A Effective Cryptosystem For Privacy-Preserving User Profile Matching in Social Networks

***Mrs.Priya A P [1]**

[1]Research scholar, Department of computer science, Sree Narayana Guru College, Coimbatore

Abstract: *Now a day's protect privacy and Profile matching of user in social networks is more important and challenging task to online matching service provider. This matching service provider such as finding friend and dating services are asking too much personal information from user When registration and profile creation for an online matching service. The matching service provider has thus full knowledge of the users' personal information, which leads dating user profiles data disclosure along with privacy issues, as the matching service provider may leak user personal information. To solve this kind of issues, proposed research system is effectively use* ***homomorphic NTRU Cryptosystem*** *for user profile data encryption and decryption. This NTRU cryptographic technique to permit computation on encrypted data directly. The research work also introduces secret sharing techniques to solve profile matching. Based on the user search query, dating service provider servers, which secretly share the decryption key, compare the preferred user profile finally matching user' contact information is returned to the user. The main aim of proposed system is achieve effective privacy Preserving and profile matching on user profile data which is maintain in online matching service provider. The result shows the proposed work outperforms than the existing approaches and improves the User Profile matching accuracy and better security.*

Keywords: **Cryptosystem, Profile Matching, NTRU, Privacy-Preserving, Social Networks.**

1. INTRODUCTION

Social network services allow individuals user can create profile that others can browse based on their preferences. Matching more than one social network users with correlated interests is a crucial problem in each and every online service matching sites such as finding friends, and dating services [1]. On-line matching services completely maintain the user personal information which leads some of the serious issue to user. Whenever new user registration for an online matching service, user may be reveal some personal details, such as religion, location, behavior, hobbies, income, favorite places, phone number, address, etc.This completely information maintain in server for provide service to other user. But the problem is here server has thus full knowledge of the users' preferences, which raises Privacy relates issues**.** Sometime server may be leak user personal and sensitive information either purposely or by mistake. Online matching service may be share user personal data without customer permission. Even after an account is canceled from social Networks matching sites, most sites may retain such user personal information.

1.1 Social Networks

Social network is a website that brings people mutually to talk, they can share ideas and interests, or make new friends. Profile matching is one of the important for social networks because finding and searching the nearby individuals of the similar or same interests is forever the first important step for any social networking. Social networks service provider introduces privacy levels for secure user profile matching [2]. However, it is not easy to find out the matching users efficiently. Because of before upload user information or profile to a social network sites, each user completely encrypts the profile and personal information by an encryption scheme with a common secret key. Social service provider completely keeps the user encrypted profile data in dedicated server. Therefore, profile matching is very difficult process every time server needs to decrypt the information after that only profile matching process can be done .This take more time consuming and server has full information of the users, which causes data may be leak or raise serious privacy issues. An important challenging task for social service provider is protect privacy of user profiles using effective Cryptosystem [3].

1.2 Cryptosystem

Nowadays privacy leakage trouble for increase individuals in every social network matching sites. Maintain data security is very complex and challenging. External threats are increasing. Cryptography is a technique that is able of providing information security. Cryptography is also known as cryptosystem which deals with the actual securing of digital information. Encryption and decryption is a key concept in cryptography. Cryptosystem consists of set of algorithms that provide basic information security services.

Types of Cryptosystem

Fundamentally, two types of cryptography system Follows. The main important difference between these two cryptosystems is encryption and the decryption key.

1. **Symmetric cryptography:**

Symmetric cryptography is a type of encryption that uses the single key is use to data encrypt and decrypt .This is generally more efficient than Asymmetric cryptography. This type of Symmetric cryptography used for large amounts of data store and exchanged.

2. **Asymmetric cryptography**.

Asymmetric cryptography is a type of encryption that uses the public key is use to data encrypt and private key is used to data decrypt. Asymmetric cryptography is mostly used communication over the Internet. This type of cryptography used for small amounts of data store and transmit.

1.3 Privacy-Preserving

Huge amount of user data being collect and maintain by the social network service provider Sometime this data has led to risk of data leakage also data may be share to unknown user without user knowledge. Protect privacy of user profiles Social network user requires effective privacy protection before the data is store or uploaded by the network service provider. Service provider must ensure the privacy of the user. So far, some of the privacy preserving data mining technique available for user sensitive information [4]. Important Privacy preserving Techniques are

A. **Data Anonymization**

Data anonymization is the one of the most important process of protecting user private or sensitive information .This anonymization reduces the complete risk of data disclosure during the store and transmits of information. In Data Anonymization ensure user privacy using Generalization is one of the methods this methods eliminates some sensitive parts of the data to make it less identifiable. Another important method is Perturbation this method achieves user privacy with help of lightly modifies a dataset by adding random noise.

B. **Slicing**

Slicing is one of the most important a popular data Anonymization technique for ensure the user data privacy. Slicing approach complete user sensitive information is partitioned in both horizontal and vertical direction to protect the privacy.

C. **Randomization**

This is the recent methods for achieve ensure privacy of user in social network. Randomization technique is an effective approach for privacy preserving data mining. This method applies for preserve

individual privacy. The randomization approach protects the user sensitive information by adding some noise in original information, so that privacy of user will be maintain effectively. The main problem of the Privacy-Preserving approaches in data mining every method completely ensure the privacy but privacy preserving methods not suitable for profile matching .This is one of the challenging problem.

2. LITERATURE REVIEW

In [5] paper proposed ElGamal Public Key encryption scheme, which allow social network user to find out or search some matching users with the help of query from the servers without revealing to anyone privacy. The ElGamal provide an option to the RSA for public key encryption. Problem found with ElGamal is security flaw in the encryption scheme which means hacker or attacker decrypts the server cipher texts without the private key. Another problem with ElGamal cipher text is twice as long as the plaintext.

In [6] Y. Sang, H. Shen, and N. Xiong proposed Privacy Preserving Set Matching (PPSM) protocol. In this paper work, the social network user profile data information is shared by all matching servers and as a result every server is necessary to maintain and store user information. This lead too much of data complexity to server. Suppose any one of the server target by attacker means they can get complete user profile information.

In [7] paper proposed dissimilarity threshold with profile matching technique. In this paper work, a query user may wish to specify one dissimilarity threshold which mean user can search with query to find people with example age 20 for user matching. User can not search between 40 and 50 for user matching. This paper work user profile matching process is full based on numerical attributes values only.

In [8] paper proposed a solution for the private two-party set-intersection problem this work server hold a set of multiple user data information to together calculate the intersection of their inputs data, without leaking any additional information. Finally comparing which elements appears in both sets that element will return to user. Main problem with this solution needs to compute a large number of exponentiations.

Li et al. [9] proposed FindU scheme for profile matching in social networks. This is first privacy-preserving user private profile matching scheme for mobile social networks. Social network user can find from a group of users profile information one whose profile best matches with search user. This approach only essential and minimum information is exchanged. This approach only suitable for mobile social networks

Huang et al [10] proposed private fingerprint matching protocol that completely compares two fingerprints using minutia-based fingerprint matching algorithm. The protocol enable two parties, each one holding a personal fingerprint, to find out if their fingerprints belong to the same individual. Initially compare finger print minutia pairs from the two fingerprints based on their types, locations info, and orientations, after that check if the number of matching minutia pairs is more than threshold user profile information will return. This work assumes user complete data encrypted and store but finger print of the two parties only in clear text.

Sun et al. [11] proposed privacy-preserving distance-aware encoding protocol to compare numerical values in the anonymous space. This work completely similar to homomorphic encryption, that allow performs some computation on cipher texts. The main important purpose of homomorphic encryption is to allow effective computation on encrypted data, but this scheme which support any one of the operation either addition or multiplication on encrypted data.

3. EXISTING SYSTEM

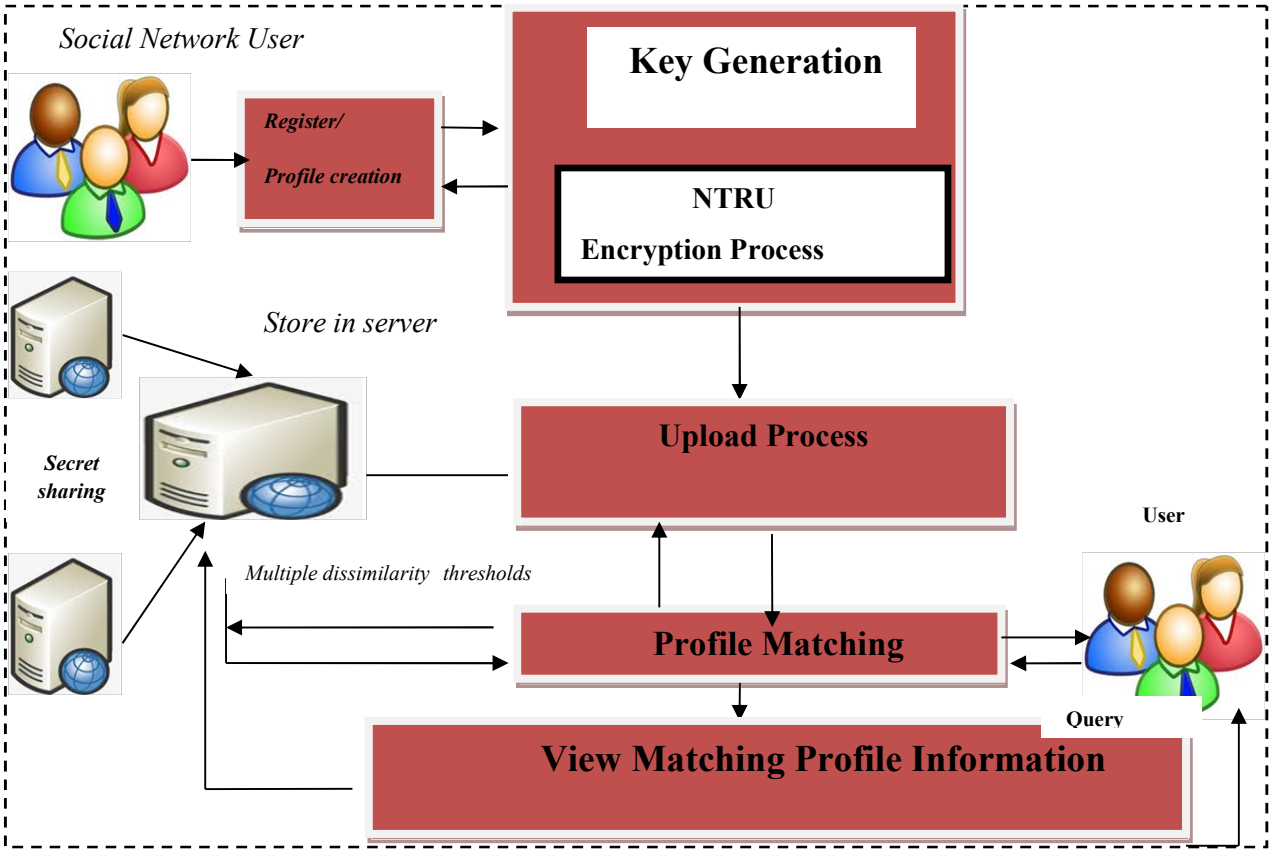
To provide privacy-preserving solution for user profile matching and protect privacy of user profiles in social networks is more important recent research work. So far, some of the existing papers work on the above problem .Existing work ElGamal homomorphic encryption is used to data encryption Problem found with ElGamal is security flaw because of two prime factors of the modulus are public

parameters which attacker decrypts the server cipher texts without the private key. Existing work, user profile information is shared by all servers and therefore each social network server is mandatory to maintain a user profile database completely. This leads server overhead problem. Query user can specify only one dissimilarity threshold for user matching.Exiisitng work Privacy-Preserving User Profile Matching is based on numerical attributes. Existing none of the work not satisfied effective User Profile Matching in social network.

4. PROPOSED WORK

This chapter completely discusses regarding the proposed system methodology and the process involved in this proposed system. The system proposes a new effective Model for protect privacy which is called ***homomorphic NTRU Cryptosystem with secret sharing*** for effective user profile matching and protect privacy of user profiles in social networks.

Architecture Diagram of Proposed system



The proposed system completely focuses on protect privacy and profile matching over encrypted data. Initially User can make signing up and user can create profile after successful profile creation user encrypts the profile by a NTRU homomorphic encryption after that user uploading his/her profile to a social network. Profile matching is completely depends on User query when ever user enter query with multiple dissimilarity thresholds this matching request goes to Social Networks server. Server allows performs some computation on numerical attributes cipher texts and profile matching result display to user effectively .Proposed work also extends user profile matching with categorical attributes which means User can search categorical data such as location,hobbies,address,etc for user matching .performing computation on categorical attributes cipher texts is difficult process so that proposed system

used secret sharing technique which means every server share some part of the secret key information to main server. Finally main sever collect shared secret key and decrypted the information and matching user profile information will display to user effectively.

Advantages of proposed system

1. Proposed system gives query user to specify multiple dissimilarity thresholds for user matching.
2. NTRU homomorphic encryption gives high level security with performs better computation
3. User profile data is shared by social service provider only so that maintains user profile data easier.

5. METHODOLOGY

The proposed system develops and implements an efficient framework "***homomorphic NTRU Cryptosystem with secret sharing***" for effective profile matching in *Social Networks* Environment. Finally, the proposed system works with the following algorithms and techniques.

Module 1: User Registration and profile creation

This module helps the user to register them with the application. Registration is mandatory Social Networks for them to match profile. After successfully registration authentication phase defines the security and authority to access, for example every social network should be authenticated for Profile Matching. User can able to create profile information such age, sex, education details , geographic location, hobbies, income details , religion info , home and work addresses, favorite places these complete information will be maintain in Excel Sheet before uploaded in to server that others can browse or search above information.

*Server***:** the storage server has the responsible to respond for the user search request.

Module 2: Data set collection and preprocessing

The first step is extraction of user profile data from Excel sheet. Here the sentence which contains set of text will be extracted for the analysis. Identifying data's and splitting into terms is the major process ,Before process the document the given input document is processed for removing redundancies, inconsistencies, separate words, stemming and documents are prepared for next step.

Modules 3: Encryption process Using NTRU

Encryption is the process of translating plain text data (plaintext) into something that appears to be random and meaningless (cipher text).NTRU homomorphic process work on public and private key. The purpose of homomorphism encryption is to allow effective computation on encrypted data.

Nth degree Truncated Ring polynomial Unit

- The two keys used in this algorithm are: public key and private key
- Public Key always used for secure data encryption purpose .Public key can know any one for some purpose
- Private Key is used for cloud data decryption. This key knows by only one person.

NTRU homomorphic Algorithm its major involves three different steps: key generation process, encryption and decryption process. It involves a public key and a private key cryptosystem so that public key can be known to everyone and is used for encrypting secret messages of client. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the secure share private key.

NTRU Parameter

1. Parameter Selection: NTRU-Encrypt include n, p, q, df, dg and dr.
2. N is the prime number to choose the degree of truncated polynomials.
3. P and q values should be relatively prime number. One of the important condition is q should be significantly larger than p.

4. N df, dg and dr can significantly used for efficient computation.

Key Generation

Step 1: Randomly choose a polynomial g(x) ∈ Lg.

Step 2: To find and calculate fq(x) and fp(x) which are respectively the inverses of polynomial f(x) mod q and f(x) mod p.

Step 3: Compute h(x) = p × fq(x) × g(x) mod q.

Now consider h(x) is the public key of NTRU encryption system, while the pair (f(x), fp(x)) are the correspond private key of NTRU .Public key is used for encryption process private key is used for decryption process.

NTRU CRYPT SYSTEM

Input: User profile, Key

Process: Return Encrypted Content

Output: Key apply, view Content

Step 1**:** Encryption

Read the user profile content from Excel file.

Step 2: randomly chooses 2 small polynomials f and g

F (x) = x^6−x^4+x^3+x^2−1

G(x) = x^6+x^4−x^2−x

Step 3: Find N such that N = F G

N will be used as the modulus for both the public and private keys

Find the toting of n, ϕ(n) ϕ(n)=(f-1)(g-1)

Step 4: e = n*f +m (modulo q),

e is encrypted message, m is plaintext, f is public key

step 5: Take the decryption files from computer and read its content.

Step 6: strings from file then store in string builder then convert that string in to char array.

Step 7: Here N will be used as the modulus for two keys

Find the totient of n1, ϕ1(n1) ϕ1(n)=(g-1)(f-1)

Step 8: d = n1*fg1+e (modulo q),

D is decrypted message, m is encrypted text, f is private key

Modules 4: Profile Matching

Find matching users from the social network, user need to specify his preferred profile attributes along with some e dissimilarity threshold. After succeful receiving the query receiving the query servers help to find matching users profile information from the storage server.

User Query Generation

Step 1: Initially take as input the common public key PK from social networking service. Public key available for every user.

Step 2: specified N number of profile attributes a1, a2, a3,a4 along with corresponding weight w,w1,w2,w3,w4, ..wm.

Step 3: dissimilarity threshold δ, example (age<30 and age>25)

Step 4: Finally query denoted as Q = QG (PK, a1, w1, a2, w2 · · , am, wm, δ) which is submitted by user to the social networking service provider. Server will make profile matching process.

Step 5: Response generation from server. Server takes as input the query denoted as Q ,then user profile from database, taking private keys k1, k2, · , kn, for decryption.

Step 6: Finally profile matching response from server outputs a response denoted R.

Step 7: R = RG (Query, DB profile, private key k1, k2,, kn). R, will hold the contact information of the first t profile matching users this stores in array list then returned to the user,

Step 8: User retrieves profile matching response t0 = min (t, T) and T denotes the total number of matching profile users details in server.

Modules 5. Secret sharing

Secret sharing also called as secret splitting Achieve better privacy preserving Server will split the secret key distributing a secret key to among a group of server. User can submit query with some categorical data such as location, address .Server receives the query request from user server will collect the secret sharing key from every server. Finally server completely decrypted the profile information and match the information using pattern matching technique then matching user result will be shown to user.

Step 1: Consider Pk is private key
Step 2: Get No of server in social network N denote no of server
Step 3: Secret key divided into N parts: PK1, PK2, and PK3… PKn.
Step 4: User Need to define K .K is the integer values selected by the user order to decrypt.
Step 5: Share divided Secret key to N number of server.
Step 6: server cannot get private key secret reconstructed with (K – 1) parts or fewer.
Step 7: finally secret share equal to K value or higher than k values means server can decrypt and will return profile match user result.

6. RESULTS AND DISCUSSION

The Sample some experiments are design conduct for know the performance of NTRU proposed algorithm using software, hardware. Then the experimental is performed on an Intel core 2 duo 4 GHz processor with the maximum 8 GB RAM capacity. The proposed researches algorithms are successfully implemented in JAVA programming language are run under Windows platform. Finally, the performance of this proposed Research NTRU homomorphic Cryptosystem work Scheme was compared with the existing algorithms based on the following parameters.

- Time taken – Determines the encryption/decryption processing time involved.

Table 1. Sample Datasheet File for Encryption/Decryption

Metrics	User Profile File Size	ElGamal homomorphic	Proposed NTRU Encryption
	300Mb	1600	1400
Time Comparison (ms)	500Mb	2250	2000
	700 Mb	2450	2200

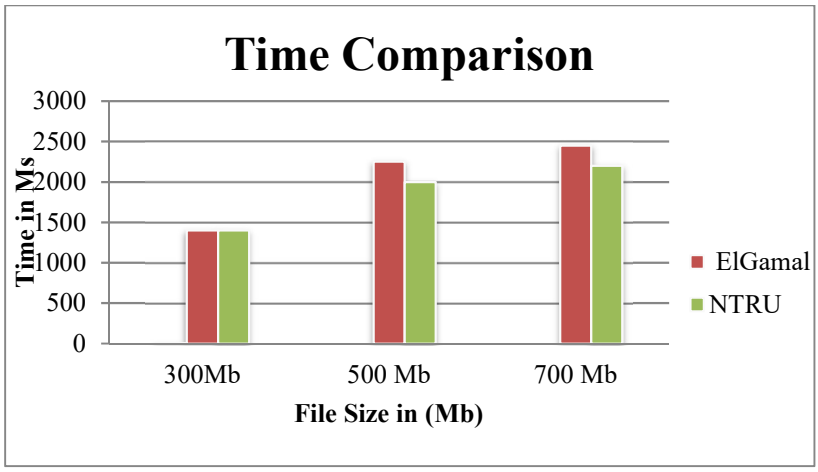


Figure 1. Encryption/Decryption Time comparison

The graph shows encryption and decryption Performance comparison of the proposed system with existing approaches based on Encryption/Decryption Time. From the results shown in the graphs, it can be observed that the proposed approaches provide better accuracy and increased less time taken for perform encryption and decryption for different number of datasets.

7. CONCLUSION

The Main motivation of proposed work research is to provide the data mining services to ensure user privacy in social network. Proposed system successfully Integrate with homomorphic NTRU Cryptosystem with secret sharing algorithm to provide better security. Our proposed NTRU Cryptosystem Model will be more effective with efficient encryption. Important objective of this proposed work is to build Profile Matching on encrypted data with high matching accuracy. The new scheme completely offer multiple dissimilarity thresholds along with Proposed work also extends user profile matching with categorical attributes this will helps improve profile matching accuracy in social network From the sample experimental results, the encryption and decryption execution time and security matrix is calculated. Proposed system almost produce less time consumption for encryption and decryption clearly shows proposed system better than the existing system.

REFERENCES

[1] Xu An Wang, Fatos Xhafa, Xiaoshuang Luo, Shuaiwei Zhang and Yong Ding Journal: Soft Computing, 2018, Volume 22, Number 8, Page 2517.

***[2]** Ying Zou, Yanting Chai, Sha Shi, Lei Wang, Yunfeng Peng, Yuan Ping, Baocang Wang, "Improved Privacy-Preserving Profile-Matching Scheme in Mobile Social Networks , Security and Communication Networks, vol.* 2020*, Article ID 4938736, 12 pages, 2020.*

[3] B. Liu and H. Wu, "Efficient multiplication architecture over truncated polynomial ring for NTRUEncrypt system," 2016 IEEE International Symposium on Circuits and Systems (ISCAS), 2016, pp. 1174-1177, doi: 10.1109/ISCAS.2016.7527455.

[4]. *F. A. N. Pathak and S. B. S. Pandey, "An efficient method for privacy preserving data mining in secure multiparty computation," 2018 Nirma University International Conference on Engineering (NUiCONE), 2018, pp. 1-3*

[5]. X. Yi, A. Bouguettaya, D. Georgakopoulos, A. Song. Privacy protection for wireless medical sensor data, IEEE Transactions on Dependable and Secure Computing, 13(3): 369-380, 2015..

[6]. Y. Sang, H. Shen, and N. Xiong, Efficient protocols for privacy preserving matching against distributed datasets, in ICICS 2006, pp. 210-227.

[7]. X. Yi, E. Bertino, F. Y. Rao, A. Bouguettaya, Practical privacy-preserving user profile matching in social networks, in ICDE 2016, pp. 373-384

[8]. C. Hazay and Y. Lindell, Efficient protocols for set intersection and pattern matching with security against malicious and covert adversaries, in TCC 2008, pp. 155-175.

[9]. M. Li, N. Cao, S. Yu and W. Lou, "FindU: Privacy-preserving personal profile matching in mobile social networks," 2011 Proceedings IEEE INFOCOM, 2011, pp. 2435-2443, doi: 10.1109/INFCOM.2011.5935065.

[10]. S. F. Shahandashti, R. Safavi-Naini, P. Ogunbona, Private fingerprint matching, in ACISP 2012, pp 426-433.

[11]. D. Karapiperis, A. Gkoulalas-Divanis and V. S. Verykios, "Distance-Aware Encoding of Numerical Values for Privacy-Preserving Record Linkage," 2017 IEEE 33rd International Conference on Data Engineering (ICDE), 2017, pp. 135-138, doi: 10.1109/ICDE.2017.58.