International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/214506 Volume 9, Issue 4, July – August (2022)

RESEARCH ARTICLE

Solitude Adaptable User Profile Matching for Mobile Social Cloud Networks

M. Gobi
Department of Computer Science, Chikkanna Government Arts College, Tiruppur, Tamil Nadu, India
mgobimail@yahoo.com

B. Arunapriya
Department of Computer Science, Chikkanna Government Arts College, Tiruppur, Tamil Nadu, India
arunapriyanataraj@gmail.com

Received: 24 June 2022 / Revised: 21 July 2022 / Accepted: 27 July 2022 / Published: 30 August 2022

Abstract – Profile matching (PM) is a crucial method in cloud-based applications including Health Care and Social Networks (HC-SNs). In Mobile Social Cloud Networks (MSCNs), matching user profiles while maintaining privacy is a demanding challenge that has garnered greater attention in recent days. This article represents a new scheme called Modified Cipher Text based Policy Encryption Scheme (MCT-PES), proposed for Solitude Adaptable User Profile Matching for MSCNs (SA-UPM) using Homomorphic Encryption (Ho-En) technique for multiple recipients. In this module, a client submits a Priority-Profile (PP) and searches decentralized MSCNs for people with MP. In this method, neither the participant's profile nor the PP given by the participant is revealed. Furthermore, a Secure Transmission Medium (STM) may be formed between the pair of correctly matched users (MUs). Initially, it ensures verifiability, ensuring that no participant may deceive the initiator by providing an incorrect matching result. Then, the matched profile pair may be used it to create a STM that can withstand an eavesdropping attempt. Furthermore, the mismatched user may be promptly ruled out. Additionally, just a limited exchange between the originator and MUs are required since the MUs can determine the similar outcome without the assistance of the originator, which is beneficial for lowering computational problems and costs.

Index Terms – Profile Matching, Mobile Social Cloud Networks, Secure Transmission Medium, Homomorphic Encryption Matched Users, Priority Profile, Cipher Text.

1. INTRODUCTION

A Mobile Social Cloud Networks (MSCNs) is a social network where individuals with similar goals interact and communicate using a mobile phone or tablet [1]. It's comparable to web-based a method which is used in virtual communities, but the technology it uses is different. MSCNs make use of mobile messaging applications, which are seen to be one of the greatest methods to improve user involvement and engagement. As an example, (i) a passenger seeks to connect and interact with other passengers from the same institution at the airports. (ii) Depending on their sickness symptoms and treatments, a patient in the health centre seeks out like-minded persons for physical or mental support. By swiftly and properly matching UPs, they might all act as MSCNs [2].

Profile-Matching (PM) is the efficient method for determining the similarity of users' confidential profiles [3]. In functional uses, a user's personal profile is frequently delineated as a vector, with each dimension representing an attribute corresponding to a leisure activity, such as soccer, photo editing, or religious doctrine. Each attribute value is represented by an integer ranging from 0 to 10 or a greater range. The attribute value indicates the level of interest. The integer 0 indicates that the user has no interest in the item, while value 10 indicates that the user is extremely fond of it. Also, social proximity is frequently defined as the inner product of the vectors of two users [4]. The inner product will add the product of the relevant qualities in the two vectors which cannot depict user proximity with any degree of accuracy.

Furthermore, people are reluctant to discover individual details because their profiles regularly comprise sensitive data. Data encryption using cryptographic methods is supportive in protecting the users' privacy, but the configuration of the original data is essentially changed after encryption, making it complicated to handle the data again. The homomorphic encryption technique [5, 6, 7] has distinct benefits in the sorting of encrypted files. The partial Ho-En approach [8] is desirable in many practical applications. In general, the PM plays an important role in MSCNs. For instances, when users join social networking sites, they create a User Profile (UP) [9], which is a collection of attributes that they use to identify oneself for the goal of special connections. In the initial incident, a passenger's UP may comprise, among other things, his or her age, sex, university of graduation, firm where he or she works, and destination. In the second scenario, a patient's UP may comprise, among

RESEARCH ARTICLE

other things, medical symptoms, medicines utilized, and doctor. The term "matching" can be defined from a variety of perspectives. When two UPs are compared as an attribute set, the number of comparable qualities between them surpasses a certain threshold, they are matched. The desire of mobile social programmes has made them an important part of the daily lives of millions of consumers [10]. In 2016, two prominent mobile messaging apps, Facebook Messenger and Whatsapp, each had one billion monthly active users.

Several mobile social applications are allowing users to socialise with their nearby peers who share similar interests and are in close proximity to them [11, 12]. Examples include Lovegety, PeopleNet, and Proxidating. PM of individuals who chance to be in close vicinity enables this spontaneous social networking. Despite providing exciting potential for mobile users, mobile social network programmes raise serious privacy concerns about users' private data, such as divulging personal contact information or revealing restricted accounts. Numerous security based threats have been launched against the users of MSCNs [13], highlighting the need of privacy protection in this industry.

As a result, the need to preserve one's privacy drives consumers to seek for PPPM algorithms that make MSCN's familiar companion safer. The most straightforward way is to employ a relied medial network to gather data from particular clients who generate, and distribute corresponding outcomes on request [14]. In contrast, this method might not be suitable for MSCNs.It initially necessitates the client's connection to the Internet access. However, this access may not be accessible at all time, and it will be quite costly in actuality. Second, if the central server fails or is attacked, it may constitute a bottleneck [15]. As a result, the distributed strategy, in which clients will safeguard their secured data without the support of a preserved medial network, is better suited to MSCNs, especially MSCNs using low period communication devices such as Wi-Fi and Bluetooth [16, 17].

In this research work, an MCT-PES based SA-UPM in MSCNs is designed to overcome the problem of numerous receivers utilising Ho-En. In this technique, a user submits a PP and secures the participant's profile and PP before searching decentralised MSCNs for additional users with comparable profiles. Additionally, a STM can be established between the two individuals that have been successfully matched. It guarantees verifiability at first, guaranteeing that no one may trick the initiator by supplying an inaccurate matching result. The matched pair may then utilise it to construct a secure communication channel that is impenetrable to eavesdroppers. Furthermore, the mismatched user may be ruled out right away. Furthermore, there are some data connections between the originator and the MUs, which saves time and expense since the MUs will choose a corresponding outcomes independently of the originator.

The remaining sections of this article are prepared as follows: Section 2 studies the different existing works associated with profile matching techniques. Section 3 briefly describes about the proposed model and Section 4 portrays its performance efficiency. Section 5 concludes the entire work and provides the future enhancement.

2. LITERATURE SURVEY

Shewale& Babar [18] developed an effective PM protocol using Privacy Preserving (PP) in MSCNs. Between the parties, the originator and the responder, an explicit Comparison-based PM method ($eCPM$) was established and modifies the implicit CPM ($iCPM$), which enables the originator to acquire few messages immediately from the respond rather than waiting for the comparison result. Then, for complicated similarity criteria encompassing several characteristics, $iCPM$ were developed to an implicit Predicate-based PMprotocol ($iPPM$).However, it requires an efficient PM protocol against malicious adversaries.

Zouari et al. [19] suggested a PPPM technique based on a modified version of cryptosystem's fuzzy extractor. This procedure is divided into various stages. The first stage was an emerging stage, in which the client uses a Wi-Fi or Bluetooth connection to monitor the neighbourhood. Using the matching process against adjacent people, the profile with the closest distance metric was chosen. Finally, a link was formed between the matched users under their mutual approval. However, this approach only works in conjunction with a selective access control system

Huang et al. [20] proposed a Secure Data Sharing and PM technique (SDSPM) for mobile HC-SNs in cloud computing. Patients could utilize an Identity-Based Broadcast Encryption (IBBE) approach to offshore their enciphered medical records to cloud storage and disseminate them to a set of providers in a preserved and efficient approach. On the other hand, Massive bilinear mapping operations resulted in less efficiency.

Chandrasekaran et al. [21] developed an effective Relational Multi-Authority Attribute – Encrypted technique for PM in a cloud network by using the Rapid Ate Pairing approach. This method aims to eliminate the key leakage, singular node rejection, and efficiency slowdown concerns. However, this method was not preferable to larger datasets.

Gao et al. [22] present a new Cloud Assisted (CA)-PPPM technique using a proxy re-encryption strategy with compulsive homomorphism for multiple keys. This approach uses numerous keys to quickly calculate the social closeness between two users, allowing users to find possible buddies while maintaining their anonymity. On the other hand, this method necessitates fine-grained access control to achieve a higher extent of security.

RESEARCH ARTICLE

Luo et al. [23] presented a new PP matching scheme using both identity authentication and private matching. The scheme was based on a trusted third party with powerful computation capabilities that can reduce the workload on intelligent terminals. Furthermore, the scheme employs encryption and authentication methods to ensure that the attacker does not obtain the relevant data of the user's attribute credentials, thereby protecting subjective privacy during the friend matching procedure. However, this approach had a high computational cost issues.

Yi et al. [24] proposed a new method for PP-UPM using Ho-Enand numerous servers. This approach allows a user to locate matched users using various servers while keeping the query and UPs hidden. However, this technique requires parallel processing to increase the performance of computing conditional gates.

Zou et al. [25] developed an Improved CA-PPPM (ICA-PPPM) Scheme for determining the client's proximity in MSCNs, which computes the cosine result among the adjusted matrices as the criterion. This approach enhances a Homomorphic Re-Encryption System (HRES) by allowing for a single homomorphic replication as well as an unlimited number of homomorphic extensions. The clouds' agreed $PK$was used to authenticate the client's context, eliminating key leakage and management difficulties while also protecting the users' data privacy. However, this approach had a considerable computational cost.

Qian et al. [26] presented a Verifiable Private Interactive technique to achieve Fine-grained PM (VPI-FPM). In this process, the privacy patient's information was splitted into diverse-tag portion to obtain the fine-grained operations. Then, the re-encryption algorithm was utilized to protect the patient's privacy Moreover, a verifiable mechanism was used to ensure that the computation was correct because the cloud server could violate this whole scheme. However, the data encryption might strictly obstruct PM over outsourced encrypted data.

Li et al. [27] presented a new User Identification method which incorporates Spatio-Temporal awareness (UIdwST) information. Initially, the kernel density estimation (KDE)-based solution was determined to compute the proximity of two users' check-in records by coupling the interactions among spatial and temporal data in a check-in record. Then, various check-in records was assigned with different weights in order to favour the more informative ones to improve the model's performance. Then, if two check-in record sets contain some conflicting records, a penalty term was attached to the proximity measurement. Finally, the similarities between the two accounts were verified. If the similarity exceeds a certain threshold then these two accounts belong to the one user. But, more effective strategies were required to enhance efficacy and security of this method.

3. PROPOSED METHODOLOGY

In this section, the entire SA-UPM process in MSCNs is shown as follows.

3.1. System Architecture

The figure 1 depicts the Overall architecture of proposed scheme.

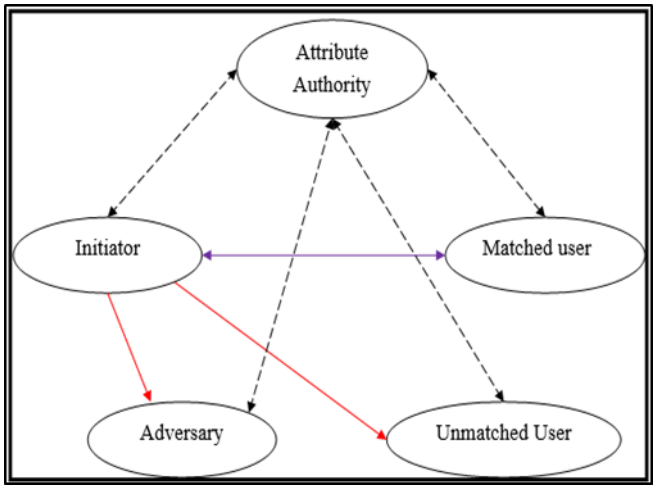

Figure 1 Overall Architecture of Proposed Scheme

In a cloud-assisted scenario, the suggested system architecture incorporates UPs, profile matching, attribute authority, adversary matched and unmatched users, as well as a conventional SA-UPM model.

3.1.1. User Profile (UP)

All clients in the MSCNs model have an account; that contains his or her own interpretation. In this work, the UP is a collection of attributes. Consider $\mathcal{A}$ be the feature space consisting of n feature sections$\boldsymbol{A} = \{a_1, a_2, \ldots . a_n\}$. Each $a_i \in \mathcal{A}$ has m_i candidate values,$a_i = \{a_{i1}, a_{i2}, \ldots . a_{in_i}\}$. Two stages are required to create a UP, which will be referred to as a query attribute listA_{L_r}. Choose the attribute categories in the first phase. After that, assign a specific value to each category. $A_{L_i} = \{ A_{L_i}^1, A_{L_i}^2, \ldots . A_{L_i}^3\}$ may be used to describe the attribute list of useru_i. Each $A_{L_i}^k$is made up of distinct attribute groups. For various users, the number of characteristics does not have to be the same. Particularly, the elements in the A_{L_r} are sorted in the order of the relevant features divisions in a, which is important for PM in this analysis.

3.1.2. Profile Matching

Allow $A_{L_i}$to access the query A_{L_r}given by an initiator i_r who wishes to find friends in this model, and A_{L_i} to be the $A_{L_r}$of users UA and UB who are physically close to$U_r.U_r, UA$, and UBPM will be severely illustrated as a function matching:

RESEARCH ARTICLE

$$matching\ (U_r, UA\&\ UB) = \begin{cases} 1, & if\ A_{L_r} \subseteq A_{L_i}, A_{L_A}, A_{L_B} \\ 0, & if A_{L_r} \nsubseteq A_{L_i}, A_{L_A}, A_{L_B} \end{cases} (1)$$

According to equation (1), If the A_{L_r} is a subset of the $UA\ \&\ UB$, A_{L_i}, then the matching process will be successful. Some of the terminologies used in this research work are listed below.

- The Attribute Authority (AA) is a trustworthy central server that all users may access. Surprisingly, it's only available during the initial step, when the clients creates an account, registers, and obtains the attribute private key pk. The PM procedure does not necessitate the use of a network.
- Initiator is the person who sends out the inquiry A_{L_r}
- Matched users are those whose A_{L_r}satisfies the originatorA_{L_r}.
- Unmatched users are those whose A_{L_r}does not satisfies that of the originator query.
- Antagonist is a malevolent mismatched client who tries to anticipate the queryA_{L_r}'s information and also deceive the user further. This strategy assumes that all will be in charge of only one mobile device.

In this scheme, clients must first download and install the mobile application based on the approach from the Network into their smart phone. Initially, when the app runs, all user must create their own A_{L_r} by choosing features from a specified function level and reporting it to the AA for authentication. The AA then generates the attribute secret key from the A_{L_r} and returns it to the consumer with the public keyPK. In addition, all clients must produce a pair of keys using a preset Public Key Encryption (PKE) algorithm.

When an authenticator wants to find a MUs in a certain locations like a bar, airport, or hospital, he or she first produces a$A_{L_r}$and then, it is utilized as the $w$to generate a CT that includes his or her ownPK. This CT is distributed to clients in the region. The CT can only be decrypted by the person who matches the criteria. After then, the matched user can choose to engage with the originator and return a ks that is encrypted with the initiator's PK. Apparently, this action does not necessitate the use of the AA server.

Only the matched user can learn the A_{L_r}information under this technique. If each respondent executes the method honestly, No mismatched client may deduce any information from the CT provided by the originator. However, the adversary may utilise a succession of malicious assaults to obtain the private information of genuine users for some criminal reason. The following are two strong malicious assaults that are examined in this paper.

1. Profiling: The attacker attempts to identify the A_{L_r} by identifying or predicting all prospective permutations of parameters.

2. Malfunctions: The opponent may mislead throughout the PM process by straying from the concurred-upon protocol, such as supplying the initiator with an incorrect pairing result.

3.2. MCT-PES Mechanism

The MCT-PES idea is established in this study work employing Ho-En approach for multiple recipients (users) with better verifiability system, which means that the initiator and any unpaired user cannot fool each other to appear to be paired. The primary procedure of the SA-UPM Scheme is depicted in Figure 2.

Assume the query A_{L_r} as the MCT-PES algorithm's parameter w. To encrypt a message, use $Encrypt(PK, M, w)$ and send it to users in close proximity. Only the user whose attribute list A_L matches $A_{L_r} \subseteq A_L$ may successfully decode the message, and then utilise the information recovered from the encrypted message to create a secure communication medium with the initiator.

This approach uses a MCT-PES structure, which contains two elements are listed below.

(i) It's receiver anonymity, which means the A_{L_r}, i.e., w, is encipher in $CT$and only the MUs can decode it.

(ii) The length of the ciphertext and the time required to decrypt it are both constant.

The AA assigns PK and SK' to each user at first. The user's attribute pk isSK', and it is produced and assigned by the AA based on theA_{L_i}. Meanwhile, ku (public key) and kr (secret key) are produced independently using the same PKE technique, such as RSA. This key pair will be utilized to establish a protected interaction route between the MUs.

An initiator begins up the matching process by constructing a PP. Then, in the following phases, transformed to a $A_{L_r}$and a rl_R, utilised for rapid sorting. When a match is successful, the initiator creates an arbitrary value of N, which will be used for key interchange registration. A message containing ku and N is then encrypted using the algorithm Encrypt with the parameters $A_{L_r}$and PK. It generates the CT. Finally, a query package including rl_R, CT, and ku is produced and gets off for thePM.When a consumer near the originator accepts the query package, he or she does a short filtering computation using the received message's rl_R and his or her own attribute listA_L, and then outputs a set of candidate attribute lists $\mathcal{L}_{cand}$. $\mathcal{L}_{can}$ is made up of subsets of l, which is also known as

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/214506 Volume 9, Issue 4, July – August (2022)

RESEARCH ARTICLE

a$\mathcal{L}_{cand}$ and may be equivalent to A_{L_r}.The PM fails if $\mathcal{L}_{cand}$ is nil. Otherwise, a pk collection is determined using $\mathcal{L}_{cand}$ and SK' as input. The matching user utilizes each candidate private key Sk_{cand} in this set to attempt to decode theCT.

To ensure that the decryption result is valid,ku', which is obtained from decrypting CT, is compared to ku. If these two keys are equivalent, the decryption result is valid, indicating that the matching was successful. Then, the MUs has the option of communicating with the originator or not. For example, He or she may generate a shared secret key, enciphered it using N and transmit it to the initiator by ku. when the initiator receives the ks, the suitable pair can use Ho-Ento create a secure coupled information route.

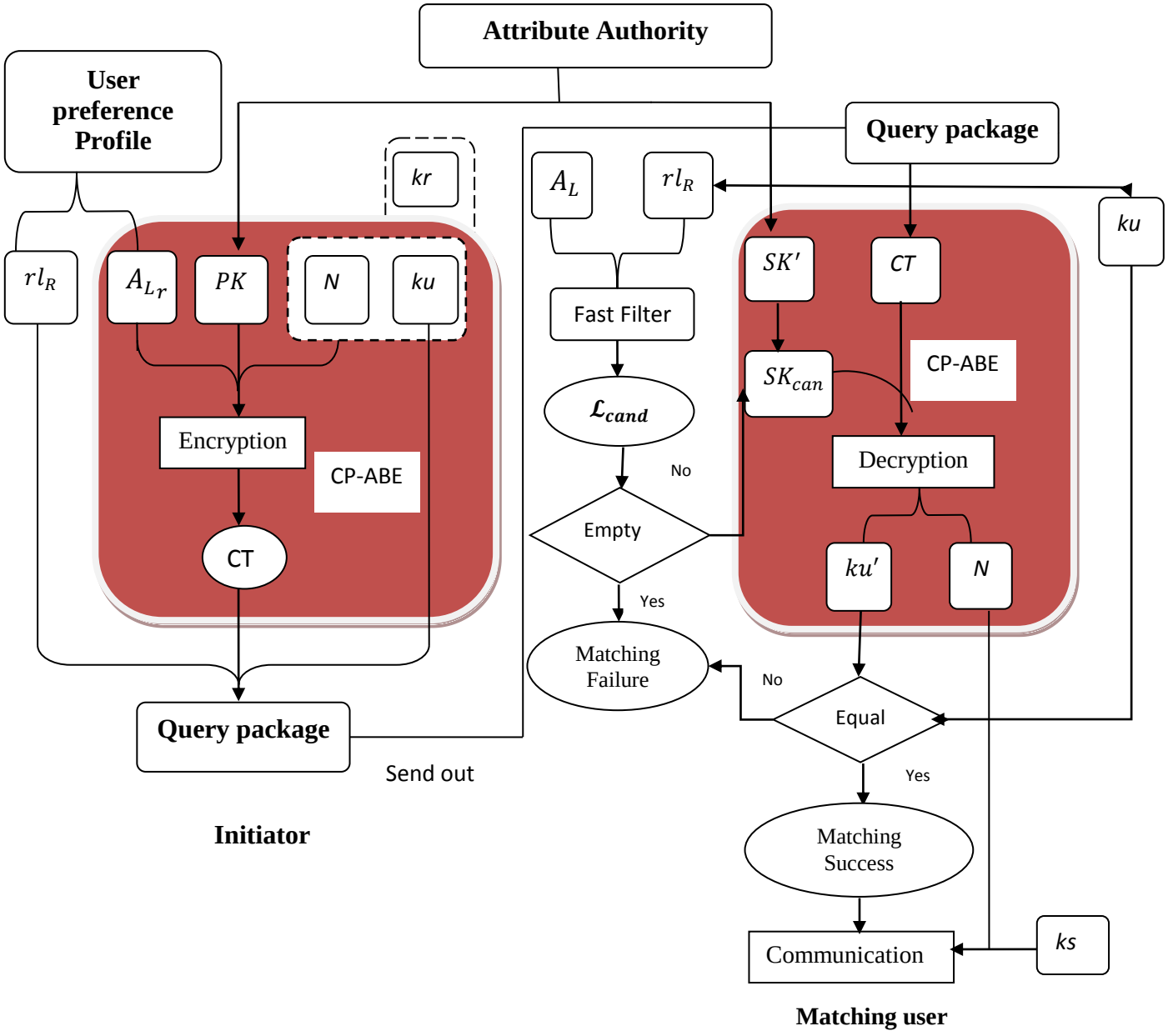

Figure 2 Main Process of SA-UPM Scheme

3.3. MCT-PES Algorithm

The MCT-PES algorithm is regarded as the framework's heart. The CTlength is fixed in this approach, and the $w$is concealed. As a result, a change in the key generation method is implemented, and it is briefly illustrated as follows:

(1) $Setup\ (1^k)$

RESEARCH ARTICLE

During the system starting phase, an AA selects several groups$G$, $\hat{G}$with the same prime order p based on the security requirement. Let $e: G \times \hat{G} \rightarrow G_T$be the bilinear map, and $g, \hat{g}$ denote the $G, \hat{G}$ generators, respectively. The AA then selects secrets $\alpha\epsilon_r z_{p,}^{*} \beta\epsilon_r z_{p,}^{*} \delta\epsilon_r z_{p,}^{*}$and obtains value$\hat{t}_1 = \hat{t}^{\alpha}$, $\hat{t}_2 = \hat{t}^{\beta},$, $t_2 = t^{\beta}$, $\hat{d} = \hat{t}^{\delta}, d = t^{\delta}$. The sign$\epsilon_r$ stands for "randomly selected from."

Let $\boldsymbol{A} = \{a_1, a_{2,} \dots \dots a_n\}$ is the attribute space. Each $a_i \epsilon \boldsymbol{A}$ is an attribute category with a set of attributes $\boldsymbol{A_i}$=$\{a_{i1}, a_{i2,} \dots \dots a_{im}\}$. The AA picks $a_{ij} \epsilon \boldsymbol{A_i}$and computes$\Psi_{ij} = t^{\Psi_{ij}}$for each attribute$\Psi_{ij} \epsilon_R z_{p,}^{*}$. Assuming $Y = f(t_2, \hat{t}_1)$, the PK and master key MK are generated in equation (2) and (3).

$PK = \{t, t_2, \hat{t}, \hat{t}_1, \hat{t}_2, d, y, \Psi_{ij} (1 \leq i \leq n, 1 \leq j \leq m_i)\}(2)MK = \{\hat{t}_2^{\alpha}\, \hat{d}, \Psi_{ij}\ (1 \leq i \leq n, 1 \leq j \leq m_i)\}$ (3)

(2) Key-Generation

$\boldsymbol{KeyGen}(\boldsymbol{MK}, \boldsymbol{A_L})$:Let$\boldsymbol{A_L} = \{A_{L_1}, A_{L_2} \dots \dots A_{L_n}\}$which containsa collection of attributes. Each A_{L_i} in $A_L$belongs to a certain attribute category, such as $A_{L_i} \epsilon A_K$. The following code generates a pk for A_L. To begin, a random $r \epsilon_R z_{p,}^{*}$is chosen. Then it is calculated in equation (4)

$$C_0 = \hat{t}^r, C_1 = \hat{t}_2^{\alpha}\left(\hat{d}.\left(\hat{t}^{\sum_{\alpha_{ij} \epsilon A_L} \Psi_{ij}}\right)\right) \quad (4)$$

Now, the secret key is $SK = C_O, C_1$. The original $KeyGeneration$ is changed one further by breaking it into two phases.

(i) $KeyGenA(MK, A_L) \rightarrow SK'$:This method operates on the AA side, using the same input parameter as the original algorithm. For the given security parameter k, let $n = uv$ be a safe Rivest, Shamir, Adleman (RSA), a safe RSA modulus, in which u and v are primes of the form of $u = 2u'+1$, $v = 2v'+1$; u' and v' are the primes of equal bit length, Let f be an element of the maximal order $\lambda(n^2) = lcm(\bigcirc(p^2), (q^2)) = 2np'q'$ in $\mathcal{Z}_{n^2}$.

(ii)$KeyGenU(SK', \mathcal{L}_{cand}) \rightarrow SK_{can}$: This algorithm is executed by the user. It is necessary for two cloud users, UA and UB, to produce their own key pairs like$sk_{UA} = a \epsilon \mathcal{Z}_{\lambda(n^2)}$, : $pk_{UA} = f^a (mod\ n^2)$ and $sk_{UB} = a \epsilon \mathcal{Z}_{\lambda(n^2)}$, : $pk_{UB} = f^b (mod\ n^2)$. As a result, UA strikes a deal with UB to generate their Diffie–Hellman key $sk_{UA} = a \epsilon \mathcal{Z}_{\lambda(n^2)}$, : $pk_{UA} = f^a (mod\ n^2)$ and $sk_{UB} = a \epsilon \mathcal{Z}_{\lambda(n^2)}$, : $pk_{UB} = f^b (mod\ n^2)$.

(iii) E$ncrypt(PK, M, w)$:Output the CT as mentioned inequation (5), provided a message $m \epsilon Z_n$ and the Diffie–Hellman keyPK:

$c = E_{PK}(m) = (\xi, \zeta) = ((1 + mn) PK^r (mod n^2), f^r (mod n^2)$,(5)

$E_{PK}(m)$ represents the CTenciphered with PK and r represents aarbitrary number chosen from$Z_{\lambda(n^2)}$.

(iv)$Decrypt(PK, CT, SK)$:A decryptor computes $m = \hat{P}\, f(P_1, C_0) \backslash f(P_0, C_1)$ in this procedure. The original $KeyGen$ algorithm is used in this calculation. The $CT$is calculated as $CT = \hat{P}\, f(P_1, C_0) \backslash f(P_0, C_{cand})$ if the input parameter is SK_{cand}, as shown in two methods.

$Partial\ Dec$ 1. Consider, $SK_{UA} = a$ and $CT = E_{PK}(m) \mathcal{Z}_{n^2}^2$, the user UA can convert the aforesaid CTinto another as $E_{PK}(m) = (\xi_2, \zeta_2) = (\xi_2, \zeta^a (mod n^2)$, where $E_{PK_{UB}}(m)$ indicates that the CTcan be decrypted SK_{UB}.

$Partial\ Dec$ 2. The cloud UB can decrypt the plaintext given $SK_{UB} = b$ and a $CT = E_{PK_{UB}}(m)$as given in equation (7) and key generation is defined in equation (6).,

$\eta = \zeta_2 = \zeta^{ab} = g^{rab} = PK^r (mod n^2)$(6)

$$m = A_{L_r}\left(\left(\frac{\xi}{\eta}\right)(mod n^2)\right) = A_{L_r}(1 + mn) \quad (7)$$

In equation (7), the function $A_{L_r}(.)$ is defined as $A_{L_r}(x) = x - {}^{1}/_{n}$

The attacker can estimate the access policy w using the Dedicated Host (DDH) test if the bilinear map $e: G \times \hat{G} \rightarrow G_T$is parallel, which indicates $G = \hat{G}$. That is, antagonist selects an access policy w' at random, computes$f(P_0, d \prod_{\alpha_{ij} \in w'} \Psi_{ij}) = f(t^s d \prod_{\alpha_{ij} \in w'} \Psi_{ij})$, and checks if it equals $f(t, P_1) = f(t, (d \prod_{\alpha_{ij} \in A_L} \Psi_{ij})^s)$.

The antagonist can keep doing this until he discovers the w' that is equivalent to w. In this context, however, $G = \hat{G}$ and the opponent cannot obtain $\hat{t}^s$. As a result, the antagonist is unable to use the DDH test described here to predict the w. The MCT-PES system is often utilised in this scheme to mask the $w$and achieve receiver anonymity for the reasons stated above.

3.4. Terminating the Unmatched User Profile

In most networks, the number of potential MUs is far lower than the total count of users. This system is constructed that quickly filtered out unpaired users in order to increase PM efficiency. The mechanism's fundamental data structure is the rl_R, whose components are the fraction of the hash values of the appropriate attributes in the A_{L_r} divided by λ.

The initiator sends this rl_Rtogether with the $A_{L_r}$to other users.Individuals concerned in comparing must first determine if they are a likely subject of the initiator by evaluating their own A_{L_r} to the rl_Rafter obtaining the request package.If this is not the case, the PM procedure will come to an end. Otherwise, the matching computation is carried out.

RESEARCH ARTICLE

3.4.1. Reminder vector (rl_R)

Consider the $A_{L_r} = \{A_{L_r}^1, A_{L_r}^2, A_{L_r}^3, \ldots\ldots, A_{L_r}^q\}$.$\lambda$ is a prime that is greater than Q. This research employs a cryptographic hash function $(Hash)$ to generate $n - bit$ hash values. The quotient of all hash values of characteristics in A_{L_r}split by λ form a vector r_{l_R}. Assume$R_k = Hash\ (\mathcal{L}_R^k) mod\ \lambda$,then$r_{l_R} = \{R_1, R_2, \ldots\ldots, R_q\}$.

3.4.2. Determination of Fast Filtering Algorithm (FFA)

This method illustrates how to quickly rule out a user that is mismatched. It returns a $\mathcal{L}_{cand}$ with three inputs: a recall vector r, A_{L_i}, and a prime λ.$\mathcal{L}_{cand} = \oslash$ indicates that the user'sA_{L_r} does not match the A_{L_r}. The amount of characteristics in this structure does not have to be the same for each user. The extent of every feasible MUs, $A_L$exceeding the length of any A_{L_r}determines his or her "$matching$" under this architecture.

3.5. Decryption and Validation

To determine whether there is a l_{cand}in $\mathcal{L}_{cand}$that is similar to the A_{L_r}(i.e., the A_{L_i}suits the A_{L_r}), a candidate private key SK_{can} is generated for all $\mathcal{L}_{cand}$, and then the CT is decoded using it. The characters ku' and N will appear in a pair as a result of the decipherion. If ku' equals ku, the decryption result is valid, indicating a successful profile match. Then, the N is returned for succeeding stages.

3.6. Constructing STM

The MUs should select whether or not to respond to the request if the match procedure is successful. He/she starts by creating a ks and a temporary interaction number$N$, an arbitrary value produced by the originator. When a match is successful, it is utilised for authorised key exchange. Then, he\she encrypts ks and N and sends it back to the initiator using the initiator's public key ku. When the instigator receives a response, the customer uses their own private key kr to decode it. By authenticating N and creating an STM with the MUs, the instigator may confirm that this respond is from the customer whose A_{L_i}matches the A_{L_r}. The algorithm1describes about developing the secure transmission medium.

Input:

1. CiphertextCT

2. Attribute Public Key P

3. Attribute Private KeySK' (generated by $KeyGenA(MK, A_L)$)

4. Candidate Attribute Lists Set $\mathcal{L}_{cand}$

5. Initiator's Public Key ku

Output: Temporary Inactive Number (N)

1. if $\mathcal{L}_{cand} = \oslash$then

2. $return\ NULL$

3. $end\ if$

4. $for\ each \mathcal{L}^i{}_{cand} \in \mathcal{L}_{cand}\ do$

5. $SK_{cand} = KeyGenU(SK', \mathcal{L}^i{}_{cand})$

6. $(ku', N, UA) = Decrypt(PK, CT, SK_{UA})$

7. $(ku', N, UB) = Decrypt(PK, CT, SK_{UB})$

7. if $ku' = ku$ then

8. $return\ N$

9. $else$

10. $return\ NULL$

11. $end\ if$

12. $end\ for$

Algorithm1 Secure Transmission Medium Construction

3.7. User based PPPM Protocol

This proposed method describes the whole process of developing a PPPM technique. Initial stage, matching stage, and secure transmission phase are the three phases of this protocol. Only at the initial step does a user communicate with the attribute authority. Unless extraordinary conditions arise, the user will not contact with the server once the conversation has ended. In other terms, the user and the AA will only communicate when a person produces or modifies his or her attributes list. As a result, the PM method has been completely scattered among users. The User based PPPM Protocol algorithm consists of three stages like initial, matching, and STM stage, the flow of these stages are given in below algorithm 2.

Initial Stage:

1. The authority attribute createsPK, MK, A calls $Setup(1^k)$.

2. Based on attribute space A, each participant u_i constructs his or her own attribute list L_{u_i}

3. Each participantu_i sends $L_{u_i}$to A, who then executes $KeyGenA(MK, L_{u_i})$ to create SK'_{u_i} ' and return PK, SK'_{UA}, SK'_{UB} to u_i.

4. Each participant u_i creates a key pair (ku, kr) using a PKE technique.

Matching Stage

1. The A_{L_r} is generated by the initiator u a to characterise the person he wishes to match.

2. UA creates the remainder vector $rl_R(mod\ \lambda)$ for A_{L_r}

RESEARCH ARTICLE

3. UB creates the integer N at random.

4. UA produces the CT by running$Encrypt(PK, M, A_{L_r}).M = ku||N$.

5. The tuple(rl_R, ku, CT) is sent out viaUB.

6. After receivingrl_R, ku, CT), the user u_b uses the Fast-Filter algorithm to solve $\mathcal{L}_{cand}$ usingrl_R, l_{u_b} , and prime number λ as inputs.

7. The PM procedure is completed if $\mathcal{L}_{cand} = \oslash$, Otherwise, the Cipher-Decryption technique is still being used byUB.

STM phase

1. If the Cipher-Decryption algorithm returns$N$, it signifies that the A_{L_r} matches l_{u_b}. Then u_b creates a ks, encrypts ks and N usingku, and returns it.

2. UA and UB use their private key kr to decode the response.

3. If N is right, UA and UB use a predetermined symmetric cryptographic approach to make a further secure connection via ks.

Algorithm 2 User Based PPPM Protocol

3.8. Security Analysis

Consider a decision function has $PS(A_{L_r}, UA, UB)$. If a client $u_i$discovers the information of the A_{L_r}, $PS(A_{L_r}, UA, UB) = 1$; if not, $PS(A_{L_r}, UA, UB) = 0$. The purpose of our method is that, $PS(A_{L_r}, UA, UB) = 1$ just for u_i whose $A_L$may match A_{L_r}.

The essential assurance of privacy preservation is provided by the security of the MCT-PES structure used in this approach. The $rl_R$and accompanying method are offered to provide quick matching and enhance matching efficiency by achieving subset matching. However, because the rl_Rreveals someA_{L_r}, information, such a time-saving approach violates privacy security. Lexical profiled attacks may possibly be launched using the rl_R.

3.8.1. Attack Prevention Using Dictionary Profiling

The most dangerous malicious attack against this protocol appears to be it. Although the attacker cannot deduce any data about theA_{L_r}, from the returned CT, he or she can do lexical profiling using the rl_Rin this approach. A successful dictionary profiling attack involves two stages.

Step 1: By identifying attribute pairs from attribute space A in a supplied rl_R, the attacker must construct$\mathcal{L}_{cand}$. The rl_Rs of these prospective $A_L$should be equal to the provided rl_R.

Step 2: The opponent must first engage with the AA in order to get the $pk$for each$\mathcal{L}_{cand}$, before attempting to decrypt the CT.

In actuality, such an assault is difficult to carry out, and our strategy can successfully avoid it. In contrast to earlier systems, this scheme's UPs cannot be modified locally, which will be the main technique for preventing dictionary profiling. Consider that $\boldsymbol{A}$ has n attribute categories, with each category having on average m characteristics. The number of $\mathcal{L}_{cand}$ created by adversary will be $\binom{n}{q}\left\lfloor\frac{m}{\lambda}\right\rfloor^q$ given a recall vector R of length q and primeλ. Certainly, if the attribute space A is larger and properly configured, this value will be higher. To prohibit the attacker from obtaining pks for each $\mathcal{L}_{cand}$from the attribute authority, we may use some simple approaches to limit the frequency of pkproduction for the same user in the attribute authority. As a result, this approach is capable of effectively counteracting word profiling attacks.

3.8.2. Verifiability

The initiator of this protocol checks the matching results using the temporary interactive number$N$. By decrypting the query CT, only the matching user can have access to N. When the originator gets the response from the "MUs" he or she deciphers it with his or her private key kr and evaluates the N in the decryption result. If N is accurate, the initiator can be certain that the response is from a genuine MUs. Because a mismatched attackers will not get the correct$N$, he or she cannot manufacture a response that will pass verification.

3.8.3. Transmission Defense

The ks established by the MUs may be safely sent to the originator by using this methodology, which depends on a PKE mechanism such as RSA, according to this protocol. The matched pair can then speak with each other via ks. As a consequence, an opponent could not gain any important information.

4. RESULT AND DISCUSSION

The performance of SA-UPM for multiple receivers has been evaluated using experimental analysis of current and new methods in this section. The existing PP-UPM [24], ICA-PPPM [25], VPI-FPM [26] and UIdwSTand [27] schemes are implemented in Java JDK 1.6 language and operates on a Microsoft Windows 7 computer with a 2.70 GHz Intel CPU and 4GB of RAM. The efficiency of these schemes is tested in terms of Initialization Time, Key Generation Time, Encryption Time and Decryption Time based on different number of attributes confirms the efficiency of cloud based PM system to multiple recipients.

4.1. Initialization Time (s) vs. No. of. Attributes

The Initialization process is linked to the authority hierarchy and the amount of attributes handled by AA. The amount of qualities has a linear connection with this phase. Table 1 depicts an encryption time for PP-UPM, ICA-PPPM, VPI-FPM

RESEARCH ARTICLE

and UIdwST scheme with proposed SA-UPM schemes under different of attributes.

No. of. Attributes	Initialization Time (s)				
	PP-UPM	ICA-PPPM	VPI-FPM	UIdwST	SA-UPM
5	4.9	3.8	3.2	2.6	2.2
10	8.4	7.5	6.9	6.5	4.9
15	12.1	11.4	10.3	9.8	8.4
20	16.1	15.3	14.4	13.6	12.5
25	22.4	20.1	19.3	18.2	17.1

Table 1 Initialization Time vs. No. of. Attributes

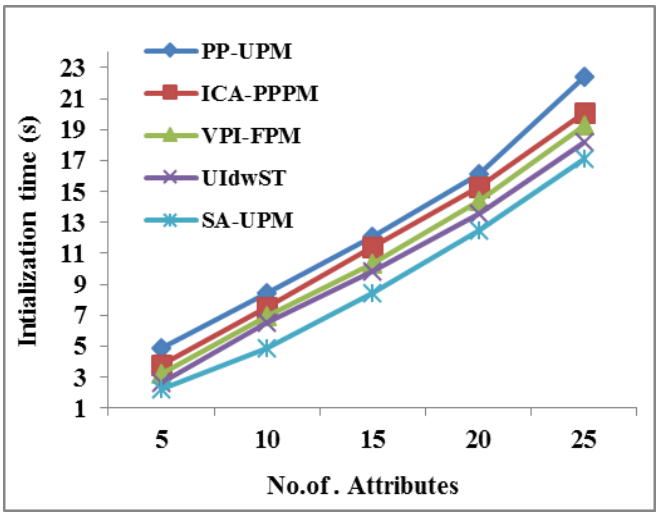

Figure 3 Evaluation of Initialization Time Results Dependent on the Number of Attributes

Figure 3 shows the Initialization phase (s) PP-UPM, ICA-PPPM, VPI-FPM, UIdwST and SA-UPM schemes. When the number of attributes is 25, the proposed SA-UPM initialization phase is 23.66%, 14.92% 11.39% and 6.04% is lesser than the existing PP-UPM, ICA-PPPM, VPI-FPM and UIdwST schemes. From this analysis, it is proved that the proposed SA-UPM scheme has less Initialization phase than other existing methods for cloud assisted PM system.

4.2. Key Generation Time (s) vs. No. of. Attributes

The time it takes to verify whether or not a key is safe is known as the key generation time. If the key in question is created using a weak encryption technique, any attacker might readily figure out the encryption key's value in a short amount of time. Furthermore, if the key is generated in an unsecured place, it may be compromised as soon as it is generated, leading in a key that cannot be used safely for encryption time. The Table 2 depictsKey generation time for PP-UPM, ICA-PPPM, VPI-FPM and UIdwST schemes with proposed SA-UPM schemes under different of attributes.

No. of. Attributes	Key Generation Time (s)				
	PP-UPM	ICA-PPPM	VPI-FPM	UIdwST	SA-UPM
5	5.1	4.8	4.2	3.6	2.5
10	7.6	6.4	5.9	5.5	4.3
15	13.2	11.9	10.5	8.8	7.5
20	15.9	14.1	13.5	12.8	11.7
25	23.4	22.1	20.8	19.7	16.5

Table 2 Key Generation Time (s) vs. No. of. Attributes

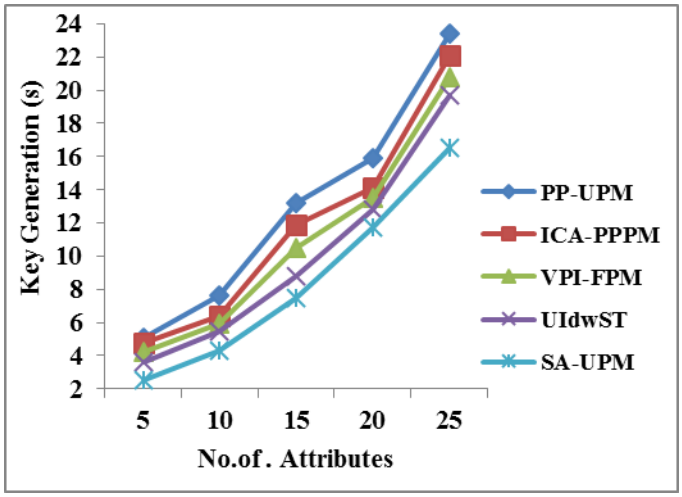

Figure 4 Comparison of Outcomes Based on the Number of Attributes for Key Generation Time (s)

The Key Generation time of the PP-UPM, ICA-PPPM, VPI-FPM, UIdwST and SA-UPM schemes is shown in Figure 4. When the No. of Attributes is 25, the for Key Generation time of developed SA-UPM is 29.48%, 25.33%20.67% and 16.24% is lower than the existing PP-UPM, ICA-PPPM, VPI-FPM and UIdwST schemes. From this analysis, it is proved that the proposed SA-UPM scheme has less Key generation time than other existing methods for cloud assisted PM system.

4.3. Encryption Time (s) vs. No. of. Attributes

Encryption time is the amount of time required to encrypt an initial CTbased on the number of independent keywords with a certain time interval (s). Table 3 depicts an encryption time for PP-UPM, ICA-PPPM, VPI-FPM and UIdwST schemes with proposed SA-UPM schemes under different of attributes.

RESEARCH ARTICLE

No. of. Attributes	Encryption Time (s)				
	PP-UPM	ICA-PPPM	VPI-FPM	UIdwST	SA-UPM
5	5.3	4.9	4.3	3.4	2.7
10	8.4	6.4	5.9	5.5	4.3
15	15.5	14.3	13.5	12.8	9.7
20	17.2	16.7	15.6	14.8	13.8
25	24.2	21.6	20.1	18.4	15.3

Table 3 Encryption Time (s) vs. Number of Attributes

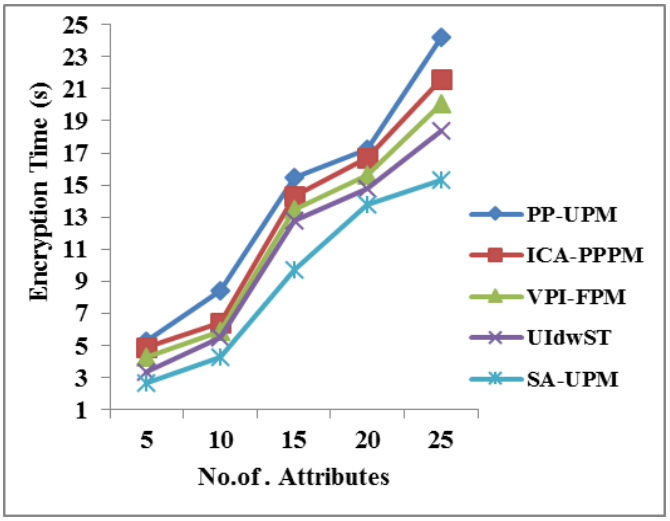

Figure 5 Comparison of Encryption Time (s)

The execution time on encryption using PP-UPM, ICA-PPPM, VPI-FPM, UIdwST and SA-UPM schemes for various No. of. Attributes is shown in Figure 5. The encryption time of the proposed SA-UPM is 36.77%, 29.16%, 23.88% and 16.85% is lesser than the existing PP-UPM, ICA-PPPM, VPI-FPM and UIdwST schemes when the number of characteristics is 25.From this analysis, it is proved that the proposed SA-UPM scheme has less of Encryption Time than other existing methods for cloud assisted PM system.

4.4. Decryption Time (s) vs. No. of. Attributes

Decryption times for CT (Decryption-I) and modified CT(Decryption-II) are independent of the number of keywords with a given time interval (s).The Table 4 depicts the execution time for PP-UPM, ICA-PPPM, VPI-FPM and UIdwST with proposed SA-UPM schemes under different of attributes.

The execution time on Decryption using PP-UPM, ICA-PPPM, VPI-FPM, UIdwST and SA-UP schemes for different number of attributes is shown in Figure 6. When the number of attributes is 25, Decryption time of proposed SA-UPM is 39.59%, 31.48%, 19.12%and 12.42%lesser than the existing PP-UPM, ICA-PPPM, VPI-FPM and UIdwST schemes. From this analysis, it is proved that the proposed SA-UPM scheme has less of Decryption Time than other existing methods for cloud assisted PM system.

No. of. attributes	Decryption Time (s)				
	PP-UPM	ICA-PPPM	VPI-FPM	UIdwST	SA-UPM
5	4.8	3.9	3.5	3.1	2.4
10	8.5	6.3	5.8	5.6	4.4
15	14.9	14.8	13.7	13.1	8.9
20	18.1	15.7	14.6	13.8	12.5
25	24.5	21.6	18.3	16.9	14.8

Table 4 Decryption Time vs. Number of Attributes

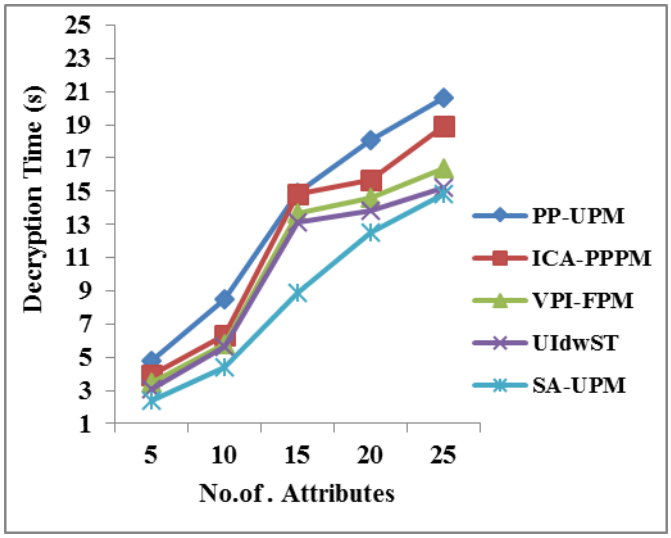

Figure 6 Comparison of Decryption Time (s)

5. CONCLUSION

In this paper, MCT-PES based scheme SA-UPM for MSCNs is developed to multiple recipients. This technique employs a unique MCT-PES structure that ensures receiver obscurity. In this approach, a user is able to identify matched individuals using different networks while keeping the query and UPs hidden. By efficiently securing a participant's profile or PP, a user may also submit a PP and search decentralised MSCNs for individuals with similar profiles. This protocol delivers effective UPS privacy and user query privacy, according to security evaluations. Furthermore, this whole process completely reduces the computational difficulties and expense.

RESEARCH ARTICLE

REFERENCES

[1] E. S. T. Wang, &N. P. Y. Chou, "Examining social influence factors affecting consumer continuous usage intention for mobile social networking applications", International Journal of Mobile Communications, vol. 14, no. 1, 2016, pp. 43-55.

[2] M. Li, N. Cao, S. Yu, &W. Lou, "Findu: Privacy-preserving personal profile matching in mobile social networks", In 2011 Proceedings IEEE INFOCOM, IEEE, 2011, pp. 2435-2443.

[3] R. Zhang, J. Zhang, Y. Zhang, J. Sun, &G. Yan, "Privacy-preserving profile matching for proximity-based mobile social networking", IEEE Journal on Selected Areas in Communications, vol. 31, no. 9, 2013, pp. 656-668.

[4] M. Jalasri, &L. Lakshmanan, "Code-based encryption techniques with distributed cluster head and energy consumption routing protocol", Complex & Intelligent Systems,2021, pp. 1-13.

[5] A.Acar, H. Aksu, A. S. Uluagac, &M. Conti, "A survey on homomorphic encryption schemes: Theory and implementation",ACM Computing Surveys (Csur), vol. 51, no. 4, 2018, pp. 1-35.

[6] C. Gentry, A. Sahai, &B. Waters, Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In Annual Cryptology Conference, Springer, Berlin, Heidelberg, 2013, pp. 75-92.

[7] Z. Brakerski, &V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) LWE", SIAM Journal on computing, vol. 43, no. 2, 2014, pp. 831-871.

[8] D. Boneh, C. Gentry, S. Halevi, F. Wang, &D. J. Wu, "Private database queries using somewhat homomorphic encryption" ,In International Conference on Applied Cryptography and Network Security, Springer, Berlin, Heidelberg, 2013, pp. 102-118.

[9] C. I. Eke, A. A. Norman, L. Shuib, &H. F. Nweke, "A survey of user profiling: State-of-the-art, challenges, and solutions", IEEE Access,vol. 7, 2019, pp. 144907-144924.

[10] W. Cui, C. Du, & J. Chen, "CP-ABE based privacy-preserving user profile matching in mobile social networks", PloS one, vol. 11, no. 6, 2016, pp. e0157933.

[11] N. Jabeur, S. Zeadally, &B. Sayed, "Mobile social networking applications", Communications of the ACM, vol. 56, no. 3, 2013, pp. 71-79.

[12] R. Ajami, N. Al Qirim, &N. Ramadan, "Privacy issues in mobile social networks", Procedia Computer Science, vol. 10, 2012, 672-679.

[13] A. Shikfa, M. Önen, & R. Molva, "Broker-based private matching", In International Symposium on Privacy Enhancing Technologies Symposium, Springer, Berlin, Heidelberg, 2011, pp. 264-284.

[14] P. Gasti,&K. B. Rasmussen, "Privacy-preserving user matching",In Proceedings of the 14th ACM Workshop on Privacy in the Electronic Society, 2015, pp. 111-120.

[15] L. Zhang, X. Ding, Z. Wan, M. Gu, &X. Y. Li, "Wiface: a secure geosocial networking system using wifi-based multi-hop manet", In Proceedings of the 1st ACM workshop on mobile cloud computing & services: social networks and beyond, 2010, pp. 1-8.

[16] M. Li, S. Yu, N. Cao, &W. Lou, "Privacy-preserving distributed profile matching in proximity-based mobile social networks",IEEE Transactions on Wireless Communications, vol. 12, no. 5, 2013, pp. 2024-2033.

[17] W. Dong, V. Dave, L. Qiu, &Y. Zhang, "Secure friend discovery in mobile social networks",In 2011 proceedings ieeeinfocom, IEEE, 2011, pp. 1647-1655.

[18] K. Shewale, &S. D. Babar, " An efficient profile matching protocol using privacy preserving in mobile social network",Procedia Computer Science, IEEE, vol. 79, pp. 922-931.

[19] J. Zouari, M. Hamdi, &T. H. Kim, "Private Profile Matching for Mobile Social Networks Based on Fuzzy Extractors", In SCSS, 2017, pp. 63-67.

[20] Q. Huang, W. Yue, Y. He, &Y. Yang, "Secure identity-based data sharing and profile matching for mobile healthcare social networks in cloud computing",IEEE Access, vol. 6, 2018, pp. 36584-36594.

[21] B. Chandrasekaran, Y. Nogami, &R. Balakrishnan, "An efficient hierarchical multi-authority attribute based encryption scheme for profile matching using a fast ate pairing in cloud environment", Journal of communications software and systems, vol. 14, no. 2, 2018, pp. 151-156.

[22] C. Z. Gao, Q. Cheng, X. Li, &S. B. Xia, "Cloud-assisted privacy-preserving profile-matching scheme under multiple keys in mobile social network", Cluster Computing, vol. 22, no. 1, 2018, pp. 1655-1663.

[23] E. Luo, K. Guo, Y. Tang, X. Ying, & W. Huang, "Hidden the true identity and dating characteristics based on quick private matching in mobile social networks",Future Generation Computer Systems, 109, 2020, pp. 633-641.

[24] X. Yi, E. Bertino, F. Y. Rao, K. Y. Lam, S. Nepal, & A. Bouguettaya, "Privacy-preserving user profile matching in social networks" IEEE Transactions on Knowledge and Data Engineering, vol. 32, no. 8, 2020, pp. 1572-1585.

[25] Y. Zou, Y. Chai, S. Shi, L. Wang, Y. Peng, Y. Ping, &B. Wang, "Improved Cloud-Assisted Privacy-Preserving Profile-Matching Scheme in Mobile Social Networks", Security and Communication Networks, vol. 2020, 2020.

[26] Y. Qian, J. Shen, P. Vijayakumar, &P. K. Sharma, "Profile matching for IoMT: a verifiable private set intersection scheme",IEEE journal of biomedical and health informatics, vol. 25, no. 10, 2021, pp. 3794-3803.

[27] Y. Li, W. Ji, X. Gao, Y. Deng, W. Dong, &D. Li, "Matching user accounts with spatio-temporal awareness across social networks", Information Sciences, vol. 570, 2021, pp. 1-15.

Authors

Dr. M. Gobi working as Assistant Professor in the Department of Computer Science, Chikkanna Government Arts College, Tiruppur ,Tamilnadu, India. Previously he was worked as Assistant Professor at P.S.G. College of Arts and Science, Coimbatore. His area of interests includes Network Security, Cryptography and Biometric Security.

B. Arunapriya doing her Ph.D research at Department of computer Science, Chikkanna Government Arts College, Tiruppur. Previously, she was worked as assistant Professor in the Department of Computer Science, Michael Job College of Arts & Science for Women, Sulur, Coimbatore. Her area of Interests includes Network Security, Cloud Security, Data mining.

How to cite this article:

M. Gobi, B. Arunapriya, "Solitude Adaptable User Profile Matching for Mobile Social Cloud Networks", International Journal of Computer Networks and Applications (IJCNA), 9(4), PP: 451-461, 2022, DOI: 10.22247/ijcna/2022/214506.