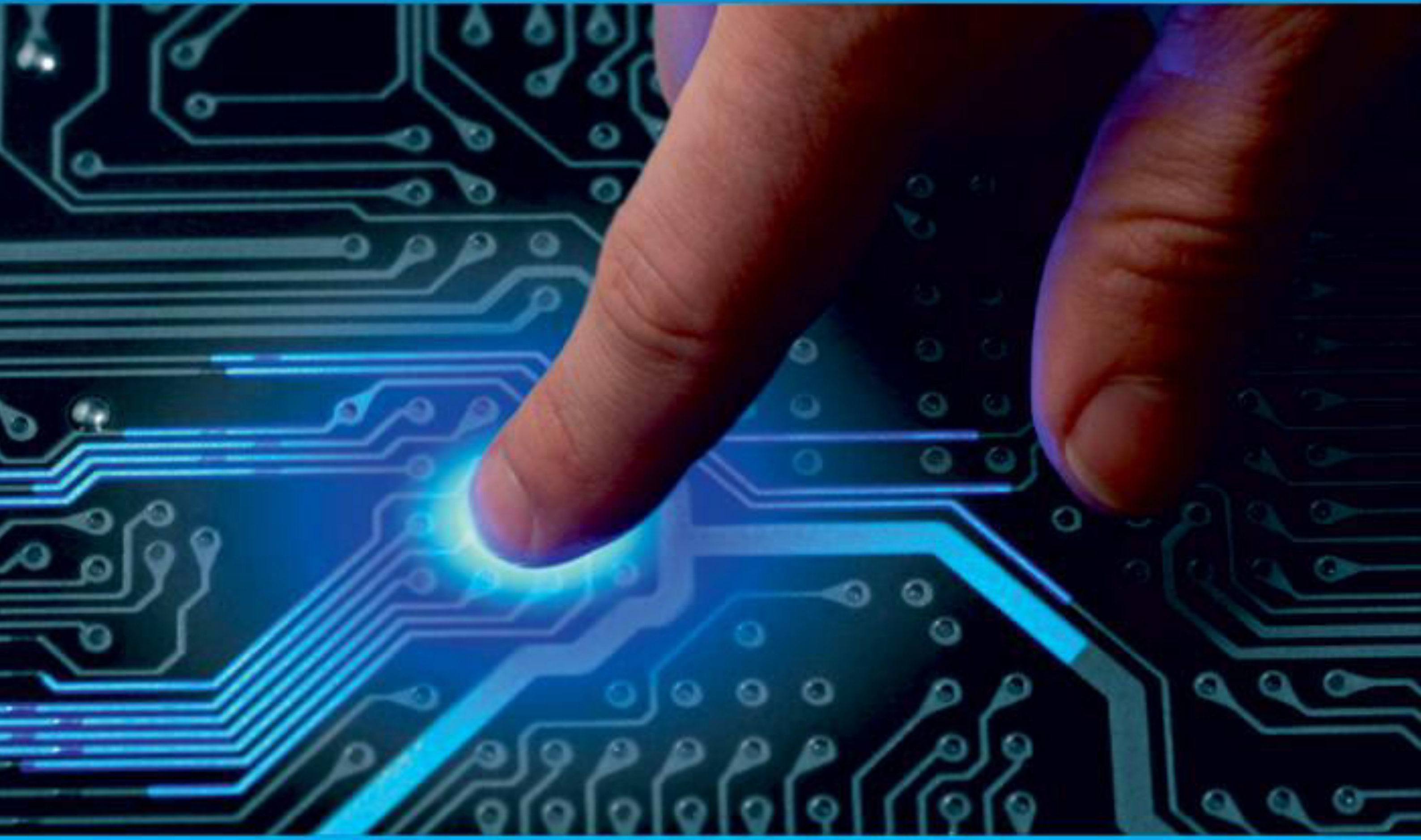
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 7, July 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

| DOI: 10.15680/IJIRCCE.2021.0907229 |

# Privacy Preserving Attribute Matching Framework in Social Networks

**Prashant Dhanaji Kate, Prof. Prathamesh S. Powar**

Dept. of Computer Science and Engg, Ashokrao Mane Group of Institutions, Kolhapur, Maharashtra, India

Dept. of Computer Science and Engg, Ashokrao Mane Group of Institutions, Kolhapur, Maharashtra, India

**ABSTRACT:** Privacy-preserving attribute matching is a challenging task in social networks and is getting more attention in recent years. In social networks, the personal attributes or hobbies of the users are exposed to the server to establish the relationships. So it is required to propose a novel scheme that is based on cipher text-policy attribute-based encryption and bloom filter to satisfy the requirements of the users to make friend discovery with privacy preserving. Protection saving record linkage encourages the coordinating of records that relate to similar true elements across various information bases while safeguarding the security of the people in these data sets. A Bloom channel (BF) is a space effective probabilistic information structure that is getting famous in PPRL as a productive protection strategy to encode delicate data in records while as yet empowering surmised comparability calculations between quality qualities. Notwithstanding, BF encoding is powerless to protection assaults which can re-recognize the qualities that are being encoded. Our procedures utilize adjoining pieces in a BF to create new piece esteems. An experimental examination on enormous genuine information bases shows that our procedures give high protection from security assaults, and accomplish better comparability calculation precision and linkage quality contrasted with other security enhancements that can be applied on BF encoding.Social interpersonal interaction gives an online stage to individuals to fabricate social associations with others, who have comparable individual credits. Be that as it may, there is a danger of security leakage. Social network stages may utilize client ascribes for factual, publicizing or benefit making purposes . Such conduct will bargain clients' protection, which influence clients' reality . There are three classifications to companion disclosure utilizing likeness of qualities in informal communities. The principal class utilizes a bunch of qualities to sum up client's data, and utilizes Private Set Intersection(PSI) or Private Set Intersection Cardinality(PSICA). The subsequent classification utilizes vectors to speak to client's data, and the vector separation is determined by speck item count to speak to social separation. The third class exploits Ciphertext Policy Attribute-Based Encryption(CP-ABE) and access control to accomplish companion disclosure . There are a few issues in existing plans like devour huge registering assets or are helpless against measurable examination assaults or take the protection of others.To tackle the issues of trait coordinating in social network,framework is proposed utilizing CP-ABE which can accomplish the characteristic coordinating in informal community stages and diminish figuring utilization of client and is more suitable to the real circumstance of making companions.An option in contrast to building unified information bases is to keep data set frameworks decentralized and every association keeps their own (security touchy) information. In this case, different gatherings (physically) need to send a request for certain information, which permits an association to deal with approval for that information inside. Nonetheless, this presents the difficult that gathering has to know where to request. Basically distributing a total rundown of (interesting) information record credits, for example federal retirement aide numbers, isn't just wasteful, it likewise settles protection if recognizable data is included. A generally utilized methodology for record query in disseminated data set frameworks is based upon Bloom channels , which is a productive set information structure for participation testing. As a symptom of the effective portrayal, Bloom channels inquiries can bring about bogus positives, along these lines conceivably coordinating with components that were definitely not expressly encoded into the channel. In the record query conspire, the diverse information base suppliers can encode a chosen of characteristics of their informational index and offer this with a customer, who would then be able to utilize it to request if an information base contains some chosen information record. Here, bogus positives can present some overhead as some information base will be wrongly questioned. In any case, contingent upon the arrangement of a Bloom channel, a compromise can be made between the bogus positive likelihood of a question and the time also, space productivity. Moreover, using the bogus positive likelihood, a Bloom channel can give a specific degree of protection, as more bogus positives will make it more hard to perceive them from genuine components. In this system, we consider a record query conspire like that proposed by Little et al. , where all channels are put away on the customer side. For this reason, we characterize a bunch of measurements to assess various parts of probabilistic record query plots as, for example, Bloom channel based plans. Utilizing these measurements, we break down the impact of various Bloom channel designs on the security, utility and proficiency of the plan. Finally, in

request to lessen potential spillage while questioning, we present a productive intelligent variation of this plan utilizing homomorphic encryption.

## II. RELATED WORK

Li et al. [7] propose the Private Set Intersection(PSI) procedure for accomplishing characteristic matching which depends on Secure Multi-party Computing.

Yi et al. [5] proposed a profiles coordinating plan dependent on homomorphic encryption in different informal organizations, which gives profile security safeguarding. The fundamental thought is to decide whether the divergence of two clients is not exactly the edge given by the client

Gao et al. [1] introduced a different keys profile-coordinating convention dependent on added substance homomorphism to figure the speck result of two vectors. At that point, some spot item conspires were proposed which desert homomorphic encryption and have lower processing costs.

Luo et al. [3] set load for each property, i.e., the trait set is spoken to as a grid, and afterward utilized a lightweight disarray network change calculation to ensure client data.

Li et al. [8] proposed a highlight point pre-coordinating plan, utilizing Bloom channel to decrease the computational heap of clients performing unscrambling of CP-ABE, and they explained how to set up an unquestionable secure correspondence channel between coordinated clients.

Cui et al. [6] planned a recipient unknown quality coordinating plan utilizing CP-ABE and sprout channel.

Qi et al. [9] consolidated accessible encryption with CP-ABE and proposed a companion disclosure convention with shrouded traits and fine-grained admittance control.

## III. IMPLEMENTATION

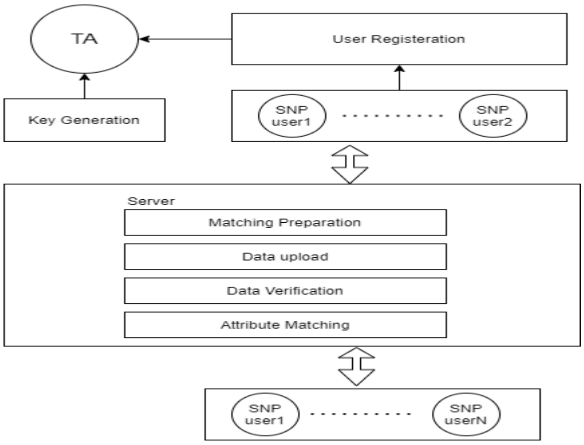


**Fig 1. Architecture Diagram**

### Key Generation

Cryptographic key is the most important factor for supporting encryption of condential data before it is transmitted in a communication network. A good cryptographic key has properties of random sequence and long period. For these purposes, a randomness capable and lightweight computing algorithm is required. The randomness capability and computation time of such an algorithm can be measured by using randomness test and algorithmic complexity analysis, respectively.the proposed system model consists of five entities, Trusted Authority(TA), Social Networking Platform(SNP), Users, Consortium Blockchain(BC), Proxy Cloud Computing Server(PCCS).In the system initiation phase, TA generates various keys for the system, and transmits them to the corresponding entities via secure channel. The asymmetrical key (PUbc, PRbc) are generated for blockchain consensus nodes to communicate with users. Then TA generates the master key MK and the public key PK. Transformation key TK and secret key SK are generated for each user based on their attribute sets S. The outsourcing decryption of CP-ABE is constructed based on scheme [38]. In addition, the smart contract for periodically selecting PCCS from SNPs is deployed on the blockchain.

1) CP-ABE INITIALIZATION TA selects a security parameter $\lambda$ and generates a universe description $U = \{0, 1\} *$ . Then it chooses a bilinear group G1 of prime order p, a generator g. TA then selects two random numbers $\alpha, \beta \in Zp$. Besides, it needs to choose a hash function F that maps U to G1. After that, the public key is published: $PK = \{g, g \beta , e(g, g) \alpha , F\}$ (1) TA secretly stores the master key $MK = (PK, g \alpha )$ and exposes PK to SNPs and users, respectively.

**User Registration and Data Upload**

The system sets the attribute space A that contains a large amount of attribute information such as gender, income, age, sports preference, education background, etc. When a new user joins the system, he/she first selects his/her attribute sets S and R from the attribute space A, then uploads S to TA to get transformation key TK and secret key SK. TA picks a random number t

0 ∈ Zp to create a temp key as: K 0 = g α g βt 0 , L 0 = g t 0 , ∀x ∈ S K0 x = F(x) t 0 (2) Then it chooses another random number z ∈ Zp and sets t = t 0 /z. Then it generates the transformation key TK as: PK,K = K 01/z = g (α/z) g β(t 0 /z) = g (α/z) g βt , L = L 01/z = g t 0 /z = g t ,{Kx }x∈S = {K 01/z x }x∈S .The TK is sent to the PCCS. The private key SK = {z, TK} is sent to the user. Noted that when the user's personal attribute set changes, TK and SK should be regenerated.

**Data Verification and Partial Query Decryption**

SNPs in the platformlayer unscrambles CTapc with PRbc to get Capc and check informal uprightness and accessibility with T and hash values.Then, the blockchain checks whether the information is legitimate, i.e.whether there are symmetric mystery key or plaintext of access approaches in CTapc.After check, the current PCCS performs halfway unscrambling of CP-ABE disconnected.The PCCS uses users' transformation key TK to decrypt CTab in Capc to get the partially decrypted data CT 0 ab. If a user does not satisfy the requirements of Alice, that is, his/her S and TK does not meet the access structure(M, ρ), the decryption fails. Suppose that S meets the access structure and let I ⊂{1, 2, 3, . . . , `} be defined as I = {i : ρ(i) ∈ S}. Then, let {ωi ∈ Zp}i∈I be a set of constants such that if {λi} are valid shares of any secret s according to M, then s can be computed as P i∈ Iωiλi = s. Therefore, the PCCS can computes

**Attribute Matching**

After the exchange started by Bob is gotten, the con-sensus hubs initially affirm the legitimacy and the information integrityby T and hash esteem. From that point forward, keen agreement is executed by SNP, which predominantly checks whether Alice fulfills Bob's prerequisites by means of a blossom channel. On the off chance that all components of R0b are in Bloom Filter B, it demonstrates that Alice addresses Bob's issues for making companions. Plus, the shrewd agreement likewise needs to ascertain whether the level of property closeness among Alice and Bob is more noteworthy or equivalents to the edge needed by Bob. Calculation 1 represents the trait coordinating with calculation, which checks whether Alice and Bob can be companions and matches up to max_num companions for Alice. In the event that the match is effective, a correspondence channel will be set up among Alice and Bob. Furthermore, in light of the fact that the shrewd con-parcel will be conjured by different responders, blossom channelis more proficient than crossing S 0a and R 0 b. The coordinating with records will be put away in the blockchain. Note that we storethe hash worth of the information boundaries rather than the first information, which can accomplish coordinating with straightforwardness while securing client protection. On the off chance that unique boundaries are put away.

## IV. ANALYSIS

The absolute time utilization of every substance is displayed in Figure 2. Alice performs encryption of CP-ABE, encryption of AES and Bloom channel age. For Bob,he needs to finish neighborhood decoding of CP-ABE and encryption of AES. For the blockchain, it performs savvy contract introduction and characteristic coordinating. For PCCS, it performs rethinking unscrambling of CP-ABE. From the figure, the blockchain activity and rethinking unscrambling of CP-ABE take the most time. It shows the need of moving complex computations from the blockchain to the off-chain, which can essentially decrease the calculation cost on the blockchain. In addition, an initiator will have numerous responders, so the decrease of time spent by the responder can successfully diminish the utilization of the whole coordinating with measure. The trial bring about Figure 6(d) shows that Bob's time utilization is insignificant, which demonstrates the viability of our plan. In outline, exploratory outcomes show that the plan is viable and practical.

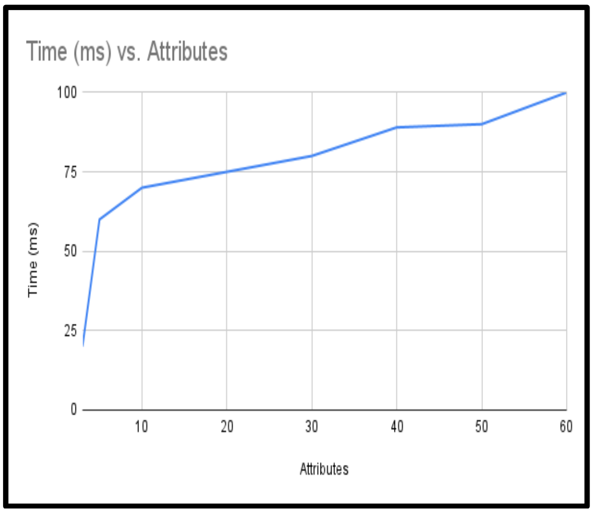


**Figure 2. Time chart against attributes.**

## V. CONCLUSION

We have successfully implemented the key generation and user registration with data upload,Data Verification and Partial Query Decryption, Attribute Matching .we present a privacy-preserving attribute matching scheme under multiple semi-trusted servers. In our scheme, we utilize CP-ABE and bloom filter to conduct bidirectional attribute matching and relieve the computation cost of users by outsourcing decryption. In addition, we design a novel hierarchical blockchain architecture, which massively reduces the storage consumption of the blockchain and improves operating efficiency. Security analysis and experiment results demonstrate that our scheme can resist single point failure attack, collusion attack, internal attack and external attack, and also provide effectively friend matching for users.In the future, we consider using blockchain instead of the trusted third party to initialize CP-ABE, which is a challenge issue. In addition, we plan to analyze the security and efficiency of blockchain consensus and friend matching in practical application.

## REFERENCES

[1] S. Oukemeni, H. Rifà-Pous, and J. M. M. Puig, ''Privacy analysis on microblogging online social networks: A survey,'' ACM Comput. Surv., vol. 52, no. 3, pp. 1–36, Jul. 2019.
[2] Y. Lin, Z. Cai, X. Wang, and F. Hao, ''Incentive mechanisms for crowdblocking rumors in mobile social networks,'' IEEE Trans. Veh. Technol., vol. 68, no. 9, pp. 9220–9232, Sep. 2019.
[3] Y. Pu, T. Xiang, C. Hu, A. Alrawais, and H. Yan, ''An efficient blockchainbased privacy preserving scheme for vehicular social networks,'' Inf. Sci., vol. 540, pp. 308–324, Nov. 2020.
[4] Z. Cai, Z. He, X. Guan, and Y. Li, ''Collective data-sanitization for preventing sensitive information inference attacks in social networks,'' IEEE Trans. Dependable Secure Comput., vol. 15, no. 4, pp. 577–590, Aug. 2018.
[5] X. Yi, E. Bertino, F.-Y. Rao, and A. Bouguettaya, ''Practical privacy preserving user profile matching in social networks,'' in Proc. IEEE 32$^{nd}$ Int. Conf. Data Eng. (ICDE), May 2016, pp. 373–384.
[6] P. Chaudhary and B. B. Gupta, ''A novel framework to alleviate dissemination of XSS worms in online social network (OSN) using view segregation,'' Neural Netw. World, vol. 27, no. 1, pp. 5–25, 2017.
[7] M. Li, N. Cao, S. Yu, and W. Lou, ''FindU: Privacy-preserving personal profile matching in mobile social networks,'' in Proc. IEEE INFOCOM, Apr. 2011, pp. 2435–2443.
[8] Y. Ishikuro and K. Omote, ''Privacy-preserving profile matching protocol considering conditions,'' in Proc. Int. Conf. Netw. Syst. Secur. Taipei, Taiwan: Springer, 2016, pp. 171–183.
[9] D. He, Z. Cao, X. Dong, and J. Shen, ''User self-controllable profile matching for privacy-preserving mobile social networks,'' in Proc. IEEE Int. Conf. Commun. Syst., Nov. 2014, pp. 248–252.
[10] E. Luo, Q. Liu, J. H. Abawajy, and G. Wang, ''Privacy-preserving multihop profile-matching protocol for proximity mobile social networks,'' Future Gener. Comput. Syst., vol. 68, pp. 222–233, Mar. 2017.

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details