ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

Multi-Authority Attribute based Encryption in OSN

Madhuri R. Rajput[1], Prof. Yogesh B. Jadhao[2], Prof. Arvind S. Kapse[3]

P.G. Student, Department of Computer Engineering, VBKCOE, Malkapur, Maharashtra, India[1]

Assistant Professor, Department of Computer Engineering, VBKCOE, Malkapur, Maharashtra, India[2]

Assistant Professor, Department of Computer Science and Engineering, Prof. P. R. Pote (Patil) COE & M, Amravati, Maharashtra, India[3]

ABSTRACT: Online social networks such as Facebook, Myspace, and Twitter have practiced exponential growth in recent years..Social networking is the most effective and convenient way for interacting with the people around the whole worldwith the help of social networking services, people can communicate interact with the others who are away from themThese OSNs offer attractive means of online social interactions and communications, but also raise privacy and security concerns The existing social networking system recommends a friends base on their lreminder matrix suitable to that user's preference. For selection of friends, so in the given paper I proposed a friend idea system which is supported on an user's profile.In this paper I discuss the design issues for the security and privacy of OSNs. I find there are inherent design conflicts between these and the traditional design goals of OSNs such as usability and sociability. A multi-authority structure is offered in which allclient has an id and they can interact with each key generator (authority) using different pseudonyms. assurances the secrecy of Data Consumers' uniqueness information; and tolerates compromise attacks on the authorities or the collusion attacks by theauthorities.In this paper, Iplan novel mechanisms, when given a preference-profile submitted by a user that search persons with matching-profile in distributed mobile public networks. Meanwhile, our appliancescreate a secure communication channel between the initiator and matching users at the time when a matching user is found. These techniques can also be useful to conduct privacy preserving keywords based search without any secure communication channel.This analysis shows that this mechanism is privacy-preserving, verifiable.

KEYWORDS:OSN Attribute, Proximity, security, Privacy, communication.

I. INTRODUCTION

Friending and communication are two important basic functions of social networks. When people join social networks, they usually begin by creating a profile, and then interact with other users. The content of profile could be very broad, such as personal background, hobbies, contacts, places they have been to, etc. Profile matching is a public and helpful way to make new friends with common interests or experiences, find lost connections or search for experts. Some applications help a user automatically find users with similar profile within a certain distance.[6] For example, in the social network Colour, people in close proximity (within 50 meters) can share photos automatically based on their similarity. MagnetU [1] matches one with nearby people for dating and friend-making. Small-talks connect proximate users based on common interests. These presentations use profiles to support friending between proximate strangers and allow privacy conserving people searching to some extent. Note that in practice the mobile Internet connection may not permanently be available and it may incur high expense. Thus, in this work I focus on proximity-based distributed mobile social networks (MSN) based on short-range wireless technologies such as WiFi and Bluetooth. However the growingsecrecy concern becomes a block for adopting MSN. People are unwilling to disclose personal profiles to arbitrary persons in physical proximity before deciding to interact with them. The insecure wireless communication channel and potentially untrusted service provider increase the risk of revealing private information. Friending

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

established on private profile matching allows two users to match their personal profiles without disclosing them to each other. There are two mainstreams of approaches to solve this problem. The first group gives a user's profile as a set of attributes and provides private attributes matching based on private set intersection (PSI) and private cardinality of set intersection (PCSI).[4] The second category considers a user's profile asa vector and measures the social proximity by private vector dot product [6], [10]. They rely on public-key cryptosystem and homomorphism encryption, which results in expensive computation cost and usually requires a trusted third party. Multiple rounds of interactions are required to perform the presenting (e.g. exchange public keys) and private matching between each pair of users, which causes high communication cost. Moreover, most of those protocols are unverifiable: in the final step of these protocols, only one party learns the matching result and there lack efficient methods to verify the result.[4]
A secure statement channel is so important but often ignored in MSN. Though the similar method is private, One simple solution is to build a secure communication channel using public key cryptosystem[2].This involves a trusted third party and key management, which is difficult to manage in decentralized MSN.

II. LITERATURE SURVEY

Lan Zhang, Xiang-Yang Li says that , Numerous nearness based versatile interpersonal organizations are produced to enctheage associations between any two individuals, or to help a client to discover individuals with coordinated profile inside of a sure separation. A testing undertaking in these applications is to ensure the security the members' profiles and individual hobbies. Author summaries novel tools, when given an inclination profile place together by a customer that hunt a man with coordinating profile in decentralized multi-bounce versatile interpersonal organizations. The systems are security protecting: no members' profile and the submitted inclination profile are uncovered. The systems set up a safe correspondence channel between the initiator and coordinating clients when the coordinating client is found. The thorough examination demonstrates that the system is secure, protection safeguarding, obvious, and productive both in correspondence and calculation. Wide assessments using genuine personal organization material and real framework execution on advanced cells demonstrate that the systems are essentially more effective than existing arrangements.[1]

Zhi Wang, Student Member, IEEE, Lifeng Sun, Member said that Online interpersonal organization is developing as a promising option for clients to specifically get to video substance. By permitting clients to import recordings and re-offer them through the social associations, countless are accessible to clients in the online interpersonal organization. The quick development of the client produced recordings gives huge potential to clients to locate the ones that intrigue them; while the meeting of online informal organization administration and online video sharing administration makes it conceivable to perform proposal utilizing social components and substance considers mutually. In this paper, we outline a joint social-content proposal system to recommend clients which recordings to import or re-offer in the online informal organization. In this system, we first propose a client content lattice upgrade approach which redesigns and fills in icy client video sections to give the establishments to the suggestion. At that point, taking into account the redesigned client content framework, we build a joint social-substance space to gauge the pertinence in the middle of clients and recordings, which can give a high exactness to video importing and re-sharing proposal.[3] We direct tests utilizing genuine follows from TencentWeibo and Youku to check the calculation and assess its execution. The outcomes exhibit the viability of the methodology and demonstrate that the methodology can significantly enhance the suggestion precision[8]

Bhoopathy, V., Parvathi, R.M.S said that In a little conveyed frameworks a customer ought to just have the capacity to get to information if a client groups a sure arrangement of certifications or properties. As of now, the main strategy for upholding such approaches is to utilize a trusted server to store the information and intercede access control. Not with standing, if any server putting away the information is traded off, then the confidentiality of the information will be traded off. In this paper we show a framework for acknowledging complex access control on scrambled information that we call Ciphertext-Policy Attribute-Based Encryption.[2] By using the events programmed material can be saved private regardless of the possibility that the stockpiling server is untrusted; in addition, the routines are secure against agreement assaults. Past Attribute-Based Encryption frameworks utilized credits to portray the scrambled information and incorporated arrangements with client's keys; while in the framework

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

credits are utilized to depict a client's qualifications, and a gathering encoding information decides an planning for who can decode. In this manner, the techniques are theoretically closer to customary access control systems.
Melissa Chase, Sherman S.M. Chow said that Trait based encryption (ABE) decides unscrambling capacity in view of a client's qualities. In a multi-power ABE plan, many trait rules screen characteristic arrangements of properties and issue comparing unscrambling keys to clients, and encryptors can require that a client acquire keys for fitting qualities from every power before decoding a message. Pursue gave a multi-power ABE plan utilizing the concepts of aimportantmain power (CA) and worldwide identifiers (GID). In any case, the CA in that development has the ability to unscramble each ciphertext, which appears to be by one means or another conflicting to the first objective of dispersing control over numerous possibly untrusted powers.[3] Additionally, in that development, the utilization of a reliable GID permitted the powers to join their data to construct a full profile with the greater part of a client's properties, which pointlessly bargains the client's protection. In this paper, we propose an answer which uproots the trusted focal power, and secures the clients' protection by keeping the powers from pooling their data on specific clients, along these lines making ABE more usable practically speaking.[4]

Emiliano De Cristofaro and Gene Tsudik said that The always expanding reliance on whenever anyplace accessibility of information and the comparably expanding apprehension of losing protection spur the requirement for security saving methods. One between besting and regular issue happens when two gatherings need to secretly figure a convergence of their particular arrangements of information. In doing as such, one then again both sides must get the crossing point (if one exists), while not one and the other should learn anything about other set components. Albeit former work has yielded various effective and exquisite Private Set Intersection (PSI) methods, [7]the mission for efficiency is still in progress. This paper investigates some PSI varieties and builds a few secure conventions that are appreciably more efficient than the cutting edge.[11]

III. PROPOSED SYSTEM

In propose system we design and style novel mechanisms, when provided a preference-profile submitted by a consumer, that search individual persons with matching-profile in on-Line social networks. Meanwhile, this mechanism generates a safe communication channel in between the initiator and matching end users at the time when a matching consumer is identified. The initiator packs the encoded message, the remainder vector and the hint matrix into a request bundle and sends him out. The demand profile is a set of arrangedqualities by each reminder and hint matrix attributes. Then he/she encodes the qualities of the request profile a single by one particular to make a request profile vector.A profile is important created primarily based on the request profile vector manufacture use of some publicly familiar hashing perform by submitted attributes. A remainder vector of the profile vector is produce for quick exclusion by a huge portion of unmatched individual persons. To help a useful search needful no excellent match, the initiator can define the required attributes, optional attributes and the similarity threshold of the matching profile. And a hint matrix is created from the request profile vector in agreement to the similarity definition, which allows the matching individual person to get the profiles important key to matched end users. When a send consumer accepts a request from an additional consumer, he/she initial practices a quick check out of his/her personal profile vector with the remainder vector. If no sub-vector of his/ her profile vector fits the remainder vector, he/she is aware of that he/she is unmatched and will forward the request to other relay end users quickly. Otherwise, he/she is a candidate target and will yield a candidate profile vector set by some linear computation with his/her profile and the hint matrix. Then a candidate profile key is important to obtained set. In the fundamental mechanism, if any of his/her candidate keys can decrypt the message appropriately; he/she is a matching user and the browsing and secret important key exchange totally. Otherwise, he/she just forwards the request to other relay end users. This procedure will continues until consumer or initiator will get relayed end users primarily based on reminder and hint matrix attributes.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

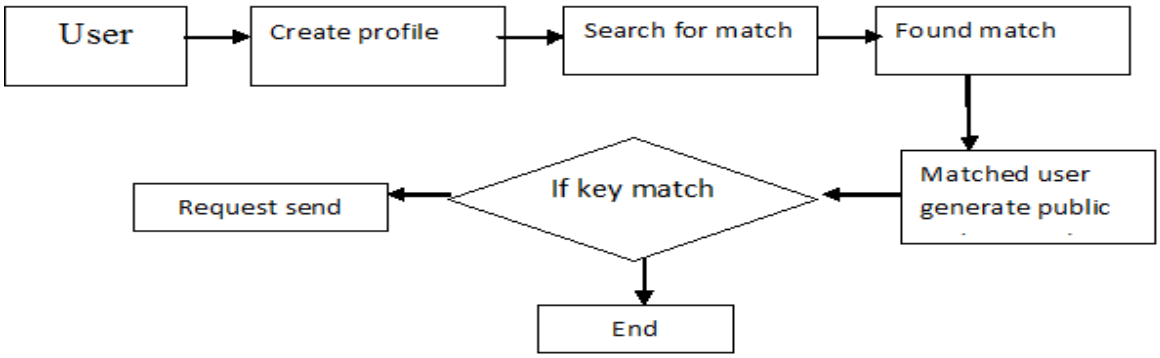

Fig. 1 System Architecture

ALGORITHM:

AES

AES is the Advance Encryption Standard is symmetric encryption algorithm, which was developed by Vincent Rijmen and Joan Daemen. AES algorithm is repeated procedure which is based on substitution and permutation network. AES allows three different key lengths 128,192 and 256 bits. Encryption contains 10 rounds for 128 bit keys,12 rounds for 192 bit keys and 14 rounds for 256 bit keys. The nature of substitutions and permutations in AES allows for a fast software implementation of the algorithm.. The encryption process uses a set of specially derived keys called round keys. These are useful, along with other actions, on an array of files that holds accurately one block of files? thefiles to be encrypted. This array we call the state array.

Following are the steps used in AES algorithm

1) Sub Bytes

The 16 byte as input are substituted by usingS-box

2) Shift rows

Each row of the matrix is shifted to the left.

3) Mix Columns

Mixing the data inall column of the State array

4) Adding a Round Key to the State

for adding the round key to the output of the prior step in the forward process

You take the following aes steps of encryption for a 128-bit block

- Derive the set of round keys from the cipher key.
- Initialize the state array with the block data (plaintext).
- Add the initial round key to the starting state array
- Perform nine rounds of state manipulation.
- Perform the tenth and final round of state handling.
- Copy the final state array out as the encoded data (ciphertext).

If this is the final round then the output is the cipher text. Else the resultant 128 bits are used as 16 bytes and we begin another similar round.TheCode transformations can be reversed and then executed in reverse order to produce plaintext by using the AES algorithm. The separate transformations used in the ReverseEncryption.

1. **Inverse Sub Bytes**
2. **Inverse Shift Rows**
3. **Inverse Mix Columns**
4. **Add RoundKey**

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

The AES reverse encryptionbasicconsist of a key progress module, a key reversal buffer, an initial permutation module, a round permutation module and a final permutation module. The key reversal buffer first accumulate keys for all rounds &used them in reverse order to the rounds. The round permutation module will loop maternally to perform 14 iterations.

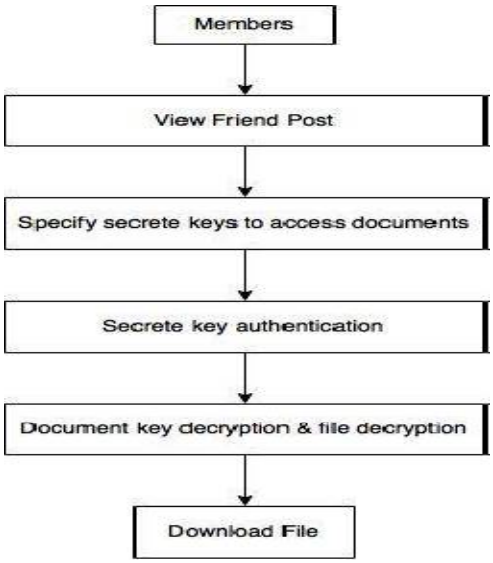

Fig.2 AES flow chart for AES decryption

Privacy-Preserving Profile Matching Protocols:

Protocol 1: Under Protocol 1, an unmatched user doesn't know anything about the request. The matching user knows the intersection of the required profile and his/her own profile after Step 1 in the HBC model, and he/she can decide whether to reply. The creator doesn't know anything about any contributor until he/she gets a reply. With responses, he/she identifies the similar clients and even the most similar replier by the cardinality information.

Steps:

1) The initiator encrypts a random number x and public predefined confirmation information in the secret message EKt ð confirmation; xÞ by the required profile key Kt. And he/she sends the request out.
2) A candidate relay user can verify whether he/she decrypts the message correctly by the confirmation information. If he/she does not match, he/she just forwards the request to the next user. If he/she is matching, he/she can answer the request by encoading the predefined ack information and a random number y along with any other message (e.g. the intersection cardinality) by x, say Exðack; yÞ, and sends it.

Protocol 2: To avoid malicious members, we design Protocol 2, which is similar to Protocol 1, but it rejects the validation information from the encoded message.

Steps:

1) The initiator encrypts a random number x in the secret message EKt(x) by the request profile key Kt.
2) A candidate similar user cannot validate whether he/she decrypts the message correctly. Let the runner profile key set be Rt=($k_{c,}^{1} k_c^2 \ldots\ldots k_c^z$)

He/she decrypts the message in the request with each candidate profile key to get a set of numbers, say U={uj|uj=Dk_c^j(Ekt(x))} Then he/she encrypts the predefined ack information and a random number y by each uj as the key, and sends the acknowledge set Euj(ack, y)to the initiator, for a public ack.

3) The initiator rejects the potential malicious repliers whose reply time exceeds the time window or the cardinality of reply set exceed the threshold. He/she decrypts the answers with x. If he/she gets a rightack information from a reply, the agreeing replier is a similar user.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

Protocol 3: To avoid the dictionary profiling by malicious initiator, progress Protocol 2 to Protocol 3 which offers a user personal defined secrecy safety.

Steps:

1) The initiator encrypts a random number x in the secret message without any confirmation information by the required profile key, say Ekt(x).
2) A candidate matching user cannot confirm whether he/she decrypts the message properly. He/she selects a set of candidate profile. ($a_{c,}^1 a_c^2$ …… a_c^z) .And he/she generates the corresponding candidate profile keys ($k_{c,}^1 k_c^2$……k_c^z) He/she decrypts the message in the request with each candidate profile key get a set of numbers, say U={uj|uj=Dk_c^j(Ekt(x))} Then he/she encrypts the predefined ack information and a random number y by each uj, and sends back the acknowledge set Euj(ack, y) back to the initiator.
3) The initiator eliminates the malicious replier whose response time exceeds the time window or the cardinality of reply set exceeds the threshold and decrypts the replies with x. If he/ she get correct ack information from a reply, the corresponding replier is matching.

Opertion:

Process

Let S is the Entire System Contains:

S = {P, PR,S PS, BA, R}.

1. P is the set of generated profile.
   P= {P1, P2,P3… Pn}.
2. S is the set of search for match.
   S= {S1, S2,S3, … Sn}.
3. .PR is set of protection
   PR= {PR1, PR2,PR3….PRn}.
4. PS is set of securitysystem sharing.
   PS= {PS1, PS2,PS3,… PSn}.
5. BA is set block malicious attack.
   BA= {BA1.BA2,BA3….BAn}.

Step 1: multiple client, client create profile

P= {P1, P2,P3…Pn}.

Step 2: Then it examine for match .If match is found then it offer a protection else search for another.

S= {S1, S2,…Sn}.

Step 4: If search is found then security is providing.

PR= {PR1, PR2,PR3,….PRn}.

Step 5: Then private systemallotment is functional.

PS= {PS1, PS2…PSn}.

Step 6: Then malicious code is blocked.

BA= {BA1, BA2….BAn}.

Result : Message is sent to accurate matching user securely

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

IV. RESULT AND DISCUSSION

Following figure illustrate that in proposed system time need for key recovery is less than time need for key recovery in existing system. And propose system also offer more security, prevention and confidentiality than existing system.

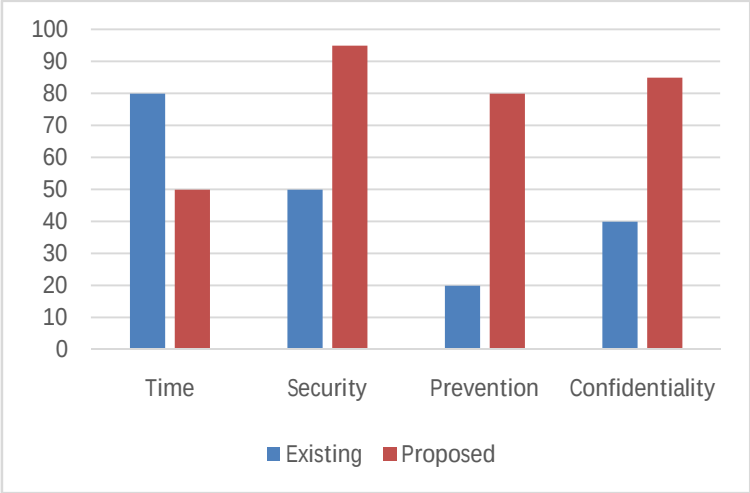

Fig. 2: Result analysis

Following table shows relationshipbetween existing system and propose system in terms of time, security, prevention and Confidentiality.

	Existing System	Proposed System
Time	80	50
Security	50	95
Prevention	20	80
Confidentiality	40	85

Table 1: Experimental Result

V. CONCLUSION

In this paper, I plan a novel symmetric key encryption based protection safe guarding profile coordinating and secure correspondence divert foundation system in decentralized MSN with no presetting or trusted outsider. In this system log in page is created for user to log in the system and for new users sign up page is available on that user have to fill some simple information then validation of their account on the successful creation mail will be sent to their respective mail id. After that user will be forwarded to the home screen on which many options are there user can sent friend request to other user and accept vice versa. Also worker can share media or some files or status on the system and others can like or dislike the shared items. As compared to the existing recommendation methods, the proposed method searches the friends to satisfy a user's current contexts.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

REFERENCES

[1] Lan Zhang_, Xiang-Yang Li "Message in a Sealed Bottle: Privacy Preserving Friending in Social Networks" ,IEEETRANSACTIONS ON MOBILE COMPUTING, VOL 14, NO. 9,SEPTEMBER 2015
[2] J. Bethencourt, A. Sahai, and B. Waters, "Cipher text-policy attribute- based encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334
[3] M. Chase, "Multi-authority attribute based encryption," in Proc. 4th Conf. Theory Cryptography, 2007, pp. 515–534.
[4] E. De Cristofaro and G. Tsudik, "Practical private set intersection protocols with linear complexity," in Proc. 14th Int. Conf. Financial Cryptography Data Security, 2010, pp. 143–159.
[5] W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure friend discovering mobile social networks," in Proc. IEEE INFOCOM, 2011,pp. 1647–1655
[6] Zhi Wang, Zhibo Wang and Qing Cao "Friend-book- A Semantic- based Friend Recommendation System for Social Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING.
[7] Zhimin Yang*, Boying Zhang*, Jiangpeng Dai*, Adam C. Champion*, Dong Xuan* and Du Li†E- "SmallTalker: A Distributed Mobile System for Social Networking in Physical Proximity" 2010 International conference on Distributed Computing System
[8] Chi Zhang and Jinyuan,SunXiaoyan Zhu, Yuguang Fang "Privacy and Security for Online Social
[9] Networks: Challenges and Opportunities", IEEE Network • July/August 2010 0890-8044/10/$25.00 © 2010 IEEE.
[10] Rui Zhang*, Yanchao Zhang*, Jinyuan (Stella) Sun, and Guanhua Yan "Fine-grained Private Matching for Proximity-based Mobile Social Networking"2012 proceeding IEEE INFOCOM
[11] Kshitija Nandgaonkar1, SwarupaKamble "A SURVEY ON PRIVACY-PRESERVING DATA AGGREGATION WITHOUT SECURE CHANNEL" International Research Journal of Engineering and Technology (IRJET) Volume: 03 Issue: 01 | Jan-2016