to chat with his/her friends, some are surfing different groups, some of them are listening songs, some of them are watching movies, and some of them are playing different types of online social games. Among those activities, users usually do this activities one after another. Let us consider one users activities. After logged in he used to check his friend request then see his unread message then see his notification, then play a game. Some other user may do the same activities but in different sequence. Here the activities are same but the sequences are different. The sequence of activities defines the behavior of the system. So, from here we can determine the common and uncommon behavior and these common and uncommon behaviors can be used for friends to be recommended.

B. Common Behavior

Common behavior means the common activities of the users. This common behavior is not fixed or pre-defined. For different data set the common behavior will be different. Common behavior will not be only one activity. Two or more activity can make a common behavior. In ourmethodology the common behavior is the max frequency of the any activity in the dataset. Formally, we can define common behavior as like, B1 and B2 has a common behavior of u1 and u2, if and only if activities r1 & r2 have some common activities.
Mathematically,
max(Common(B1, B2, …, B3, …, Bn)) if and only if
$r1 \wedge r2 \wedge r3 \ldots\ldots r_{n\neq\Phi}$ (6)

C. Uncommon Behavior

Uncommon behaviors are the uncommon activities of the user apart from the common behavior. Any activity of a user will be considered as uncommon behaviors that are not in the common behavior. For different data set the uncommon behavior will be different. Uncommon behaviors could be one activity or more than one activity.

V. FRIEND RECOMMENDATION FRAMEWORK

In this section, we proposed a novel friend recommendation framework based on the user's online behavior defined in the previous section. The framework is considered for a graph as the popular SNS's are architecture as graph based network. There are five step sequencing in the framework: extracting sub-network, finding frequency of the activities, find the common behavior, find the uncommon behavior within the common behavior and finally friend recommendation.

A. Extracting Sub-Network

SNS's are very large entity and has large-scale databases. Day by day the size of the network is increasing and as the people are joining, there is huge number of information overload happens on these sites. For experiment of our proposed system, we take the whole network of a random individual. After getting the whole network of a client for who are going to suggest friends, we extract the subnetwork of 'x' no of people from the visualized graph.

B. Finding Frequency of Activities

Activities are the main base of social networking sites. The behavior of a particular user depends on the type of activities he/she does on the SNS. The definition of behavior also describes the related or considered activities actually define the behavior of that user. There are huge number of activities on SNS's nowadays and increasing day by day because of technological advancement and user's involvement from different spheres of life. For our proposed method we can consider different set of activities like types of songs user like, types of videos user often watches, types of online social games user take part etc. for each type of activities there will be many entities like a user may listen to "Michel Jackson" as well as "Metallica". So there are two entities is listening song activity. From all the activities we find out the entity with maximum frequency.

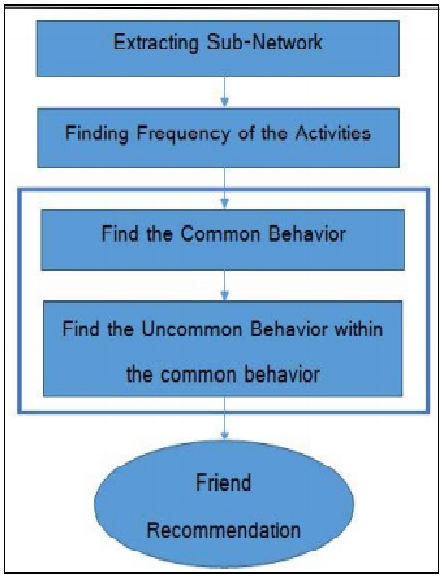
Extracting Sub-Network
Finding Frequency of the Activities
Find the Common Behavior
Find the Uncommon Behavior within the common behavior
Friend Recommendation

Fig. 4. Propose Friend Recommendation Framework

We make the network scrutinized by using this frequency where the maximum frequency related activities are there. So all activities come down to the number of activities, where the every categorized activity contains one activity with the maximum frequency. After this step only the activities with maximum frequencies will be selected.

B. Find the Behavior

To find the desired user behavior (common and uncommon) we use FP-growth algorithm in our modified dataset. FP-growth algorithm gives us the pattern from the dataset. Among this pattern the desired behavior will be found.FP-Growth works in a divide and conquers way. It requires two scans on our model database. FP-Growth algorithm first computes a list of frequent items sorted by frequency in descending order (F-List) during its first database scan. In its second scan, the database is compressed into a FP-tree. Then FP-Growth starts to mine the FP-tree for each item whose support is larger than Ị by recursively building its conditional FP-tree. The algorithm performs mining recursively on FPtree. The problem of finding frequent item sets is converted to searching and constructing trees recursively. Thus, applying FP Growth algorithm in our dataset we find the behaviors patterns. From the acquired pattern we find out the common behavior by using the maximum number of frequency for any pattern with the single activities of the user behavior. Naturally single activities will give the highest frequency value.

After finding the common behavior our next step is to find the uncommon behavior. If we recommend friend only using the common behavior it will just like the natural recommendation process using only one feature like "fof" (friend of friend). So for more integrity we use uncommon behavior. This uncommon activity is different from the natural uncommon process. We actually find out the less no of frequency of other two activities from the user behavior containing the common user behavior. We call it uncommon because it appears less among the user whose have similar interest early. Actually this behavior can be considered as their unique behavior. Therefore, multilayer thresholding is done to find out the uncommon behaviors.

C. Friend Recommendation

In this final step we recommend the users with the user behavior found in previous steps. We can take any random user from any other sub network and recommend them as friend. So many friends or connections could be recommended to a particular user in any social network. The Fig-4 describes the recommendation framework more precisely. The total activity set is defined by the large circle where the inscribed circles define the different users and the activities they have performed in a particular timestamp.

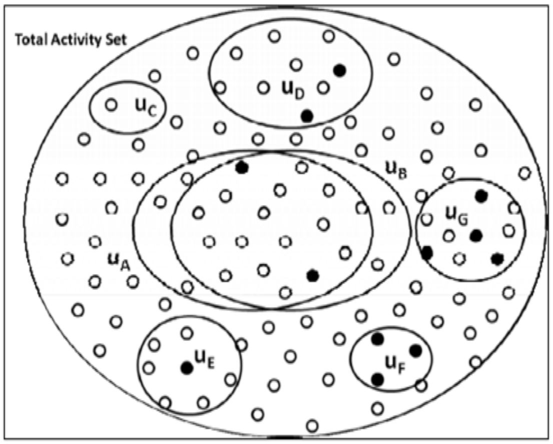

Fig. 5. Behaviour Analysis for Friend Recommendation For Several Users (Black dots Specifies The Least Frequently Performed Activities And White Dots Specifies Most Frequently Performed Activities)

Each user could have least frequently and most frequently performed activities which are denoted as black and white dots in the figure, respectively. Some users could have only most frequently done activities (i.e. uC), some could have only least frequently done activities (i.e. uF) or both (i.e. uA, uB, uD, uE, uG). Now, the uA and uB have many common activities as the sets overlaps and have two least frequently performed activities which is the commonly uncommon behavior that we have define in section III. Based on these activities these two users could be recommended to be friend to each other.

VI. DES-DATA ENCRYPTION

DES algorithm, developed by IBM in cooperation with National Security Agency (NSA), has been worldwide encryption standard for more than 20 years. DES encryption algorithm falls in the category of ciphers known as blck ciphers. Block ciphers divide the message into equal sized blocks and encrypt them separately. DES encrypts 64 bit block of plaintext into 64 bit cipher text using a 52 bit key.

DES relies on encryption techniques of confusion and diffusion. Confusion means that each character of the cipher text should depend on several parts of the key. Diffusion means that a small change in the plaintext should reflect a big change in the cipher text, and similarly, a small change in cipher text, should reflect a big change in the plaintext. Confusion is accomplished through substitution, whereas diffusion is accomplished through permutation of the plaintext and the key. DES has a set of look up tables known as S-boxes and P-boxes, for substitution and transposition of plaintext, respectively.

A. Enciphering

The 64 bit input block to be encrypted is first subjected to a permutation(IP) table

TABLE 1.

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	54	46	38	30	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Fig. 6. initial permutation (ip) table

The permutated input is then fed to a complex 16 round encryption process in Figure 1. This permutation table shows, when reading the table from left to right then from top to bottom, that the 58th bit of the 64 bit block is in first position, the 50th in second position and so forth. The permuted input is divided into 2 parts: left and right, named L and R respectively.

The 32 bits of the R block are expanded to 48 bits with respect to the expansion table (E) shown in Figure 7, in which the 48 bits are mixed together and 16 of them are duplicated. As such, the last bit of R (that is, the 7th bit of the original block) becomes the first, and thn the first becomes the second and so on.

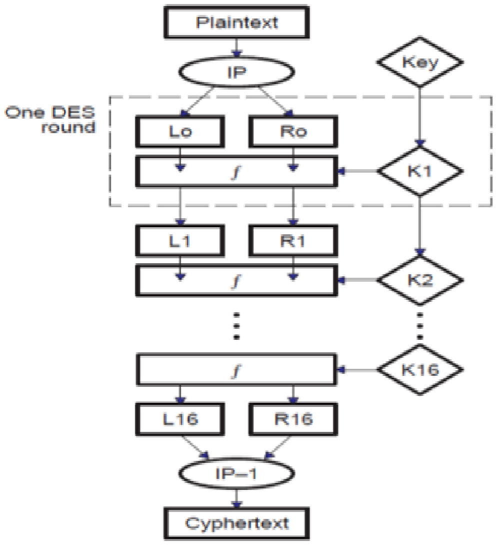

Fig. 7. DES Encryption

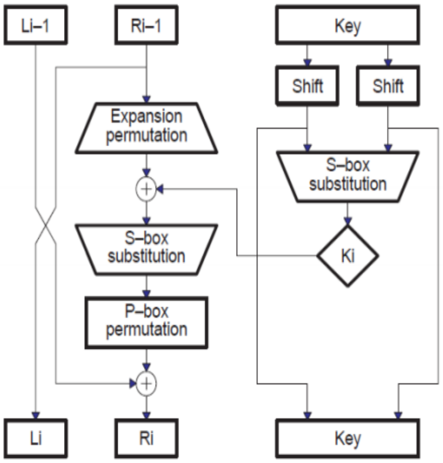

Fig. 8. Encryption Process In One DES Round.

In addition, the bits, 1,4,5,8,9,12,13,16,17,20,21,24,25,28 and 29 of R(respectively 57, 33, 25, 1, 59, 35, 27, 3, 61, 37, 29, 5, 63, 39, 31 and 7 of the original block) are duplicated and scattered in the table.

TABLE II

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Fig. 9. expantion table(e)

VII. PERFORMANCE EVALUATION AND ANALYSIS

In the evaluation, a particular popular public storage service is used as a public cloud service because it is familiar and discloses its API to service developers. Ideally, performance should be evaluated with many varieties of cloud services, but here, one service is used with multiple accounts in order to clarify the basic characteristics because the effect on internet communication should be estimated first rather than the difference of various kinds of CSPs. Here, we use multiple accounts of the public cloud service as multiple CSPs. Evaluation with various services is future work.

A. Evaluation Environment

The configuration of the evaluation environment is depicted in Fig. 2. A PC for evaluation (Core i7, 2.8GHz) were connected through LAN (100 Mbps). A broadband connection for The Internet was used to communicate with the public cloud service as storage service. All programs were written in JAVA. AES was used as the encryption algorithm. The PC has functions of both client and DDS.

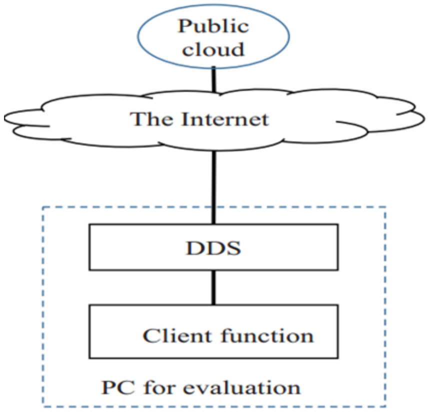

Fig. 10. Evaluation Environment

Here, A fast (k, L, n) threshold secret sharing ramp scheme using XOR, proposed by [13], was used for secret share generation.

The communication with the public storage service was performed by using disclosed API by the public storage service.

A. Experimental Evaluation and Analysis

Here, all measured point values are the value averaged by measuring 5 times. The results of evaluating pure processing performance where the parameters of the secret sharing scheme were fixed to k=3, L=2, n=5 in Fig. 3. Here, the secret data sizes were 1 and 10 MB. In Fig.3, process times of AES encryption/distribution comparing to process time of AES decryption/restoring are depicted except communication time to public cloud service. As shown in Fig.3, secret sharing process take more time than AES process. Secret sharing process time is almost twice as long compared to AES process time, even in the case of encryption / distribution and decryption/ restoration. As shown in Fig.12, upload and download time with single account (no secret shearing) and the case that the secret sharing scheme were fixed to k = 3, L = 2, n = 5 were evaluated. In this case, multiple accesses (multiple accounts) perform in parallel. The upload uses 5 (n=5) accounts simultaneously, and the download uses 3 (k=3) accounts simultaneously. Both upload time and download time are nearly the same, though communication channels are varied. This is because communication speed of each channel is much lower than communication band and process time.

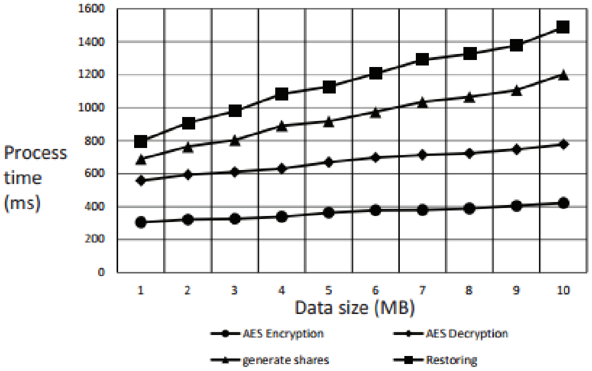

Fig. 11. Process Time(K = 3, L = 2, N = 5)

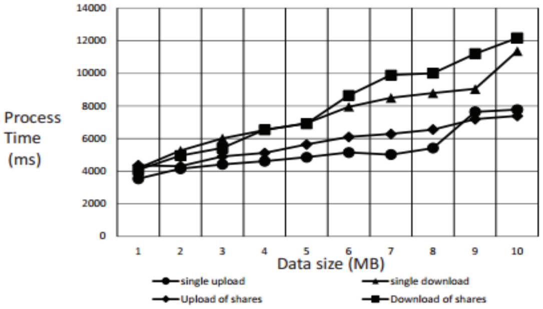

Fig. 12. Upload And Download Time (K = 3, L = 2, N = 5)

Upload and download times in Fig. 12 are much slower than other process times in Fig.11. So, upload and download times become dominant. However, the upload and download speed is not critical to the user from the viewpoint of usability in normal way of usage, because communication and user action are assumed to be synchronous with local cash as a background job, As shown in Fig.12, usability of usual single usage of the public cloud service and that of the proposed service is expected to almost equal. Consequently, the proposed system is feasible for use from the viewpoint of performance.

A. Experimental result

For experiment purpose of the proposed algorithm, we have used a model dataset having the same features of connection and relationships like Facebook. The social graph is generated to visualize the complexity of social networking sites. Interest Database (ID), Activity Database (AD) and User Database (UD) have been modeled to gain the same features of SNS. The interest database keeps all the interests of a particular user. The activity database tracks all the user activities as well as the frequencies of activities, sequentially. The user database contains the information of user and his/her friend list. The FP Growth algorithm is implemented on the connection of all three databases and the algorithm outputs the common and uncommon behaviors which are used for recommendation. The framework shows around 94% accuracy for the model dataset with some limitations. If two users have many interest in common he is certainly recommended for friendship, again users having one or two activities in common are also recommended for friendship. By using some data mining algorithms like clustering or frequency measurement this type of error could be minimized.

VIII. CONCLUSION

In this paper, we have proposed a novel friend or connection recommendation framework which could be used in any social networking sites. The framework is based on user's online behavior. In this paper, we have contributed the user's online behavior definition as well as an approach to use the online behavior to recommend friend. The applications of this framework is huge and this approach could be used to recommend friend, community or group,online games matches with the users behavior or interest and many more. The FP Growth algorithm could be modified to determine a new recommendation system having more accuracy. Differentdata mining rules could be applied to simplify the model dataset and find the required connection. Our future work is to work with different data mining algorithms and large scale datasets from Facebook, Twitter, and MySpace etc.

In this paper, we have discussed strengths and weakness of DES algorithm. We saw that DES purely depends over the key and the substitution-transposition matrices for encryption. Hence is subjected to brute force attack, and DES fails. Dynamic permutation proposes a good stratergy of making most out of DES's advantages while trying to eliminate its limitations. Dynamic permutation strengths DES algorithm, and protects is from brute force attacks. Dynamic permutation may induce additional computational over-head to DES but considering the fact that it induces much larger burden over crypt analyst to break DES cipher text, it's much negligible.

We experimentally evaluated the performance of a proposed data management approach for multiple clouds that use secret sharing schemes by implementing the prototype. A actual particular public cloud service was used as a CSP in the prototype. The result shows that the performance was feasible for use and that the secret sharing processing time was much less than communication time. We will evaluate the performance with various kind of CSPs in the future.

REFERENCES

[1] F. Jiang, C. K. S. Leung, S. K. Tanbeer, “Finding Popular Friends in Social Networks”, Second International Conference on Cloud and Green Computing, 2012,pp.501-508.

[2] Facebook, www.facebook.com

[3] Twitter, www.twitter.com

[4] Flickr, www.flickr.com

[5] LinkedIn, www.linkedin.com

[6] MySpace, www.myspace.com

[7] Google+, www.plus.google.com

[8] S. Catanese, P. D. Meo, E. Ferrara, G. Fiumara, “Analyzing the Facebook Friendship Graph”, 1st International Workshop on Mining the Future Internet, MIFI, 2010.

[9] L. Jin, Y. Chen, T. Wang, P. Hui, A. V. Visalakos, “Understanding User Behavior in Online Social Networks: A Survey”, IEEE Communication Magazine, September 2013, pp. 144-150.

[10] C. Wilson, B. Boe, A. Sala, K. P. N. Puttaswamy, B. Y. Zhao, “User Interactions in Social Networks and Their Implications”, EuroSys, April 1-3, 2009.

[11] X. Xie, “Potential Friend Recommendation in Online Social Network”, IEEE/ACM International Conference on Green Computing and Communications, 2010.

[12] Z. Deng, B. He, C. Yu, Y. Chen “Personalized friend recommendation in social network based on clustering method”, 6th International Symposium, ISICA 2012, Wuhan, China, October 27-28, 2012, pp. 84- 91.

[13] F. T. O’Donovan, C. Fournelle, S. Gaffigan, O. Brdiczka, S. Jianqiang, J. Liu, K. E. Moore, “Characterizing user behavior and information propagation on a social multimedia network”, IEEE conference on Multimedia and Expo Workshops (ICMIEW), July 15-19, 2013, pp. 1-6.

[14] M. N. Hamid, M. A. Naser, M. K. Hasan, H. Mahmud “A cohesionbased friend-recommendation system”, International Journal of Social Network Analysis and Mining, ISSN 1869-5450, February, 2014.

[15] M. Moricz, Y. Dosbayev, M. Berlyant, “PYMK: friend recommendation at myspace”, ACM SIGMOD 2010, International Conference on Management of Data, 2010, pp. 999-1002.